Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding

Nadia Heninger and Henry Cohn

Princeton University

Microsoft Research New England

January 8, 2011

A cryptographer's fairy tale...

Once upon a time there was a princess who ruled a land far, far away.

And that princess would receive updates from her military commanders encrypted using her 2048-bit RSA key.

As the enemy army approached, she decided to protect her private key.

She wrote half of it on one scroll and sent it with a horseman riding west, and wrote the other half on another scroll and sent it with a horseman riding east.

However, one of these men was apprehended by the enemy.

Is her key safe?

The key recovery problem.

A simplified version, without details of RSA.

The princess's public key is known to the enemy, with

$$N = pq.$$

p and q are secret, the princess keeps p as her private key.

The west horseman has the most significant half of p, the east has the least significant half.

$$p_w \cdot 2^{512} + p_e = p$$

Given N and p_w, can p_e be found?

The key recovery problem, continued.

In our application, let

$$f(x) = p_w \cdot 2^{512} + x \qquad \text{so} \qquad f(p_e) \equiv 0 \bmod p$$

Theorem (Coppersmith)

Given $f(x) = x^d + \cdots + f_0$, N an integer, can find all x_0 such that

$$f(x_0) \equiv 0 \bmod N$$

$$|x_0| \leq N^{1/d}$$

in time polynomial in $\log N$ *and* d *without factoring* N.

The key recovery problem, continued.

In our application, let

$$f(x) = p_w \cdot 2^{512} + x \qquad \text{so} \qquad f(p_e) \equiv 0 \bmod p$$

Theorem (Coppersmith/Howgrave-Graham)

Given $f(x) = x^d + \cdots + f_0$, N an integer, can find all x_0 such that

$$f(x_0) \equiv 0 \bmod B \qquad \gcd(B, N) \geq N^{\beta}$$

$$|x_0| \leq N^{\beta^2/d}$$

in time polynomial in $\log N$ *and* d *without factoring* N.

Coppersmith's theorem, proof outline.

Theorem (Coppersmith/Howgrave-Graham)

Given $f(x) = x^d + \cdots + f_0$, N *an integer, can find all* x_0 *such that*

$$\gcd(f(x_0), N) \geq N^\beta \qquad |x_0| \leq N^{\beta^2/d}$$

Proof outline.

1. Create a new polynomial $Q(x)$ so that
   all desired x_0 are roots of Q over $\mathbb{Z}$.

2. Factor Q to find roots.

Proof outline, continued.

1. Ensure any root of f mod B is a root of Q mod B^k:

   Q will be linear combination of $f(x)^i N^{k-i}$.

2. Bound coeffs of Q and $|x_0|$ to bound $|Q(x_0)|$.

   If $|Q(x_0)| < B^k$, then x_0 is a root of Q over $\mathbb{Z}$.

   (Thus we can forget N and B and just factor Q.)

3. How to find Q with small coeffs?

   Lattice basis reduction.

   (LLL's approximation factor only translates into a constant here.)

Analogy between $\mathbb{Z}$ and $\mathbb{F}[z]$.

There is a well-known mathematical analogy between integers and polynomials.

ring of integers	**ring of polynomials (with coeffs in a field)**
primes	**irreducible polynomials**
absolute value	**degree of polynomial**

Things work the way you want them to:

division, unique factorization, GCDs, Chinese remaindering...

lattice over $\mathbb{Z}$	**$\mathbb{F}[z]$-module**

The theorem we just proved is over the integers.

Let's translate the theorem to polynomials!

A polynomial version of Coppersmith's theorem.

Theorem (for integers)

Given

$f(x) = x^d + \cdots + f_0$

with coefficients in $\mathbb{Z}$,

N *an integer,*

can find all

x_0

such that

$\gcd(f(x_0), N) \geq N^\beta$

$|x_0| \leq N^{\beta^2/d}$

Theorem (for polynomials)

Given

$f(x) = x^d + \cdots + f_0(z)$

with coefficients in $\mathbb{F}[z]$,

$N(z)$ *of degree* n,

can find all

$g(z)$

such that

$\deg \gcd(f(g(z)), N(z)) \geq n\beta$

$\deg g(z) \leq n\beta^2/d$

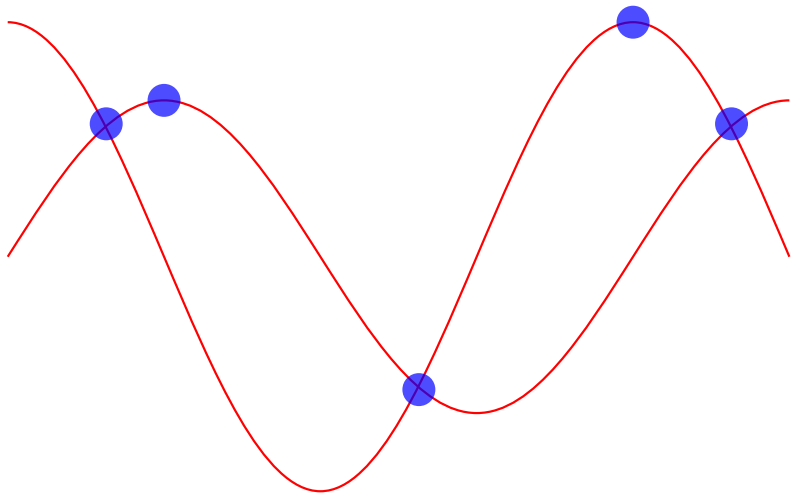
Reed-Solomon list decoding

Input: $\{(x_1, y_1), \ldots, (x_n, y_n)\}$

Problem: Find all polynomials g of degree less than ℓ such that

$$g(x_i) = y_i$$

for at least $n - e$ pairs.



Theorem (Guruswami-Sudan)

There is an efficient algorithm to do so for $e < n - \sqrt{n\ell}$.

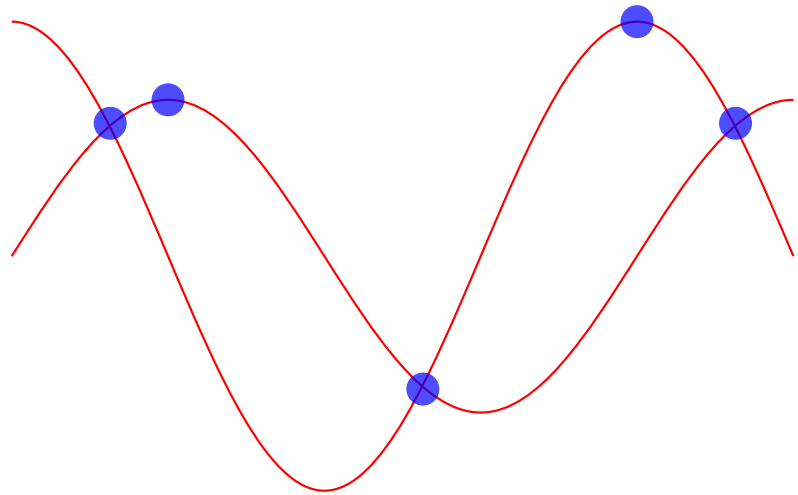
Reed-Solomon list decoding

Input: $\{(x_1, y_1), \ldots, (x_n, y_n)\}$

Problem: Find all polynomials g of degree less than ℓ such that

$$g(x_i) = y_i$$

for at least $n - e$ pairs.



$$g(x_i) = y_i \qquad \longleftrightarrow \qquad g(x) \equiv y_i \bmod (x - x_i).$$

Set $f(x, y)$ s.t. $f(x_i, y_i) = 0$ and $N(x) = \prod(x - x_i)$.

$$\beta = (n - e)/n.$$

Check proof for polynomial theorem.

1. Create a new polynomial $Q(x)$ (with coeffs in $\mathbb{F}[z]$).

   $Q(x)$ will be linear combination of $f(x)^i N(z)^{k-i}$.

2. Bound degree of coeffs of $Q(x)$ and $g(z)$ to bound $Q(g(z))$.

   If $\deg Q(g(z)) < k \deg B(z)$, then $g(z)$ is a root of $Q(x)$.

3. How to find $Q(x)$ with low-degree coeffs?

   Lattice basis reduction.

   For non-Archimedean absolute values we can find an exact shortest vector in polynomial time.

Algebraic-geometric codes.

Natural generalization of Reed-Solomon codes to polynomials defined on a curve in several dimensions.

- (polynomials in several vars, mod out by eqns defining curve)
- e.g., x, y satisfying $y^2 = x^3 - x$ (an elliptic curve)

AG codes beat the Gilbert-Varshamov bound.

All the machinery from the one-variable case generalizes.

A few twists: many absolute values, we must bound them all.

Recover Shokrollahi-Wasserman and Guruswami-Sudan results on list decoding.

Extends naturally to AG codes defined by multipoint divisors.

Number fields.

AG codes come from
function fields.

(finite extensions of the field of rational functions in one variable)

What about
number fields?

(finite extensions of the field $\mathbb{Q}$ of rational numbers, e.g., $\mathbb{Q}(\sqrt{5})$)

This case completes the analogy.

Find small roots of polynomials modulo ideals in the ring of integers in a number field.

What does "small" mean? Again several absolute values to bound.

Apply LLL to the canonical embedding of our ideal.
This has also come up recent in lattice-based cryptography
[Peikert Rosen], [Lyubashevsky Peikert Regev].

Running time is exponential in the degree of the number field.

Summary

Show how to extend Coppersmith's theorem to:

1. Polynomials, where it becomes list-decoding of Reed-Solomon codes.
2. Function fields, where it becomes list-decoding of algebraic-geometric codes.
3. Number fields, where it gives solutions to polynomials modulo ideals in a number field.

What's the big picture? Powerful analogies.

What about our princess?

Her enemies used lattice basis reduction to efficiently recover her private key from half the bits and discover her military secrets.

She didn't live happily ever after.

Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding

Nadia Heninger and Henry Cohn

Princeton University

Microsoft Research New England

January 8, 2011

The end.