Sub-Linear Root Detection for Sparse Polynomials Over Finite Fields

Jingguo Bi

Institute for Advanced Study
Tsinghua University
Beijing, China

October, 2014
Vienna, Austria

This is a joint work with Qi Cheng and J. Maurice Rojas.

Applications of lattice theory

Lattice theory has fruitful applications in Physics and Chemistry, such as the structure of particle systems under a variety of physical constraints, packing problems, etc, but also has applications in Computational Number Theory, Computational Algebra, Coding Theory, Theoretical Computer Science and Cryptography, etc.

The Problem

Let R be a ring. Given any univariate t-nomial

$$f(x) := c_1 + c_2 x^{a_2} + c_3 x^{a_3} + \cdots + c_t x^{a_t} \in R[x]$$

- (decision version) decide whether there is a root in R
- (search version) find one of the roots in R
- (counting version) count the number of roots in R

Previous work

- Cucker, Koiran, and Smale found a polynomial-time algorithm to find all integer roots of a univariate polynomial f in $\mathbf{Z}[x]$ with exactly t terms
- H. W. Lenstra, Jr. gave a polynomial-time algorithm to compute all factors of fixed degree over an algebraic extension of $\mathbf{Q}$ of fixed degree (and thereby all rational roots)
- Independently, Kaltofen and Koiran and Avendano, Krick, and Sombra extended this to finding bounded-degree factors of sparse polynomials in $\mathbb{Q}[x, y]$ in polynomial-time

Previous work on finite fields

- NP-hardness over even characteristic for sparse polynomials (Kipnis-Shamir 1999)
- For prime order finite field, detecting rational roots for straight-line program is prove to be NP-hard (Cheng-Hill-Wan 2012)
- Even for trinomials, no nontrivial algorithm is known

Main Results

- Given any univariate t-nomial

$$f(x) = c_0 + c_1x^{a_1} + c_2x^{a_2} + \cdots + c_{t-1}x^{a_{t-1}} \in \mathbf{F}_q[x]$$

  We can decide, within $4^{t+o(t)}q^{\frac{t-2}{t-1}+o(1)}$ deterministic bit operations, whether $f(x)$ has a root in $\mathbf{F}_q$

- Moreover, we also give the structure of the roots of $f(x)$ over $\mathbf{F}_q$
- When t is fix, this is the first sub-linear in q algorithm to solve this problem
- There is an algorithm running in time $q^{1/2+o(1)}$ to decide whether a trinomial in $\mathbf{F}_q[x]$ has a root in $\mathbf{F}_q$

What Is a Lattice?

Given n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$ $(n \leq m)$, the lattice generated by them is the set of vectors

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

The vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ form a basis of the lattice

The Shortest Vector Problem

The most famous computational problem on lattices is the shortest vector problem (SVP): Given a basis of a lattice L, find a vector $\mathbf{u} \in L$, such that $\| \mathbf{v} \| \geq \| \mathbf{u} \|$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$

The Minkowski Convex Body Theorem

There exists a nonzero lattice vector with length less than $\sqrt{n}\,\det(L)^{1/n}$

The LLL Reduction

There is a polynomial time algorithm to find a base such that the length of the shortest vector in the base $\leq (2/\sqrt{3})^n \lambda_1$, where λ_1 denotes the length of the shortest nonzero vector in the lattice

Exact algorithm for SVP

There is an algorithm to compute the shortest nonzero vector of a n-dimensional lattice which needs at most $4^{n+o(n)}$ arithmetic operations. (Micciancio-Voulgaris 2010)

Main theorem

Given any univariate t-nomial

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} \in \mathbf{F}_q[x]$$

We can decide, within $4^{t+o(t)} q^{\frac{t-2}{t-1}+o(1)}$ deterministic bit operations, whether $f(x)$ has a root in $\mathbf{F}_q$

Observation

- Detecting roots over $\mathbf{F}_q$ is the same as detecting linear factors of polynomials in $\mathbf{F}_q[x]$
- However, to detect roots in $\mathbf{F}_q$, we don't need the full power of factoring
- we need only decide whether $\gcd(x^q - x, f(x))$ has positive degree, which takes time $deg(f)^{1+o(1)}(\log q)^{O(1)}$ (E.Bach and J. Shallit 1996)

Degree reduction

- Replace x by y^e in f.

$$f(y^e) := c_0 + c_1 y^{ea_1} + c_2 y^{ea_2} + \cdots + c_{t-1} y^{ea_{t-1}}$$

Degree reduction

- Replace x by y^e in f.

$$f(y^e) := c_0 + c_1 y^{ea_1} + c_2 y^{ea_2} + \cdots + c_{t-1} y^{ea_{t-1}}$$

- If $\gcd(e, q-1) = 1$, then the map from $\mathbf{F}_q$ to $\mathbf{F}_q$ given by y^e is one-to-one, thus it will not change the solvability of f

Degree reduction

- Replace x by y^e in f.

$$f(y^e) := c_0 + c_1 y^{ea_1} + c_2 y^{ea_2} + \cdots + c_{t-1} y^{ea_{t-1}}$$

- If $\gcd(e, q-1) = 1$, then the map from $\mathbf{F}_q$ to $\mathbf{F}_q$ given by y^e is one-to-one, thus it will not change the solvability of f
- A new polynomial

$$c_0 + c_1 y^{ea_1 \pmod{q-1}} + c_2 y^{ea_2 \pmod{q-1}} + \cdots + c_{t-1} y^{ea_{t-1} \pmod{q-1}}$$

Degree reduction

- Replace x by y^e in f.

$$f(y^e) := c_0 + c_1 y^{ea_1} + c_2 y^{ea_2} + \cdots + c_{t-1} y^{ea_{t-1}}$$

- If $\gcd(e, q-1) = 1$, then the map from $\mathbf{F}_q$ to $\mathbf{F}_q$ given by y^e is one-to-one, thus it will not change the solvability of f
- A new polynomial

$$c_0 + c_1 y^{ea_1 \pmod{q-1}} + c_2 y^{ea_2 \pmod{q-1}} + \cdots + c_{t-1} y^{ea_{t-1} \pmod{q-1}}$$

- Find a suitable e to reduce the degree.

Lemma (Find e)

Given integers $a_1, \cdots, a_{t-1}, N$ satisfying $0 < a_1 < \cdots < a_{t-1} < N$ and $\gcd(N, a_1, \cdots, a_{t-1}) = 1$, one can find, within $4^{t+o(t)}$ bit operations, an integer e with the following property for all $i \in \{1, \ldots, t-1\}$:

$$m_1 \equiv ea_1 \mod N, m_2 \equiv ea_2 \mod N, \cdots, m_{t-1} \equiv ea_{t-1} \mod N$$

if $m_i \in [-N/2, N/2]$, then $|m_i| \leq \sqrt{t-1} N^{\frac{t-2}{t-1}}$

Find e

Consider the lattice L generated by the row vectors of the matrix:

$$\mathbf{B} = \begin{bmatrix} a_1 & a_2 & \cdots & a_{t-1} \\ N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & N \end{bmatrix}$$

Find e

Consider the lattice L generated by the row vectors of the matrix:

$$\mathbf{B} = \begin{bmatrix} a_1 & a_2 & \cdots & a_{t-1} \\ N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & N \end{bmatrix}$$

- $\det(L) | N^{t-2}$

Find e

Consider the lattice L generated by the row vectors of the matrix:

$$\mathbf{B} = \begin{bmatrix} a_1 & a_2 & \cdots & a_{t-1} \\ N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & N \end{bmatrix}$$

- $\det(L) | N^{t-2}$
- From Minkowski's Theorem, let $\mathbf{m} = (m_1, m_2, \cdots, m_{t-1})$ be the shortest vector of lattice L, then, $\| \mathbf{m} \| \leq \sqrt{t-1} N^{\frac{t-2}{t-1}}$

Find e

Consider the lattice L generated by the row vectors of the matrix:

$$\mathbf{B} = \begin{bmatrix} a_1 & a_2 & \cdots & a_{t-1} \\ N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & N \end{bmatrix}$$

- $\det(L) | N^{t-2}$
- From Minkowski's Theorem, let $\mathbf{m} = (m_1, m_2, \cdots, m_{t-1})$ be the shortest vector of lattice L, then, $\| \mathbf{m} \| \leq \sqrt{t-1} N^{\frac{t-2}{t-1}}$
- One can find $\mathbf{m}$ by using the Micciancio-Voulgaris algorithm

Find e

- From $\mathbf{m} = (m_1, m_2, \cdots, m_{t-1}) \in \mathcal{L}$, then there exists an integer e such that $m_1 = ea_1 \pmod N$, $m_2 = ea_2 \pmod N, \cdots, m_{t-1} = ea_{t-1} \pmod N$
- Because $\gcd(a_1, a_2, \cdots, a_{t-1}, N) = 1$, one can find integers $x_1, x_2, \cdots, x_t$ s.t.,
$$\sum_{i=1}^{t-1} x_i a_i + x_t N = 1$$
- Let
$$e = \sum_{i=1}^{t-1} x_i m_i \mod N$$
Therefore, for i, $1 \leq i \leq t-1$, we have $ea_i \equiv m_i \mod N$ and $|m_i| \leq \|\mathbf{m}\| \leq \sqrt{t-1} N^{\frac{t-2}{t-1}}$

Main theorem

Given any univariate t-nomial

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} \in \mathbf{F}_q[x]$$

We can decide, within $4^{t+o(t)} q^{\frac{t-2}{t-1}+o(1)}$ deterministic bit operations, whether $f(x)$ has a root in $\mathbf{F}_q$

The case of $\gcd(a_1, a_2, \cdots a_{t-1}, q-1) > 1$.

Let $\delta = \gcd(a_1, a_2, \cdots a_{t-1}, q-1)$. The $\mathbf{F}_q$-solvability of

$$f(x) := c_0 + c_1x^{a_1} + c_2x^{a_2} + \cdots + c_{t-1}x^{a_{t-1}}$$

is equivalent to the solvability of the following system of equations:

$$c_0 + c_1y^{a_1/\delta} + \cdots + c_{t-1}y^{a_{t-1}/\delta} = 0$$
$$y^{\frac{q-1}{\delta}} = 1$$

The main lemma

Given a finite field $\mathbf{F}_q$ and the polynomials

$(\star\star\star)$ $\qquad x^N - 1$ and $c_0 + c_1 x^{a_1} + \cdots + c_{t-1} x^{a_{t-1}}$,

in $\mathbf{F}_q[x]$ with $0 < a_1 < \cdots < a_{t-1} < N$, $\gcd(N, a_1, \cdots, a_{t-1}) = 1$, $c_i \neq 0$ for all i, and $N|(q-1)$, there exists a deterministic $q^{1/4}(\log q)^{O(1)} + 4^t(t \log N)^{O(1)} + t^{\frac{1}{2}+o(1)} N^{\frac{t-2}{t-1}+o(1)} (\log q)^{2+o(1)}$ algorithm to decide whether these two polynomials share a root in $\mathbf{F}_q$.

Remark: One can find a generator g of $\mathbf{F}_q^\star$ within $q^{1/4}(\log q)^{O(1)}$ bit operations. (Shparlinski, 1996)

Proof of the main lemma

we can find an integer e in time $4^{t+o(t)}$ by reducing the lattice

$$\mathbf{B} = \begin{bmatrix} a_1 & a_2 & \cdots & a_{t-1} \\ N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & N \end{bmatrix}$$

such that if $m_1, \ldots, m_{t-1}$ are the unique integers in the range $[-\lfloor N/2 \rfloor, \lceil N/2 \rceil]$ respectively congruent to $ea_1, \ldots, ea_{t-1}$, then $|m_i| < \sqrt{t-1} N^{\frac{t-2}{t-1}}$ for each $i \in \{1, \ldots, t-1\}$.

- Since $N|(q-1)$, we have $x^N - 1|x^q - x$, then the roots of $x^N - 1 = 0$ the same as $x \in \langle g^{\frac{q-1}{N}} \rangle$, let $\zeta_N = g^{\frac{q-1}{N}}$, and $k = \gcd(e, N)$
- If $k = 1$, the map

$$\begin{array}{rcl} \varphi :< \zeta_N > & \longrightarrow & < \zeta_N > \\ x & \longmapsto & x^e \end{array}$$

  is one-to-one
- finding a solution for $(\star\star\star)$ is equivalent to finding $x \in \langle \zeta_N \rangle$ such that $c_0 + c_1 x^{ea_1} + \cdots + c_{t-1} x^{ea_{t-1}} = 0$
- The last equation can be rewritten as the lower degree equation $c_0 + c_1 x^{m_1} + \cdots + c_{t-1} x^{m_{t-1}} = 0$
- Time complexity: $(\sqrt{t-1} N^{\frac{t-2}{t-1}})^{1+o(1)} (\log q)^{2+o(1)}$

- if $k > 1$, the map from $\langle \zeta_N \rangle$ to $\langle \zeta_N \rangle$ given by $x \mapsto x^e$ is no longer one-to-one. Instead, it sends $\langle \zeta_N \rangle$ to a smaller subgroup $\langle \zeta_N^k \rangle$ of order N/k
- Any element $x \in \langle \zeta_N \rangle$ can be written as $\zeta_N^i z$ for some $i \in \{0, \ldots, k-1\}$ and $z \in \langle \zeta_N^k \rangle$
- Now, $\gcd(e/k, N/k) = 1$, so the map φ_1

$$\begin{array}{rcl} \varphi_1 :< \zeta_N^k > & \longrightarrow & < \zeta_N^k > \\ y & \longmapsto & y^{e/k} \end{array}$$

is one-to-one

$$
\begin{aligned}
& x^N - 1 = 0 \ \text{ and } \ c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} = 0 \\
\Leftrightarrow \ & x \in < \zeta_N > \ \text{ and } \ c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} = 0 \\
\Leftrightarrow \ & \exists i, 1 \leq i \leq k, x = (\zeta_N)^i y, y \in < \zeta_N^k > \\
& \ \text{and } \ c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} = 0 \\
\Leftrightarrow \ & \exists i, 1 \leq i \leq k, y \in < \zeta_N^k > \ \text{ and} \\
& c_0 + c_1 ((\zeta_N)^i y)^{a_1} + \cdots + c_{t-1} ((\zeta_N)^i y)^{a_{t-1}} = 0 \\
\Leftrightarrow \ & \exists i, 1 \leq i \leq k, y \in < \zeta_N^k > \ \text{ and} \\
& c_0 + c_1 ((\zeta_N)^i y^{e/k})^{a_1} + \cdots + c_{t-1} ((\zeta_N)^i y^{e/k})^{a_{t-1}} = 0 \\
\Leftrightarrow \ & \exists i, 1 \leq i \leq k, y^{N/k} - 1 = 0 \ \text{ and} \\
& c_0 + c_1 (\zeta_N)^{a_1 i} y^{m_1/k} + \cdots + c_{t-1} (\zeta_N)^{a_{t-1} i} y^{m_{t-1}/k} = 0
\end{aligned}
$$

Let

$$
f_i(y) = c_0 + c_1 (\zeta_N)^{a_1 i} y^{m_1/k} + \cdots + c_{t-1} (\zeta_N)^{a_{t-1} i} y^{m_{t-1}/k}
$$

- If f_i is identically zero then we have found a whole set of solutions for $\begin{cases} x^N - 1 = 0 \\ c_0 + c_1x^{a_1} + c_2x^{a_2} + \cdots + c_{t-1}x^{a_{t-1}} = 0 \end{cases}$: the coset $\zeta_N^i\langle\zeta_N^k\rangle$
- If f_i is not identically zero then let

$$\ell := \min_i \min(m_i/k, 0)$$

The polynomial $z^{-\ell}f_i(z)$ then has degree bounded from above by $2\sqrt{t-1}N^{\frac{t-2}{t-1}}/k$. Deciding whether the pair of equations

$$\begin{cases} y^{N/k} - 1 = 0 \\ y^{-l}f_i(y) = 0 \end{cases}$$

has a solution for some i takes deterministic time $k\left(\sqrt{t-1}N^{\frac{t-2}{t-1}}/k\right)^{1+o(1)}(\log q)^{2+o(1)}$

Roots structure

Let γ be the number of $f_i \neq 0$, then the solutions of equations

$$\begin{cases} x^N - 1 = 0 \\ c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{t-1} x^{a_{t-1}} = 0 \end{cases}$$

has two parts over $\mathbf{F}_q$. The first part contains at most $2\gamma\sqrt{t-1}N^{\frac{t-2}{t-1}}/k$ isolated roots, the other part includes $k-\gamma$ subgroup of $\mathbf{F}_q^*$ with order N/k

Thank you !