# CSE291-14: The Number Field Sieve

https://cseweb.ucsd.edu/classes/wi22/cse291-14

Emmanuel Thomé

January 25, 2022

# Part 3d

## NFS: a quick analysis

Tools

Parameters

First order

Second order

Summary

# Motivation

- NFS has many parameters.
- The asymptotic analysis can be a rough guide... asymptotically.
  It is not wise to take these values as granted for a practical computation.

We will (probably) come back to the complexity analysis of NFS in March.

Goal today: do the analysis, just to fix ideas.

# Plan

Tools

Parameters

First order

Second order

Summary

# The $L$ function

The following notation is attributed to R. Schroeppel.

$$L_x[a, \alpha] = \exp\left(\alpha(\log x)^a(\log\log x)^{1-a}\right).$$

## CEP with the $L$ function

A random integer $n \leq L_x[a, \alpha]$ is $L_x[b, \beta]$-smooth with probability:

$$L_x\left[a - b, -\frac{\alpha}{\beta}(a - b)(1 + o(1))\right].$$

This formulation is very important for analyzing sieve algorithms.

# Calculus with $L_x[a,\alpha] = \exp\left(\alpha(\log x)^a(\log\log x)^{1-a}\right).$

## Basic formulae with $L$

$$L_x[a,\alpha] \times L_x[b,\beta] = \begin{cases} L_x[a,\alpha+o(1)] & \text{if } a > b, \\ L_x[b,\beta+o(1)] & \text{if } b > a, \\ L_x[a,\alpha+\beta] & \text{if } a = b. \end{cases}$$

$$L_x[a,\alpha] + L_x[b,\beta] = \begin{cases} L_x[a,\alpha+o(1)] & \text{if } a > b, \\ L_x[b,\beta+o(1)] & \text{if } b > a, \\ L_x[a,\max(\alpha,\beta)] & \text{if } a = b. \end{cases}$$

$$L_x[b,\beta]^{\log_{\log x} L_x[a,\alpha]} = L_x[a+b,\alpha\beta].$$

$$L_{L_x[b,\beta]}[a,\alpha] = L_x[ab,\alpha\beta^a b^{1-a} + o(1)].$$

$$\log_{\log x} L_x[a,\alpha] \cdot \log_{\log x} L_x[-a,1/\alpha] = 1.$$

# Plan

Tools

Parameters

First order

Second order

Summary

# Many parameters

Three main parameters.

- The degree $d$ of the polynomial $f$.
- The smoothness bound: $B = L_N[b, \beta]$.
- The bound on $a$ and $b$ in $a - b\alpha$: $A = L_N[a, \alpha]$.

Caveat: obvious notation clashes!

# Many parameters

Three main parameters.

- The degree $d$ of the polynomial $f$.
- The smoothness bound: $B = L_N[b, \beta]$.
- The bound on the coefficients of $\phi(x)$: $A = L_N[a, \alpha]$.

# Convenient form for $d$

The simplistic base-$m$ polynomial selection works for arbitrary $N$.

- Set $m = \lceil N^{1/(d+1)} \rceil$.
- Write $N$ in base $m$: $N = \sum_{i=0}^{d} f_i m^i$ where $0 \leq f_i < m$.
- Set $f = \sum_{i=0}^{d} f_i x^i$. (not monic!)

It will be convenient to choose $d$ so that $N^{1/(d+1)}$ has a nice expression.

Asymptotically, we expect that $d$ grows to $\infty$ as $N \to \infty$, so $N^{1/(d+1)} = \left(N^{1/d}\right)^{1+o(1)}$.

## Use $L$ notation

We have $N = L_N[1, 1]$, so let us take $d = \log_{\log N} L_N[D, \delta]$.
This yields $m = L_N[1 - D, 1/\delta \cdot (1 + o(1))]$.

# Checklist

- $d = \deg f = \log_{\log N} L_N[D, \delta]$.
- The smoothness bound: $B = L_N[b, \beta]$.
- The bound on the coefficients of $\phi(x)$: $A = L_N[a, \alpha]$.
- This yields $m = L_N[1 - D, 1/\delta \cdot (1 + o(1)]$.

Next step: how large are $a - bm$ and $\mathrm{Norm}(a - b\alpha)$?

# Checklist

- $d = \deg f = \log_{\log N} L_N[D, \delta]$.
- The smoothness bound: $B = L_N[b, \beta]$.
- The bound on the coefficients of $\phi(x)$: $A = L_N[a, \alpha]$.
- This yields $m = L_N[1 - D, 1/\delta \cdot (1 + o(1)]$.

~~Next step: how large are $a - bm$ and $\mathrm{Norm}(a - b\alpha)$?~~
Next step: how large are $\mathrm{Res}(\phi(x), x - m)$ and $\mathrm{Res}(\phi(x), f(x))$?

# How large is $|a - bm| = |\operatorname{Res}(\phi(x), x - m)|$?

The coefficients of $\phi(x)$ are at most $A = L_N[a, \alpha]$.

We have $|\operatorname{Res}(\phi(x), x - m)| = O(Am)$.

## $|\operatorname{Res}(\phi(x), x - m)|$

| condition | $\lvert\operatorname{Res}(\phi(x), x - m)\rvert$ |
|---|---|
| $a < 1 - D$ | $m^{1+o(1)} = L_N[1 - D, 1/\delta \cdot (1 + o(1))]$ |
| $a = 1 - D$ | $L_N[1 - D, (\alpha + 1/\delta) \cdot (1 + o(1))]$. |
| $a > 1 - D$ | $L_N[a, \alpha \cdot (1 + o(1))]$. |

# How large is $|\mathrm{Res}(\phi(x), f(x))|$?

The coefficients of $\phi(x)$ are at most $A = L_N[a, \alpha]$.

We have:

$$\mathrm{Res}(u - vx, f(x)) = f_d u^d + f_{d-1} u^{d-1} v + \cdots + f_0 v^d.$$

- All summands have the same size: $\approx m \cdot A^d$.
  Note: $A^d = L_N[a + D, \alpha\delta]$.
- The degree-dependent multiplication has negligible impact.
- FYI, more general formula: $\approx C \times \|\phi\|^{\deg f} \|f\|^{\deg \phi}$
  with $C$ a combinatorial term that depends on $\deg f$ and $\deg \phi$.

# How large is $|\operatorname{Res}(\phi(x), f(x))|$?

The coefficients of $\phi(x)$ are at most $A = L_N[a, \alpha]$.

We have:

$$\operatorname{Res}(u - vx, f(x)) = f_d u^d + f_{d-1} u^{d-1} v + \cdots + f_0 v^d.$$

- All summands have the same size: $\approx m \cdot A^d$.
  Note: $A^d = L_N[a + D, \alpha\delta]$.

## $|\operatorname{Res}(\phi(x), f(x))|$ ; which one of $m$ and $A^d$ wins?

| condition | $\lvert\operatorname{Res}(\phi(x), f(x))\rvert$ |
|---|---|
| $a + D < 1 - D$ | $m^{1+o(1)} = L_N[1 - D, 1/\delta \cdot (1 + o(1))]$ |
| $a + D = 1 - D$ | $L_N[1 - D, (\alpha\delta + 1/\delta) \cdot (1 + o(1))]$. |
| $a + D > 1 - D$ | $L_N[a + D, \alpha\delta \cdot (1 + o(1))]$. |

# Checklist

- $d = \deg f = \log_{\log N} L_N[D, \delta]$.
- This yields $m = L_N[1 - D, 1/\delta \cdot (1 + o(1))]$.
- The smoothness bound: $B = L_N[b, \beta]$.
- The bound on the coefficients of $\phi(x)$: $A = L_N[a, \alpha]$.
- $|\operatorname{Res}(\phi, x - m)| \leq |\operatorname{Res}(\phi, f)| = L_N[\underbrace{\max(1 - D, a + D)}_{\nu}, \cdot]$.
- The smoothness probability is $L_N[\nu - b, \cdot]$, by CEP.

The total cost is:

$$\underbrace{(\text{finding smooth pairs}) + (\text{factoring into relations})}_{L_N[\max(a,b),\cdot] \text{ is a safe upper bound}} + (\underbrace{\text{linear algebra}}_{L_N[b,\cdot]}).$$

# Plan

Tools

Parameters

First order

Second order

Summary

# We need enough relations

$$L_N[a, \mathbf{+}] \times L_N[\max(1-D, a+D) - b, \mathbf{-}] \geq L[b, \mathbf{+}].$$

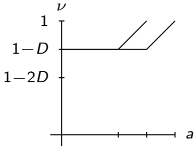
Several consequences (as we had in the QS case):

- $a \geq \max(1-D, a+D) - b$.
- Furthermore, $a > b$ or $a > \max(1-D, a+D) - b$ cannot be optimum choices, as we can improve the overall cost if it happens to be the case.
  - If $a > b$ and $1 - D \leq a + D$: decrease $a$ to $\max(b, 1-2D)$.
  - If $a > b$ and $1 - D \geq a + D$: increase $b$, decrease $a$.
  - If $a = b$ and $a > \max(1-D, a+D) - b$: decrease $a$ and $b$.

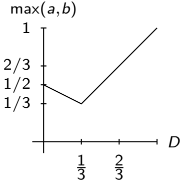
We can thus assume $a = b = \max(1-D, a+D) - b$ (possibly with a $o(1)$ shift).

# Optimum choice for $D$

- We don't know what $D$ is, plot the size of both resultants as a function of $a$. (using $|\operatorname{Res}(\phi, f)| = L_N[\nu, \cdot]$.)



- Given our reasoning, here's how the optimum $\max(a, b)$ looks like as a function of $D$.



We do the analysis with $D = a = b = 1/3$, and see what we get. In particular: pay attention to whether **+** and **−** compensate well!

# Checklist

- $d = \deg f = \log_{\log N} L_N[1/3, \delta]$.
- $m = L_N[2/3, 1/\delta \cdot (1 + o(1))]$.
- The smoothness bound: $B = L_N[1/3, \beta]$.
- The bound on the coefficients of $\phi(x)$: $A = L_N[1/3, \alpha]$.
- Note: this makes $A^2 = L_N[1/3, 2\alpha + o(1)]$ polynomials $\phi$ to choose from.
- $|\operatorname{Res}(\phi, x - m)| = L_N[2/3, 1/\delta + o(1)]$.
- $|\operatorname{Res}(\phi, f)| = L_N[2/3, \alpha\delta + 1/\delta + o(1)]$.
- The smoothness probability is $L_N[1/3, \cdot]$, by CEP.

And the total cost would be $L_N[1/3, \cdot]$ if we find a solution.

# Plan

Tools

Parameters

First order

Second order

Summary

# Smoothness

## Heuristic

We have to assume that values such as $\mathrm{Res}(\phi, x-m)$ or $\mathrm{Res}(\phi, f)$ behave like random integers of the same size.
This is mandatory if we want to apply CEP.
This heuristic is also present in QS, but not in Dixon's random squares.

Assuming that, the probability that both $\mathrm{Res}(\phi, x-m)$ and $\mathrm{Res}(\phi, f)$ are smooth is:

$$L_N\left[1/3, -\frac{1}{3\beta}\cdot\frac{1}{\delta}(1+o(1))\right] \times L_N\left[1/3, -\frac{1}{3\beta}\cdot(\alpha\delta+\frac{1}{\delta})(1+o(1))\right].$$

$$= L_N\left[1/3, -\frac{1}{3\beta}\cdot(\alpha\delta+\frac{1}{\delta}+\frac{1}{\delta})(1+o(1))\right].$$

# More characterization of the optimum

The probability of smoothness:

$$L_N\left[1/3, -\frac{1}{3\beta}\cdot(\alpha\delta+\frac{1}{\delta}+\frac{1}{\delta})(1+o(1))\right].$$

Notice that $\delta$ no longer appears anywhere else.

### Pick the best $\delta$

The smaller the Res values, the better the smoothness probability. We minimize $\alpha\delta+\frac{2}{\delta}$ by with $\delta=\sqrt{2/\alpha}$.

"Having enough relations" translates to:

$$2\alpha-\frac{1}{3\beta}\cdot 2\sqrt{2\alpha}\geq\beta.$$

# Factoring into relations

Spoilers:

- sieving will crush the cost of factoring relations to something asymptotically negligible,
- linear algebra will cost $(B^2)^{1+o(1)}$,

... so that the total cost is $L_N[1/3, 2\max(\alpha, \beta) + o(1)]$.

Given this total cost, it makes sense to search for a solution with $\alpha = \beta$. Can we find one?

# Complexity of NFS

We have a solution with $\alpha = \beta$ if we find a solution to:

$$2\alpha - \frac{1}{3\beta} \cdot 2\sqrt{2\alpha} \geq \beta \text{ with } \alpha = \beta.$$

$$3\beta^2 \geq 2\sqrt{2\beta}.$$

$$\beta^{3/2} \geq \sqrt{8/9}$$

$$\alpha = \beta \geq \sqrt[3]{8/9}.$$

$$2\beta \geq \sqrt[3]{64/9}.$$

## Complexity of NFS

Asymptotically, and heuristically, NFS has a complexity of:

$$L_N\left[1/3, (64/9)^{1/3} + o(1)\right].$$

# Plan

Tools

Parameters

First order

Second order

Summary

# Complexity of NFS: key equations

$$
\begin{aligned}
B &= L_N\left[1/3, (8/9)^{1/3} + o(1)\right].\\
A &= L_N\left[1/3, (8/9)^{1/3} + o(1)\right].\\
d &= \log_{\log N}\left(L_N\left[1/3, 3^{1/3} + o(1)\right]\right)\\
&= (3^{1/3} + o(1)) \cdot \left(\frac{\log N}{\log\log N}\right)^{1/3}.\\
\mathrm{Res}(\phi, f) &= L_N\left[1/3, \frac{3}{2}\cdot\sqrt{2\alpha} + o(1)\right] = L_N\left[1/3, 3\cdot 3^{-1/3} + o(1)\right].\\
\mathrm{Res}(\phi, x-m) &= L_N\left[1/3, \frac{1}{2}\cdot\sqrt{2\alpha} + o(1)\right] = L_N\left[1/3, 3^{-1/3} + o(1)\right].
\end{aligned}
$$

**Do not over-interpret this!**

“In theory”, algebraic norm is 3× rational norm. Not in practice.

# Huge difference with QS

$$\text{QS:}\ \exp\left(1\cdot(\log N)^{1/2}(\log\log N)^{1/2}\cdot(1+o(1))\right).$$

$$\text{NFS:}\ \exp\left((64/9)^{1/3}\cdot(\log N)^{1/3}(\log\log N)^{2/3}\cdot(1+o(1))\right).$$

(note: $(64/9)^{1/3} = 1.923\ldots$)

Asymptotics can be tricky, but the complexity difference is really a major one.

# Wrap up

- NFS complexity for arbitrary $N$ is:

$$L_N[1/3, (64/9)^{1/3} + o(1)].$$

- It is for arbitrary $N$, thus General NFS (GNFS).
- We left much aside, including:
    - How do the inner algorithms work?
    - In particular, is it true that sieving can eliminate the cost of factoring into relations?
    - And is it true that we solve the linear system in time $B^{2+o(1)}$?