New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields

Palash Sarkar and Shashank Singh

Indian Statistical Institute, Kolkata

May, 2016

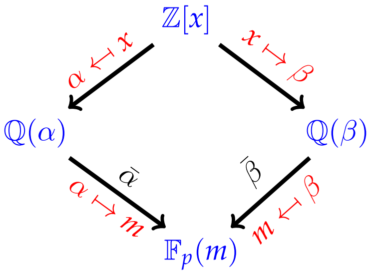
Eurocrypt 2016

Number Field Sieve for DLP in $\mathbb{F}_{p^n}$

Choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

> $f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

$\mathbb{Q}(\alpha) := \frac{\mathbb{Q}[x]}{\langle f(x)\rangle}$, $\mathbb{Q}(\beta) := \frac{\mathbb{Q}[x]}{\langle g(x)\rangle}$ and $\mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle \varphi(x)\rangle} = \mathbb{F}_p(m)$, $m \in \mathbb{F}_{p^n}$.



NUMBER FIELD SIEVE FOR DLP IN $\mathbb{F}_{p^n}$

Choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

> $f(x)$ mod p and $g(x)$ mod p, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

$$\mathbb{Q}(\alpha) := \frac{\mathbb{Q}[x]}{\langle f(x) \rangle}, \mathbb{Q}(\beta) := \frac{\mathbb{Q}[x]}{\langle g(x) \rangle} \text{ and } \mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle \varphi(x) \rangle} = \mathbb{F}_p(m), m \in \mathbb{F}_{p^n}.$$

$\phi(x)$

$\downarrow$

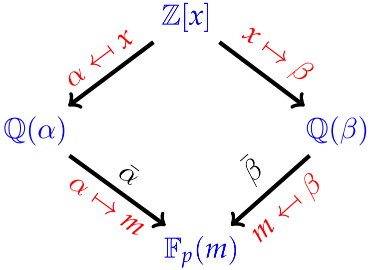
$\phi(\alpha)\mathcal{O}_1 = \prod_i \mathfrak{a}_i^{\,e_i}$

(Ideal Fact.)

$\downarrow$

$\phi(\alpha)^{h_1} = u_1 \prod_i a_i^{e_i}$

(Ideal to Element)



$\phi(x)$

$\downarrow$

$\phi(\beta)\mathcal{O}_2 = \prod_i \mathfrak{b}_i^{\,\ell_j}$

(Ideal Fact.)

$\downarrow$

$\phi(\beta)^{h_2} = u_2 \prod_i b_i^{\ell_i}$

(Ideal to Element)

Number Field Sieve for DLP in $\mathbb{F}_{p^n}$

Choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

> $f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

$$\mathbb{Q}(\alpha) := \frac{\mathbb{Q}[x]}{\langle f(x) \rangle}, \mathbb{Q}(\beta) := \frac{\mathbb{Q}[x]}{\langle g(x) \rangle} \text{ and } \mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle \varphi(x) \rangle} = \mathbb{F}_p(m), m \in \mathbb{F}_{p^n}.$$

$\phi(x)$

$\downarrow$

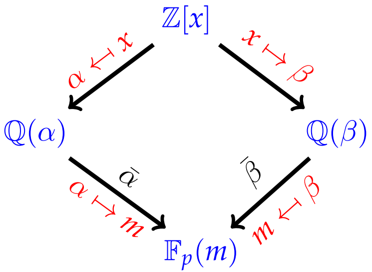
$\phi(\alpha)\mathcal{O}_1 = \prod_i \mathfrak{a}_i^{\ e_i}$

(Ideal Fact.)

$\downarrow$

$\phi(\alpha)^{h_1} = u_1 \prod_i a_i^{e_i}$

(Ideal to Element)



$\phi(x)$

$\downarrow$

$\phi(\beta)\mathcal{O}_2 = \prod_i \mathfrak{b}_i^{\ \ell_j}$

(Ideal Fact.)

$\downarrow$

$\phi(\beta)^{h_2} = u_2 \prod_i b_i^{\ell_i}$

(Ideal to Element)

> Since $\overline{\phi(\alpha)} = \overline{\phi(\beta)}$, we get a relation.

Number Field Sieve for DLP in $\mathbb{F}_{p^n}$

Choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

> $f(x)$ mod p and $g(x)$ mod p, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

$$\mathbb{Q}(\alpha) := \frac{\mathbb{Q}[x]}{\langle f(x)\rangle}, \mathbb{Q}(\beta) := \frac{\mathbb{Q}[x]}{\langle g(x)\rangle} \text{ and } \mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle \varphi(x)\rangle} = \mathbb{F}_p(m), m \in \mathbb{F}_{p^n}.$$

$\phi(x)$

$\downarrow$

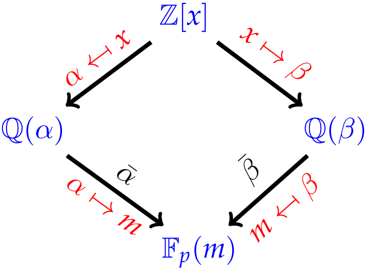
$\phi(\alpha)\mathcal{O}_1 = \prod_i \mathfrak{a}_i^{\,e_i}$

Factor $\mathrm{Res}(f, \phi)$

$\downarrow$

$\phi(\alpha)^{h_1} = u_1 \prod_i a_i^{e_i}$

(Ideal to Element)



$\phi(x)$

$\downarrow$

$\phi(\beta)\mathcal{O}_2 = \prod_i \mathfrak{b}_i^{\,\ell_j}$

Factor $\mathrm{Res}(g, \phi)$

$\downarrow$

$\phi(\beta)^{h_2} = u_2 \prod_i b_i^{\ell_i}$

(Ideal to Element)

Number Field Sieve for DLP in $\mathbb{F}_{p^n}$

Choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

$f(x)$ mod p and $g(x)$ mod p, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

$$\mathbb{Q}(\alpha) := \frac{\mathbb{Q}[x]}{\langle f(x)\rangle}, \mathbb{Q}(\beta) := \frac{\mathbb{Q}[x]}{\langle g(x)\rangle} \text{ and } \mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle \varphi(x)\rangle} = \mathbb{F}_p(m), m \in \mathbb{F}_{p^n}.$$

$\phi(x)$

$\downarrow$

$\phi(\alpha)\mathcal{O}_1 = \prod_i \mathfrak{a}_i^{\ e_i}$

Factor $\text{Res}(f, \phi)$

$\downarrow$

$\phi(\alpha)^{h_1} = u_1 \prod_i a_i^{e_i}$

(Ideal to Element)

Kalkbrener

$$|\text{Res}(f, \phi) \times \text{Res}(g, \phi)|$$

$$\approx \left(\|f\|_\infty \|g\|_\infty\right)^{t-1} E^{(\deg f + \deg g)2/t}$$

where $t = \deg(\phi) + 1$ and

$$\text{Coefficient}(\phi) \in \left[-E^{2/t}, E^{2/t}\right]$$

$\phi(x)$

$\downarrow$

$\phi(\beta)\mathcal{O}_2 = \prod_i \mathfrak{b}_i^{\ \ell_j}$

Factor $\text{Res}(g, \phi)$

$\downarrow$

$\phi(\beta)^{h_2} = u_2 \prod_i b_i^{\ell_i}$

(Ideal to Element)

Notation:

Let $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_1 x + \varphi_0$ and $r \geq \deg(\varphi)$.

$$M_{\varphi,r} = \begin{bmatrix} p & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & p & & & & \\ \varphi_0 & \varphi_1 & \cdots & \varphi_{n-1} & 1 & & & \\ & \ddots & \ddots & & \ddots & & & \\ & & \varphi_0 & \varphi_1 & \cdots & \varphi_{n-1} & 1 & \end{bmatrix} \begin{matrix} px^0 \\ \vdots \\ \vdots \\ px^n \\ \varphi(x) \\ \vdots \\ x^{r-n}\varphi(x) \end{matrix}$$

Apply the LLL algorithm to $M_{\varphi,r}$ and let the first row of the resulting LLL-reduced matrix be $[g_0, g_1, \ldots, g_{r-1}, g_r]$. Define

$$g(x) = g_0 + g_1 x + \cdots + g_{r-1}x^{r-1} + g_r x^r. \quad (1)$$

Notation: $g = \mathrm{LLL}(M_{\varphi,r})$

Some of the Polynomial Selection Methods

Given n and p, choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

$f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

Some of the Polynomial Selection Methods

Given n and p, choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

$f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

Algorithm: Generalised Joux-Lercier(GJL)[Barbulescu et al., D. Matyukhin]

Let $r \geq n$;

repeat

- Choose $f(x)$ irr of deg $(r+1)$ in $\mathbb{Z}[x]$, having small coefficients($= O(\ln p)$).
- Modulo p, $f(x)$ has a factor $\varphi(x)$ of degree n.
- $g(x) = \text{LLL}\left(M_{\varphi,r}\right)$

until *$f(x)$ and $g(x)$ are irr over $\mathbb{Z}$ and $\varphi(x)$ is irr over $\mathbb{F}_p$*;

Note: $\deg(f) = r+1 \quad \text{and} \quad \deg(g) = r$

$$\|f\|_\infty = O(\ln p) \quad \text{and} \quad \|g\|_\infty = O\left(p^{n/(r+1)}\right)$$

Some of the Polynomial Selection Methods

Given n and p, choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

$f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

Algorithm: Conjugation Method(Conj) [Barbulescu et al.]

Let $r \geq n$;

repeat

- Choose a quadratic monic $\mu(x)$ irr in $\mathbb{Z}[x]$, having small coefficients($= O(\ln p)$) and has a root $\mathfrak{t}$ in $\mathbb{F}_p$.
- Choose $g_0(x)$ and $g_1(x)$ with small coefficients such that $\deg g_1 < \deg g_0 = n$.
- Let (u, v) be such that $\mathfrak{t} \equiv u/v \bmod p$.
- $g(x) = vg_0(x) + ug_1(x), f(x) = \mathrm{Res}_y\big(\mu(y), g_0(x) + y\, g_1(x)\big)$.

until *$f(x)$ and $g(x)$ are irr over $\mathbb{Z}$ and $\varphi(x)$ is irr over $\mathbb{F}_p$.*;

SOME OF THE POLYNOMIAL SELECTION METHODS

Given n and p, choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

> $f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

Algorithm: Conjugation Method(Conj) [Barbulescu et al.]

Let $r \geq n$;

repeat

- Choose a quadratic monic $\mu(x)$ irr in $\mathbb{Z}[x]$, having small coefficients($= O(\ln p)$) and has a root $\mathfrak{t}$ in $\mathbb{F}_p$.
- Choose $g_0(x)$ and $g_1(x)$ with small coefficients such that $\deg g_1 < \deg g_0 = n$.
- Let (u, v) be such that $\mathfrak{t} \equiv u/v \bmod p$.
- $g(x) = vg_0(x) + ug_1(x), f(x) = \mathrm{Res}_y\big(\mu(y), g_0(x) + y\, g_1(x)\big)$.

until *$f(x)$ and $g(x)$ are irr over $\mathbb{Z}$ and $\varphi(x)$ is irr over $\mathbb{F}_p$.;*

$\deg(g) = n, \|g\|_\infty = O(\sqrt{p})$
$\deg(f) = 2n, \|f\|_\infty = O(\ln p)$

Some of the Polynomial Selection Methods

Given n and p, choose $f(x), g(x) \in \mathbb{Z}[x]$, such that

$f(x) \bmod p$ and $g(x) \bmod p$, have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

Algorithm: Conjugation Method(Conj) [Barbulescu et al.]

Let $r \geq n$;

repeat

- Choose a quadratic monic $\mu(x)$ irr in $\mathbb{Z}[x]$, having small coefficients($= O(\ln p)$) and has a root t in $\mathbb{F}_p$.
- Choose $g_0(x)$ and $g_1(x)$ with small coefficients such that $\deg g_1 < \deg g_0 = n$.
- Let (u, v) be such that $t \equiv u/v \bmod p$. LLL
- $g(x) = v g_0(x) + u g_1(x)$, $f(x) = \mathrm{Res}_y\big(\mu(y), g_0(x) + y\, g_1(x)\big)$.

until *$f(x)$ and $g(x)$ are irr over $\mathbb{Z}$ and $\varphi(x)$ is irr over $\mathbb{F}_p$.;*

$\deg(g) = n$, $\|g\|_\infty = O(\sqrt{p})$

$\deg(f) = 2n$, $\|f\|_\infty = O(\ln p)$

Basic Idea

We note the following:

- Both GJL and Conjugation methods use LLL, directly or indirectly.
- GJL uses all the coefficients of $\varphi(x)$ for doing LLL.
- Conjugation uses only one coefficient for LLL.
- In there anything in between? The answer is YES and is given by a new polynomial selection algorithm which both subsumes and generalises to GJL and Conjugation method.
- The new polynomial selection algorithm is parametrised by a divisor d of n and a value $r \geq n/d$.

Algorithm: $\mathcal{A}$: A new method of polynomial selection.

Input: p, n, d (a factor of n) and $r \geq n/d$.
Output: $f(x)$, $g(x)$ and $\varphi(x)$.

Let $k = n/d$;
repeat

Randomly choose a monic irr $A_1(x)$ with small coeff.:
$\deg A_1 = r + 1$; mod p, $A_1(x)$ has an irr factor $A_2(x)$ of deg k.
Choose monic $C_0(x)$ and $C_1(x)$: $\deg C_0 = d$ and $\deg C_1 < d$.
Define

$$\begin{aligned} f(x) &= \mathrm{Res}_y\left(A_1(y), C_0(x) + y\, C_1(x)\right); \\ \varphi(x) &= \mathrm{Res}_y\left(A_2(y), C_0(x) + y\, C_1(x)\right) \bmod p; \\ \psi(x) &= \mathrm{LLL}(M_{A_2,r}); \\ g(x) &= \mathrm{Res}_y\left(\psi(y), C_0(x) + y\, C_1(x)\right). \end{aligned}$$

until *$f(x)$ and $g(x)$ are irr over $\mathbb{Z}$ and $\varphi(x)$ is irr over $\mathbb{F}_p$.*;

return $f(x)$, $g(x)$ and $\varphi(x)$.

Algorithm: $\mathcal{A}$: A new method of polynomial selection.

Input: p, n, d (a factor of n) and $r \geq n/d$.
Output: $f(x)$, $g(x)$ and $\varphi(x)$.

Let $k = n/d$;
repeat

Table: Parameter estimates of various polynomial selection methods($t = 2$)

Methods	$\deg f$	$\deg g$	$\|f\|_\infty$	$\|g\|_\infty$	$\|f\|_\infty \|g\|_\infty E^{(\deg f + \deg g)}$
JLSV1	n	n	$Q^{\frac{1}{2n}}$	$Q^{\frac{1}{2n}}$	$E^{2n} Q^{\frac{1}{n}}$
GJL ($r \geq n$)	$r+1$	r	$O(\ln p)$	$Q^{\frac{1}{r+1}}$	$E^{2r+1} Q^{\frac{1}{r+1}}$
Conjugation	$2n$	n	$O(\ln p)$	$Q^{\frac{1}{2n}}$	$E^{3n} Q^{\frac{1}{2n}}$
$\mathcal{A}$ ($d \mid n, r \geq n/d$)	$d(r+1)$	dr	$O(\ln p)$	$Q^{\frac{1}{d(r+1)}}$	$E^{d(2r+1)} Q^{1/(d(r+1))}$

until $f(x)$ *and* $g(x)$ *are irr over* $\mathbb{Z}$ *and* $\varphi(x)$ *is irr over* $\mathbb{F}_p$.;

return $f(x)$, $g(x)$ and $\varphi(x)$.

EXAMPLE 1

Let $n = 6$, and p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835361211$$

Taking $d = 1$ and $r = n/d$, we get

$$\begin{aligned}
f(x) &= x^7 + 18\,x^6 + 99\,x^5 - 107\,x^4 - 3470\,x^3 - 15630\,x^2 - 30664\,x - 23239 \\
g(x) &= 712965136783466122384156554261504665235609243446869\,x^6 + 16048203858903 \\
&\quad 260691766216702652575435281807544247712\,x^5 + 1486772077481415492035898 9 \\
&\quad 0852868028274077107624860184\,x^4 + 72408538453914392579556483572292625 61 \\
&\quad 71920852986660372\,x^3 + 1946932041954939829697950384964684583780249722 18 \\
&\quad 5345772\,x^2 + 2718971797270235171234259793142851416923331519178675874\,x \\
&\quad +1517248296800681060244076172658712224507653769252953211
\end{aligned}$$

Note that $\|g\|_\infty \approx 2^{180}$.

EXAMPLE 1

Let $n = 6$, and p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835361211$$

Taking $d = 1$ and $r = n/d$, we get

$$f(x) = x^7 + 18x^6 + 99x^5 - 107x^4 - 3470x^3 - 15630x^2 - 30664x - 23239$$

Note that $\|g\|_\infty \approx 2^{180}$.

Taking $d = 2$ and $r = n/d$, we get

$$\begin{aligned} f(x) &= x^8 - x^7 - 5x^6 - 50x^5 - 181x^4 - 442x^3 - 801x^2 - 633x - 787 \\ g(x) &= 833480932500516492505935839185008193696457787\,x^6 + 2092593616641287655 \\ &\quad 0657400328969863435806986 15\,x^5 + 1298540899568952261791537743468335194 \\ &\quad 3188533320\,x^4 + 2186974159096635789762016746153996714153297062 2\,x^3 + 6 \\ &\quad 440309722463426267727380347199267174786096856 4\,x^2 + 558647116952815842 \\ &\quad 839094556655210927495027938 07\,x + 92177835405907782725278435670487132 7 \\ &\quad 10722661831 \end{aligned}$$

Note that $\|g\|_\infty \approx 2^{156}$.

Example 1

Let $n = 6$, and p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835361211$$

Taking $d = 1$ and $r = n/d$, we get

Taking $d = 2$ and $r = n/d$, we get

Taking $d = 3$ and $r = n/d$, we get

$$\begin{aligned}
f(x) &= x^9 - 4x^8 - 54x^7 - 174x^6 - 252x^5 \\
&\quad -174x^4 - 76x^3 - 86x^2 - 96x - 42 \\
g(x) &= 288974236450838155759331239249780100 6712\,x^6 + 83633695370646306085610 \\
&\quad 87765146274738509\,x^5 + 108280788065240857055064127834087729418 77\,x^4 + \\
&\quad 418128248897304001690003974172671977011 79\,x^3 + 14974213477775324762 13 \\
&\quad 3150889796948238735 4\,x^2 + 24094671698944321029344296555261130559219 4\,x \\
&\quad +151696455655104744403073743333940426598833
\end{aligned}$$

N

Note that $\|g\|_\infty \approx 2^{137}$.

EXAMPLE 1

Let $n = 6$, and p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835361211$$

Taking $d = 1$ and $r = n/d$, we get

Taking $d = 2$ and $r = n/d$, we get

Taking $d = 3$ and $r = n/d$, we get

Taking $d = 6$ and $r = n/d$, we get

$$\begin{aligned} f(x) &= x^{12} + 3\,x^{10} + 10\,x^9 + 53\,x^8 + 112\,x^7 + 163\,x^6 \\ &\quad + 184\,x^5 + 177\,x^4 + 166\,x^3 + 103\,x^2 + 72\,x + 48 \\ g(x) &= -666878138402353195498832669848\,x^6 - 186725327107492474601184918889\,x^5 \\ &\quad - 560175981322477423803554756667\,x^4 - 666875380176521094806391526505\,x^3 \\ &\quad - 426800353642006784703788222697\,x^2 - 693551609002948062903321290636\,x \\ &\quad - 746901308429969898404739675555 6 \end{aligned}$$

Note that $\|g\|_\infty \approx 2^{102}$.

Example 2

Let $n = 2$, and p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835301611$$

Taking $d = 2$ and $r = n/d = 1$, we get

$$\begin{aligned} f(x) &= x^4 - x^3 - 2x^2 - 7x - 3 \\ g(x) &= 717175561486984577278242843019\, x^2 + 218943531319777505644294654318 8\, x \\ &\quad + 290661087468475963372118938620 7 \end{aligned}$$

Note that $\|g\|_\infty \approx 2^{101}$. If we take $d = 2$ and $r = 2$, we get the following set of polynomials where $\|g\|_\infty \approx 2^{69}$.

$$\begin{aligned} f(x) &= x^6 - 4x^5 - 53x^4 - 147x^3 - 188x^2 - 157x - 92 \\ g(x) &= 1508727900272230098 5\, x^4 + 12461674372075387993 4\, x^3 \\ &\quad + 4517854600589942373 97\, x^2 + 7497643949399642450 00\, x \\ &\quad + 5672029895723497926 20 \end{aligned}$$

Asymptotic Complexity Analysis

Recap ($\mathbb{F}_Q$ where $Q = p^n$)

$\phi(x)$

$\downarrow$

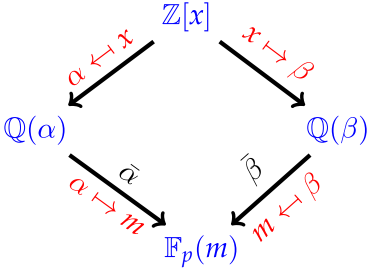
$\phi(\alpha)\mathcal{O}_1 = \prod_i \mathfrak{a}_i^{\ e_i}$

(Factor Res(f, ϕ))

$\downarrow$

$\phi(\alpha)^{h_1} = u_1 \prod_i a_i^{e_i}$

(Ideal to Element)



$\phi(x)$

$\downarrow$

$\phi(\beta)\mathcal{O}_2 = \prod_i \mathfrak{b}_i^{\ \ell_j}$

(Factor Res(g, ϕ))

$\downarrow$

$\phi(\beta)^{h_2} = u_2 \prod_i b_i^{\ell_i}$

(Ideal to Element)

$$\mathcal{F}_1 = \left\{ \begin{matrix} \text{prime ideals } \mathfrak{a}_i \text{ in } \mathcal{O}_1 \text{, either having norm less than } B \\ \text{or lying above the prime factors of } l(f) \end{matrix} \right\}$$

$$\mathcal{F}_2 = \left\{ \begin{matrix} \text{prime ideals } \mathfrak{b}_j \text{ in } \mathcal{O}_2 \text{, either having norm less than } B \\ \text{or lying above the prime factors of } l(g) \end{matrix} \right\}$$

Asymptotic Complexity Analysis

- The size of the factor basis = $B^{1+o(1)} \approx B$. Cost of Linear Algebra $\approx B^2$.
- Let E be such that the coefficients of ϕ are in $\left[-\frac{1}{2}E^{2/t}, \frac{1}{2}E^{2/t}\right]$ i.e. $\|\phi\|_\infty \approx E^{2/t}$.Total number of polynomial considered is E^2, which is, in fact, the cost of relation collection step.

ASYMPTOTIC COMPLEXITY ANALYSIS

- The size of the factor basis = $B^{1+o(1)} \approx B$. Cost of Linear Algebra $\approx B^2$.
- Let E be such that the coefficients of ϕ are in $\left[-\frac{1}{2}E^{2/t}, \frac{1}{2}E^{2/t}\right]$ i.e. $\|\phi\|_\infty \approx E^{2/t}$.Total number of polynomial considered is E^2, which is, in fact, the cost of relation collection step.

Let π be the probability of getting a single relation.

Requirements:

- Cost(L. A.)=Cost(R. C.)
- Sufficient Relations

Asymptotic Complexity Analysis

- The size of the factor basis = $B^{1+o(1)} \approx B$. Cost of Linear Algebra $\approx B^2$.
- Let E be such that the coefficients of ϕ are in $\left[-\frac{1}{2}E^{2/t}, \frac{1}{2}E^{2/t}\right]$ i.e. $\|\phi\|_\infty \approx E^{2/t}$.Total number of polynomial considered is E^2, which is, in fact, the cost of relation collection step.

Let π be the probability of getting a single relation.

Requirements:

- Cost(L. A.)=Cost(R. C.)
- Sufficient Relations

$E^2\pi = B$ and $B^2 = E^2$ $\Rightarrow$ $E = B = \pi^{-1}$

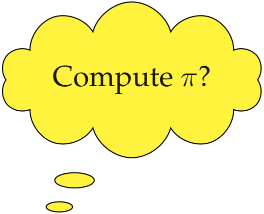
ASYMPTOTIC COMPLEXITY ANALYSIS

- The size of the factor basis = $B^{1+o(1)} \approx B$. Cost of Linear Algebra $\approx B^2$.
- Let E be such that the coefficients of ϕ are in $\left[-\frac{1}{2}E^{2/t}, \frac{1}{2}E^{2/t}\right]$ i.e. $\|\phi\|_\infty \approx E^{2/t}$.Total number of polynomial considered is E^2, which is, in fact, the cost of relation collection step.

Let π be the probability of getting a single relation.

Requirements:

- Cost(L. A.)=Cost(R. C.)
- Sufficient Relations



$E^2\pi = B$ and $B^2 = E^2$ $\Rightarrow$ $E = B = \pi^{-1}$

Let $B = L_Q(b, c_b) = E$, for some $0 < b < 1$

Asymptotic Complexity Analysis..

π is Computed using Canfield-Erdös-Pomerance theorem.

Canfield-Erdös-Pomerance (CEP) theorem

Let $\pi = \Psi(\Gamma, B)$ be the probability that a random positive integer which is at most Γ is B-smooth. Let $\Gamma = L_Q(z, \zeta)$ and $B = L_Q(b, c_b)$. Then

$$(\Psi(\Gamma, B))^{-1} = L_Q\left(z - b, (z - b)\frac{\zeta}{c_b}\right). \tag{2}$$

Asymptotic Complexity Analysis..

π is Computed using Canfield-Erdös-Pomerance theorem.

Canfield-Erdös-Pomerance (CEP) theorem

Let $\pi = \Psi(\Gamma, B)$ be the probability that a random positive integer which is at most Γ is B-smooth. Let $\Gamma = L_Q(z, \zeta)$ and $B = L_Q(b, c_b)$. Then

$$(\Psi(\Gamma, B))^{-1} = L_Q\left(z - b, (z-b)\frac{\zeta}{c_b}\right). \qquad (2)$$

We have Γ equal to,

$$\begin{aligned} |\mathrm{Res}(f, \phi) \times \mathrm{Res}(g, \phi)| &\approx (\|f\|_\infty \|g\|_\infty)^{t-1} \times E^{2(\deg f + \deg g)/t} \\ &= O\left(E^{2d(2r+1)/t} \times Q^{(t-1)/(d(r+1))}\right). \end{aligned}$$

ASYMPTOTIC COMPLEXITY ANALYSIS..

We have,

$$p = L_Q(a, c_p) \text{ and } B = L_Q(b, c_b) \tag{3}$$

Lemma

Let $n = kd$ for positive integers k and d. Using the expressions for p and $E(= B)$ given by (3), we obtain the following.

$$\left.\begin{array}{rcl} E^{\frac{2}{t}d(2r+1)} & = & L_Q\left(1 - a + b, \frac{2c_b(2r+1)}{c_p kt}\right); \\ Q^{\frac{t-1}{d(r+1)}} & = & L_Q\left(a, \frac{kc_p(t-1)}{(r+1)}\right). \end{array}\right\} \tag{4}$$

Boundary Case

Let $p = L_Q(2/3, c_p)$ for some $0 < c_p < 1$. Equation (4) becomes

$$\left.\begin{aligned} E^{\frac{2}{t}d(2r+1)} &= L_Q\left(\frac{1}{3}+b, \frac{2c_b(2r+1)}{c_p k t}\right); \\ Q^{\frac{t-1}{d(r+1)}} &= L_Q\left(\frac{2}{3}, \frac{kc_p(t-1)}{(r+1)}\right). \end{aligned}\right\} \qquad (5)$$

Boundary Case

Let $p = L_Q(2/3, c_p)$ for some $0 < c_p < 1$. Equation (4) becomes

$$\left.\begin{aligned} E^{\frac{2}{t}d(2r+1)} &= L_Q\left(\tfrac{1}{3}+b, \tfrac{2c_b(2r+1)}{c_pkt}\right); \\ Q^{\frac{t-1}{d(r+1)}} &= L_Q\left(\tfrac{2}{3}, \tfrac{kc_p(t-1)}{(r+1)}\right). \end{aligned}\right\} \tag{5}$$

Choosing $b = 1/3$, we get

$$\Gamma = |\mathrm{Res}(f,\phi) \times \mathrm{Res}(g,\phi)| \approx L_Q\left(\frac{2}{3}, \frac{2c_b(2r+1)}{c_pkt} + \frac{kc_p(t-1)}{(r+1)}\right).$$

Using CEP, we get

$$\pi^{-1} = L_Q\left(\frac{1}{3}, \frac{1}{3}\left(\frac{2(2r+1)}{c_pkt} + \frac{kc_p(t-1)}{c_b(r+1)}\right)\right).$$

Boundary Case..

Since $B = \pi^{-1}$, we get

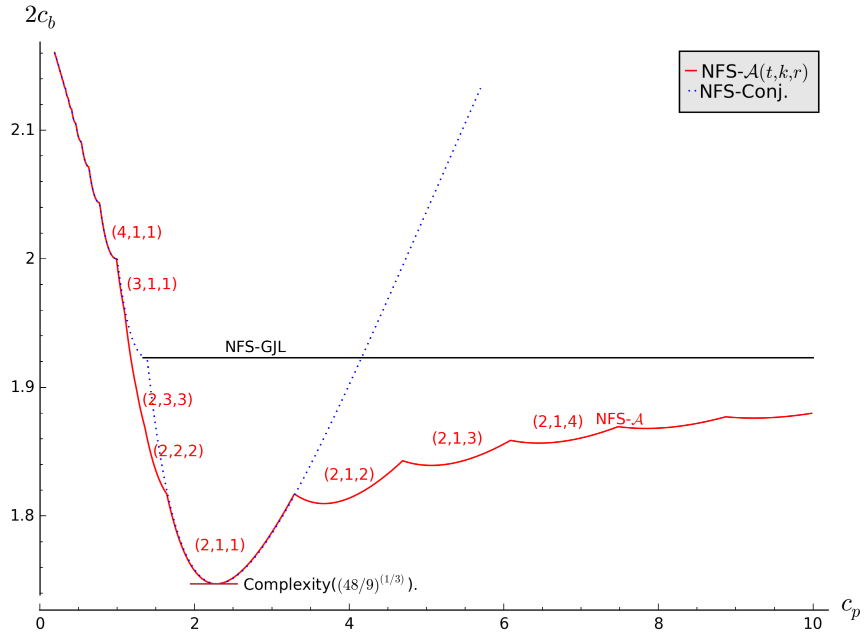
$$c_b = \frac{1}{3}\left(\frac{2(2r+1)}{c_p k t} + \frac{k c_p (t-1)}{c_b (r+1)}\right). \tag{6}$$

Solving the quadratic for c_b and choosing the positive root gives

$$c_b = \frac{2r+1}{3c_p k t} + \sqrt{\left(\frac{2r+1}{3c_p k t}\right)^2 + \frac{k c_p (t-1)}{3(r+1)}}. \tag{7}$$

Overall Complexity is given by $L_Q(1/3, 2c_b)$.

New Complexity Trade-Offs for NFS



NEW COMPLEXITY TRADE-OFFS FOR NFS

For $k = 1$ and $t = 2$, we have

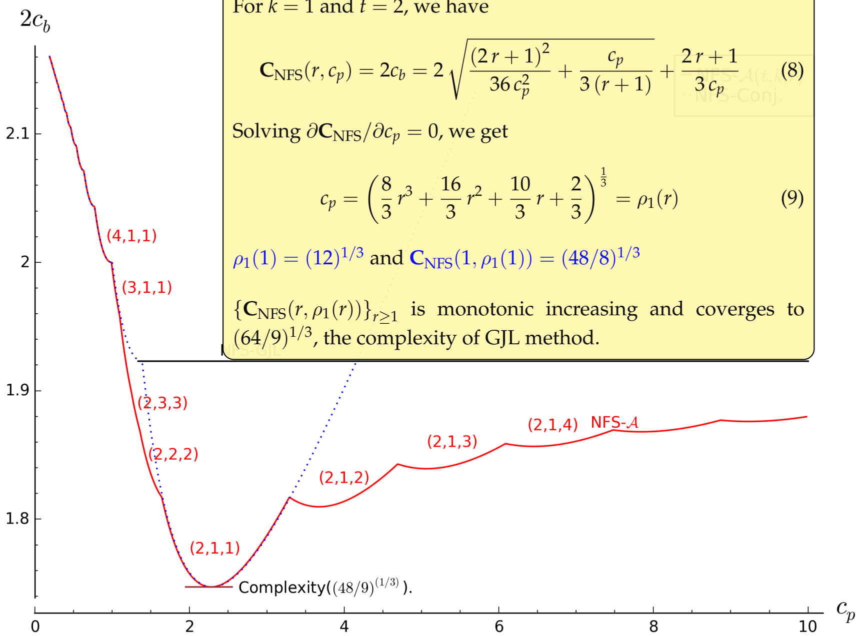
$$\mathbf{C}_{\text{NFS}}(r, c_p) = 2c_b = 2\sqrt{\frac{(2\,r+1)^2}{36\,c_p^2} + \frac{c_p}{3\,(r+1)}} + \frac{2\,r+1}{3\,c_p} \qquad (8)$$

Solving $\partial \mathbf{C}_{\text{NFS}}/\partial c_p = 0$, we get

$$c_p = \left(\frac{8}{3}\,r^3 + \frac{16}{3}\,r^2 + \frac{10}{3}\,r + \frac{2}{3}\right)^{\frac{1}{3}} = \rho_1(r) \qquad (9)$$

$\rho_1(1) = (12)^{1/3}$ and $\mathbf{C}_{\text{NFS}}(1, \rho_1(1)) = (48/8)^{1/3}$

$\{\mathbf{C}_{\text{NFS}}(r, \rho_1(r))\}_{r \geq 1}$ is monotonic increasing and coverges to $(64/9)^{1/3}$, the complexity of GJL method.



Multiple Number Field Sieve Analysis

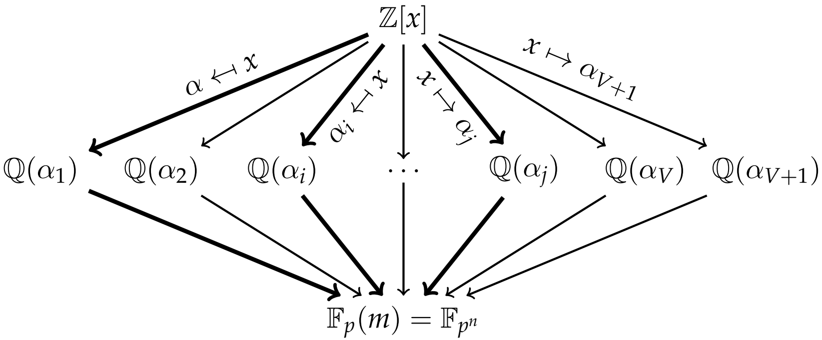


Figure: A work-flow of MNFS.

Multiple Number Field Sieve Analysis

$f_i(x) \bmod p$ should have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

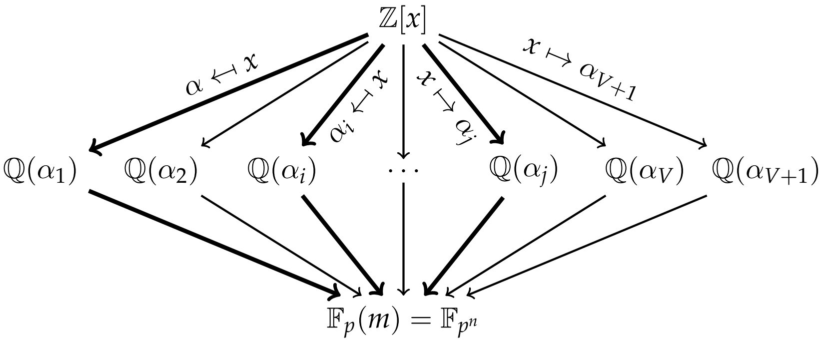
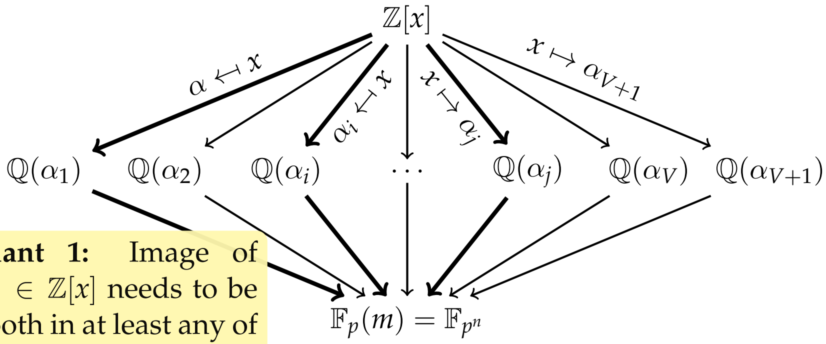


Figure: A work-flow of MNFS.

Multiple Number Field Sieve Analysis

$f_i(x) \bmod p$ should have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.

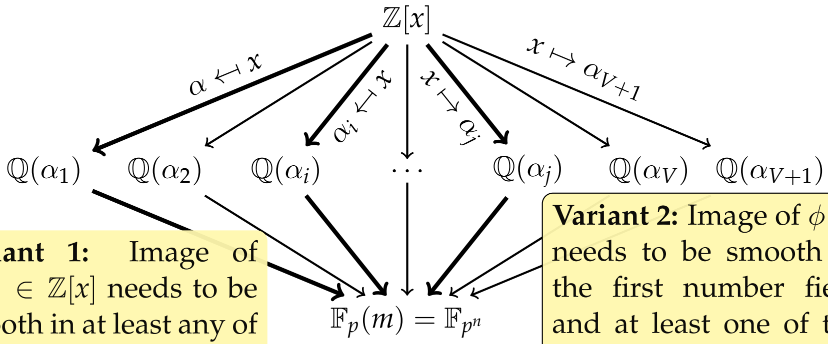


Variant 1: Image of $\phi(x) \in \mathbb{Z}[x]$ needs to be smooth in at least any of the two number fields.

Figure: A work-flow of MNFS.

Multiple Number Field Sieve Analysis

$f_i(x) \bmod p$ should have a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.



Variant 1: Image of $\phi(x) \in \mathbb{Z}[x]$ needs to be smooth in at least any of the two number fields.

Variant 2: Image of $\phi(x)$ needs to be smooth in the first number field and at least one of the other V number fields.

Figure: A work-flow of MNFS.

Polynomial Selection in MNFS

Recall that,

✓ Algorithm $\mathcal{A}$ produces $f(x)$ and $g(x)$ of degrees $d(r+1)$ and dr respectively.

✓ $g(x) = \mathrm{Res}_y(\psi(y), C_0(x) + yC_1(x))$ where $\psi(x) = \mathrm{LLL}(M_{A_2,r})$.

- Let $g_1(x) = g(x)$.
- $g_2(x) = \mathrm{Res}_y(\psi'(y), C_0(x) + yC_1(x))$, where $\psi'(x)$ be the polynomial defined by the second row of the matrix $\mathrm{LLL}(M_{A_2,r})$.
- $g_i(x) = s_i g_1(x) + t_i g_2(x)$, for $i = 3, \ldots, V$. Note that the coefficients s_i and t_i are of the size of $\sqrt{V}$.

All the g_i's have degree dr. Asymptotically $\|\psi\|_\infty = \|\psi'\|_\infty = Q^{1/(d(r+1))}$.

Asymptotic Analysis of MNFS

- Let B and B' be the bounds on the norms of the ideals for factor basis defined by f and each of the g_i's respectively.
- So, the size of the entire factor basis is $B + VB'$. Let $B \approx VB'$.
- Cost of linear algebra is $4B^2 \approx B^2$.
- As before, let $\|\phi\|_\infty \approx E^{2/t}$, and so the cost of relation collection step is E^2.
- Let π be the probability of getting a relation.

Asymptotic Analysis of MNFS

- Let B and B' be the bounds on the norms of the ideals for factor basis defined by f and each of the g_i's respectively.
- So, the size of the entire factor basis is $B + VB'$. Let $B \approx VB'$.
- Cost of linear algebra is $4B^2 \approx B^2$.
- As before, let $\|\phi\|_\infty \approx E^{2/t}$, and so the cost of relation collection step is E^2.
- Let π be the probability of getting a relation.

Requirements:

- Cost(L. A.)=Cost(R. C.)
- Sufficient Relations

$E^2\pi = B$ and $B^2 = E^2$ $\Rightarrow$ $E = B = \pi^{-1}$

Asymptotic Analysis of MNFS..

Similar to NFS case, let π be the probability of getting a relation.

$$\pi = \Psi(\Gamma_1, B)\, V\, \Psi(\Gamma_2, B') \text{ where } \Gamma_1 = \text{Res}_x(f(x), \phi(x))$$
$$\Gamma_2 = \text{Res}_x(g_i(x), \phi(x))$$

We have all the necessary tools available to compute π i.e.,

$$\|\phi\|_\infty \approx E^{2/t}, \|f\|_\infty \approx O(\ln p) \text{ and } \|g\|_\infty \approx Q^{1/d(r+1)}$$

Asymptotic Analysis of MNFS..

Let,

$B = L_Q\left(1/3, c_b\right)$ and $V = L_Q\left(1/3, c_v\right)$, so $B' = L_Q\left(1/3, c_b - c_v\right)$.

Assume $p = L_Q(\frac{2}{3}, c_p)$, proceeding similar to the NFS case, we get

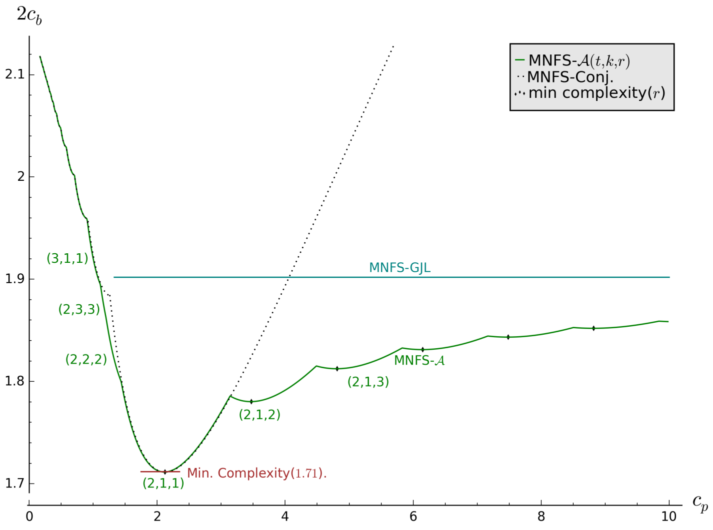
$$c_b = \frac{4r+2}{6ktc_p} + \sqrt{\frac{r(3r+2)}{(3ktc_p)^2} + \frac{c_p k(t-1)}{3(r+1)}}. \quad (10)$$

Hence the overall complexity of MNFS for the boundary case is $L_Q\left(\frac{1}{3}, 2c_b\right)$.

<u>For $t = 2$ and $k = 1$:</u>

$$\mathbf{C}_{\mathrm{MNFS}}(c_p, r) = 2c_b = 2\sqrt{\frac{c_p}{3\,(r+1)} + \frac{(3\,r+2)r}{36\,c_p^2}} + \frac{2\,r+1}{3\,c_p}.$$

New Complexity Trade-Offs for MNFS



[1] This equation is incorrect in the proceedings version.

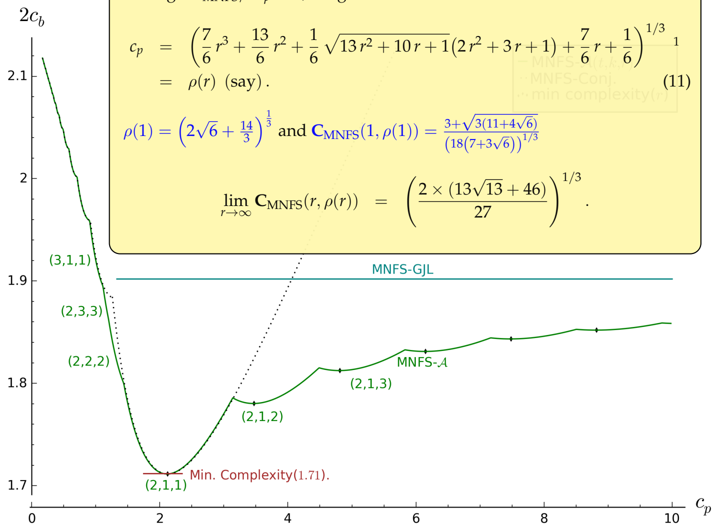
New Complexity Trade-Offs for MNFS

Solving $\partial \mathbf{C}_{\mathrm{MNFS}}/\partial c_p = 0$, we get

$$\begin{aligned} c_p &= \left(\frac{7}{6}r^3 + \frac{13}{6}r^2 + \frac{1}{6}\sqrt{13\,r^2 + 10\,r + 1}\,(2\,r^2 + 3\,r + 1) + \frac{7}{6}r + \frac{1}{6}\right)^{1/3} {}^{1} \\ &= \rho(r)\ \ (\text{say})\,. \end{aligned} \tag{11}$$

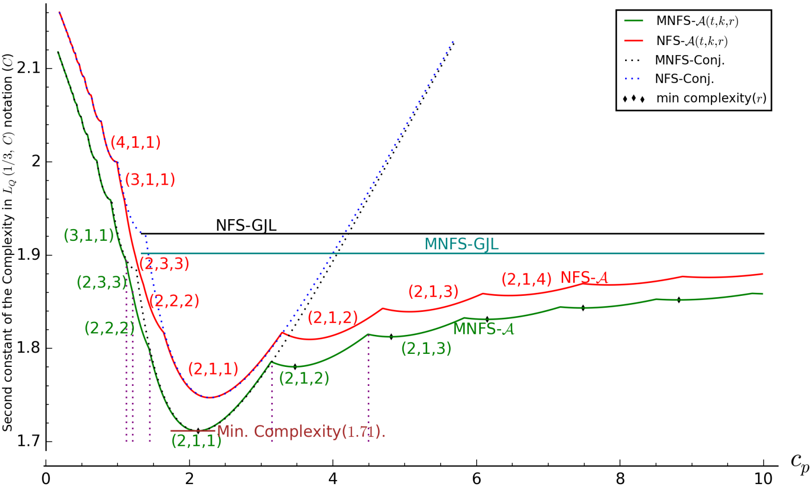
$\rho(1) = \left(2\sqrt{6} + \frac{14}{3}\right)^{\frac{1}{3}}$ and $\mathbf{C}_{\mathrm{MNFS}}(1, \rho(1)) = \frac{3+\sqrt{3(11+4\sqrt{6})}}{\left(18(7+3\sqrt{6})\right)^{1/3}}$

$$\lim_{r\to\infty} \mathbf{C}_{\mathrm{MNFS}}(r, \rho(r)) = \left(\frac{2 \times (13\sqrt{13} + 46)}{27}\right)^{1/3}.$$



[1] This equation is incorrect in the proceedings version.

NEW COMPLEXITY TRADE-OFFS



Questions?