# *Factoring Supersparse (Lacunary) Polynomials*

Erich Kaltofen
North Carolina State University
`google->kaltofen`

Joint work with Pascal Koiran
ENS Lyon, France

# Supersparse (lacunary) polynomials

The supersparse polynomial

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{t} c_i X_1^{\alpha_{i,1}} \cdots X_n^{\alpha_{i,n}}$$

is input by a list of its coefficients and corresponding term degree vectors.

$$\mathrm{size}(f) = \sum_{i=1}^{t} \Bigl(\text{dense-size}(c_i) + \lceil \log_2(\alpha_{i,1} \cdots \alpha_{i,n} + 2) \rceil \Bigr)$$

Term degrees can be very high, e.g., $\geq 2^{500}$

# Supersparse (lacunary) polynomials

The supersparse polynomial

$$f(X_1,\ldots,X_n) = \sum_{i=1}^{t} c_i X_1^{\alpha_{i,1}} \cdots X_n^{\alpha_{i,n}}$$

is input by a list of its coefficients and corresponding term degree vectors.

$$\mathrm{size}(f) = \sum_{i=1}^{t} \Big(\text{dense-size}(c_i) + \lceil \log_2(\alpha_{i,1} \cdots \alpha_{i,n} + 2) \rceil \Big)$$

Term degrees can be very high, e.g., $\geq 2^{500}$

Over $\mathbb{Z}_p$: evaluate by repeated squaring

Over $\mathbb{Q}$: cannot evaluate in polynomial-time exept for $X_i = 0, e^{2\pi i/k}$

## Easy problems for supersparse polynomials $f = \sum_i c_i X^{\alpha_i} \in \mathbb{Z}[z]$

Cucker, Koiran, Smale 1998: Compute root $a \in \mathbb{Z}: \quad f(a) = 0.$

Gap idea: if $f(a) = 0, a \neq \pm 1$ then $g_1(a) = \cdots = g_s(a) = 0$
where $f(X) = \sum_j g_j(X) X^{\alpha_j}$ and $\alpha_{j+1} - \alpha_j - \deg(g_j) \geq \chi.$

## Easy problems for supersparse polynomials $f = \sum_i c_i X^{\alpha_i} \in \mathbb{Z}[z]$

Cucker, Koiran, Smale 1998: Compute root $a \in \mathbb{Z}: \quad f(a) = 0.$

Gap idea: if $f(a) = 0, a \neq \pm 1$ then $g_1(a) = \cdots = g_s(a) = 0$
where $f(X) = \sum_j g_j(X) X^{\alpha_j}$ and $\alpha_{j+1} - \alpha_j - \deg(g_j) \geq \chi$.

Write $f(X) = \underbrace{g(X)}_{\deg(g) \leq k} + X^u h(X), \quad \|f\|_1 = |c_1| + \cdots + |c_t|.$

For $a \neq \pm 1$, $h(a) \neq 0:$

$$\begin{aligned} |g(a)| &< \|f\|_1 \cdot |a|^k \\ |a^u h(a)| &\geq |a|^u \end{aligned}$$

## Easy problems for supersparse polynomials $f = \sum_i c_i X^{\alpha_i} \in \mathbb{Z}[z]$

Cucker, Koiran, Smale 1998: Compute root $a \in \mathbb{Z}: \quad f(a) = 0.$

Gap idea: if $f(a) = 0, a \neq \pm 1$ then $g_1(a) = \cdots = g_s(a) = 0$
where $f(X) = \sum_j g_j(X) X^{\alpha_j}$ and $\alpha_{j+1} - \alpha_j - \deg(g_j) \geq \chi$.

Write $f(X) = \underbrace{g(X)}_{\deg(g) \leq k} + X^u h(X), \quad \|f\|_1 = |c_1| + \cdots + |c_t|.$

For $a \neq \pm 1,\ h(a) \neq 0$:
$$\begin{aligned} |g(a)| &< \|f\|_1 \cdot |a|^k \\ |a^u h(a)| &\geq |a|^u \end{aligned}$$

$$u - k \geq \chi = \log_2 \|f\|_1 \Longrightarrow |a|^u \geq 2^\chi \cdot |a|^k \geq \|f\|_1 \cdot |a|^k \Longrightarrow f(a) \neq 0.$$

Polynomial time root-finder uses the fact that for

$$g_j(X) = c_1 + c_2 x^{\beta_2} + \cdots + c_s x^{\beta_s}, \quad \beta_i - \beta_{i-1} < \chi, \quad s \leq t$$

we have

$$\beta_i \leq (i-1)(\chi - 1),$$

so

$$\deg(g_j) \leq (t-1)(\chi - 1)$$

# Easy problems for supersparse polynomials $f = \sum_i c_i X^{\alpha_i} \in K[X]$

H. W. Lenstra, Jr. 1999:

*Input:* $\varphi(\zeta) \in \mathbb{Z}[\zeta]$ monic irred.; let $K = \mathbb{Q}[\zeta]/(\varphi(\zeta))$
a supersparse $f(X) = \sum_{i=1}^{t} c_i X^{\alpha_i} \in K[X]$
a factor degree bound $d$

*Output:* a list of all irreducible factors of $f$ over $K$ of degree $\leq d$
and their multiplicities (which is $\leq t$ except for $X$)

Let $D = d \cdot \deg(\varphi)$
There are at most $O(t^2 \cdot 2^D \cdot D \cdot \log(Dt))$ factors of degree $\leq d$

Bit complexity is $\left(\mathrm{size}(f) + D + \log\|\varphi\|\right)^{O(1)}$

Special case $\varphi = \zeta - 1, d = D = 1$: Algorithm finds all rational roots in polynomial-time.

## Our ISSAC '06 result for supersparse polynomials

$f = \sum_i c_i \overline{X}^{\overline{\alpha_i}} \in K[\overline{X}]$ where $\overline{X}^{\overline{\alpha_i}} = X_1^{\alpha_{i,1}} \cdots X_n^{\alpha_{i,n}}$

*Input:* $\varphi(\zeta) \in \mathbb{Z}[\zeta]$ monic irred.; let $K = \mathbb{Q}[\zeta]/(\varphi(\zeta))$
a supersparse $f(\overline{X}) = \sum_{i=1}^{t} c_i \overline{X}^{\overline{\alpha_i}} \in K[\overline{X}]$
a factor degree bound $d$

*Output:* a list of all irreducible factors of $f$ over $K$ of degree $\leq d$
and their multiplicities (which is $\leq t$ except for any $X_j$)

Bit complexity is:

$\big(\mathrm{size}(f) + d + \deg(\varphi) + \log \|\varphi\|\big)^{O(n)}$ (sparse factors)

$\big(\mathrm{size}(f) + d + \deg(\varphi) + \log \|\varphi\|\big)^{O(1)}$ (blackbox factors)

# Linear and quadratic bivariate factors [ISSAC'05]

*Input:* a supersparse $f(X,Y) = \sum_{i=1}^{t} c_i X^{\alpha_i} Y^{\beta_i} \in \mathbb{Z}[X,Y]$ that is monic in $X$;
an error probability $\varepsilon = 1/2^l$

*Output:* a list of polynomials $g_j(X,Y)$ with $\deg_X(g_j) \le 2$ and $\deg_Y(g_j) \le 2$;
a list of corresponding multiplicities.

The $g_j$ are with probability $\ge 1-\varepsilon$ all irreducible factors of $f$ over $\mathbb{Q}$ of degree $\le 2$ together with their true multiplicities.

Bit complexity: $\left(\mathrm{size}(f) + \log 1/\varepsilon\right)^{O(1)}$

## Linear and quadratic bivariate factors [ISSAC'05]

*Input:* a supersparse $f(X,Y) = \sum_{i=1}^{t} c_i X^{\alpha_i} Y^{\beta_i} \in \mathbb{Z}[X,Y]$
that is monic in $X$;
an error probability $\varepsilon = 1/2^l$

*Output:* a list of polynomials $g_j(X,Y)$
with $\deg_X(g_j) \leq 2$ and $\deg_Y(g_j) \leq 2$;
a list of corresponding multiplicities.

The $g_j$ are with probability $\geq 1-\varepsilon$ all irreducible factors of $f$ over $\mathbb{Q}$ of degree $\leq 2$ together with their true multiplicities.

Bit complexity: $\left(\mathrm{size}(f) + \log 1/\varepsilon\right)^{O(1)}$

With É. Schost + [Tao 2005]: remove monicity restriction
factors of degree $O(1)$.

# Linear and quadratic bivariate factors [ISSAC'05]

*Input:* a supersparse $f(X,Y) = \sum_{i=1}^{t} c_i X^{\alpha_i} Y^{\beta_i} \in \mathbb{Z}[X,Y]$ that is monic in $X$;
an error probability $\varepsilon = 1/2^l$

*Output:* a list of polynomials $g_j(X,Y)$ with $\deg_X(g_j) \leq 2$ and $\deg_Y(g_j) \leq 2$;
a list of corresponding multiplicities.

The $g_j$ are with probability $\geq 1-\varepsilon$ all irreducible factors of $f$ over $\mathbb{Q}$ of degree $\leq 2$ together with their true multiplicities.

Bit complexity: $\left(\mathrm{size}(f) + \log 1/\varepsilon\right)^{O(1)}$

With É. Schost ~~+ [Tao 2005]~~: remove monicity restriction
simple argument: factors of degree $O(1)$.

Algorithm

Step 0: compute all factors of $f$ that are in $\mathbb{Q}[Y]$ by Lenstra's method on the coefficients of $X^{\alpha_i}$

Step 1: compute linear and quadratic factors in $\mathbb{Q}[X]$ of $f(X,0)$, $f(X,1)$ and $f(X,-1)$ by Lenstra's method

Step 2: interpolate all factor combinations;
Test if $g(X,Y)$ divides $f(X,Y)$ by

$0 \equiv f(X,a) \bmod (g(X,a),p)$ where $a \in \mathbb{Z}$, $p$ prime are random

# Leading coefficient problem

If the leading (trailing) coefficient in $X$ does not vanish for $Y = 0, e^{2\pi i/k}$, then one can impose *a factor* of the leading (trailing) coefficient on $g$.

We can generalize gap theorem and compute all small degree factors of supersparse polynomials deterministically.

## Concepts from algebraic number theory

Weil height for algebraic number $\eta$ :

$$\mathrm{Height}(\eta) = \prod_{\nu \in M_{\mathbb{Q}(\eta)}} \max(1, |\eta|_\nu)^{\frac{d_\nu}{[\mathbb{Q}(\eta):\mathbb{Q}]}}$$

where $M_{\mathbb{Q}(\eta)}$ are all absolute values in $\mathbb{Q}(\eta)$, $d_\nu$ their local degrees.

# Concepts from algebraic number theory

Weil height for algebraic number $\eta$:

$$\mathrm{Height}(\eta) = \prod_{\nu \in M_{\mathbb{Q}(\eta)}} \max(1, |\eta|_\nu)^{\frac{d_\nu}{[\mathbb{Q}(\eta):\mathbb{Q}]}}$$

where $M_{\mathbb{Q}(\eta)}$ are all absolute values in $\mathbb{Q}(\eta)$, $d_\nu$ their local degrees.

**Theorem** [cf. Amoroso and Zannier 2000]
Let $L$ be a cyclotomic, hence Abelian extension of $\mathbb{Q}$.
For any algebraic $\eta \neq 0$ that is not a root of unity

$$\mathrm{Height}(\eta) \geq \exp\left(\frac{C_1}{D}\left(\frac{\log(2D)}{\log\log(5D)}\right)^{-13}\right) = 1 + o(1),$$

where $C_1 > 0$ and $D = [L(\eta) : L]$.

# Concepts from algebraic number theory

Weil height for algebraic number $\eta$:

$$\mathrm{Height}(\eta) = \prod_{v \in M_{\mathbb{Q}(\eta)}} \max(1, |\eta|_v)^{\frac{d_v}{[\mathbb{Q}(\eta):\mathbb{Q}]}}$$

where $M_{\mathbb{Q}(\eta)}$ are all absolute values in $\mathbb{Q}(\eta)$, $d_v$ their local degrees.

**Theorem** [cf. Amoroso and Zannier 2000]
Let $L$ be a cyclotomic, hence Abelian extension of $\mathbb{Q}$.
For any algebraic $\eta \neq 0$ that is not a root of unity

$$\mathrm{Height}(\eta) \geq \exp\left(\frac{C_1}{D}\left(\frac{\log(2D)}{\log\log(5D)}\right)^{-13}\right) = 1 + o(1),$$

where $C_1 > 0$ and $D = [L(\eta) : L]$.

We do not know a $C_1$ explicitly, hence $\exists$ an algorithm.

# Concepts from diophantine geometry

Let $P(X_1,\ldots,X_n) \in \mathbb{C}[X_1,\ldots,X_n]$ be irreducible
$V(P) =$ rootset (variety, hypersurface) of $P$
$S \subseteq V(P)$ is Zariski dense iff $S \subseteq V(Q) \Longrightarrow Q = P$

Example: $\{(\xi,\xi,0) \mid \xi \in \mathbb{C}\}$ is not dense for $X_1 - X_2 + X_3$.

## Concepts from diophantine geometry

Let $P(X_1,\ldots,X_n) \in \mathbb{C}[X_1,\ldots,X_n]$ be irreducible
$V(P) =$ rootset (variety, hypersurface) of $P$
$S \subseteq V(P)$ is Zariski dense iff $S \subseteq V(Q) \implies Q = P$

Example: $\{(\xi,\xi,0) \mid \xi \in \mathbb{C}\}$ is not dense for $X_1 - X_2 + X_3$.

**Theorem** [cf. Laurent 1984]
Let $P(X_1,\ldots,X_n) \in \mathbb{C}[X_1,\ldots,X_n]$ be irreducible
and let $S \subseteq V(P)$ where each coordinate of each point is a root of unity (torsion points).
Then

$$S \text{ is dense for } P \iff P = \prod_{i=1}^{n} X_i^{\beta_i} - \theta,$$

where $\theta$ is a root of unity and $\beta_i \in \mathbb{Z}$.

Example: $\{(e^{2\pi\boldsymbol{i}/(2j)}, e^{2\pi\boldsymbol{i}/(3j)})\}$ is dense for $X_1^2 - X_2^3$.

# Gap theorem for factors where cyclotomic points are not dense

Let $P$ be the irreducible factor of $f$.

Step 1: construct dense set $\{(\theta_1, \ldots, \theta_{n-1}, \eta)\}$ for $P$ such that all $\theta_i$ are roots of unity, $\eta$ are not.

# Gap theorem for factors where cyclotomic points are not dense

Let $P$ be the irreducible factor of $f$.

Step 1: construct dense set $\{(\theta_1,\ldots,\theta_{n-1},\eta)\}$ for $P$ such that all $\theta_i$ are roots of unity, $\eta$ are not.

Step 2: If $f(X_1,\ldots,X_n)=g+X_n^u h$, $\deg_{X_n}(g)<k$, apply Lenstra's gap argument to

$$g(\theta_1,\ldots,\theta_{n-1},\eta)=-\eta^u h(\theta_1,\ldots,\theta_{n-1},\eta)$$

and get

$$u-k\geq\chi\Longrightarrow g(\theta_1,\ldots,\theta_{n-1},\eta)=0$$

where

$$\chi=\frac{D}{C_2}\left(\frac{\log(2D)}{\log\log(5D)}\right)^{13}\log(t(t+1)\,\mathrm{Height}(f)).$$

## Lenstra's argument

Assume $g(\theta_1,\ldots,\theta_{n-1},\eta) = -\eta^u h(\theta_1,\ldots,\theta_{n-1},\eta) \neq 0$.
Use absolute values $\nu$ and Weil height

$$\max(1,|\eta|_\nu)^{u-k} \cdot |g(\theta_1,\ldots,\eta)|_\nu \leq \max(1,|t|_\nu) \cdot |f|_\nu \cdot |\eta|_\nu^u.$$

Taking a fractional power $d_\nu/[K:\mathbb{Q}]$ and product over all $\nu$, using the product formula $\prod_\nu |\eta|_\nu^{d_\nu} = 1$ $(\eta \neq 0)$,

$$\mathrm{Height}(\eta)^{u-k} \leq t \cdot \mathrm{Height}(f).$$

The Bogomolov property for algebraic number fields implies that

$$\mathrm{Height}(\eta) > 1 + \varepsilon(\deg f).$$

# Factors for which cyclotomic points are dense

Consider irreducible factor

$$P_{\beta,\gamma,\theta} = P(X_1,\ldots,X_n) = \prod_{i=1}^{n} X_i^{\beta_i} - \theta \prod_{i=1}^{n} X_i^{\gamma_i}$$

with $\forall i\colon \beta_i = 0 \vee \gamma_i = 0$ and $\mathrm{GCD}_{1\le i\le n}(\beta_i - \gamma_i) = 1.$

Suppose $(\beta_n,\gamma_n) \neq (0,0)$. Plugging into $f = \sum_j c_j \overline{X}^{\overline{\alpha_j}}$

$$X_n = \lambda \left(\prod_{i=1}^{n-1} X_i^{\gamma_i - \beta_i}\right)^{\frac{1}{\beta_n - \gamma_n}}$$

we find $j$ and $k = \pm\mathrm{GCD}_{1\le i\le n}(\alpha_{0,i} - \alpha_{j,i})$:

$$\alpha_{0,n} \neq \alpha_{j,n} \text{ and } \forall i\colon \gamma_i - \beta_i = (\alpha_{0,i} - \alpha_{j,i})/k,$$

# Factors for which cyclotomic points are dense (cont.)

Step 1: compute candidates for $(\beta, \gamma)$.

Step 2: compute $\lambda$ as cyclotomic roots of bounded order of sets of supersparse univariate polynomials in $\lambda$.

Step 3: compute the norm of $P(X_1, \ldots, X_n)$, which must be irreducible over the ground field.

# Hard problems for supersparse polynomials $\sum_i c_i z^{e_i} \in \mathbb{Z}[z]$

Plaisted 1977: Let $N = \prod_{i=1}^{n} p_i$, where $p_i$ distinct primes.

| Formula | Polynomial | Rootset |
|---|---|---|
| $x_j$ | $z^{\frac{N}{p_j}} - 1$ | $\{(e^{\frac{2\pi \mathbf{i}}{N}})^a \mid a \equiv 0 \pmod{p_j}\}$ |
| $\neg x_k$ | $\dfrac{z^N - 1}{z^{\frac{N}{p_k}} - 1} = \sum_{i=0}^{p_k - 1} z^{\frac{iN}{p_k}}$ | $\{(e^{\frac{2\pi \mathbf{i}}{N}})^b \mid b \not\equiv 0 \pmod{p_k}\}$ |
| $L_1 \vee L_2$ | $\mathrm{LCM}(\mathrm{Poly}(L_1), \mathrm{Poly}(L_2))$ | $\mathrm{Roots}(L_1) \cup \mathrm{Roots}(L_2)$ |
| $x_j \vee \neg x_k$ | $\dfrac{(z^{\frac{N}{p_j p_k}} - 1)(z^N - 1)}{z^{\frac{N}{p_k}} - 1}$ | (is supersparse polynomial) |

## Hard problems for supersparse polynomials $\sum_i c_i z^{e_i} \in \mathbb{Z}[z]$

Plaisted 1977: Let $N = \prod_{i=1}^{n} p_i$, where $p_i$ distinct primes.

| Formula | Polynomial | Rootset |
|---|---|---|
| $x_j$ | $z^{\frac{N}{p_j}} - 1$ | $\{(e^{\frac{2\pi\mathbf{i}}{N}})^a \mid a \equiv 0 \pmod{p_j}\}$ |
| $\neg x_k$ | $\dfrac{z^N - 1}{z^{\frac{N}{p_k}} - 1} = \sum_{i=0}^{p_k-1} z^{\frac{iN}{p_k}}$ | $\{(e^{\frac{2\pi\mathbf{i}}{N}})^b \mid b \not\equiv 0 \pmod{p_k}\}$ |
| $L_1 \vee L_2$ | $\mathrm{LCM}(\mathrm{Poly}(L_1), \mathrm{Poly}(L_2))$ | $\mathrm{Roots}(L_1) \cup \mathrm{Roots}(L_2)$ |
| $x_j \vee \neg x_k$ | $\dfrac{(z^{\frac{N}{p_j p_k}} - 1)(z^N - 1)}{z^{\frac{N}{p_k}} - 1}$ | (is supersparse polynomial) |
| $C_1 \wedge C_2$ | $\mathrm{GCD}(\mathrm{Poly}(C_1), \mathrm{Poly}(C_2))$ | $\mathrm{Roots}(C_1) \cap \mathrm{Roots}(C_2)$ |

***Theorem*** $C_1 \wedge \cdots \wedge C_l$ *is satisfiable*

$$\iff \mathrm{GCD}(\mathrm{Poly}(C_1), \ldots, \mathrm{Poly}(C_l)) \neq 1.$$

# Other hard problems [Plaisted 1977/78]

1. Given sequences $a_1, \ldots, a_m \in \mathbb{Z}$ and $b_1, \ldots b_n \in \mathbb{Z}$ determine whether

$$\prod_{i=1}^{m}(z^{a_i}-1) \quad \text{is not a factor of} \quad \prod_{i=1}^{n}(z^{b_i}-1).$$

2. Given a set $\{a_1, \ldots, a_m\} \subset \mathbb{Z}$ determine whether

$$\int_0^{2\pi} \cos(a_1\theta)\cdots\cos(a_m\theta)d\theta \neq 0.$$

## Hard problems for supersparse polynomials in $K[X,Y]$

Theorem
The set of all monic (in $X$) irreducible supersparse polynomials in $K[X,Y]$ is co-NP-hard for $K=\mathbb{Q}$ and $K=\mathbb{F}_q$ for all $p$ and all sufficiently large $q=p^k$, via randomized reduction.

Corollary
Suppose we have a Monte Carlo polynomial-time irreducibility test for monic supersparse polynomials in $\mathbb{F}_{2^k}[X,Y]$ (for sufficiently large $k$).
Then large integers can be factored in Las Vegas polynomial-time.

# Another hard problem for supersparse polynomials in $\mathbb{F}_{2^k}[X]$ (Reference thanks to Jintai Ding)

Theorem [Kipnis and Shamir CRYPTO '99]
The set of all supersparse polynomials in $\mathbb{F}_{2^k}[X]$ that have a root in $\mathbb{F}_{2^k}$ is NP-hard for all sufficiently large $k$.

Corollary (cf. Open Problem in our ISSAC'05 paper)
It is NP-hard to determine if a polynomial in $X$ over $\mathbb{F}_{2^k}$ given by a division-free straight-line program has a root in $\mathbb{F}_{2^k}$.

Danke schön!
(Thank you!)