Finding Small Roots of Polynomial Equations

Phong Nguyễn

INRIA Paris and ENS/PSL

November, 2020

Coppersmith's Theorem (EURO-96)

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

Remarks

- The particular case $P(x) = x^\delta - c$ is easy.
- Hastad (1985) proved the weaker bound $N^{2/[\delta(\delta+1)]}$.
- Corollary: the number of small roots $|x_0| \leq N^{1/\delta}$ is polynomial in $(\log N, \delta)$. This was independently proved by [KonyaginSteger1994].

Generalizations

Finding all small x_0 such that $P(x_0) \equiv 0 \pmod{N}$ is a particular case of:

- GCD (1999 - Many people): find all small $x_0 \in \mathbb{Z}$ such that $\gcd(P(x_0), N)$ is large. This is provable.
- Bivariate Equations over the Integers [Copper-EURO96;Coron-EURO04;BlomerMay-EURO05]: find all small (x_0, y_0) such that $P(x_0, y_0) = 0$. This is provable. Three variables and more are heuristic.
- Multivariate Congruences [Copper-EURO06;BoDu-EURO99;etc.]: find all small (x_0, y_0) such that $P(x_0, y_0) \equiv 0 \pmod{N}$. This is heuristic.

The GCD Generalization (1999 - Many people)

Remember Coppersmith's Theorem

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

The GCD Generalization

- Let $\alpha = r/s \in \mathbb{Q}$ such that $0 \leq \alpha \leq 1$.
- In time polynomial in $(\log N, \log r, \log s, \delta)$, one can compute all integers $|x_0| \leq N^{\alpha^2/\delta}$ such that $\gcd(P(x_0), N) \geq N^{\alpha}$.
- Coppersmith's theorem is the particular case $\alpha = 1$.

Proving Coppersmith's Theorem: A naive approach

Remember Coppersmith's Theorem

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

- Let $P(x) = p_0 + p_1 x + \cdots p_{\delta-1} x^{\delta-1} + x^{\delta}$.
- Let x_0 be such that $P(x_0) \equiv 0 \pmod{N}$
- Is x_0 related to some short vector in some lattice?

Proving Coppersmith's Theorem: A naive approach

Remember Coppersmith's Theorem

- Let $P(x) = p_0 + p_1 x + \cdots p_{\delta-1} x^{\delta-1} + x^\delta$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

- If $P(x_0) \equiv 0 \pmod{N}$, then $\vec{x_0} = (1, x_0, \ldots, {x_0}^\delta)$ belongs to the lattice L orthogonal mod N to $\vec{P} = (p_0, p_1, p_{\delta-1}, 1)$.
- When could $\vec{x_0}$ be a shortest vector of L?
- Do we really need to make $\vec{x_0}$ a shortest vector to find x_0? This is Coppersmith's original idea.
- How can we modify L and $\vec{x_0}$ to improve the bound X?

Proving Coppersmith's Theorem: The dual approach

Remember Coppersmith's Theorem

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

- The case $P(x) = x^\delta - c$ worked because we had a polynomial equation over $\mathbb{Z}$ satisfied by all small roots. And any univariate polynomial equation over $\mathbb{Z}$ can be solved in polynomial time.

Proving Coppersmith's Theorem

Remember Coppersmith's Theorem

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

The Philosophy of the Proof (following [Howgrave97])

- Any sufficiently small integer must be zero. This is how congruences can sometimes be transformed into equations over $\mathbb{Z}$.
- Using lattice reduction, we will find a univariate polynomial equation over $\mathbb{Z}$ satisfied by all the small roots x_0.

From Small Roots to Integer-Valued Polynomials

Remember Coppersmith's Theorem

- Let $P(x)$ be a monic polynomial of degree δ and N an integer of unknown factorization.
- In time polynomial in $(\log N, \delta)$, one can compute all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod{N}$.

Idea 1

- Consider $Q(x) = P(x)/N \in \mathbb{Q}[x]$. If $P(x_0) \equiv 0 \pmod{N}$, then $Q(x_0) \in \mathbb{Z}$.
- Can we make sure that $Q(x_0)$ is actually zero?

"Short" Integer-Valued Polynomials

A Sufficient Condition

- Assume that $|x_0| \leq X$ for some known bound X.
- Write $Q(x) = \sum_{i=0}^{n} q_i x^i$ and let $\|Q(x)\|^2 = \sum_{i=0}^{n} q_i^2$. Then: $Q(x_0) = \sum_{i=0}^{n} (q_i X^i) \cdot (x_0/X)^i$.
- Cauchy-Schwarz:

$$Q(x_0)|^2 \leq \left(\sum_{i=0}^{n} (q_i X^i)^2 \right) \left(\sum_{i=0}^{n} (x_0/X)^{2i} \right) \leq \|Q(xX)\|^2 (n+1).$$

- So if ever $\|Q(xX)\| < 1/\sqrt{1 + \deg Q}$, then $P(x_0) \equiv 0 \pmod{N}$ implies $Q(x_0) = 0$.

To Summarize

- To find all small $|x_0| \leq X$ such that $P(x_0) \equiv 0 \pmod{N}$, it suffices to find $Q(x) \in \mathbb{Q}[x]$ such that:
  - $\|Q(xX)\| < 1/\sqrt{1 + \deg Q}$: a certain norm is small.
  - $Q(x_0) \in \mathbb{Z}$ whenever $P(x_0) \equiv 0 \pmod{N}$.
- What are the possible candidates for such a $Q(x)$?
  - $Q(x) = P(x)/N$.
  - Every polynomial $Q_{u,v}(x) = x^u(P(x)/N)^v$ where $u, v \in \mathbb{N}$.
  - And any integral linear combination of such polynomials!
- In other words, it suffices to find a short vector in a lattice.

An Example with $\delta+1$ Polynomials

- We identify polynomials of degree $\leq \delta$ to vectors in $\mathbb{Q}^{\delta+1}$.
- We build the lattice spanned by the polynomials $Q_{0,0}(xX), Q_{1,0}(xX), \ldots, Q_{\delta-1,0}(xX), Q_{0,1}(xX)$ that is $1, Xx, X^2x^2, \ldots, X^{\delta-1}x^{\delta-1}$ and $P(xX)/N$.

$$L = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & X & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & X^{\delta-1} & 0 \\ ? & \ldots & \ldots & ? & X^{\delta}/N \end{pmatrix}$$

An Example with $\delta + 1$ Polynomials

- The lattice has dimension $\delta + 1$.
- Its volume is $X^{1+2+\cdots+\delta-1} \times X^{\delta}/N = X^{\delta(\delta+1)/2}/N$.
- So using the LLL algorithm, we can find efficiently a non-zero lattice vector shorter than $2^{(\delta)/2}\mathrm{vol}(L)^{1/(\delta+1)} \approx X^{\delta/2}/N^{1/(\delta+1)}$.
- In other words, we can find a non-zero $Q(x) \in \mathbb{Q}[x]$ such that roughly, $\|Q(xX)\| \leq X^{\delta/2}/N^{1/(\delta+1)}$.
- We need $\|Q(xX)\| < 1/\sqrt{\delta+1}$, This will hold if roughly, $X \ll N^{2/[\delta(\delta+1)]}$.
- We've just proved Hastad's 1985 result: we can find all roots $|x_0| \leq N^{2/[\delta(\delta+1)]}$.

The Proof

- More generally, we take $h\delta$ polynomials where h grows to infinity:
- $Q_{0,0}(xX), Q_{1,0}(xX), \ldots, Q_{\delta-1,0}(xX)$,
- $Q_{0,1}(xX), Q_{1,1}(xX), \ldots, Q_{\delta-1,1}(xX)$,
- $\vdots$
- $Q_{0,h}(xX), Q_{1,h}(xX), \ldots, Q_{\delta-1,h}(xX)$.
- The lattice volume is easy to compute. The LLL bound gives a bound X which grows to $N^{1/\delta}/\sqrt{2}$ when h grows to ∞. h should not be too big to ensure polynomial time.
- We thus obtain all integers $|x_0| \leq N^{1/\delta}$ such that $P(x_0) \equiv 0 \pmod N$.

How to Extend to GCDs

- Consider a linear combination $Q(x)$ of the $Q_{u,v}(x) = x^u(P(x)/N)^v$ where $0 \leq v \leq h$.
- If the gcd of $P(x_0)$ with N is $\geq N^\alpha$, then $Q(x_0)$ is a rational number whose denominator is $\leq N^{h(1-\alpha)}$.
- This rational is therefore zero if $< 1/N^{h(1-\alpha)}$.
- This still reduces the problem to finding short lattice vectors, but the proof is more technical.