An arithmetic Bernštein-Kušnirenko inequality

César Martínez
joint with Martín Sombra

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Normandie

MEGA
June 12th 2017

Schema

- Counting the number of solutions.
- Size of a solution.
- Arithmetic Bernštein-Kušnirenko.
- Size of $\boldsymbol{u}$-resultants.
- Size of rational univariate representations.

Counting the number of solutions I

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, and $Z(f_1, \ldots, f_n)$ be the set of isolated solutions in $(\mathbb{Q}^\times)^n$ of the system

$$f_1(\boldsymbol{x}) = \cdots = f_n(\boldsymbol{x}) = 0.$$

Bézout's Theorem: $\#Z(f_1, \ldots, f_n) \leq \deg(f_1) \cdots \deg(f_n)$.

Counting the number of solutions I

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, and $Z(f_1, \ldots, f_n)$ be the set of isolated solutions in $(\mathbb{Q}^\times)^n$ of the system

$$f_1(\boldsymbol{x}) = \cdots = f_n(\boldsymbol{x}) = 0.$$

Bézout's Theorem: $\#Z(f_1, \ldots, f_n) \leq \deg(f_1) \cdots \deg(f_n)$.

But what happens when dealing with sparse polynomials?

Toy example

Let $H, d \in \mathbb{N}_{>0}$, and

$$f_1 = x_1 - H, \quad f_2 = x_2 - H\,x_1^d, \quad \ldots, \quad f_n = x_n - H\,x_{n-1}^d.$$

Then $Z(\boldsymbol{f}) = (H, H^{1+d}, \ldots, H^{1+d+\cdots+d^{n-1}})$ is a single point!

Counting the number of solutions I

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, and $Z(f_1, \ldots, f_n)$ be the set of isolated solutions in $(\mathbb{Q}^\times)^n$ of the system

$$f_1(\boldsymbol{x}) = \cdots = f_n(\boldsymbol{x}) = 0.$$

Bézout's Theorem: $\#Z(f_1, \ldots, f_n) \leq \deg(f_1) \cdots \deg(f_n)$.

But what happens when dealing with sparse polynomials?

Toy example

Let $H, d \in \mathbb{N}_{>0}$, and

$$f_1 = x_1 - H, \quad f_2 = x_2 - H\,x_1^d, \quad \ldots, \quad f_n = x_n - H\,x_{n-1}^d.$$

Then $Z(\boldsymbol{f}) = (H, H^{1+d}, \ldots, H^{1+d+\cdots+d^{n-1}})$ is a single point!

...even if $\deg(f_i) = d$, $\forall i \geq 2$.

Couting the number of solutions II

Write, $f_i(\boldsymbol{x}) = \sum_{\boldsymbol{m} \in \mathbb{Z}^n} \alpha_{i,\boldsymbol{m}}\, \boldsymbol{x}^{\boldsymbol{m}}$. The *support* of f_i is

$$\mathrm{supp}(f_i) = \{\boldsymbol{m} \in \mathbb{Z} \mid \alpha_{i,\boldsymbol{m}} \neq 0\} \subset \mathbb{Z}^n;$$

and the *Newton polytope* of f_i is its convex hull

$$\mathcal{N}(f_i) = \mathrm{conv}(\mathrm{supp}(f_i)) \subset \mathbb{R}^n.$$

Couting the number of solutions II

Write, $f_i(\boldsymbol{x}) = \sum_{\boldsymbol{m}\in\mathbb{Z}^n} \alpha_{i,\boldsymbol{m}}\, \boldsymbol{x}^{\boldsymbol{m}}$. The *support* of f_i is

$$\mathrm{supp}(f_i) = \{\boldsymbol{m} \in \mathbb{Z} \mid \alpha_{i,\boldsymbol{m}} \neq 0\} \subset \mathbb{Z}^n;$$

and the *Newton polytope* of f_i is its convex hull

$$\mathcal{N}(f_i) = \mathrm{conv}(\mathrm{supp}(f_i)) \subset \mathbb{R}^n.$$

Bernštein-Kušnirenko Theorem:

$$\#Z(f_1, \ldots, f_n) \leq \mathrm{MV}(\mathcal{N}(f_1), \ldots, \mathcal{N}(f_n)).$$

where MV is the *mixed volume*. In particular, if $\mathcal{N}(f_i) = \Delta$, $\forall i$, we have $\#Z(f_1, \ldots, f_n) \leq n!\,\mathrm{vol}(\Delta)$.

For dense polynomials, we recover Bézout's Theorem.

Counting the number of solutions III

Toy example

Let $H, d \in \mathbb{N}_{>0}$, and

$$f_1 = x_1 - H, \quad f_2 = x_2 - H\,x_1^d, \quad \ldots, \quad f_n = x_n - H\,x_{n-1}^d.$$

Their support consists of two points:

$$\mathrm{supp}(f_1) = \{e_1, 0\}; \quad \mathrm{supp}(f_i) = \{e_i, e_{i-1}\}, \forall i \geq 2.$$

And so their respective Newton polytopes are just the segments in $\mathbb{R}^n$ connecting these points.
Then

$$\mathrm{MV}(\mathcal{N}(f_1), \ldots, \mathcal{N}(f_n)) = \mathrm{vol}(\mathcal{N}(f_1) + \cdots + \mathcal{N}(f_n)) = 1.$$

Size of a solution I

Which one is more complex,

$$\frac{1}{2} \quad \text{or} \quad \frac{1000}{2001} \quad ?$$

Size of a solution I

Which one is more complex,

$$\frac{1}{2} \quad \text{or} \quad \frac{1000}{2001} \quad ?$$

The *Weil height* of a rational number $q = \frac{a}{b} \in \mathbb{Q}^{\times}$, with a, b coprime, is

$$\begin{aligned} \mathrm{h}_{\mathrm{Weil}}(q) &= \log \max\{|a|, |b|\} \\ &= \sum_{p \in \{\text{primes}\} \cup \{\infty\}} \log \max\{1, |q|_p\}. \end{aligned}$$

Size of a solution I

Which one is more complex,

$$\frac{1}{2} \quad \text{or} \quad \frac{1000}{2001} \quad ?$$

The *Weil height* of a rational number $q = \frac{a}{b} \in \mathbb{Q}^{\times}$, with a, b coprime, is

$$\begin{aligned} \mathrm{h}_{\mathrm{Weil}}(q) &= \log \max\{|a|, |b|\} \\ &= \sum_{p \in \{\text{primes}\} \cup \{\infty\}} \log \max\{1, |q|_p\}. \end{aligned}$$

We can extend this notion to a point $(a_0 : \cdots : a_r) \in \mathbb{P}^r_{\mathbb{Q}}$, $a_i \in \mathbb{Z}$ and $\gcd(a_i) = 1$:

$$\mathrm{h}_{\overline{\mathcal{O}(1)}^{can}}(a_0 : \cdots : a_r) = \log \max\{|a_i|\}$$

which is the *canonical height* (or Weil height).

Size of a solution II

There are different notions of height, for instance the ones attached to a monomial map:

$$\begin{aligned} \varphi : (\mathbb{Q}^\times)^n &\longrightarrow \mathbb{P}^r_{\mathbb{Q}} \\ \boldsymbol{x} &\longmapsto (\alpha_0 \boldsymbol{x}^{\boldsymbol{m}_0} : \cdots : \alpha_N \boldsymbol{x}^{\boldsymbol{m}_r}); \end{aligned}$$

where $r > 0$, $\alpha_j \in \mathbb{Q}^\times$, and $\boldsymbol{m}_j \in \mathbb{Z}^n$. Then, for a point $\boldsymbol{p} \in (\mathbb{Q}^\times)^n$,

$$\mathsf{h}_{\varphi^* \overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) = \mathsf{h}_{\overline{\mathcal{O}(1)}^{can}}(\varphi(\boldsymbol{p})).$$

The Weil height is the one associated to the natural embedding $(\mathbb{Q}^\times)^n \hookrightarrow \mathbb{P}^r_{\mathbb{Q}}$.
One extends the notion of height of a point to height of a 0-cycle by linearity.

Size of a solution III

The size, or complexity, of the set of isolated solutions depends on how we represent it!

Size of a solution III

The size, or complexity, of the set of isolated solutions depends on how we represent it!

Toy example

Let $H, d \in \mathbb{N}_{>0}$, and

$$f_1 = x_1 - H, \quad f_2 = x_2 - H\,x_1^d, \quad \ldots, \quad f_n = x_n - H\,x_{n-1}^d.$$

Its solution is the single point $\boldsymbol{p} = (H, H^{1+d}, \ldots, H^{1+d+\cdots+d^{n-1}})$.
For the natural embedding into $\mathbb{P}^n_{\mathbb{Q}}$, one has

$$\mathrm{h}_{\overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) = (1 + d + \cdots + d^{n-1})\,\log(H).$$

However, if we consider the embedding $\jmath : (\mathbb{Q}^\times)^n \hookrightarrow \mathbb{P}^n_{\mathbb{Q}}$, $(x_1, \ldots, x_n) \mapsto (1 : x_1 : x_2 x_1^{-d} : \cdots : x_n x_{n-1}^{-d})$, one obtains

$$\mathrm{h}_{\jmath^* \overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) = \log(H).$$

Arithmetic Bernštein-Kušnirenko

An arithmetic version of Bernštein-Kušnirenko's bound has to depend on the *size* of the coefficients of the defining polynomials, and of the ones of the monomial map.

Given a vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r) \in (\mathbb{Q}^\times)^r$, we denote its *logarithmic length* by

$$\ell(\boldsymbol{\alpha}) = \sum_p \log \max_j |\alpha_j|_p \; + \log \sum_j |\alpha_j|_\infty \, .$$

Then, the *logarithmic length* of a polynomial is the length of its vector of non-zero coefficients.

Arithmetic Bernštein-Kušnirenko

Theorem

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with Newton polytopes Δ_i, and vector of non-zero coefficients $\boldsymbol{\alpha}_i$. Let $\varphi : (\mathbb{Q}^\times)^n \to \mathbb{P}^r_{\mathbb{Q}}$ be the monomial map given by the vector $\boldsymbol{\alpha}_0 \in (\mathbb{Q}^\times)^{r+1}$ and the matrix $(\boldsymbol{m}_0, \ldots \boldsymbol{m}_r) \in (\mathbb{Z}^n)^{r+1}$:

$$\varphi(\boldsymbol{x}) = (\alpha_{0,0}\boldsymbol{x}^{\boldsymbol{m}_0} : \cdots : \alpha_{0,r}\boldsymbol{x}^{\boldsymbol{m}_r}).$$

Set $\Delta_0 = \mathrm{conv}(\boldsymbol{m}_0, \ldots, \boldsymbol{m}_r)$. Then

$$\mathrm{h}_{\varphi^* \overline{\mathcal{O}(1)}^{can}}(Z(\boldsymbol{f})) \leq \sum_{i=0}^{n} \mathrm{MV}(\Delta_0, \ldots, \Delta_{i-1}, \Delta_{i+1}, \ldots, \Delta_n)\ell(\boldsymbol{\alpha}_i).$$

Arithmetic Bernštein-Kušnirenko

Toy example

Let $H, d \in \mathbb{N}_{>0}$, and

$$f_1 = x_1 - H, \quad f_2 = x_2 - H\,x_1^d, \quad \ldots, \quad f_n = x_n - H\,x_{n-1}^d.$$

And $Z(\boldsymbol{f}) = \boldsymbol{p} = (H, H^{1+d}, \ldots, H^{1+d+\cdots+d^{n-1}})$.

The bounds given by the Theorem are:

$$\mathrm{h}_{\overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) \leq (\sum_j d^{j-1})\,\log(H+1), \quad \mathrm{h}_{\jmath^*\overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) \leq n\log(H+1).$$

While the actual heights are:

$$\mathrm{h}_{\overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) = (\sum_j d^{j-1})\,\log(H), \quad \mathrm{h}_{\jmath^*\overline{\mathcal{O}(1)}^{can}}(\boldsymbol{p}) = \log(H).$$

Toric Dictionary

$$\begin{array}{l} X \text{ toric variety} \\ + D \text{ toric ample divisor} \end{array} \quad \leftrightarrow \quad \begin{array}{c} \Delta \subset \mathbb{R}^n \text{ convex polytope} \\ \updownarrow \\ \Psi_\Delta(\boldsymbol{u}) = \min\limits_{\boldsymbol{x} \in \Delta} \langle \boldsymbol{x}, \boldsymbol{u} \rangle \text{ concave} \end{array}$$

$$\deg_D(X) = n! \operatorname{vol}(\Delta) \rightsquigarrow \text{classical BKK.}$$

Toric Dictionary

$$\begin{array}{l} X \text{ toric variety} \\ + D \text{ toric ample divisor} \end{array} \quad \leftrightarrow \quad \begin{array}{c} \Delta \subset \mathbb{R}^n \text{ convex polytope} \\ \updownarrow \\ \Psi_\Delta(\boldsymbol{u}) = \min\limits_{\boldsymbol{x}\in\Delta} \langle \boldsymbol{x}, \boldsymbol{u} \rangle \text{ concave} \end{array}$$

$$\deg_D(X) = n! \operatorname{vol}(\Delta) \rightsquigarrow \text{classical BKK.}$$

$$\{\|\cdot\|_v\} \text{ metrics on } D \quad \leftrightarrow \quad \begin{array}{c} \psi : \mathbb{R}^n \to \mathbb{R} \text{ concave and} \\ |\psi - \Psi_\Delta| \textit{ bounded} \end{array}$$

$$\mathrm{h}_{(D,\{\|\cdot\|_v\})}(X) = (n+1)! \int_\Delta \psi^\vee \mathrm{d}\mu \rightsquigarrow \text{arithmetic BKK.}$$

Size of $\boldsymbol{u}$-resultants I

Let W be a 0-cycle of $\mathbb{P}^r_{\mathbb{Q}}$, and $\boldsymbol{u} = (u_0, \ldots, u_r)$ a vector of $r+1$-variables.
Write $W_{\overline{\mathbb{Q}}} = \sum_{\boldsymbol{q}} \mu_{\boldsymbol{q}} \boldsymbol{q}$ as the 0-cycle obtained by the base change $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$.
The $\boldsymbol{u}$-*resultant* of W is defined as

$$\mathrm{Res}(W) = \prod_{\boldsymbol{q}} (q_0 u_0 + \cdots + q_r u_r)^{\mu_{\boldsymbol{q}}} \in \mathbb{Q}(\boldsymbol{u})^{\times}.$$

It is well-defined up to a factor in $\mathbb{Q}^{\times}$.

Size of $\boldsymbol{u}$-resultants II

Theorem

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with Newton polytopes Δ_i, and vector of non-zero coefficients $\boldsymbol{\alpha}_i$. Let $\varphi : (\mathbb{Q}^\times)^n \to \mathbb{P}^r_{\mathbb{Q}}$ be the monomial map given by the vector $\boldsymbol{\alpha}_0 \in (\mathbb{Q}^\times)^{r+1}$ and the matrix $(\boldsymbol{m}_0, \ldots \boldsymbol{m}_r) \in (\mathbb{Z}^n)^{r+1}$. Set $\Delta_0 = \mathrm{conv}(\boldsymbol{m}_0, \ldots, \boldsymbol{m}_r)$. Then

$$\ell(\mathrm{Res}(\varphi_* Z(\boldsymbol{f}))) \leq \sum_{i=0}^{n} \mathrm{MV}(\Delta_0, \ldots, \Delta_{i-1}, \Delta_{i+1}, \Delta_n) \ell(\boldsymbol{\alpha}_i).$$

Size of rational univariate representations I

Let W be a 0-cycle in $(\overline{\mathbb{Q}}^{\times})^r$ defined over $\mathbb{Q}$, such that the first coordinate of all the distinct points in its support $|W|$ is different. By the *shape lemma*, there exist polynomials $h, g_0, \ldots, g_r \in \mathbb{Q}[t]$ such that

$$|W| = \{(g_1(t)/g_0(t), \ldots, g_r(t)/g_0(t)) \in (\overline{\mathbb{Q}}^{\times})^r \mid t \in \overline{\mathbb{Q}},\ h(t) = 0\},$$

with $deg(g_j) \leq \deg(h)$ and the multiplicity of the points is given by the multiplicity of the corresponding root of h.

This is called the rational univariate representation of W.

Size of rational univariate representations II

Fixed the natural embedding $(\mathbb{Q}^\times)^r \hookrightarrow \mathbb{P}^r_{\mathbb{Q}}$, we identify W with its image. We may then compute its $\boldsymbol{u}$-resultant.
Then, for every $\boldsymbol{u} \in (\overline{\mathbb{Q}}^\times)^r$ such that $\mathrm{Res}(W)(\boldsymbol{u}) = 0$, we have

$$\left(\frac{\partial\ \mathrm{Res}(W)}{\partial\, u_0}(\boldsymbol{u}) : \cdots : \frac{\partial\ \mathrm{Res}(W)}{\partial\, u_r}(\boldsymbol{u})\right) \in |W|\,.$$

Size of rational univariate representations II

Fixed the natural embedding $(\mathbb{Q}^\times)^r \hookrightarrow \mathbb{P}^r_{\mathbb{Q}}$, we identify W with its image. We may then compute its $\boldsymbol{u}$-resultant.
Then, for every $\boldsymbol{u} \in (\overline{\mathbb{Q}}^\times)^r$ such that $\mathrm{Res}(W)(\boldsymbol{u}) = 0$, we have

$$\left(\frac{\partial\, \mathrm{Res}(W)}{\partial\, u_0}(\boldsymbol{u}) : \cdots : \frac{\partial\, \mathrm{Res}(W)}{\partial\, u_r}(\boldsymbol{u})\right) \in |W|\,.$$

If the coordinates of two different points in $|W|$ are pairwise distinct, one can then take $\boldsymbol{u}$ raging through the line $x_2 = \cdots = x_r = 0$. Then, we have that

$$\begin{cases} h(t) = \mathrm{Res}(W)(1, t, 0, \ldots, 0); \\ g_j(t) = \dfrac{\partial\, \mathrm{Res}(W)}{\partial\, u_j}(1, t, 0, \ldots, 0), \quad j = 0, \ldots, n. \end{cases}$$

is a rational univariate representation of W.

Size of rational univariate representations III

Corollary

Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let $\varphi : (\mathbb{Q}^\times)^n \to (\mathbb{Q}^\times)^r$ be the monomial map given by $\boldsymbol{x} \mapsto (\alpha_{0,1}\boldsymbol{x}^{\boldsymbol{m}_1}, \ldots, \alpha_{0,r}\boldsymbol{x}^{\boldsymbol{m}_r})$. Set $\Delta_0 = \mathrm{conv}(0, \boldsymbol{m}_1, \ldots, \boldsymbol{m}_r)$, and $\boldsymbol{\alpha}_0 = (1, \alpha_{0,1}, \ldots, \alpha_{0,r})$. Assume that the first coordinates of the points in $\varphi_* Z(\boldsymbol{f})$ are pairwise distinct. Then there exists a rational univariate representation of $\varphi_* Z(\boldsymbol{f})$ such that

$$\ell(h) \leq \sum_{i=0}^{n} \mathrm{MV}(\Delta_0, \ldots, \Delta_{i-1}, \Delta_{i+1}, \Delta_n)\ell(\boldsymbol{\alpha}_i);$$

and, for every $j = 0, \ldots, r$,

$$\ell(g_j) \leq \log(\mathrm{MV}(\Delta_1, \ldots, \Delta_n)) + \sum_{i=0}^{n} \mathrm{MV}(\Delta_0, \ldots, \Delta_{i-1}, \Delta_{i+1}, \Delta_n)\ell(\boldsymbol{\alpha}_i).$$