OVERDETERMINED SYSTEMS OF SPARSE POLYNOMIAL EQUATIONS

MARTÍN SOMBRA

JOINT WORK WITH F. AMOROSO AND L. LEROUX (U. CAEN)

PB: GIVEN $f, g \in \mathbb{Z}[x]$ SPARSE POLYNOMIALS (= FEWNOMIALS)

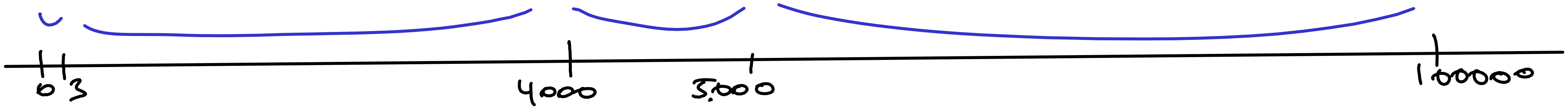
COMPUTE $p \in \mathbb{Z}[x]$ ST

$$V(f,g) = V(p)$$

ZERO SETS IN $\mathbb{C}$

SPARSE POLYNOMIALS

$$f = x^{10000} - 3x^{5000} + 7x^{4000} - x^3 - 2$$



WRITE $f = \sum_{i=1}^{N} \alpha_i x^{a_i} \in \mathbb{Z}[x] \quad (\alpha_i \neq 0, \quad a_i \neq a_j \text{ FOR } i \neq j)$

- $\sigma(f) = \sum_i \log \alpha_i + \log a_i$ SPARSE SIZE
- $d = \max_i a_i$ DEGREE
- $h = \max_i \log |\alpha_i|$ HEIGHT
- N # TERMS

$$\tau(f) \asymp (N\, h \log(d))^{O(1)}$$

CAN WE COMPUTE THE GCD ?

EX: LET $a, b \geq 1$ COPRIME

$$\gcd\left((x^a-1)(x^b-1),\ x^{ab}-1\right) = \frac{(x^a-1)(x^b-1)}{x-1}$$

HAS $\min(a,b)$ NONZERO TERMS

THM (PLAISTED 1977) GIVEN $f, g \in \mathbb{Z}[x]$ IN SPARSE ENCODING, DECIDING IF

$$\gcd(f,g) = 1$$

IS NP-HARD

THM (ALS) LET $f, g \in \mathbb{Z}[x]$ OF DEGREE $\leq d$, BOUNDED HEIGHT AND # TERMS. WE CAN COMPUTE $p \in \mathbb{Z}[x]$ ST

$$V(f,g) = V(p)$$

WITH $\widetilde{O}(\log(d))$ OPS.

IMPROVES PREVIOUS RESULT BY FILASETA - GRANVILLE - SCHINZEL (2010)

IN THE EXAMPLE: $V\left((x^a-1)(x^b-1),\, x^{ab}-1\right) = V\left((x^a-1)(x^b-1)\right)$

COR: WE CAN DECIDE IF $\gcd(f,g)=1$ WITH $\widetilde{O}(\log(d))$ OPS.

THM (Bombieri–Zannier 2005)

Given $F, G \in \mathbb{Z}[y_1, \dots, y_N]$ coprime, $\exists\ \Lambda_{F,G} \subset \mathbb{Z}^N$ finite

$\forall\ \xi \in \overline{\mathbb{Q}}^\times \setminus \mu_\infty$ and $\underline{a} = (a_1, \dots, a_N) \in \mathbb{Z}^N$ st

$$(\xi^{a_1}, \dots, \xi^{a_N}) \in V(F,G) \subset (\mathbb{C}^\times)^N$$

$\exists\ \underline{b} \in \Lambda_{F,G}$ st $\underline{a} \in \underline{b}^\perp$

Algorithm: Let $f, g \in \mathbb{Z}[x]$ st $V(f,g) \cap \mu_\infty = \phi$

Set $F, G \in \mathbb{Z}[y_1, \dots, y_N]$ linearization of f, g

$\underline{a} \in \mathbb{Z}^N$ exponents of f, g

Then

$$\begin{tikzcd} \mathbb{C}^\times \arrow[r, "\varphi_{\underline{a}}"] & (\mathbb{C}^\times)^N \\ V(f,g) \arrow[u, hook] \arrow[r] & V(F,G) \arrow[u, hook] \end{tikzcd}$$

If $V(f,g) \neq \phi$, $\exists\ \underline{b} \in \Lambda_{FG}$ st $\underline{a} \in \underline{b}^\perp$

$\leadsto$ the problem reduces to $(\mathbb{C}^\times)^{N-1}$, etc

Unlikely Intersections on Tori:

Conj (Zilber 2002) Given $W \subset (\mathbb{C}^\times)^N$, $\exists$ $G_W \subset (\mathbb{C}^\times)^N$ subgroup of codim 1 st:

$\forall$ $T \subset (\mathbb{C}^\times)^N$ subgroup and $C \subset W \cap T$ irred comp st

$$\dim(C) > \dim(T) - \operatorname{codim}(W)$$

then $C \subset G_W$

Cases and Related Results

- $\dim(T) = 0$ (ex Manin-Mumford conj, Laurent 1984)
- $\dim(T) = 1$ (Bombieri-Masser-Zannier 2007)
- $\dim(W) = 1$ (Maurin 2008)
- "Bounded Height Conj" (Habegger 2009)

THE MULTIVARIATE CASE

THM (ALS) ASSUME THE EFFECTIVE ZILBER COND.

GIVEN $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$ OF DEGREE $\leq d$

WE CAN COMPUTE A FAMILY Γ OF LOCALLY CLOSED

SUBSETS $Y \subset (\mathbb{C}^\times)^n$ ST

- Y EITHER COMPLETE INTERSECTION OR $\emptyset$
- $V(f_1, \dots, f_s) = \bigcup_{Y \in \Gamma} Y$

WITH $\widetilde{O}(\log(d))$ OPS

A SPARSE NSS

THM (ALS) ASSUME THE EFFECTIVE ZILBER COND.

GIVEN $f_1, \dots, f_s \in \mathbb{Z}[x_0, \dots, x_n]$ HOMOGENOUS OF DEGREE $\leq d$

WE CAN DECIDE IF

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

WITH $\widetilde{\mathcal{O}}(\log(d))$ OPS

THANK YOU!