Finding Small Degree Factors of Multivariate Supersparse (Lacunary) Polynomials Over Algebraic Number Fields

Erich Kaltofen

Massachusetts Institute of Technology

`google->kaltofen`

Joint work with Pascal Koiran (ENS-Lyon)

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.

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

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 $f = \sum_i c_i X^{\alpha_i} \in K[X]$

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

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 $\le d$
and their multiplicities (which is $\le t$ 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 $\le d$

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 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:

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

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

Our ISSAC '05 result: $K = \mathbb{Q}, n = 2, d = 1$

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 ≤ 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 ≤ 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 $\deg_X(g_j) \le 2$ 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 ≤ 2 together with their true multiplicities.

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

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

Concepts from algebraic number theory

Weil height for algebraic number η:

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

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

Concepts from algebraic number theory

Weil height for algebraic number η :

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

where $M_{\mathbb{Q}(\eta)}$ are all absolute values in $\mathbb{Q}(\eta)$, d_ν 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 η :

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

where $M_{\mathbb{Q}(\eta)}$ are all absolute values in $\mathbb{Q}(\eta)$, d_ν 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 θ 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 θ_i are roots of unity, η 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 θ_i are roots of unity, η 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

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

Factors for which cyclotomic points are dense

Consider irreducible factor

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

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

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

Factors for which cyclotomic points are dense (cont.)

Step 1: compute candidates for (β,γ).

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

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

Example

$X^{\beta} - \theta Y^{\gamma} \mid X^n Y^0 - X^0 Y^{n+1}$ if

$$k = \pm \mathrm{GCD}(n-0, 0-(n+1)) = \pm 1$$

and

$$-\beta = (n-0)/k, \quad \gamma = (0-(n+1))/k$$

Therefore there is no such factor,
even in Stephen Watt's symbolic polynomial sense.

Similar symbolic irreducibility criteria with gap theorem.

Another hard problem for supersparse polynomials in $\mathbb{F}_{2^k}[X]$

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 $\mathbb{F}_{2^k}$.

Grazie mille!