Capacity Theory and Cryptography

Ted Chinburg
joint work with Brett Hemenway,
Nadia Heninger and Zach Scherr

U.C. Irvine, Sept. 3, 2015

A classical result

Theorem: (*Coppersmith 1995*) If one knows a factor $p \geq N^{1/2}$ of N to within an error bounded by $N^{1/4}$, one can find p exactly in polynomial time.

The method: Use LLL to produce quickly a rational function $h(x) \in \mathbb{Q}(x)$ which must have p as a root. The constraints on $h(x)$ which are used to force this are on the next slide.

Capacity theory: Work of FSCR = (Fekete, Szëgo, Cantor, Rumely) and others leads to systematic way to decide whether there are $h(x)$ satisfying these constraints.

One implication: One cannot use such $h(x)$ to improve $N^{1/4}$ to N^{β} for any $\beta > 1/4$.

Rational functions which constrain factors of N

Given: An integer N and an approximation $\tilde{p}$ to a divisor of N.

Goal: For a given $\epsilon > 0$, determine if there is a factor $p|N$ so

$$|p - \tilde{p}| < N^{\epsilon}.$$

We might as well assume $\tilde{p} \geq N^{1/2}$.

Let $\overline{\mathbb{Z}} =$ the ring of all algebraic integers.

Idea: Try to find a non-zero $h(x) = h_\epsilon(x) \in \mathbb{Q}(x)$ such that:

(1) $h(P) \in \overline{\mathbb{Z}}$ whenever $N = PQ$ and $P, Q \in \overline{\mathbb{Z}}$.

(2) $|h(t)| < 1$ if $t \in \mathbb{R}$ and $|\tilde{p} - t| \leq N^\epsilon$.

One would like to find $h(x)$ in polynomial time (depending on ϵ).

Then: If $p|N$ in $\mathbb{Z}$ and $|\tilde{p} - p| \leq N^\epsilon$ then

$$h(p) \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z} \quad \text{and} \quad |h(p)| < 1$$

so $h(p) = 0$. We can find roots of $h(x)$ quickly, and one is p.

Why $N^{1/4}$ is optimal

D. Cantor's capacity theory on the projective line $\mathbb{P}^1$ implies:

Theorem There is a function $N(\epsilon)$ so that for $N > N(\epsilon)$ the following is true:

(A) If $\epsilon < 1/4$ there is a rational function $h_\epsilon(x) \in \mathbb{Q}(x)$ satisfying both of the constraints (1) and (2).

(B) If $\epsilon > 1/4$, no such $h_\epsilon(x)$ exists when $\tilde{p} = N^{1/2}$. So one cannot use this method to find p in this case if $\epsilon > 1/4$.

Facts:

(1) If $\tilde{p} = N^\lambda$ for some $1/2 \leq \lambda < 1$ then one can make an $h_\epsilon(x)$ for all $\epsilon < \lambda/2$.

(2) In case (A) one can find an $h_\epsilon(x)$ quickly using LLL. More on this later.

Capacity theory and divisors of N

Heuristic: Auxiliary functions provide a 'magnifying glass' for detecting divisors of N which lie in particular subsets of $[0, N]$ and/or satisfy congruence constraints.

Questions:

(1) (Existence) Given a set of constraints on divisors, when does there exist an auxiliary $h(x)$ (the magnifying glass) which will work?

(2) (Algorithms) When one exists, can it be found quickly?

Classical capacity theory gives a very nice answer to (1) for a very wide class of constraints. When $h(x)$ exists, one can show this by a Minkowski argument.

To deal with (2), one needs to convert the Minkowski existence proof to the problem of finding a small vector in a lattice. This amounts to showing a certain convex symmetric body is closely approximated by a generalized ellipsoid.

A jargon-free cartoon of how capacity theory works

Suppose we want to know if there is a polynomial $0 \neq h(x) \in \mathbb{Z}[x]$ which has sup norm less than 1 on an interval $[a, b]$ on the real line.

One approach is to consider:

$V_n =$ the real vector space of all $m(x) \in \mathbb{R}[x]$ of degree $\leq n$.

$L_n =$ the lattice of $h(x) \in V_n \cap \mathbb{Z}[x]$.

$C_n =$ the convex symmetric subset of all $m(x) \in V_n$ with

$$\sup\{|m(x)| : x \in [a, b]\} < 1.$$

Minkowski: If $\mathrm{Vol}(C_n) \geq 2^n \mathrm{covol}(V_n/L_n)$ then there is a non-zero $h(x) \in C_n \cap L_n$ of the kind we seek.

Capacity theory computes $\mathrm{Vol}(C_n)$ asymptotically as $n \to \infty$ in this and much more general contexts.

A deeper theorem

In the above context, Fekete and Szegö proved that if $\mathrm{Vol}(C_n)$ has an asymptotic growth rate that is too small (by a natural margin) for the above Minkowski argument to produce an $h(x)$, then in fact no such $h(x)$ can exist.

They did this by producing infinitely many algebraic integers α which have all their conjugates in $[a, b]$. These α are roots of some other special 'oscillating' polynomials constructed first with real coefficients via potential theory and then corrected to have integer coefficients.

If the $h(x)$ we were looking for existed, it would have all of these α as roots, and this is not possible.

Cantor and Rumely's work

Cantor and Rumely generalized all of this to rational functions $h(x)$ on algebraic curves over global fields.

They considered $h(x)$ which have all their poles in a prescribed set, and which have bounded absolute values on prescribed subsets of the complex and v-adic points of the curve. Here v ranges over all finite places of the global field over which the curve is defined.

In the classical case, the curve is the projective line $\mathbb{P}^1$ over $\mathbb{Q}$, and the only poles are at infinity (so one is talking about polynomials).

A subtlety in the theory has to do with the pole orders of $h(x)$. Cantor and Rumely used game theory to define a number, the capacity, which determines whether or not one can succeed in constructing an $h(x)$ of the above kind.

Crypto-capacity theory

When the Minkowski argument says an $h(x)$ must exist, the question capacity has not addressed until now is how hard it is to construct.

Following Coppersmith et al, one would like to use LLL to construct $h(x)$ quickly.

Suppose in the example of polynomials with sup norm less than 1 on $[a, b]$, the convex symmetric set C_n miraculously turned out to be a sphere. Then finding a point of $C_n \cap L_n$ amounts to finding an element of the lattice L_n which has (close to) minimal length. Now use LLL!

In general, if C_n is close enough to an ellipsoid, relative to some choice of basis for V_n, then one can reduce the problem to finding a close-to-minimal length vector in L_n relative to a suitable positive definite inner product. This step is non-trivial, and puts additional conditions on the kinds of conditions one can impose on $h(x)$.

Some other problems to which capacity theory applies

Small solutions of congruences
Input:

$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0$ in $\mathbb{Z}[x]$ and $N \geq 1$

Theorem: (*Coppersmith, 1996*) One can find all $r \in \mathbb{Z}$ such that

$$(*) \quad |r| \leq N^{1/d} \quad \text{and} \quad f(r) \equiv 0 \mod N$$

in polynomial time.

Point: One can find small solutions of polynomial congruences quickly.

Method: Construct $0 \neq h(x) \in \mathbb{Q}[x]$ using LLL so $h(r) = 0$.

Theme: Capacity theory predicts when such $h(x)$ exist and explains why $1/d$ is optimal.

Bivariate polynomials

Input: $f(x,y) = \sum_{0 \leq i,j \leq d} c_{i,j} x^i y^j$ in $\mathbb{Z}[x,y]$, irreducible.

Bounds X and Y on $|x|$ and $|y|$, respectively.

Set $W = \max_{i,j} |c_{i,j}| X^i Y^j$

Theorem: (*Coppersmith 1996*) One can find in polynomial time all $(x_0, y_0) \in \mathbb{Z}^2$ such that $f(x_0, y_0) = 0$ and $|x_0| \leq X$ and $|y_0| \leq Y$ provided that $XY \leq W^{\frac{3}{2d}}$.

Point: One can find small integral points on plane curves quickly.

Optimize this: Rumely's capacity theory on curves can determine whether there are auxiliary rational functions of the kind Coppersmith uses that must vanish on small integral points.

Unknown: Is the Theorem optimal?

The future?

A rational function $h(x)$ on a curve C gives a finite flat map $C \to \mathbb{P}^1$.

In higher dimensions, Chinburg, Moret-Bailly, Pappas and Taylor have been considering a new capacity theory based on considering finite flat maps from an m-dimensional variety X to $\mathbb{P}^m$.

This has application to the following "common g.c.d." problem. Suppose we are given an integer N and integer approximations $a_1, \ldots, a_m$ to divisors $d_1, \ldots, d_m$ of N with a large g.c.d.. In other words, there are "small" integers $r_1, \ldots, r_m$ with $d_i = (a_i + r_i) | N$ and

$$gcd(N, a_1 + r_1, \ldots, a_m + r_m) \geq N^{\beta}$$

for some $0 < \beta < 1$. Heninger has experimental results on finding such $r = (r_1, \ldots, r_m)$ when

$$|r_i| < N^{(1+o(1))\beta^{m+1}/m} \quad \text{and} \quad \beta >> \frac{1}{\sqrt{\ln(N)}}$$

Warning: This slide rated NT-13

To apply higher dimensional capacity theory to this problem, one lets $X = \mathbb{P}^m$ over $\mathbb{Q}$ and one lets D be the hyperplane at infinity. Let $\mathbb{A}^m = \mathbb{P}^m - D$.

One considers adelic sets

$$\mathbb{E} = \prod_v E_v \subset \prod_v \mathbb{A}^m(\overline{\mathbb{Q}}_v)$$

where v runs over all places of $\mathbb{Q}$. If v is finite, E_v is the annulus of $(r_1, \ldots, r_m) \in \mathbb{A}^m(\overline{\mathbb{Q}}_v)$ with $|N|_v \leq |a_i + r_i|_v \leq 1$. If v is the infinite place, E_v is the polydisc of $(r_1, \ldots, r_m) \in \mathbb{A}^m(\overline{\mathbb{Q}}_v)$ with $|r_i|_v < N^\epsilon$.

Effectively constructed finite flat maps $h : X \to \mathbb{P}^m$ which send such $\mathbb{E}$ to polydiscs of generalized radius less than 1 must send $r = (r_1, \ldots, r_m)$ as above to $(0, \ldots, 0)$. The determination of all such r then comes down to finding the fiber of such h over $(0, \ldots, 0)$.

Summary

Suppose you have a number theoretic or cryptographic problem in which auxiliary rational functions are used to find solutions.

1. Capacity theory is a technique for determining whether or not such rational functions exist.

2. Capacity theory is also useful for setting up an LLL search for such rational functions. On curves, it predicts the spaces of functions to use and which kinds of generalized ellipsoids to construct in order to convert the problem to that of finding a short vector in a lattice.

Sectional capacity theory. (These slides rated NT-XXX)

$K =$ global field, $v \in M(K) =$ places of K, $K_v \subset \overline{K}_v$.

X/K projective normal connected variety, dimension δ.

$D =$ effective ample divisor on X. An adelic set is $\mathbb{E} = \prod_{v \in M(K)} E_v$ where

$E_v \subset X(\overline{K}_v)$ is stable under $\mathrm{Gal}(\overline{K}_v/K_v)$

E_v is bounded away from $D(\overline{K}_v)$ in the v-adic metric from a projective embedding of X.

For almost all finite v, E_v is the set of $z \in X(\overline{K}_v)$ which don't reduce mod v to the reduction of a point of $D(\overline{K}_v)$.

Sectional Capacity: $0 \leq S(\mathbb{E}, D) \in \mathbb{R}$.
Main Property: $S(\mathbb{E}, D) < 1$ implies $\exists$ a rational function $h(x) \in K(X)$ on X regular off D so $\forall v \in M(K), \forall x \in E_v$ one has $|h(x)|_v \leq 1$, with $|h(x)|_v < 1$ if v is archimedean.

The idea behind sectional capacity

We are given X, D and $\mathbb{E} = \prod_{v \in M(K)} E_v$ as before.

Sectional capacity measures the rate of growth with n

of the volume of the adelic functions on X with two properties:

(1) They have poles no worse than nD, and

(2) They have v-adic sup norm ≤ 1 on E_v for all v.

Point: If this rate of growth with n is large, an adelic Minkowski argument shows there is a global function $h(x) \in K(X)$ for which (1) and (2) hold for some n.

Details of how to define sectional capacity

Given X, D and $\mathbb{E} = \prod_{v \in M(K)} E_v$ as before.

For $1 \leq n \in \mathbb{Z}$ let $H^0(nD) = H^0(X, O_X(nD)) \subset K(X)$

Example: $X = P^1_{\mathbb{Q}}$ and $D = \{\infty\}$. Then
$H^0(nD) = \{h(x) = b_0 + b_1 x + \cdots b_n x^n : b_i \in \mathbb{Q}\}$

Let $F_n(E_v)$ be the set of $h_v \in H^0(nD)_v = K_v \otimes_F H^0(nD)$ such that $|h_v(x)|_v \leq 1$ (resp. $|h_v(x)|_v < 1$) if $x \in E_v$ if v is non-archimedean (reps. if v is archimedean).

Let $\mathbb{A}_K = \prod'_{v \in M(K)} K_v$ be the adeles of K.

Choose any Haar measure ψ on $H^0(nD)_{\mathbb{A}} = \mathbb{A}_K \otimes_K H^0(nD)$. Then $H^0(nD)$ is a discrete subset of $H^0(nD)_{\mathbb{A}}$ with finite covolume $\psi(H^0(nD)_{\mathbb{A}}/H^0(nD)))$ with respect to ψ

Example: In the $\mathbb{P}^1$ case, $\mathbb{A}_{\mathbb{Q}}$ is the set of $\alpha = \prod_v \alpha_v \in \prod_v \mathbb{Q}_v$ such that $\alpha_v \in \mathbb{Z}_v$ for all but finitely many non-archimedean v. We have $H^0(nD)_{\mathbb{A}} = \prod'_v H^0(nD)_v$. A natural choice for ψ is $\prod_v \psi_v$ where
(i) for finite v, ψ_v is the Haar measure on the polynomials $H^0(nD)_v$ in x of degree $\leq n$ with coefficients in $\mathbb{Q}_v$ which gives the polynomials with coefficients in $\mathbb{Z}_v$ volume 1;
(ii) if v is the infinite place, the polynomials with integral coefficients have covolume 1 inside the space $H^0(nD)_v$ of real polynomials of degree $\leq n$.
Exercise: $\psi(H^0(nD)_{\mathbb{A}}/H^0(nD))) = 1$ in the $\mathbb{P}^1$ case.

Back to the general case!
Define

$$F_n(\mathbb{E}) = H^0(nD)_{\mathbb{A}} \cap \prod_{v \in M(K)} F_n(E_v).$$

$$\lambda_n(\mathbb{E}, D) = \frac{\psi(F_n(\mathbb{E}))}{\psi(H^0(nD)_{\mathbb{A}}/H^0(nD)))}.$$

The sectional capacity $S(\mathbb{E}, D) \geq 0$ of $\mathbb{E}$ with respect to D is defined by

$$\ln(S(\mathbb{E}, D)) = -\lim_{n \to \infty} n^{-(\delta+1)}(\delta + 1)! \ln(\lambda_n(\mathbb{E}, D)).$$

where $\delta = \dim(X)$.

Point: $S(\mathbb{E}, D) < 1$ means the volume of $F_n(\mathbb{E})$ grows quickly with n.

Sectional capacity supported on a divisor

We are interested in constructing global functions on X which are regular off of D and which have bounded sup norms on all the E_v.

To do this, we can replace D by any divisor D' in the set $T(D)$ of all divisors with the same support as D. Let $|D'| > 0$ be the δ-fold self intersection number of D'.

Define $S_\gamma(\mathbb{E}, \mathrm{supp}(D))$ to be the infimum of

$$S_\gamma(\mathbb{U}, X_1')^{|X_1'|^{-(\delta+1)/\delta}}$$

over all open adelic neighborhoods $\mathbb{U}$ of $\mathbb{E}$ and over all $D' \in T(D)$.

Fekete Szego Theorems

We will say that a function $h(x) \in F(X)$ is $(\mathbb{E}, D)$ bounded

if it is regular off of D and if it its v-adic sup norm on E_v is ≤ 1

(resp < 1) if v is non-archimedean (reap. if v is non-archimedean).

Theorem: (*Fekete-Szego 1920's, Cantor 1981, Rumely 1989*)
Suppose $\delta = \dim(X) = 1$ so that X is a curve.

(1) If $S(\mathbb{E}, \mathrm{supp}(D)) < 1$ there is a $(\mathbb{E}, D)$ bounded function.

(2) If $S(\mathbb{E}, \mathrm{supp}(D)) > 1$, there is no such function.

Theorem: (*Chinburg 1991; Rumely, Lau and Varley 2000*) For X of any dimension if $S(\mathbb{E}, \mathrm{supp}(D)) < 1$ then there is $(\mathbb{E}, D)$ bounded function.

Conjecture: (*Chinburg, Moret-Bailly, Pappas, Taylor 2013*) For X of any dimension, if $S(\mathbb{E}, \mathrm{supp}(D)) > 1$ then there is no $(\mathbb{E}, D)$ bounded function.