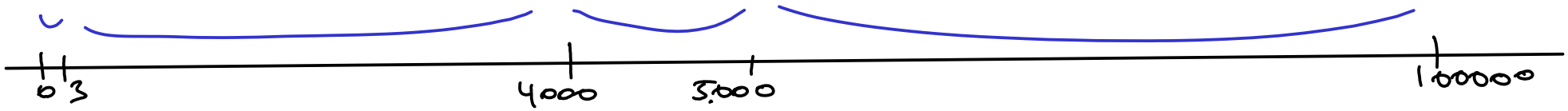
Overdetermined Systems of Lacunary Equations

Martín Sombra

joint work with Francesco Amoroso & Louis Leroux

Lacunary Polynomials

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



Lacunary encoding:

$$f = \sum_{i=1}^{N} \alpha_i x^{a_i} \in \mathbb{Z}[x] \quad \text{with} \quad 0 \le a_1 \le a_2 \le \cdots \le a_N = d$$

Lacunary size: $\tau(f) = \sum_i \log \alpha_i + \log a_i$

$$\left.\begin{matrix} h(f) + \log d \\ N-2 \end{matrix}\right\} \le \tau(f) \le N\,(h(f) + \log d)$$

Things we can do & Things we can not

- We can not evaluate f at $\beta \neq 0, \pm 1$ (in POLYTIME)

  Ex: $f = x^{2^\tau} \Rightarrow f(2) = 2^{2^\tau}$ has $2^\tau + 1$ bits !

- We can decide if $f(\beta) = 0$

  More generally, given $e \geq 1$, we can compute

$$\{ p \in \mathbb{Z}[x]_e \mid p | f \}$$

  in $(e \cdot \tau(f))^{O(1)}$ ops

  Cucker-Koiran-Smale, Lenstra (1998) using Dobrowolski's theorem

Can we compute the gcd ?

- Ex (Schinzel) $a, b \geq 1$ 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

- Pb: given $f, g \in \mathbb{Z}[x]$ & $c \geq 1$, decide

$$\deg(\gcd(f,g)) = c \quad ?$$

is NP-hard (Plaisted 1977)

THM 1 (ALS) Given $f, g \in \mathbb{Z}[x]$, we can compute $p \in \mathbb{Z}[x]$ s.t.

$$V(f,g) = V(p) \subset \bar{\mathbb{Q}}$$

in $\underbrace{\tilde{C}_{N,h}(\log d)}$ ops

$$\leq c(N,h) \log d \, (\log\log d)^3$$

Improves previous result of Filaseta-Granville-Schinzel (2010)

In Schinzel's example

$$V((x^2-1)(x^b-1),\ x^{2b}-1) = V((x^2-1)(x^b-1))$$

Some Consequences

Thm 2 (ALS) We can compute $\deg(\gcd(f,g))$

in $\tilde{O}_{N,d}(\log d)$ ops.

Cor 3 (ALS) We can decide $g \mid f$?

in $\tilde{O}_{N,R}(\log d)$ ops

Unlikely Intersections

Thm Given $W \subset (\overline{\mathbb{Q}}^\times)^N$, $\exists\ c(W) \geq 1$ s.t.

$\forall\ \xi \in \overline{\mathbb{Q}}^\times$ & $\underline{a} \in \mathbb{Z}^N \setminus \{0\}$ s.t

$$\eta = (\xi^{a_1}, \dots, \xi^{a_N}) \in W_{\geq 2}$$

$$\Rightarrow \exists\ b \in \mathbb{Z}^N \setminus \{0\},\ \|b\| \leq c(W) \text{ with } \eta_1^{b_1} \cdots \eta_N^{b_N} = 1$$

If η not torsion $\Rightarrow$ $\langle a, b \rangle = 0$

Conjectured by Schinzel & proved by Bombieri-Masser-Zannier (2007)

The Algorithm

Input: $f = \sum \alpha_i x^{a_i}$, $g = \sum \beta_i x^{a_i}$

Inicialization: $F = \sum \alpha_i y_i$, $G = \sum \beta_i y_i \in \mathbb{Z}[y_1, \dots, y_N]$

$a = (a_1, \dots, a_N) \in \mathbb{Z}^N$, $k = N$

1) Test $\langle a, b \rangle = 0$ for $b \in \mathbb{Z}^k \setminus \{0\}$ with $\|b\| \leq c(V(F,G))$

2) If $\exists b$ st $\langle a, b \rangle = 0$:

   i) Find a basis $\{b_1, \dots, b_{k-1}\}$ of $b^\perp \cap \mathbb{Z}^N$
   and write $a = \sum \lambda_j b_j$

   ii) Set $F \leftarrow F(x_1^{b_{11}} \cdots x_{k-1}^{b_{k-1,1}}, \dots, x_1^{b_{1k}} \cdots x_{k-1}^{b_{k-1,k}})$, idem G

   $a \leftarrow (\lambda_1, \dots, \lambda_{k-1})$

   $k \leftarrow k-1$

   Repeat

Else: $p \leftarrow \gcd(F,G)(x^{a_1}, \dots, x^{a_k})$

Dimension $n \geq 2$

Thm 4 Assume the effective Zilber-Pink conjecture holds.
Given $f_1, \dots, f_{n+1} \in \mathbb{Z}[x_1, \dots, x_n]$ s.t. $\dim V(f_1, \dots, f_{n+1}) = 0$
We can compute a finite collection

$$\Gamma = \{ (p_1, \dots, p_n, q) \mid p_i, q \in \mathbb{Z}[x_1, \dots, x_n] \}$$

s.t.

$$V(f_1, \dots, f_{n+1}) = \bigcup_{(p,q) \in \Gamma} V(p_1, \dots, p_n) \setminus V(q)$$

in $\widetilde{\mathcal{O}}_{N,h}(\log d)$

Remark: $f_1 = \dots = f_{n+1} = 0$ is "overdetermined"

$p_1 = \dots = p_n = 0$ is "well-determined"
on the open set $q \neq 0$

Some Questions

A) Given $f \in \mathbb{Z}[x]$, how many lacunary factors (not binomials) does it have?

A1) Can we compute them?

B) Given $f_1, \dots, f_n \in \mathbb{Z}[x_1, \dots, x_n]$ st $\dim V(f_1, \dots, f_n) = 0$

How many rational roots does it have?

B1) Can we compute them?