# Factorization of multivariate lacunary polynomials.

Martin Avendaño.

Universidad de Buenos Aires.

Joint work with Teresa Krick and Martin Sombra.

## 1. Factorization of dense polynomials.

$$f = \sum_{|i| \le d} \frac{a_i}{b_i} x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{Q}[x_1, \ldots, x_n] \quad \text{with } a_i \in \mathbb{Z}, b_i \in \mathbb{N} \text{ and } \gcd(a_i, b_i) = 1$$

It is possible to compute the complete factorization of $f$ in $\mathbb{Q}[x_1, \ldots, x_n]$ in

$\underline{n = 1:}$ $\quad O\left(d^{15} \log^3 H_1(f)\right)$

$\underline{n > 1:}$ $\quad \left(\binom{d+n}{n} \log H_1(f)\right)^{O(1)}$

bit operations, where $d = \deg(f)$ and $H_1(f) = \frac{\gcd(\{b_i : |i| \le d\})}{\gcd(\{a_i : |i| \le d\})} \|f\|_1$.

## 2. Integer roots of a lacunary polynomial $f \in \mathbb{Z}[x]$.

**Example:**

$$f = -18 - 3x + 3x^2 + 27x^9 - x^{12} + 6x^{2007} - 20x^{2008} + 6x^{2009}$$

$$H_1(f) = \|f\|_1 = 84 \quad \log_2 \|f\|_1 \approx 6.392317$$

$$f = (-18 - 3x + 3x^2) + x^9(27 - x^3) + x^{2007}(6 - 20x + 6x^2)$$

The only common root of $-18 - 3x + 3x^2$, $27 - x^3$ and $6 - 20x + 6x^2$ is 3. Note that also 1 is a root of $f$.

## 2. Integer roots of a lacunary polynomial $f \in \mathbb{Z}[x]$.

**Example:**

$$f = -18 - 3x + 3x^2 + 27x^9 - x^{12} + 6x^{2007} - 20x^{2008} + 6x^{2009}$$

$$H_1(f) = \|f\|_1 = 84 \quad \log_2 \|f\|_1 \approx 6.392317$$

$$f = (-18 - 3x + 3x^2) + x^9(27 - x^3) + x^{2007}(6 - 20x + 6x^2)$$

The only common root of $-18 - 3x + 3x^2$, $27 - x^3$ and $6 - 20x + 6x^2$ is 3. Note that also 1 is a root of $f$.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Z}[x]$ with $\deg(g) = \alpha < \beta$. If $\beta - \alpha > \log_2 \|f\|_1$ and $r \in \mathbb{Z} - \{0, 1, -1\}$ then

$$f(r) = 0 \quad \Leftrightarrow \quad g(r) = h(r) = 0.$$

## 3. The proof.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Z}[x]$ with $\deg(g) = \alpha < \beta$. If $\beta - \alpha > \log_2 \|f\|$ and $r \in \mathbb{Z} - \{0, 1, -1\}$ then

$$f(r) = 0 \quad \Leftrightarrow \quad g(r) = h(r) = 0.$$

**Proof:** Suppose that $f(r) = 0$ and $h(r) \neq 0$. Then

$$r^\beta h(r) = -g(r) \quad \Rightarrow \quad |r|^\beta \leqslant |r|^\beta |h(r)| = |g(r)| \leqslant |r|^\alpha \|f\|_1$$

$$\Rightarrow \quad 2^{\beta-\alpha} \leqslant |r|^{\beta-\alpha} \leqslant \|f\|_1 \quad \Rightarrow \quad \beta - \alpha \leqslant \log_2 \|f\|_1.$$

■

## 4. How to control denominators?

**$p$-adic absolute values:** Let $p \in \mathbb{N}$ be a prime number. For every non-zero rational number $x = p^k \frac{a}{b}$ with $k \in \mathbb{Z}$, $p \nmid a$ and $p \nmid b$, we define

$$|x|_p = \frac{1}{p^k}.$$

**Ultrametric:** $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in \mathbb{Q}$ and $p \in \mathbb{N}$ prime.

**Product formula:** Let $x \in \mathbb{Q} - \{0\}$. Then $|x| \cdot \prod_{p \text{ prime}} |x|_p = 1$.

**Heights:** Let $x \in \mathbb{Q}$. Then

$$H(x) = \max\{1, |x|\} \cdot \prod_p \max\{1, |x|_p\} = \max\{|a|, b\},$$

where $x = \frac{a}{b}$ with $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\gcd(a, b) = 1$.

## 5. Rational roots of a lacunary polynomial $f \in \mathbb{Q}[x]$.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Q}[x]$ with $\deg(g) = \alpha < \beta$. If $r \in \mathbb{Q} - \{0, 1, -1\}$ and

$$\beta - \alpha > \log_2 H_1(f),$$

then $f(r) = 0$ if and only if $g(r) = h(r) = 0$.

## 5. Rational roots of a lacunary polynomial $f \in \mathbb{Q}[x]$.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Q}[x]$ with $\deg(g) = \alpha < \beta$. If $r \in \mathbb{Q} - \{0, 1, -1\}$ and

$$\beta - \alpha > \log_2 H_1(f),$$

then $f(r) = 0$ if and only if $g(r) = h(r) = 0$.

**Proof:** WLoG $f \in \mathbb{Z}[x]$ primitive. Let $r \in \mathbb{Q} - \{0, 1, -1\}$ such that $f(r) = 0$ and $h(r) \neq 0$. For the standard and $p$-adic absolute values, we have

$$\max\{1, |r|_p\}^{\beta-\alpha} |h(r)|_p \leqslant 1$$

$$\max\{1, |r|\}^{\beta-\alpha} |h(r)| \leqslant \|f\|_1 = H_1(f).$$

Using the product formula, we get:

$$H(r)^{\beta-\alpha} \leqslant H_1(f).$$

This implies $2^{\beta-\alpha} \leqslant H_1(f)$ and $\beta - \alpha \leqslant \log_2 H_1(f)$. ■

## 6. Small degree factors of a lacunary polynomial $f \in \mathbb{Q}[x]$.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Q}[x]$ with $\deg(g) = \alpha < \beta$. If $q \in \mathbb{Q}[x]$ is an irreducible polynomial with degree bounded by $s$, with a root that is not 0 or a root of the unity, and

$$\beta - \alpha > \frac{s \cdot \log_2^3(3s) \cdot \log_2(H_1(f))}{2},$$

then $q|f$ if and only if $q|g$ and $q|h$.

## 6. Small degree factors of a lacunary polynomial $f \in \mathbb{Q}[x]$.

**Thm:** Let $f = g + x^\beta h \in \mathbb{Q}[x]$ with $\deg(g) = \alpha < \beta$. If $q \in \mathbb{Q}[x]$ is an irreducible polynomial with degree bounded by $s$, with a root that is not 0 or a root of the unity, and

$$\beta - \alpha > \frac{s \cdot \log_2^3(3s) \cdot \log_2(H_1(f))}{2},$$

then $q|f$ if and only if $q|g$ and $q|h$.

**Algorithm:** It is possible to compute all the irreducible factors with degree bounded by $s$ of a lacunary polynomial $f \in \mathbb{Q}[x]$ with $t$ terms in

$$(s \cdot t \cdot \log(\deg f) \cdot \log H_1(f))^{O(1)} \quad \text{bit operations.}$$

## 7. The multivariate case.

**Thm:** Let $f, g, h \in \mathbb{Q}[\underline{x}, y]$ such that $f = g + y^{\beta} h$ and set $\alpha = \deg_y(g)$. Let $p \in \mathbb{Q}[\underline{x}, y]$ be an irreducible polynomial of degree bounded by $s$ which is not "cyclotomic". If

$$\beta - \alpha > 10^4 \cdot s \cdot n^4 \cdot \log_2(H_1(f)) \cdot \frac{\log^3(n \max\{s, 16\})}{\log^3(n \log(n \max\{s, 16\}))},$$

then $p|f$ if and only if $p|g$ and $p|h$.

## 7. The multivariate case.

**Thm:** Let $f, g, h \in \mathbb{Q}[\underline{x}, y]$ such that $f = g + y^{\beta} h$ and set $\alpha = \deg_y(g)$. Let $p \in \mathbb{Q}[\underline{x}, y]$ be an irreducible polynomial of degree bounded by $s$ which is not "cyclotomic". If

$$\beta - \alpha > 10^4 \cdot s \cdot n^4 \cdot \log_2(H_1(f)) \cdot \frac{\log^3(n \max\{s, 16\})}{\log^3(n \log(n \max\{s, 16\}))},$$

then $p|f$ if and only if $p|g$ and $p|h$.

**Thm:** Let $f, g, h \in \mathbb{Q}[\underline{x}, y]$ such that $f = g + y^{\beta} h$ and set $\alpha = \deg_y(g)$. Let $p \in \overline{\mathbb{Q}}[\underline{x}, y]$ be an irreducible polynomial of degree bounded by $s$ with at least three terms. If

$$\beta - \alpha > 10^{14} \cdot s \cdot n^{14} \cdot \log_2(H_1(f)) \cdot \frac{\log^5(\max\{ns, 16\})}{\log^4(n \log(\max\{ns, 16\}))},$$

then $p|f$ if and only if $p|g$ and $p|h$.

## 8. The tools for the proof I.

**Heights of algebraic numbers:** Let $r_1 \in \overline{\mathbb{Q}}$. Let $p = a(x-r_1)\cdots(x-r_d) \in \mathbb{Z}[x]$ be the primitive minimal polynomial of $r$. Then

$$H(r) = \left[|a| \prod_{i=1}^{d} \max\{1, |r_i|\}\right]^{1/d}.$$

## 8. The tools for the proof I.

**Heights of algebraic numbers:** Let $r_1 \in \overline{\mathbb{Q}}$. Let $p = a(x-r_1)\cdots(x-r_d) \in \mathbb{Z}[x]$ be the primitive minimal polynomial of $r$. Then

$$H(r) = \left[|a| \prod_{i=1}^{d} \max\{1, |r_i|\}\right]^{1/d}.$$

**Example:** Let $p \geq 5$ be a prime number. Let $\xi_p = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$ be a primitive $p$-th root of the unity. Then

$$H(1+\xi_p) = \left[\prod_{i=1}^{p-1} \max\{1, |1+\xi_p^i|\}\right]^{1/(p-1)} \geq \sqrt{2}^{(p-3)/(2p-2)} \geq 2^{1/8}.$$

## 9. The tools for the proof II.

**GAP Thm:** Let $f = f_1 + x_n^{\beta} f_2 \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ with $\deg_{x_n}(f_1) = \alpha < \beta$. Let $\eta \in \overline{\mathbb{Q}}$ and let $\xi_1, \ldots, \xi_{n-1}$ be roots of the unity such that $f(\xi_1, \ldots, \xi_{n-1}, \eta) = 0$. If

$$\beta - \alpha > \frac{\log_2 H_1(f)}{\log_2 H(\eta)}$$

then $f_1(\xi_1, \ldots, \xi_{n-1}, \eta) = f_2(\xi_1, \ldots, \xi_{n-1}, \eta) = 0$.

## 9. The tools for the proof II.

**GAP Thm:** Let $f = f_1 + x_n^{\beta} f_2 \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ with $\deg_{x_n}(f_1) = \alpha < \beta$. Let $\eta \in \overline{\mathbb{Q}}$ and let $\xi_1, \ldots, \xi_{n-1}$ be roots of the unity such that $f(\xi_1, \ldots, \xi_{n-1}, \eta) = 0$. If

$$\beta - \alpha > \frac{\log_2 H_1(f)}{\log_2 H(\eta)}$$

then $f_1(\xi_1, \ldots, \xi_{n-1}, \eta) = f_2(\xi_1, \ldots, \xi_{n-1}, \eta) = 0$.

**Example:** Let $f = g + y^{\beta} h \in \mathbb{Q}[x, y]$ with $\deg_y(g) = \alpha < \beta$. Suppose that $y - x - 1 | f$. In particular $f(\xi_p, 1 + \xi_p) = 0$ for all prime $p \geq 5$. If the GAP satisfies

$$\beta - \alpha > 8 \log_2 H_1(f)$$

then we have $g(\xi_p, 1 + \xi_p) = h(\xi_p, 1 + \xi_p) = 0$, i.e. $y - x - 1 | g$ and $y - x - 1 | h$.

## 10. The tools for the proof III.

**Def:** Let $p \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ and let $w \geq 0$.

$$C_{p,w} = \left\{ \xi \in G_\infty^{n-1} \,/\, \exists \eta \in \overline{\mathbb{Q}} : p(\xi, \eta) = 0 \wedge \log_2 H(\eta) \geq w \right\}$$

$$\lambda(p) = \sup \left\{ w \geq 0 \,/\, C_{p,w} \text{ is Zariski-dense in } \overline{\mathbb{Q}}^{n-1} \right\}$$

## 10. The tools for the proof III.

**Def:** Let $p \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ and let $w \geq 0$.

$$C_{p,w} = \left\{ \xi \in G_\infty^{n-1} \,/\, \exists \eta \in \overline{\mathbb{Q}} : p(\xi, \eta) = 0 \wedge \log_2 H(\eta) \geq w \right\}$$

$$\lambda(p) = \sup \left\{ w \geq 0 \,/\, C_{p,w} \text{ is Zariski-dense in } \overline{\mathbb{Q}}^{n-1} \right\}$$

**Lower bound:** If $p$ is (absolute) irreducible of degree $s$ and it has at least three terms, then

$$\lambda(p) \geq \frac{10^{-14}}{n^{14} s} \cdot \frac{\log^4(n \log(\max\{ns, 16\}))}{\log^5(\max\{ns, 16\})}.$$

## 11. The tools for the proof IV.

**Lower bound:** If $p \in \mathbb{Q}[x_1, \ldots, x_n]$ is irreducible of degree $s$ and it is not divisible by any binomial $x^b - \theta x^c$ with $\theta \in G_\infty$, then

$$\lambda(p) \geq \frac{10^{-4}}{n^4 s} \cdot \frac{\log^3(n \log(n \max\{s, 16\}))}{\log^3(n \max\{s, 16\})}.$$