Cryptographic Applications of Capacity Theory

Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr

Asiacrypt, Dec. 8, 2016

A theorem of Coppersmith

Theorem (Coppersmith)

Suppose $f(x) \in \mathbb{Z}[x]$ is monic of degree d and $N \in \mathbb{Z}$. There is an polynomial time algorithm in $\log N$ and d for finding all $m \in \mathbb{Z}$ for which

$$f(m) \equiv 0 \bmod N \quad \text{and} \quad |m| < N^{1/d}.$$

Main Question: Can one increase $N^{1/d}$ in this theorem to $N^{(1/d)+\epsilon}$ for some $\epsilon > 0$? What if $N = pq$ for two distinct but unknown primes p and q?

Answer: One can't use Coppersmith's method. We prove the required auxiliary functions do not exist.

What sort of auxiliary functions did Coppersmith use?

He used LLL to find a non-zero polynomial in $\mathbb{Q}[x]$ of the form

$$h(x) = \sum_{i,j \geq 0} a_{i,j}\, x^i \left(\frac{f(x)}{N}\right)^j \quad \text{with} \quad a_{i,j} \in \mathbb{Z} \tag{1}$$

such that

$$|h(z)| < 1 \quad \text{for all} \quad z \in \mathbb{C} \quad \text{with} \quad |z| < N^{1/d}. \tag{2}$$

Why h(x) is useful:

Suppose $m \in \mathbb{Z}$, $f(m) \equiv 0 \bmod N$ and $|m| < N^{1/d}$. Then:

$$h(m) \in \mathbb{Z} \quad \text{from (1)} \quad \text{and} \quad |h(m)| < 1 \quad \text{from} \quad (2).$$

So $h(m) = 0$, and one can then find all roots m of $h(x)$ quickly.

Our main theorem

You can't improve on Coppersmith's bounds for univariate polynomials using auxiliary polynomials the way he does.

Theorem

Let $f(x) \in \mathbb{Z}[x]$ be monic of degree d. Suppose $N \in \mathbb{Z}$ and $\epsilon > 0$. There is no non-zero auxiliary polynomial of the form

$$h(x) = \sum_{i,j} a_{i,j}\, x^i \left(\frac{f(x)}{N}\right)^j \quad \text{with} \quad a_{i,j} \in \mathbb{Z}$$

so that $|h(z)| < 1$ for all complex z satisfying $|z| \leq N^{1/d+\epsilon}$.

The main tool: Capacity Theory

Let E be a compact subset of $\mathbb{C}$ closed under complex conjugation. Let

$$F_n = \{p(x) \in \mathbb{R}[x], \deg p(x) \leq n, \sup_{z \in E} |p(z)| < 1\}$$

Then

$$F_n \subseteq \mathbb{R} \oplus \mathbb{R}x \cdots \oplus \mathbb{R}x^n = \mathbb{R}^{n+1}$$

is a convex symmetric subset.

Definition (Sectional capacity of E)

$$\log \gamma(E) = \lim_{n \to \infty} \frac{-2 \log \mathrm{Vol}(F_n)}{n^2}$$

Fekete Szegő Theorems

[Fekete 1923, Szegő 1955]

Theorem

Let E be a compact subset of $\mathbb{C}$ closed under complex conjugation.

- *If $\gamma(E) < 1$, there is a non-zero polynomial $h(z) \in \mathbb{Z}[x]$ such that $|h(z)| < 1$ for all $z \in E$.*
- *If $\gamma(E) > 1$, no such $h(z)$ exists.*

Application

Theorem

- *If $\gamma(E) < 1$, then there are finitely many irreducible monic polynomials with integer coefficients with all roots in E.*
- *If $\gamma(E) > 1$, then for every open neighborhood U of E, there are infinitely many irreducible monic polynomials with integer coefficients with all roots lying in U.*

Sketch of the first half of the Fekete-Szegö Theorem

Suppose $\gamma(E) < 1$. Let

$$L_n = \mathbb{Z} \oplus \mathbb{Z}x \cdots \oplus \mathbb{Z}x^n \subset \mathbb{R}^{n+1}$$

Minkowski's theorem There will be a non-zero $h(x)$ in $F_n \cap L_n$ once $\mathrm{Vol}(F_n) > 2^{n+1}\,\mathrm{Vol}(\mathbb{R}^n/L_n) = 2^{n+1}$.

Computation of volume growth as $n \to \infty$:

$$\log \mathrm{Vol}(F_n) \approx (-n^2/2) \log \gamma(E)$$

If $\gamma(E) < 1$ then $-\log \gamma(E) > 0$ so for large n:

$$\log \mathrm{Vol}(F_n) \approx (n^2/2)(-\log \gamma(E)) > (n+1)\log 2$$

So $\mathrm{Vol}(F_n) > 2^{n+1}$ for large n and Minkowski's theorem applies.

Linking capacity theory and Coppersmith's method

- In the Fekete-Szegö theorem, one starts with a compact $E \subseteq \mathbb{C}$ compact, stable under complex conjugation. One then asks:

  When does there exist a non-zero $h(x) \in \mathbb{Z}[x] - \{0\}$ so that $|h(z)| < 1$ if $z \in E$?

- For Coppersmith's theorem, we are looking for a non-zero auxiliary polynomial in $\mathbb{Q}[x]$ of the form

$$h(x) = \sum_{i,j} c_{i,j} x^i \left(\frac{f(x)}{N}\right)^j, \qquad a_{i,j} \in \mathbb{Z} \tag{3}$$

  satisfying $|h(z)| < 1$ for $z \in \mathbb{C}$ with $|z| < T$ when $T = N^{1/d}$.

  This looks a lot like the capacity theory we were talking about, except $h(x)$ might not be in $\mathbb{Z}[x]$.

  But we know (3) implies that if z and $f(z)/N$ are algebraic integers then $h(z)$ is an algebraic integer.

New Problem

When is there a non-zero $h(x) \in \mathbb{Q}[x]$ so that

1. $|h(z)| < 1$ if $z \in E \subseteq \mathbb{C}$
2. $h(z)$ is an algebraic integer for all algebraic integers z satisfying $f(z) \equiv 0 \bmod N$ in the ring of all algebraic integers.

Cantor and Rumely's enhanced capacity theory

Suppose E_p is a subset of $\overline{\mathbb{Q}}_p$ for each prime p, and that E_∞ is a subset of $\mathbb{C}$. If these satisfy the appropriate hypotheses, one can define a capacity

$$\gamma(\mathbb{E}) = \gamma_\infty(E_\infty) \cdot \prod_p \gamma_p(E_p)$$

associated to $\mathbb{E} = \prod_p E_p \times E_\infty$ for which the following is true:

Theorem (Cantor)

- *If* $\gamma(\mathbb{E}) < 1$ *then there exists a nonzero polynomial* $h(x) \in \mathbb{Q}[x]$ *satisfying*

  $$|h(z)|_p \leq 1 \, \forall p \text{ and } z \in E_p \quad \textit{and} \quad |h(z)|_\infty < 1 \text{ for } z \in E_\infty.$$

- *If* $\gamma(\mathbb{E}) > 1$ *then no such polynomial exists.*

Now we let:

$$E_p = f^{-1}\left(\{z \mid |z|_p \le |N|_p\}\right) \quad \text{and} \quad E_\infty = \{z \in \mathbb{C} \mid |z| \le T\}$$

With these choices, a polynomial $h(x) \in \mathbb{Q}[x]$ has the above properties if and only if:

1. For all algebraic integers z for which $f(z) \equiv 0 \bmod N$ in the ring of algebraic integers, $h(z)$ is an algebraic integer.
2. For all complex z with $|z| \le T$ one has $|h(z)| < 1$.

One now computes, using Rumely and Cantor's formulas, that

$$\gamma(\mathbb{E}) = TN^{-1/d}.$$

Then $\gamma(\mathbb{E}) < 1$ is equivalent to

$$T < N^{1/d}$$

and this is why Coppersmith's method cannot be improved!

Lattices of binomial polynomials

Definition (Binomial polynomial)

$$b_i(x) = \binom{x}{i} = x \cdot (x-1) \ldots (x-i+1)/i!$$

$b_i(z) \in \mathbb{Z}$ for any $z \in \mathbb{Z}$.

Theorem (Polya)

$h(x) \in \mathbb{Q}[x]$ and $h(z) \in \mathbb{Z}$ for all $z \in \mathbb{Z}$ $\iff$ $h(x)$ is a integer combination of binomial polynomials $b_i(x)$.

Coppersmith asked if one could improve the theorem using binomial polynomials:

$$h(x) = \sum_{i,j \geq 0} a_{i,j} b_i(x) b_j(\frac{f(x)}{N})$$

These no longer have the property that $h(z)$ is an algebraic integer whenever both z and $f(z)/N$ are.

Binomial polynomials don't help

Theorem

Let $\epsilon > 0$ *and* M *a positive integer,* $319 \leq M \leq 1.48774 N^{\epsilon}$.
If there is a nonzero polynomial

$$h(x) = \sum_{0 \leq i,j \leq M} a_{i,j} b_i(x) b_j(\frac{f(x)}{N})$$

with $a_{i,j} \in \mathbb{Z}$ *such that*

$$|h(z)| < 1 \text{ for } z \in \{z \in \mathbb{C} \mid |z| \leq N^{1/d+\epsilon}\}$$

then N *must have a prime factor less than* M*.*

Moral: If N does not already have a very small prime factor, any auxiliary polynomial $h(x)$ constructed from binomial polynomials would have to be of too large a degree to be useful for an algorithm that runs in polynomial time in $\ln(N)$.

Summary

Cryptographic applications of capacity theory: On the optimality of Coppersmith's method for univariate polynomials
Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr
`http://arxiv.org/abs/1605.08065`

- If you want to improve univariate Coppersmith theorem, you will need to use a new method.
- New links between capacity theory and cryptography.

Current and Future Work

- The same approach shows you can't improve the exponent $1/4$ in Coppersmith's proof that if $N = pq$ and the larger of the primes p and q is known to within $N^{1/4}$ then one can find p and q quickly.
- Bivariate polynomials.
- Solving equations modulo divisors.
- Multivariate polynomials.