The Multiple Number Field Sieve with Conjugation and Generalized Joux-Lercier Methods*

Cécile Pierrot†

Laboratoire d'Informatique de Paris 6
UPMC, Sorbonne Universités

Abstract

In this paper, we propose two variants of the Number Field Sieve (NFS) to compute discrete logarithms in medium characteristic finite fields. We consider algorithms that combine two ideas, namely the Multiple variant of the Number Field Sieve (MNFS) taking advantage of a large number of number fields in the sieving phase, and two recent polynomial selections for the classical Number Field Sieve. Combining MNFS with the Conjugation Method, we design the best asymptotic algorithm to compute discrete logarithms in the medium characteric case. The asymptotic complexity of our improved algorithm is $L_{p^n}(1/3, (8(9+4\sqrt{6})/15)^{1/3}) \approx L_{p^n}(1/3, 2.156)$, where $\mathbb{F}_{p^n}$ is the target finite field. This has to be compared with the complexity of the previous state-of-the-art algorithm for medium characteristic finite fields, NFS with Conjugation Method, that has a complexity of approximately $L_{p^n}(1/3, 2.201)$. Similarly, combining MNFS with the Generalized Joux-Lercier method leads to an improvement on the asymptotic complexities in the boundary case between medium and high characteristic finite fields.

1 Introduction

Public key cryptosystems are designed around computational hardness assumptions related to mathematical properties, making such protocols hard to break in practice by any adversary. Algorithmic number theory provides most of those assumptions, such as the presumed difficulty to factorize a large integer or to compute discrete logarithms in some groups. Given an arbitrary element h of a cyclic group, the discrete logarithm problem consists in recovering the exponent x of a generator g such that $g^x = h$. We focus here on the multiplicative group of the invertible elements in a finite field.

Current discrete logarithms algorithms for finite fields vary with the relative sizes of the characteristic p and the extension degree n. To be more precise, finite fields split into three families and so do the related algorithms. When p is small compared to n, the best choice is to apply the recent Quasi-Polynomial algorithm [BGJT14]. Medium and high characteristics share some properties since we use in both cases variants of the Number Field Sieve (NFS) that was first introduced for discrete logarithms computations in prime fields in 1993 by Gordon [Gor93]. Then, NFS was extended to all medium and high characteristic finite fields in 2006 by Joux, Lercier, Smart and

†This work is funded by DGA (Department of Defense, France) and CNRS.

Vercauteren [JLSV06]. For the past few months, discrete logarithm in finite fields has been a vivid domain and things change fast – not only for small characteristic.

In February 2014, Barbulescu and Pierrot [BP14] presented the Multiple Number Field Sieve (MNFS) that applies in both medium and high characteristic finite fields. As for NFS, the main idea came from factoring [Cop93] and was first introduced for discrete logarithms computations in prime fields in 2003 thanks to Matyukhin [Mat03]. In both medium and high characteristic cases, the idea is to go from two number fields, as in the classical NFS, to a large number of number fields, making the probability to obtain a good relation in the sieving phase higher. Yet, the sieving phase differs between medium and high characteristics since the parameters of the two first polynomials defining the number fields are equal in the medium case but unbalanced in the high case. Let us recall the notation $L_q(\alpha, c) = \exp((c+o(1))(\log q)^{\alpha}(\log\log q)^{1-\alpha})$ to be more precise about complexities, and focus on the high characteristic case. Due to unbalanced degree of the first two polynomials, the variant proposed by Barbulescu and Pierrot is dissymmetric. It means that in the sieving phase they select only elements that are small in some sense in the first number field and in at least another number field, giving to the first number field a specific role with regards to the others. With this dissymmetric MNFS, the asymptotic complexity to compute discrete logarithms in a finite field $\mathbb{F}_{p^n}$ of characteristic $p = L_{p^n}(l_p, c)$ when p is high, *i.e.* when $l_p > 2/3$, is the same as the complexity given for factoring an integer of the same size [Cop93]. Namely, it is:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{2\cdot(46+13\sqrt{13})}{27}\right)^{1/3}\right).$$

Note that MNFS as described in [BP14] is currently the state-of-the-art algorithm for computing discrete logarithms in high characteristic finite fields.

In the medium characteristic case, *i.e.* when $1/3 \leqslant l_p \leqslant 2/3$, the polynomial selection of the classical Number Field Sieve allows to construct two polynomials with same degrees and same sizes of coefficients. Making linear combination, MNFS creates then a lots of polynomials with equal parameters. Thanks to this notion of symmetry, the sieving phase of the Multiple variant consists in keeping elements that are small in any pairs of number fields, making the probability to obtain a good relation growing further.

Yet, few months later, in August 2014, Barbulescu, Gaudry, Guillevic and Morain detailed in a preprint [BGGM14] some practical improvements for the classical Number Field Sieve. Besides, they gave a new polynomial selection method that has the nice theoretical interest to lead to the best asymptotic heuristic complexity known in the medium characteristic case, overpassing the one given in [BP14]. This new polynomial selection also called Conjugation Method permits to create one polynomial with a *small* degree and *high* coefficients and another one with a *high* degree and coefficients of constant size. Finally, the authors of [BGGM14] obtain the asymptotic complexity:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{96}{9}\right)^{1/3}\right).$$

In this article, we adapt for the first time the Multiple variant of NFS to this very recent algorithm. At first sight, one could fear that the parameters of the two polynomials given with the Conjugation Method could act as a barrier, since their unbalanced features differ from the ones used in the medium characteristic case of [BP14]. Moreover, following the high characteristic dissymmetric sieving phase of [BP14] and creating the remaining polynomials with linear combination would mean spreading both *high* coefficients and *high* degrees on the polynomials defining the various number fields. This clearly would not be a good idea, as all NFS-based algorithms require to create elements with small norms. However, we show that the Conjugation Method may be adapted to overcome this difficulty. The idea is to try to keep the advantage

of the kind of *balanced dissymetry* brought by the two polynomials with *small*-degree-*high*-coefficients/*high*-degree-*small*-coefficients. We show that the Multiple Number Field Sieve with Conjugation Method (MNFS-CM) becomes the best current algorithm to compute discrete logarithms in medium characteristic finite fields. Indeed, in this case its asymptotic complexity is:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{8\cdot(9+4\sqrt{6})}{15}\right)^{1/3}\right).$$

To ease the comparison, note that our second constant $\left(8\,(9+4\sqrt{6})/15\right)^{1/3} \approx 2.156$ whereas the previous one is $(96/9)^{1/3} \approx 2.201$. MNFS-CM in the boundary case between medium and high characteristic leads also to an improvement of NFS-CM. Interestingly enough, sieving on degree one polynomials with MNFS-CM in this boundary case permits to obtain the best asymptotic complexity ever of any medium, boundary and high characteristic discrete logarithms algorithms, which is approximately $L_{p^n}(1/3, 1.71)$.

Besides the new Conjugation Method, the authors of [BGGM14] extend the polynomial selection given by Joux and Lercier in [JL03] for prime fields. Thanks to it, they get an improvement on the high cases of the boundary case. We propose here a simple dissymetric Multiple Number Field Sieve based on this Generalized Joux-Lercier method (MNFS-GJL) to get a further improvement on the same boundary case. Note that the asymptotic complexity we obtain here,

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{2\cdot(46+13\sqrt{13})}{27}\right)^{1/3}\right),$$

is exactly the one of MNFS for high characteristic finite fields, as given in [BP14].

Outline. We first detail in Section 2 how to manage the selection of numerous polynomials based on the Conjugation method to construct a dissymetric Multiple Number Field Sieve. Section 3 explains then how to combine MNFS with the Generalized Joux-Lercier method. The asymptotic complexity analyses of both medium and boundary cases are given in Section 4.

2 Combining the Multiple variant of the Number Field Sieve with the Conjugation Method

Let $\mathbb{F}_{p^n}$ denote the finite field we target, p its characteristic and n the extension degree relatively to the base field. We propose an algorithm to compute discrete logarithms in $\mathbb{F}_{p^n}$ as soon as p can be written as $p = L_{p^n}(l_p, c_p)$ with $1/3 \leqslant l_p \leqslant 2/3$ (and c_p close to 1). In this case we say that the characteristic has medium size. In Section 2.1 we explain how to represent the finite field and to construct the polynomials that define the large number of number fields we need. In Section 2.2 we give details about the variant of the Multiple Number Field Sieve we propose to follow.

2.1 Polynomial selection

Basic idea: large numbers of polynomials with a common root in $\mathbb{F}_{p^n}$

To compute discrete logarithms in $\mathbb{F}_{p^n}$, all algorithms based on the Number Field Sieve start by choosing two polynomials f_1 and f_2 with integers coefficients such that the greatest common divisor of these polynomials has an irreducible factor of degree n over the base field. If m denotes a common root of these two polynomials in $\mathbb{F}_{p^n}$ and $\mathbb{Q}(\theta_i)$ denotes the number field $\mathbb{Q}[X]/(f_i(X))$ for each $i = 1, 2$, *i.e.* θ_i is a root of f_i in $\mathbb{C}$, then we are able to draw the commutative diagram of Figure 1.

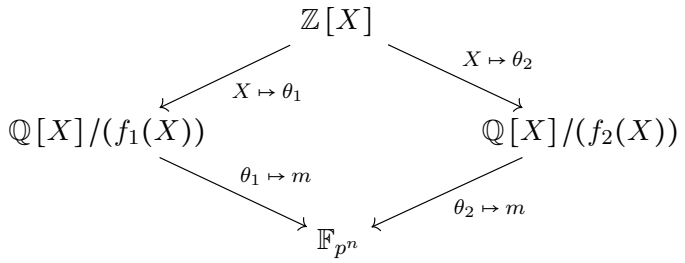

Figure 1: Commutative diagram of NFS.

Since MNFS requires to have a large number of number fields, let say V number fields, then we have to construct $V-2$ extra polynomials that share the same common root m in $\mathbb{F}_{p^n}$. The commutative diagram that is the cornerstone of all Multiple variants of the Number Field Sieve is given in Figure 2.

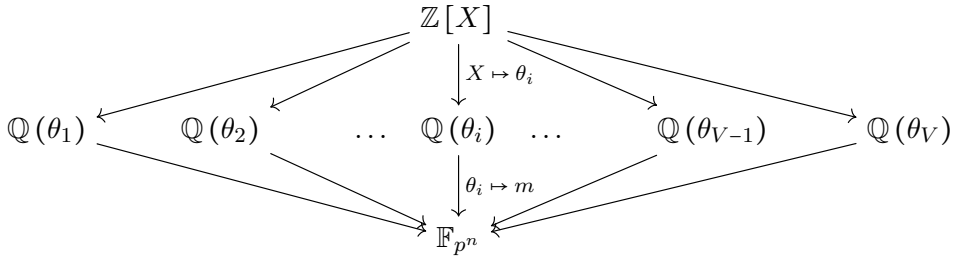

Figure 2: Commutative diagram of MNFS

Settings: construction of V polynomials with the Conjugation Method

We start with the Conjugation Method given in [BGGM14, Paragraph 6.3] to construct the first two polynomials. The idea is as follows.

We create two auxilliary polynomials g_a and g_b in $\mathbb{Z}[X]$ with small coefficients such that $\deg g_a = n$ and $\deg g_b < n$. We then search for an irreducible polynomial X^2+uX+v over $\mathbb{Z}[X]$, where u and v are small integers[1] of size $O(\log p)$, such that its roots λ and λ' are in $\mathbb{F}_p$. Since we seek a degree n irreducible polynomial over $\mathbb{F}_p[X]$ to construct the finite field, we keep the polynomial X^2+uX+v if one of the two degree n polynomials $g_a + \lambda g_b$ or $g_a + \lambda' g_b$ is irreducible over $\mathbb{F}_p[X]$. In the sequel we assume that $g_a + \lambda g_b$ is irreducible over $F_p[X]$. When we have found such parameters, we set our first polynomial $f_1 \in \mathbb{Z}[X]$:

$$f_1 = g_a^2 - u g_a g_b + v g_b^2.$$

Equivalently, f_1 is defined in [BGGM14] as equal to $\mathrm{Res}_Y(Y^2+uY+v, g_a(X)+Y g_b(X))$. Since λ and λ' are roots of $X^2 + uX + v$ in $\mathbb{F}_p$, we have the equality of polynomials $f_1 \equiv g_a^2 + (\lambda+\lambda')g_a g_b + \lambda\lambda' g_b^2 \mod p$. In other words, $f_1 \equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p$.

[1] We correct here a mistake in [BGGM14, Paragraph 6.3]. The authors propose to search for an irreducible quadratic polynomial that has constant size coefficients. However, if $|u|$ and $|v|$ are both lower than a constant C, then there exist 2^{4C^2} such polynomials. Since each one has probability 1/2 to has its roots in $\mathbb{F}_p$ for one random prime p, if we try to select such polynomials for approximately 2^{4C^2} primes, we will find one finite field $\mathbb{F}_p$ for which this method fails. Looking for quadratic polynomials with coefficients of size $O(\log p)$ bypasses this trap and does not interfere with final asymptotic complexities.

Thus we have a polynomial f_1 of degree $2n$ with coefficients of size $O(\log p)$ that is divisible by $g_a + \lambda g_b$ in $\mathbb{F}_p[X]$.

Let us construct the next two polynomials. Thanks to continued fractions we can write:

$$\lambda \equiv \frac{a}{b} \equiv \frac{a'}{b'} \mod p$$

where a, b, a' and b' are of the size of $\sqrt{p}$. We underline that these two reconstructions (a, b) and (a', b') of λ are linearly independent over $\mathbb{Q}$. We then set:

$$f_2 = bg_a + ag_b \quad \text{and} \quad f_3 = b'g_a + a'g_b.$$

Note that the Conjugation Method ends with the selection of f_1 and f_2 and does not use the second reconstruction. It is clear that both f_2 and f_3 have degree n and coefficients of size $\sqrt{p}$. Furthermore, we notice that $f_2 \equiv b(g_a + \lambda g_b) \mod p$ and similarly $f_3 \equiv b'(g_a + \lambda g_b) \mod p$, so they share a common root with f_1 in $\mathbb{F}_{p^n}$.

We finally set for all i from 4 to V:

$$f_i = \alpha_i f_2 + \beta_i f_3$$

with α_i and β_i of the size of $\sqrt{V}$. We underline that V is negligible with regards to p, as shown in Section 4. Thanks to linear combination, for all $2 \leqslant i \leqslant V$, f_i has degree n, coefficients of size $\sqrt{p}$ and is divisible by $g_a + \lambda g_b$ in $\mathbb{F}_p[X]$.

2.2 A dissymmetric Multiple Number Field Sieve

As any Index Calculus algorithm, the variant we propose follows three phases: the sieving phase, in which we create lots of relations involving only a small set of elements, the factor base ; the linear algebra, to recover the discrete logarithms of the elements of the factor base ; and the individual logarithm phase, to compute the discrete logarithm of an arbitrary element of the finite field.

We propose to sieve as usual on high degree polynomials $\phi(X) = a_0 + \cdots + a_{t-1}X^{t-1}$ with coefficients of size bounded by S. Let us recall that, given an integer y, an integer x is called *y-smooth* if it can be written as a product of prime factors less than y. We then collect all polynomials such that, first, the norm of $\phi(\theta_1)$ is B-smooth and, second, there exists (at least) one number field $\mathbb{Q}(\theta_i)$ with $i \geqslant 2$ in which the norm $\phi(\theta_i)$ is B'-smooth. In other simpler words, we create relations thanks to polynomials that cross over the diagram of Figure 3 in two paths: the one on the left side of the drawing and (at least) another one among those on the right. If we set that the factor base consists in the union of all the prime ideals in the rings of integers that have a B-or-B'-smooth norm, the smoothness bound depending on the number field, then we keep only relations that involve these factor base elements. Note that B and B' are two smoothness bounds possibly different from one another.

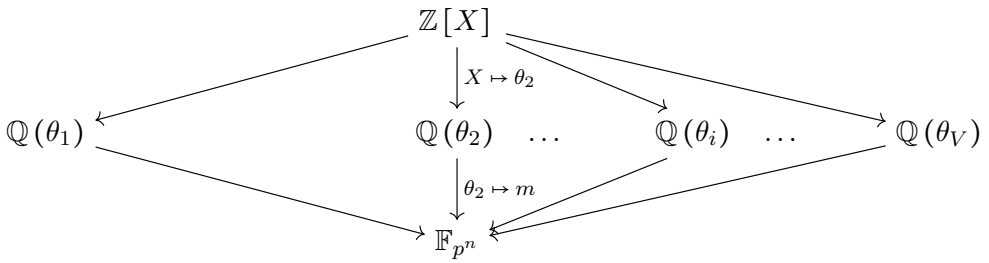

Figure 3: Commutative diagram for the dissymmetric Multiple Number Field Sieve with Conjugation Method

After the same post-processing as in [JLSV06] or as detailed in [BGGM14] more recently, each such polynomial ϕ yields a linear equation between "logarithms of ideals" coming from two number fields. Hence, from each relation we obtain a linear equation where the unknowns are the logarithms of ideals. Let us remark that by construction each equation only involves a small number of unknowns.

The sparse linear algebra and individual logarithm phases run exactly as in the classical Number Field Sieve of [JLSV06]. Even if there exists a specific way to manage the last phase with a multiple variant as detailed in [BP14], taking advantage of the large number of number fields again, we do not consider it here. In fact, the runtime of the classical individual logarithm phase is already negligible with regards to the total runtime of the algorithm, as proved by Barbulescu and Pierrot in their article.

3 Combining the Multiple Number Field Sieve with the General Joux-Lercier method

In 2003 Joux and Lercier [JL03] gave a polynomial selection to compute discrete logarithms in prime fields. Barbulescu, Gaudry, Guillevic and Morain propose in [BGGM14, Paragraph 6.2] to generalize this construction. Using again lattice reduction, they obtain an improvement on the asymptotic complexity in the boundary case where the characteristic can be written as $p = L_Q(2/3, c)$ for some specific c. We propose here to apply a Multiple variant of NFS to this construction in a very simple way.

Let us recall the General Joux-Lercier (GJL) method as presented in [BGGM14]. In order to compute discrete logarithms in the finite field $\mathbb{F}_{p^n}$, we first select an irreducible polynomial f_1 in $\mathbb{F}_p[X]$ with small coefficients (let us say of the size of $O(\log p^n)$) and such that it has an irreducible factor φ of degree n modulo p. We assume furthermore that this irreducible factor is monic. Let us write $\varphi = X^n + \sum_{i=0}^{n-1} \varphi_i X^i$ and $d+1$ the degree of f. Thus we have $d+1 > n$.[2] To assure that the second polynomial shares the same irreducible factor modulo p, we define it thanks to linear combination of polynomials of the form φX^k and pX^k. Lattice reduction permits then to obtain small coefficients. More precisely, we note M the following $(d+1) \times (d+1)$ matrix:

$$M = \underbrace{\begin{pmatrix} & & & & 1 \\ & & & \iddots & \varphi_{n-1} \\ & & 1 & \iddots & \vdots \\ & p & \varphi_{n-1} & & \varphi_0 \\ \iddots & & \vdots & \iddots & \\ p & & \varphi_0 & & \end{pmatrix}}_{n \text{ columns}} \underbrace{\qquad\qquad}_{d+1-n \text{ columns}} \begin{matrix} X^d \\ X^{d-1} \\ \vdots \\ X^{n-1} \\ \vdots \\ 1 \end{matrix}$$

A generator of this lattice of polynomials is represented in one column, meaning that each one of its coefficients is written in the row corresponding to the associated monomial (see indications on the right of the matrix). Clearly, the determinant of the lattice is p^n and its dimension is $d+1$. Hence, running the LLL algorithm on M gives a polynomial of degree at most d that has coefficients of size at most $p^{n/d+1}$ (assuming that $2^{(d+1)/4}$ stays small compared to $p^{n/d+1}$).

In a nutshell, we obtain two polynomials f_1 and f_2 that share a common degree n factor over $\mathbb{F}_p[X]$ and such that:

$$\begin{array}{ll} \deg f_1 = d+1 > n, & \|f_1\|_\infty = O(\log p^n), \\ \deg f_2 = d, & \|f_2\|_\infty = p^{n/(d+1)}. \end{array}$$

where $\|f_i\|_\infty$ denotes the largest coefficients of f_i in absolute value. This ends the GJL method. As in [BP14], we perform then linear combination of these two polynomials. Setting for all i from 3 to V:

$$f_i = \alpha_i f_2 + \beta_i f_3$$

[2] We emphasize that we require φ to be different from f_1 since we need that f_2 is not equal to f_1 mod p.

with α_i and β_i of the size of $\sqrt{V}$. Thus, for all $3 \leqslant i \leqslant V$, f_i has degree $d+1$ and coefficients of size $p^{n/(d+1)}$. Note that is is also possible to extract from the lattice reduction a second polynomial f_3 that has, as f_2, degree d and coefficients of size $p^{n/(d+1)}$. Making linear combination of f_2 and f_3 leads to polynomials of degree d instead of degree $d+1$. Yet, this little improvement has no impact on the asymptotic complexity of the algorithm.

As usual in this boundary case where $p = L_Q(2/3, c)$, we propose to sieve on degree 1 polynomials. We apply then a dissymmetric MNFS, as described in Section 2.2.

4 Asymptotic Complexity Analyses

We give now details about the asymptotic heuristic complexities we obtain with MNFS-CM in medium characteristic and with both MNFS-CM and MNFS-GJL in the boundary case between medium and high characteristics. Let us fix the notations. We write the extension degree n and the characteristic p of the target finite field $\mathbb{F}_Q$ as:

$$n = \frac{1}{c_p}\left(\frac{\log Q}{\log\log Q}\right)^{1-l_p} \quad \text{and} \quad p = \exp(c_p(\log Q)^{l_p}(\log\log Q)^{1-l_p})$$

with $1/3 \leqslant l_p \leqslant 2/3$. The parameters taking part in the heuristic asymptotic complexity analyses are: the sieving bound S, the degree of the polynomials we are sieving over $t-1$, the number of number fields V, the smoothness bound B related to the first number field and the smoothness bound B' related to the others number fields. The analyses of both MNFS-CM and MNFS-GJL work by optimizing the total runtime of the sieving and linear algebra phases while complying with two constraints.

Balancing the cost of the two first phases

We first require that the runtime of the sieving phase S^t equals the cost of the linear algebra. Since the linear system of equations we obtain is sparse, the cost of the linear algebra is asymptotically $(B + VB')^2$. Similarly to balancing the runtime of the two phases, we require that $B = VB'$. Thus, leaving apart the constant 4 that is clearly negligible with regards to the sizes of the parameters, the first constraint can be written as:

$$S^t = B^2. \tag{1}$$

Balancing the number of equations with the number of unknows

To be able to do the linear algebra phase correctly, we require that the number of unknows, that is approximately B, is equal to the number of equations produced in the sieving phase. If we note $\mathcal{P}$ the probability that a polynomial give a good relation then we want to have $S^t\mathcal{P} = B$. Combining it with the constraint (1), it leads to:

$$B = 1/\mathcal{P}.$$

4.1 Analysis of MNFS-CM in the medium characteristic case

We continue the analysis for the large range of finite fields where the characteristic can be written as $p = L_Q(l_p, c_p)$ with $1/3 \leqslant l_p < 2/3$. We consider here MNFS-CM as described in Section 2.

Evaluating the probability of smoothness

To evaluate the probability $\mathcal{P}$ we need to recall some tools about norms in number fields. For $f_i \in \mathbb{Z}[X]$ an irreducible polynomial, θ_i a complex root of f_i, and for any polynomial $\phi \in \mathbb{Z}[X]$, the norm $\mathrm{N}(\phi(\theta))$ satisfies $\mathrm{Res}(\phi, f_i) = \pm l_i^{\deg\phi}\,\mathrm{N}(\phi(\theta))$, where the term l_i is the leading coefficient of f_i. Since we treat l_i together with small primes,

we make no distinction in smoothness estimates between norms and resultants. We have the upper bound on the resultant:

$$|\operatorname{Res}(\phi, f_i)| \leq (\deg f_i + \deg \phi)! \cdot \|f_i\|_\infty^{\deg \phi} \cdot \|\phi\|_\infty^{\deg f_i}.$$

Thus, recalling that f_1 is of degree $2n$ and has constant coefficients and that every other polynomials f_i has degree n and coefficients of the size $\sqrt{p}$, we obtain that the norm of a sieving polynomial ϕ is upper-bounded by S^{2n} in the first number field and by $S^n p^{t/2}$ in every other number fields. To evaluate the probability of smoothness of these norms with regards to B and B', the main tool is the following theorem:

Theorem 1 (Canfield, Erdős, Pomerance [CEP83])**.** *Let $\psi(x, y)$ denote the number of positive integers up to x which are y-smooth. If $\epsilon > 0$ and $3 \leq u \leq (1-\epsilon)\log x/\log\log x$, then $\psi(x, x^{1/u}) = xu^{-u+o(u)}$.*

Yet, this result under this form is not very convenient. If we write the two integers x and y with the L_q-notation, we obtain a more helpful corollary:

Corollary 1. *Let $(\alpha_1, \alpha_2, c_1, c_2) \in [0,1]^2 \times [0,\infty)^2$ be four reals such that $\alpha_1 > \alpha_2$. Let $\mathcal{P}$ denote the probability that a random positive integer below $x = L_q(\alpha_1, c_1)$ splits into primes less than $y = L_q(\alpha_2, c_2)$. Then we have $\mathcal{P}^{-1} = L_q\left(\alpha_1 - \alpha_2, (\alpha_1 - \alpha_2)c_1 c_2^{-1}\right)$.*

So we would like to express both norms and sieving bounds with the help of this notation. As usual, we set:

$$t = \frac{c_t}{c_p}\left(\frac{\log Q}{\log\log Q}\right)^{2/3-l_p}, \quad S^t = L_Q(1/3, c_s c_t), \quad B = L_Q(1/3, c_b) \quad \text{and} \quad V = L_Q(1/3, c_v).$$

Thanks to this, we first remark that the first constraint can be rewritten as:

$$c_s c_t = 2c_b. \tag{2}$$

Besides, we apply the Corollary 1 to reformulate the second constraint. Let us note $L_Q(1/3, p_r)$ (respectively $L_Q(1/3, p_{r'})$) the probability to get a B-smooth norm in the first number field (respectively a B'-smooth norm in at least one other number field). The second constraint becomes $c_b = -(p_r + p_{r'})$. Using equation (2), the constants in the probabilities can be written as:

$$p_r = \frac{-2c_s}{3c_b} = \frac{-2(2/c_t)c_b}{3c_b} \qquad \text{and} \qquad p_{r'} = c_v - \frac{(2/c_t)c_b + c_t/2}{3(c_b - c_v)}.$$

That leads to require $c_b = -(-4/(3c_t) + c_v - (4c_b + c_t^2)/(6c_t(c_b - c_v)))$ and afterwards $6c_t(c_b^2 - c_v^2) = 8(c_b - c_v) + 4c_b + c_t^2$. Finally we would like to have:

$$(6c_t)c_b^2 - 12c_b - 6c_t c_v^2 + 8c_v - c_t^2 = 0. \tag{3}$$

Optimizing the asymptotic complexity

We recall that the complexity of our algorithm is given by the cost of the sparse linear algebra $L_Q(1/3, 2c_b)$, since we equalize the runtime of the sieving and linear algebra phases. Hence we look for minimizing c_b under the above constraint (3). The method of Lagrange multipliers indicates that c_b, c_v and c_t have to be solutions of the following system:

$$\begin{cases} 2 + \lambda(12c_t c_b - 12) = 0 \\ \lambda(-12c_v c_t + 8) = 0 \\ \lambda(6c_b^2 - 6c_v^2 - 2c_t) = 0 \end{cases}$$

with $\lambda \in \mathbb{R}^*$. From the second row we obtain $c_t = 2/(3c_v)$ and from the third one we get $c_b = (c_v^2 + 2/(9c_v))^{1/2}$. Together with equation (3), it gives the equation in one variable: $405c_v^6 + 126c_v^3 - 1 = 0$. We deduce that $c_v = ((3\sqrt{6} - 7)/45)^{1/3}$ and we recover

$c_b = ((9+4\sqrt{6})/15)^{1/3}$. Finally, the heuristic asymptotic complexity of the Multiple Number Field Sieve with Conjugation Method is, as announced:

$$L_Q\left(\frac{1}{3}, \left(\frac{8\cdot(9+4\sqrt{6})}{15}\right)^{1/3}\right).$$

This has to be compared with the Number Field Sieve with Conjugation Method proposed in [BGGM14] that has complexity $L_Q(1/3, (96/9)^{1/3})$. Note that our second constant is $(8(9+4\sqrt{6})/15)^{1/3} \approx 2.156$, whereas $(96/9)^{1/3} \approx 2.201$.

4.2 Analysis of MNFS-CM in the boundary case $p = L_Q(2/3, c_p)$

The analysis made in this case follows the previous one except for the fact that we have to reconsider the parameter t. We consider here a family of algorithms indexed by the degree $t-1$ of the polynomials of the sieving. We compute so the final complexity of each algorithm as a function of c_p (and t). Moreover, we underline that the round off error in t in the computation of the norms is no longer negligible.

Sieving on polynomials of degree $t-1$

Again, to easily evaluate the probability of smoothness of norms, we set the following parameters:

$$V = L_Q(1/3, c_v), \quad B = L_Q(1/3, c_b), \quad B' = L_Q(1/3, c_b - c_v) \quad \text{and} \quad S = L_Q(1/3, c_s).$$

With these notations, the first constraint becomes this time:

$$c_s t = 2c_b. \tag{4}$$

Moreover, the norms are upper-bounded by $S^{2n} = L_Q(2/3, 2c_s/c_p)$ in the first number field and by $S^n p^{(t-1)/2} = L_Q(2/3, c_s/c_p + c_p(t-1)/2)$ in all the other number fields. We apply the Canfield-Erdős-Pomerance theorem, and, with the same notation as in the previous paragraph, we obtain $p_r = -2c_s/(3c_b c_p)$ in one hand and $p_{r'} = c_v - (c_s/c_p + c_p(t-1)/2)/(3(c_b - c_v))$ in the other hand. Using equation (4), the second constraint $c_b = -(p_r + p_{r'})$ can be rewritten as $3tc_p(c_b - c_v)(c_b + c_v) = 4(c_b - c_v) + 2c_b + t(t-1)c_p^2/2$. As a consequence, we require:

$$(6tc_p)c_b^2 - 12c_b - 6tc_p c_v^2 + 8c_v - t(t-1)c_p^2 = 0. \tag{5}$$

As previously, we want to minimize $2c_b$ under the constraint (5). The method of Lagrange multipliers shows that we need that the derivative of $(6tc_p)c_b^2 - 12c_b - 6tc_p c_v^2 + 8c_v - t(t-1)c_p^2$ with respect to c_v is equal to 0. This leads to require that $c_v = 2/(3tc_p)$. Putting this value in equation (5) we get:

$$(18t^2c_p^2)c_b^2 - (36tc_p)c_b + 8 - 3t^2(t-1)c_p^3 = 0.$$

Finally, solving this equation in c_b we deduce that $c_b = (6+(20+6t^2(t-1)c_p^3)^{1/2})/(6tc_p)$. Consequently, the asymptotic complexity of the Multiple Number Field Sieve with Conjugation Method in this boundary case is:

$$L_Q\left(\frac{1}{3}, \frac{2}{c_p t} + \sqrt{\frac{20}{9(c_p t)^2} + \frac{2}{3}c_p(t-1)}\right)$$

where $t-1$ is the degree of the polynomials we are sieving on. Figure 4 compares our MNFS-CM with previous and various algorithms in this boundary case. For almost all variants of the Number Field Sieve presented in this figure (namely NFS, MNFS, NFS-CM and MNFS-CM), each hollow in the curve corresponds to a particular degree of the polynomials we are sieving on.

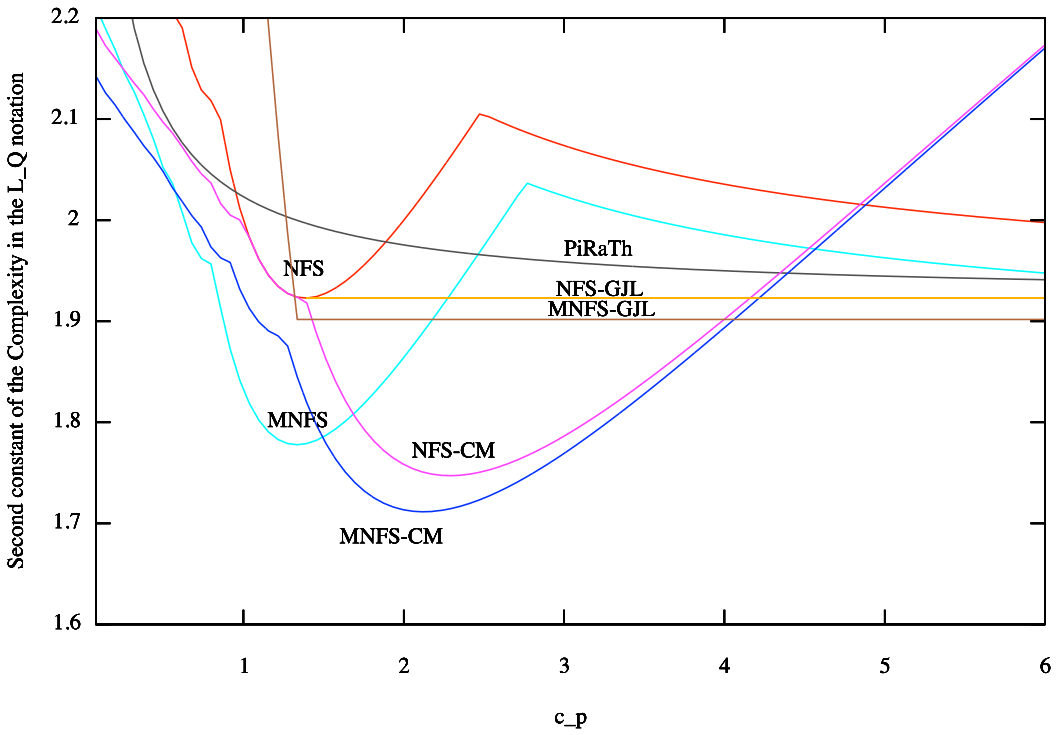

Figure 4: Asymptotic complexities $L_Q(1/3, C(c_p))$ in the boundary case, as a function of c_p with $p = L_Q(2/3, c_p)$. The dark blue curve represents the complexities obtained with our Multiple Number Field Sieve with Conjugation Method while the brown one represents the complexity of the Multiple Number Field Sieve with the General Joux-Lercier method (see next Section). The red, light blue, black, yellow and purple curves represent respectively the complexities of NFS [JLSV06], MNFS [BP14], PiRaTh, NFS-GJL [BGGM14] and NFS-CM [BGGM14].

Remark 1. *This boundary case has been the scene of various recent improvements but, as far as we know, all of them are not yet published nor available on the Internet. In particular, this is the case of the so-called PiRaTh algorithm, presented at the DLP conference in May 2014 by Pierrick Gaudry, Razvan Barbulescu and Thorsten Kleinjung. Yet, for the sake of comparison, we plot it together with already broadcast algorithms.*

The best asymptotic complexity of any variant of the Number Field Sieve: MNFS-CM on linear polynomials

According to Figure 4, sieving on linear polynomials seems to give the best complexity, as usual in this boundary case. Let us make a more precise analysis of the optimal case reached by our Multiple Number Field Sieve with Conjugation Method. We consider now c_p as a variable and we would like to find the minimal complexity obtained by each algorithm. Namely, we want to minimize:

$$C(c_p) = \frac{2}{c_p t} + \sqrt{\frac{20}{9(c_p t)^2} + \frac{2}{3} c_p (t-1)}.$$

The derivative of this function with respect to c_p vanishes when $2 \cdot 9\, t\, c_p (20/9(c_p\, t)^2 + (2/3)c_p(t-1))^{1/2} = -20 + 3(t-1)t^2 c_p^3$. This leads to the quadratic equation in c_p^3: $3^2 t^4 (t-1)^2 c_p^6 - 2^4 \cdot 3 \cdot 7\, t^2 (t-1) c_p^3 - 2^6 \cdot 5 = 0$. Thus, the optimal value comes when $c_p = 2 \cdot ((7+3\sqrt{6})/(3\, t^2 (t-1))^{1/3}$. We get for this value the minimal complexity:

$$L_Q\left(\frac{1}{3}, \left(\frac{3+\sqrt{3(11+4\sqrt{6})}}{(3^2 \cdot (7+3\sqrt{6}))^{1/3}}\right) \cdot \left(\frac{t-1}{t}\right)^{1/3}\right).$$

Looking at this formula, it is clear that the best possible complexity is obtained when $t = 2$, *i.e.* when we sieve on linear polynomials. Interestingly enough, we conclude that we have with our MNFS-CM the best complexity of any medium, boundary and high characteristics cases, which is:

$$L_Q\left(\frac{1}{3}, \frac{3+\sqrt{3(11+4\sqrt{6})}}{(2 \cdot 3^2 \cdot (7+3\sqrt{6}))^{1/3}}\right).$$

Note that the approximation of the second constant in the complexity is given by $(3+\sqrt{3(11+4\sqrt{6})}) \cdot (2 \cdot 3^2 \cdot (7+3\sqrt{6}))^{-1/3} \approx 1.71$. We get this complexity when p can be written as $p \approx L_Q(1/3, 2.12)$.

4.3 Analysis of MNFS-GJL in the boundary case $p = L_Q(2/3, c_p)$

In this setting, we recall that we propose to sieve on linear polynomials. As usual, we assume that $B = VB'$ where V is the number of number fields and B' is the smoothness bound relatively to the last $V-1$ number fields. Thus, the constraint given in Equation (1) leads to require that the sieving bound S is equal to the first smoothness bound B. With the same notations as previously, we also require that $B = 1/\mathcal{P}$. Finally, we emphasize that the polynomial selection proposed in Section 3 requires that $n < d+1$. If we set that:

$$d = \delta\left(\frac{\log Q}{\log\log Q}\right)^{1/3},$$

where δ is a parameter to define, then we have to keep in mind that our complexity results are valid provided $\delta \geqslant 1/c_p$.

Since f_1 has small coefficients and degree $d+1$ the norms in the first number field are upper-bounded by $L_Q(2/3, c_b\delta)$. The probability to get a B-smooth norm is though $L_Q(1/3, p_r)$ with $p_r = -\delta/3$. Similarly, the norms in the last $V-1$ number fields are bounded by $L_Q(2/3, c_b\delta + 1/\delta)$. The probability to get a B'-smooth norm in a least one number field is $L_Q(1/3, p_{r'})$ where $p_{r'} = -(c_b\delta + 1/\delta)/(c_b - c_v) + c_v$.

From $c_b = -(p_r + p_{r'})$ we get then:

$$\begin{aligned} & c_b + c_v = \frac{\delta}{3} + \frac{\delta^2 c_b + 1}{3\delta(c_b - c_v)} \\ \Leftrightarrow \quad & 3\delta(c_b^2 - c_v^2) = 2\delta^2 c_b - \delta^2 c_v + 1 \\ \Leftrightarrow \quad & 3\delta c_b^2 - 2\delta^2 c_b + \delta^2 c_v - 3\delta c_v^2 - 1 = 0. \end{aligned}$$

The method of Lagrange multipliers shows that we require:

$$\begin{cases} 3\delta c_b^2 - 2\delta^2 c_b + \delta^2 c_v - 3\delta c_v^2 - 1 = 0 \\ 3c_b^2 - 4\delta c_b + 2\delta c_v - 3c_v^2 = 0 \\ \delta^2 - 6\delta c_v = 0 \end{cases} \tag{6}$$

From the third line of System (6) we recover $\delta = 6c_v$. Substituting in the second line, we obtain $c_b^2 - 8c_v c_b + 3c_v^2 = 0$. Then, writing c_v as as function of c_b we get:

$c_v = ((4-\sqrt{13})/3)c_b$. Substituting the value of δ in the first line of the system gives $18c_v c_b^2 - 72c_v^2 c_b + 18c_v^3 - 1 = 0$, and, substituting again with the value of c_v we finally get: $c_b = (46+13\sqrt{13}/108)^{1/3}$. With this constant, we recover the value of δ which is $(4\sqrt{13}-14)^{1/3}$. Thus, as soon as:

$$c_p \geqslant \left(\frac{7+2\sqrt{13}}{6}\right)^{1/3},$$

which is approximately equal to 1.33, the complexity of the Multiple Number Field Sieve with the Generalized Joux-Lercier method is:

$$L_Q\left(\frac{1}{3}, \left(\frac{2\cdot(46+13\sqrt{13})}{27}\right)^{1/3}\right).$$

As expected, we recover the exact asymptotic complexity given by [BP14] when solving the discrete logarithm problem in high characteristic finite fields. This has to be compared with the asymptotic complexity of the classical Number Field Sieve with the Generalized Joux-Lercier method [BGGM14] in the same case which is $L_Q(1/3, (64/9)^{1/3})$. For the sake of comparison we recall that $(64/9)^{1/3} \approx 1.92$ whereas $(2(46+13\sqrt{13})/27)^{1/3} \approx 1.90$.

When $c_p < \left((7+2\sqrt{13})/6\right)^{1/3}$, from the constraint $\delta > 1/c_p$ we get $\delta > (4\sqrt{13}-14)^{1/3}$ and the previous simplification no longer applies. Yet, the equalities $c_b = 3c_v/(4-\sqrt{13}) = \delta/(2(4-\sqrt{13}))$ show that we minimize the complexity when $\delta = 1/c_p$. We obtain thus $c_b = (4+\sqrt{13})/(6c_p)$. Finally, when:

$$c_p < \left(\frac{7+2\sqrt{13}}{6}\right)^{1/3},$$

the asymptotic complexity of MNFS with the Generalized Joux-Lercier method is:

$$L_Q\left(\frac{1}{3}, \frac{4+\sqrt{13}}{3c_p}\right).$$

Figure 4 shows how this asymptotic complexity varies with c_p.

Acknowledgment

I would like to sincerely thank Taechan Kim for his careful proofreading.

References

[BGGM14] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improvements to the number field sieve for non-prime finite fields. INRIA Hal Archive, Report 01052449, 2014.

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *EUROCRYPT*, pages 1–16, 2014.

[BP14] Razvan Barbulescu and Cécile Pierrot. The multiple number field sieve for medium and high characteristic finite fields. *LMS Journal of Computation and Mathematics*, 17:230–246, 2014.

[CEP83] Earl Rodney Canfield, Paul Erdös, and Carl Pomerance. On a problem of Oppenheim concerning factorisatio numerorum. *Journal of Number Theory*, 17:1–28, 1983.

[Cop93] Don Coppersmith. Modifications to the number field sieve. *J. Cryptology*, 6(3):169–180, 1993.

[Gor93] Daniel M. Gordon. Discrete logarithms in *GF(P)* using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[JL03] Antoine Joux and Reynald Lercier. Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the gaussian integer method. *Math. Comput.*, 72(242):953–967, 2003.

[JLSV06] Antoine Joux, Reynald Lercier, Nigel P. Smart, and Frederik Vercauteren. The number field sieve in the medium prime case. In *CRYPTO 2006*, volume 4117, pages 326–344, 2006.

[Mat03] Dimitry V. Matyukhin. On asymptotic complexity of computing discrete logarithms over GF(p). *Discrete Mathematics and Applications*, 13(1):27–50, 2003.