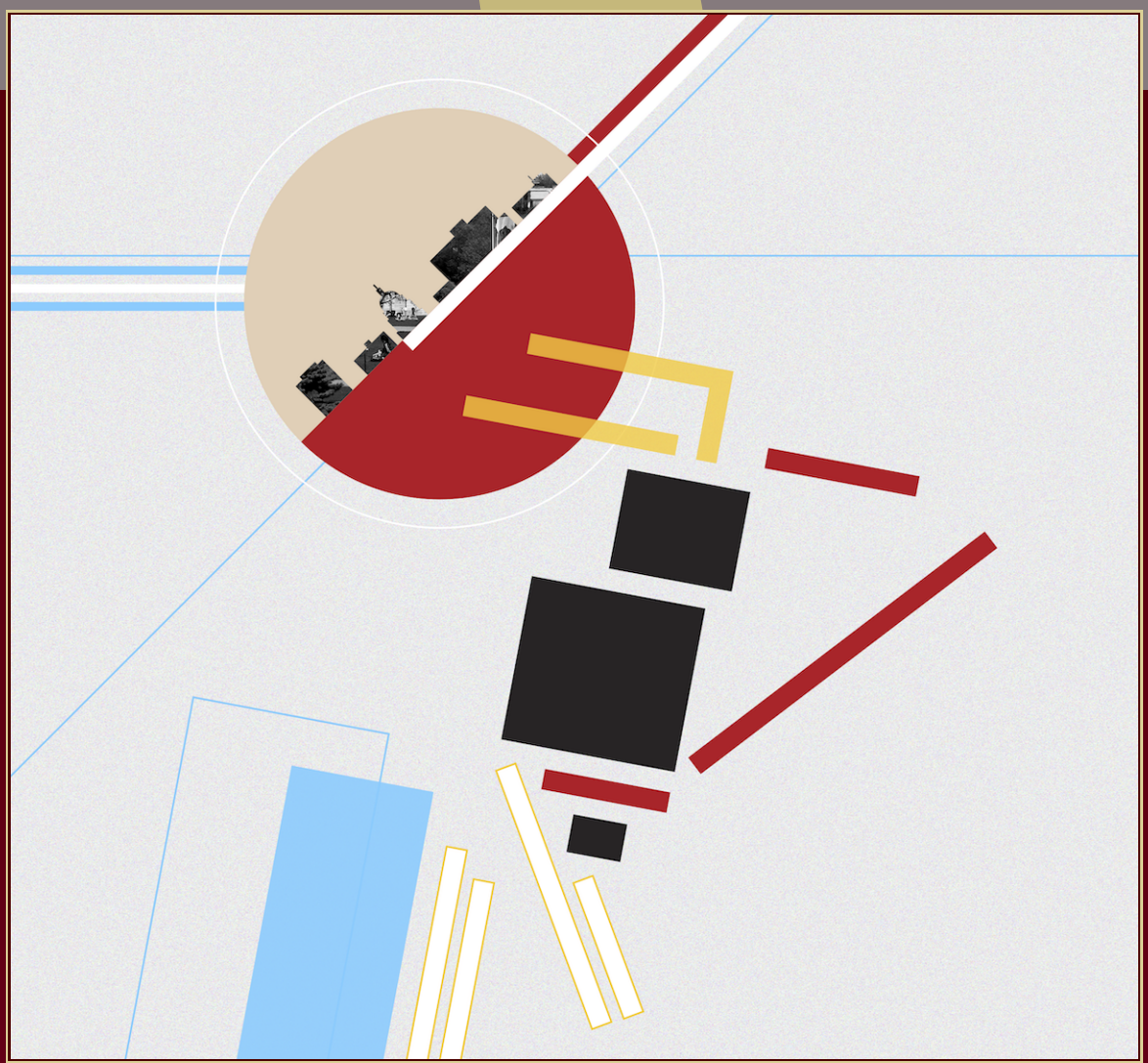
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Higher-dimensional sieving for the number field sieve algorithms

Laurent Grémy



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.275

msp

Higher-dimensional sieving for the number field sieve algorithms

Laurent Grémy

Since 2016 and the introduction of the exTNFS (extended tower number field sieve) algorithm, the security of cryptosystems based on nonprime finite fields, mainly the pairing- and torus-based ones, is being reassessed. The feasibility of the relation collection, a crucial step of the NFS variants, is especially investigated. It usually involves polynomials of degree 1, i.e., a search space of dimension 2. However, exTNFS uses bivariate polynomials of at least four coefficients. If sieving in dimension 2 is well described in the literature, sieving in higher dimensions has received significantly less attention. We describe and analyze three different generic algorithms to sieve in any dimension for the NFS algorithms. Our implementation shows the practicability of dimension-4 sieving, but the hardness of dimension-6 sieving.

1. Introduction

Nowadays, an important part of the deployed asymmetric cryptosystems bases its security on the hardness of two main number theory problems: the factorization of large integers and the computation of discrete logarithms in a finite cyclic group. In such a group $(G, \cdot)$ of order ℓ and generator g, the *discrete logarithm problem* (DLP) is, given $a \in G$, to find $x \in [0, \ell)$ such that $g^x = a$. Usual choices of group are groups of points on elliptic curves or multiplicative subgroups of finite fields.

In this article, we focus on discrete logarithms in finite fields of the form $\mathbb{F}_{p^n}$, where p is a prime and n is relatively small, namely the medium and large characteristics situation studied in [21]. Computing discrete logarithms in this type of field can affect torus-based [29; 36] or pairing-based [12] cryptography. The best-known algorithm to achieve computations in such groups is the *number field sieve* (NFS) algorithm. It has a subexponential complexity, often expressed with the $L(\alpha)$ notation $L_{p^n}(\alpha, c) = \exp[(c + o(1)) \log(p^n)^\alpha \log\log(p^n)^{1-\alpha}]$, where $\alpha = \frac{1}{3}$ for all the variants of NFS. For the general setting in medium characteristic, the first $L\left(\frac{1}{3}\right)$ algorithm was reached with $c = 2.43$ [21], improved to 2.21 [4] and now to 1.93 with exTNFS [23], the same complexity as NFS in large characteristic. In some specific context, exTNFS even reaches a lower complexity. However, theoretical complexities are not enough to estimate what a real attack would cost, since practical improvements can be hidden

Laurent Grémy was supported by the ERC Starting Grant ERC-2013-StG-335086-LATTAC. His work was started in the CARAMBA team of Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France and completed in the AriC team.
MSC2010: 11T71.
Keywords: discrete logarithm, finite fields, sieve algorithms, medium characteristic.

in the $o(1)$ term [1; 30; 7]. Experimental results are then needed to assess the concrete limits of known algorithms.

On the practical side, there has been a lot of effort to compute discrete logarithms in prime fields, culminating in a 768-bit record [27]. Although the records for $\mathbb{F}_{p^2}$ are smaller than the ones in prime fields, the computations turned out to be faster than expected [4]. However, when n is a small composite and p fits for $\mathbb{F}_{p^n}$ to be in the medium characteristic case (typically $n = 6$ [16] and $n = 12$ [18]), the records are smaller, even with a comparable amount of time spent during the computation. A way to fill the gap between medium and large characteristics is to implement exTNFS, since the computations in medium characteristic were, until now, performed with a predecessor of exTNFS.

Since exTNFS is a relatively new algorithm, there remain many theoretical and practical challenges to be solved before a practical computation can be reached. One of the major challenges concerns the sieve algorithms which efficiently perform the relation collection, one of the most costly steps of NFS. However, if there exist sieve algorithms in dimensions 2 and 3, these sieves are not efficient for higher dimensions and exTNFS needs to sieve in even dimension larger than or equal to 4.

Our contributions. We describe three new generic sieve algorithms which deal with any dimension, especially those addressed by exTNFS. Instantiating these algorithms in dimension 2 or 3 may allow to recover the existing sieve algorithms. Since these new sieves do not ensure completeness of the enumeration, unlike most of the existing sieve algorithms, we describe workarounds to ensure a trade-off between the completeness and the running-time efficiency. Finally, we analyze some quality criteria of these sieve algorithms and show the feasibility of sieving in dimension 4, but the hardness of dimension-6 sieving.

2. Overview of the NFS algorithms

Let ℓ be a large prime factor of the order $\Phi_n(p)$ of $\mathbb{F}_{p^n}^*$ that is coprime to $\Phi_k(p)$ for all prime factors k of n: the Pohlig–Hellman algorithm allows one to reduce the DLP in $\mathbb{F}_{p^n}^*$ to the DLP in all its subgroups, especially the one of order ℓ. The NFS algorithms can be split into four main steps: *polynomial selection*, *relation collection*, *linear algebra* and *individual logarithm*. The first step defines in a convenient way the field $\mathbb{F}_{p^n}$. The next two steps find the discrete logarithms of a subset of *small to medium* elements of $\mathbb{F}_{p^n}$, where sizes of the elements will be defined later. The last step computes the discrete logarithm of a *large* element of $\mathbb{F}_{p^n}$. The overall complexity of NFS is dominated by the relation collection and the linear algebra.

2A. ***Polynomial selection.*** Let $n = \eta\kappa$; the field $\mathbb{F}_{p^n}$ can be represented as a degree-κ extension of $\mathbb{F}_{p^\eta}$. Let h be an integer polynomial of degree η irreducible over $\mathbb{F}_p$ and ι be a root of h. Let $\mathbb{F}_{p^\eta}$ be defined by R/pR, where R is the ring $\mathbb{Z}[y]/h(y)$. There exist two ring homomorphisms from $R[x] = \mathbb{Z}[\iota][x]$ to $\mathbb{F}_{p^n}$; they involve a number field K_0 or K_1 defined by f_0 or f_1 respectively. The polynomials f_0 and f_1 are irreducible over R and share a common irreducible factor ϕ of degree κ modulo p. This setting allows one to define $\mathbb{F}_{p^n} = \mathbb{F}_{(p^\eta)^\kappa} \approx (R/pR)[x]/\phi(x)$. This provides the commutative diagram of Figure 1. The different polynomial selections defining f_0 and f_1 are given in Figure 2.

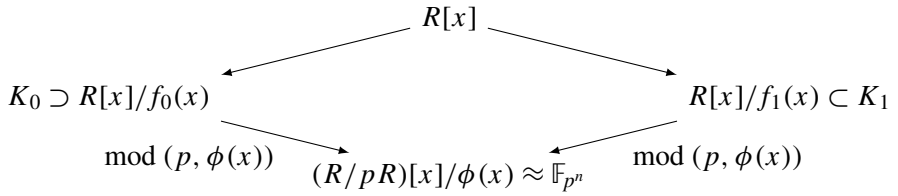


Figure 1. The NFS diagram to compute discrete logarithms in $\mathbb{F}_{p^n}$.

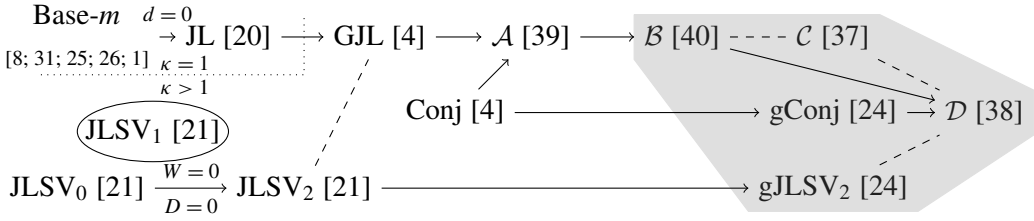


Figure 2. Polynomial selections: a link $a \to b$ means that a is a particular case of b (how to get a from b is written if this is not explicit in the articles); a dashed link means that the selection strategies in a and b strongly resemble each other. Polynomial selections in the gray area allow one to build polynomials with algebraic coefficients.

2B. ***Relation collection.*** Since the diagram of Figure 1 is the same for all the NFS variants, we use in the following the name NFS$_\eta$ to cover all the variants (see Table 1 for their names) or NFS when the parameter η does not matter.

2B1. *Relation.* A relation in NFS is given by a polynomial $a(x, y)$ in $R[x]$ of degree μ in x, often set to $\mu = 1$ to reach the best complexity (see Table 1), and $\eta - 1$ in y. Since there are $t = (\mu + 1)\eta$ coefficients to define a polynomial a, the relation collection is done in *dimension* t. A polynomial a gives a relation when the ideal factorizations of a mapped in both number fields involve prime ideals of norms smaller than two $L\left(\frac{1}{3}\right)$ smoothness bounds B_0 and B_1 respectively. Such ideals are elements of the so-called factor bases $\mathcal{F}_0$ and $\mathcal{F}_1$ respectively; see [21; 5; 23].

Since the factorization of a in prime ideals and the factorization of the norm of a are strongly linked, the relation collection looks for polynomials a of norms B_0-smooth in K_0 and B_1-smooth in K_1. To ensure the best probability of smoothness, the t-coefficients $\boldsymbol{a}$ of a are taken into a *t-search space* $\mathcal{S}$ containing $L\left(\frac{1}{3}\right)$ elements. Since an upper bound of the norm of a involves its infinity norm [6], the search spaces are usually cuboids of form $\mathcal{S} = [S_0^m, S_0^M) \times [S_1^m, S_1^M) \times \cdots \times [S_{t-1}^m, S_{t-1}^M)$, where $\mathbf{0}$ is in $\mathcal{S}$, all the $[S_i^m, S_i^M)$ are integer intervals and $S_i^M = -S_i^m$, where i is in $[0, t)$. Theoretically, all the

	$\kappa = 1$	$\kappa \geq 1$
$\eta = 1$	NFS	NFS-HD
$\eta \geq 1$	TNFS	exTNFS

	$\kappa = 1$	$\kappa \geq 1$
$\eta = 1$	$\mu = 1$	$\mu \geq 1$
$\eta \geq 1$	$\mu = 1$	$\mu = 1$

Table 1. The different variants of NFS. Left: names of the NFS variants. Right: optimal degrees.

S_i^M are equal but practically, the skewness of the polynomials f_0 and f_1 must be taken into account [31; 25; 26; 1], implying a skew search space. Since $-a$ and a give the same relation, $S_{t-1}^m = 0$. By abuse of notation, we denote by a both the polynomial and the list $\boldsymbol{a}$ of its t-coefficients.

2B2. *Practical considerations.* To ensure the best running time for the relation collection, the polynomials f_0 and f_1 must be chosen carefully. However, the two usual quality criteria, especially the α but also the Murphy-E functions [31], are only defined for NFS_1 and $\mu \leq 3$ [14]. Finding good polynomials for $\mathrm{NFS}_{>1}$, even by settling for integer coefficients to define f_0 and f_1, is yet a challenge.

The goal of the relation collection is to produce more relations than the number of ideals in both factor bases. A classical algorithm, used to analyze theoretically NFS, tests the smoothness of the norms of a in $\mathcal{S}$ by using the *elliptic curve method* (ECM) algorithm. However, if this algorithm is almost memory-free, the practical running time of such a task is prohibitive.

Instead, the common practical way is to perform ECM only on promising polynomials a, i.e., polynomials whose norms have many small factors. Finding these small factors is efficiently performed thanks to arithmetic sieve algorithms. However, sieve algorithms need a huge memory-footprint, since they need to store the norms of all the elements of $\mathcal{S}$. This problem was tackled in [33], allowing moreover a high-level parallelization, by considering many subsets of polynomials; in one number field, say K_0, the factorization into prime ideals of these polynomials involved at least an enforced ideal of medium size. Let $\mathfrak{Q}$ be such an ideal, called special-$\mathfrak{Q}$. Polynomials a such that $\mathfrak{Q}$ appears into their ideal factorization in K_0 are elements of a lattice, called $\mathfrak{Q}$-lattice, a basis of which is given by the rows of the matrix $M_\mathfrak{Q}$. To consider only polynomials fitting into $\mathcal{S}$, sieves look for elements $\boldsymbol{c}$ in the intersection of the $\mathfrak{Q}$-lattice and a t-search space $\mathcal{H} = [H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [0, H_{t-1}^M)$; a is obtained from $\boldsymbol{c}M_\mathfrak{Q}$. If theoretically $\mathcal{H}$ should depend on $\mathfrak{Q}$, it is often the same for all the special-$\mathfrak{Q}$s. In this intersection, sieve algorithms remove the contribution of small ideals. Let $\mathfrak{R}$ be such an ideal of prime norm r. Except for a tiny number of such ideals, a basis of the $\mathfrak{R}$-lattice in the $\mathfrak{Q}$-lattice can be of the form

$$\{(r,0,0,\ldots,0),(\lambda_{0,\mathfrak{Q},\mathfrak{R}},1,0,0,\ldots,0),(\lambda_{1,\mathfrak{Q},\mathfrak{R}},0,1,0,0,\ldots,0),\ldots,(\lambda_{t-2,\mathfrak{Q},\mathfrak{R}},0,0,\ldots,0,1)\} = \{\boldsymbol{b_0},\boldsymbol{b_1},\boldsymbol{b_2},\ldots,\boldsymbol{b_{t-1}}\}, \quad (1)$$

where the $\lambda_{i,\mathfrak{Q},\mathfrak{R}}$ are integers in $[0, r)$. Briefly, the different steps of the relation collection with the *special-$\mathfrak{Q}$-method* and sieving algorithms are as follows:

(1) For all the possible special-$\mathfrak{Q}$s:
  (a) For both sides i in [0, 1]:
    (i) Compute the norms $N_i[\boldsymbol{c}]$ of $a = \boldsymbol{c}M_\mathfrak{Q}$, where $\boldsymbol{c}$ is in $\mathcal{H}$.
    (ii) For all the ideals $\mathfrak{R}$ to be sieved, enumerate the elements $\boldsymbol{c}$ in $\mathcal{H} \cap \Lambda_{\mathfrak{Q}\mathfrak{R}}$ and remove the contribution of $\mathfrak{R}$ from $N_i[\boldsymbol{c}]$.
  (b) If both $N_0[\boldsymbol{c}]$ and $N_1[\boldsymbol{c}]$ are sufficiently small to have a chance to give a relation, factor the norms of a and report a if a gives a relation.

However, if there exist generic sieve algorithms in any dimension (see Section 3), they are not very efficient when $t \geq 4$, which especially arises with $\mathrm{NFS}_{>1}$. We propose algorithms for these cases in Section 4. Note that we will use the term sieve algorithms, but we only focus on the enumeration part of them, which is Step 1(a)ii without updating the array N_i. Step 1(a)i is briefly addressed in Section 5.

2C. ***Linear algebra and individual logarithm.*** Let θ_0 and θ_1 be roots of f_0 and f_1 respectively. Let a be a polynomial that gives a relation; i.e., $\langle a(\theta_k, \iota)\rangle = \prod_{\mathfrak{R}\in\mathcal{F}_k} \mathfrak{R}^{\mathrm{val}_{\mathfrak{R}}(a(\theta_k,\iota))}$, where k is in $[0, 1]$ and val denotes the valuation: the factorizations of the norms of a must be translated into such a factorization of ideals [9]. A relation can be transformed into a linear relation involving the virtual logarithms (vlog) of the ideals [42]. To be valid, this linear relation must involve the Schirokauer maps ϵ_k [41], as $\sum_{\mathfrak{R}\in\mathcal{F}_0} \mathrm{val}_{\mathfrak{R}}(a(\theta_k, \iota))\,\mathrm{vlog}(\mathfrak{R}) + \epsilon_0(a) = \sum_{\mathfrak{R}\in\mathcal{F}_1} \mathrm{val}_{\mathfrak{R}}(a(\theta_k, \iota))\,\mathrm{vlog}(\mathfrak{R}) + \epsilon_1(a) \bmod \ell$. In this equation, the virtual logarithms are unknowns, the valuations are small integers and the Schirokauer maps are large integers, close to ℓ. These large elements negatively impact the usual algorithms to solve sparse systems, but the cost of these heavy parts can be significantly decreased thanks to a modification of the block Wiedemann algorithm [10; 22; 13].

The last step of the computation is the computation of a large, say $L(1)$, unknown logarithm. This computation is achieved by rewriting the (virtual) logarithm of the target in terms of logarithms of smaller elements; these smaller elements are again rewritten in terms of smaller elements until the logarithm of the target has been rewritten using only the precomputed logarithms given by the relation collection and the linear algebra. This *descent step* uses different algorithms depending on the size of the rewritten element: the target is rewritten in elements up to $L\left(\frac{2}{3}\right)$ thanks to the so-called initial splitting (booting step) [34; 20; 2; 17; 45]; for elements in $\left[L\left(\frac{1}{3}\right), L\left(\frac{2}{3}\right)\right)$, the special-$\mathfrak{Q}$-method is used. The theoretical analysis of [13, Appendix A.2] shows that the descent by special-$\mathfrak{Q}$ may be more efficient by considering polynomials of degree not restricted to $\mu = 1$.

3. A framework to study existing sieve algorithms

Let $\mathfrak{Q}$ be a special-$\mathfrak{Q}$ and $\mathfrak{R}$ be an ideal to be sieved such that the lattice $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ is given by a basis as in (1).[1] There exist different sieve algorithms proposed for NFS that allow one to enumerate the elements in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and a search space $\mathcal{H}$. Their efficiency depends on the dimension of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and the density of the lattice in $\mathcal{H}$. This density is formally defined thanks to the *level* of a sieve algorithm in Definition 3.1, a key notion for the rest of the description and especially for Section 4. All the existing sieve algorithms used in NFS are reported in Table 2. These algorithms can be described by the following two-step algorithm. The vectors produced in Step (2) will be called *transition-vectors*:

(1) Compute an adapted set $\mathcal{B}$ of spanning vectors of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ with respect to $\mathcal{H}$.

(2) Start from $\mathbf{0}$ and use the vectors of $\mathcal{B}$ or an (often small) linear combination of them to enumerate elements in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$.

[1] Sieve algorithms can deal with other basis shapes of lattices, but this one occurs the most.

Definition 3.1 (level). Let Λ be a lattice and $\mathcal{H}$ be a search space. The level of a sieve algorithm with respect to Λ and $\mathcal{H}$ is the minimal integer value $\ell < t$ such that the intersections of the cuboids $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [H_\ell^m, H_\ell^M) \times \{c_{\ell+1}\} \times \{c_{\ell+2}\} \times \cdots \times \{c_{t-1}\}$, where $(c_{\ell+1}, c_{\ell+2}, \ldots, c_{t-1})$ are in $[H_{\ell+1}^m, H_{\ell+1}^M) \times [H_{\ell+2}^m, H_{\ell+2}^M) \times \cdots \times [H_{t-1}^m, H_{t-1}^M)$, and the lattice Λ contains more than one element on average. In the case when $\mathcal{H}$ contains less than one element on average, $\ell = t - 1$.

3A. ***Exhaustive sieve algorithms.*** The first use of a sieve algorithm in an index calculus context is attributed to Schroeppel and was successfully used by Pomerance [35; 28]. They used the 1-dimensional sieve of Eratosthenes as a factoring algorithm instead of a prime-detecting one. It was extended to any dimension and called *line sieve*; see for example its use in dimension 3 in [44]. In dimension 2, the line sieve is known to be inefficient when there is at most one element in a line, an intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $[H_0^m, H_0^M) \times \{c_1\}$ where c_1 is in $\mathbb{Z}$: the 0-level line sieve is used as a 1-level sieve algorithm. Pollard designed in this sense the *sieve by vectors* [33], now subsumed by the *lattice sieve* of Franke and Kleinjung [11]. Based on this sieve algorithm, the *plane sieve* [14] and the *3-dimensional lattice sieve* [19] were proposed for similar densities in three dimensions. The plane sieve was turned into a generic sieve algorithm in CADO-NFS [43] (see Section 4D).

The completeness of all these sieve algorithms comes from special procedures that compute transition-vectors. They are defined thanks to the *t-extended search spaces*: let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space; the t-extended search space $\mathcal{H}_k$ is the set $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [H_k^m, H_k^M) \times \mathbb{Z}^{t-(k+1)}$.

Definition 3.2 (transition-vector). Let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space. A k-transition-vector is an element $\boldsymbol{v} \neq \mathbf{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in the intersection of Λ and the t-extended search space $\mathcal{H}_k$, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the last $t - 1 - k$ coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is the smallest possible larger than $\boldsymbol{c}[k]$.

With such sieve algorithms, the small factors of both norms of all the considered polynomials a are known: this allows one to be close to the expected number of relations at the end of the relation collection. But, the number of relations is not the only efficiency criterion of the relation collection. Indeed, in dimension 2, the lattice sieve is used since it allows one to maintain the same number of relations but decrease the time per relation. The same occurs in dimension 3, switching from the line to the plane or the 3-dimensional lattice sieves. However, these sieves have some drawbacks, highlighted when there is less than one element on average in each plane $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \{c_2\}$, where c_2 is in $[H_2^m, H_2^M)$. The plane sieve is essentially the use of the lattice sieve on each plane: even if there is no element in a plane, the lattice sieve is used to report nothing instead of using it only on nonempty planes. There is no alternative to avoid these useless uses without losing completeness. The 3-dimensional lattice sieve does not have this drawback, but the procedure to generate the spanning list $\mathcal{B}$ and the one to enumerate seem difficult to analyze and may be costly for skewed lattices or skewed search spaces.

3B. ***Heuristic sieve algorithms.*** Because of these drawbacks and especially the penalty in terms of running time, the designers of the plane sieve proposed a heuristic sieve algorithm, the *space sieve* [14]. Its

	line sieve	lattice sieve [11]	3-dimensional lattice sieve [19]	plane sieve [14]	space sieve [14]	this work
$t=2$	✓	✓	✗	✗	✗	✓
$t=3$	✓	✗	✓	✓	✓	✓
$t>3$	✓	✗	✗	✓	✗	✓
level	$\ell=0$	$\ell=1$	$\ell=1$ and $\ell=2$	$\ell=1$	$\ell=2$	any
completeness of enumeration	✓	✓	✓	✓	✗	✗

Table 2. Characteristics of the sieve algorithms proposed for NFS.

use allows one to decrease the running time by 45% for the 240-bit example of [14], while at the same time lose less than 6% of the relations. This corresponds to decreasing the time per relation by 42%.

The space sieve focuses on enumerating a large portion of the elements instead of all of them, which is helpful for multiple reasons. First, all the sieve algorithms, both exhaustive and heuristic, allow one to enumerate the t-extended search space $\mathcal{H}_{t-2}$ instead of the search space $\mathcal{H} = \mathcal{H}_{t-1}$. For exhaustive sieves, it implies that the spanning set $\mathcal{B}$ is qualitatively too accurate because it allows one to generate transition-vectors that will never be used. If this accuracy implies a costly computation to find an adapted set $\mathcal{B}$, the time per relation can be drastically impacted. Secondly, completeness is not always useful, since this reports hits on polynomials a that may or may not give relations; missing some hits may not affect the number of relations in some circumstances. Furthermore, if the computation can be completed, the expected gain in the time per relation must be considered to compare heuristic and exhaustive sieves, even if the relation collection misses some relations. Finally, in dimension larger than 3, the use of a heuristic sieve seems unavoidable; to the best of our knowledge, producing all the transition-vectors can only be done by the exhaustive sieve algorithms, all of them being inefficient when there is less than one element in $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times [H_2^m, H_2^M) \times \{c_3\} \times \{c_4\} \times \cdots \times \{c_{t-1}\}$, where c_i is in $[H_i^m, H_i^M)$. Yielding to produce some transition-vectors can be done by computing the Graver basis of the lattice: these transition-vectors may lead to building a generic exhaustive sieve algorithm from the heuristic one described in Section 4. However, computing the Graver basis is often too costly in our context [15; 32].

In the following, we propose `globalntv`, `localntv` and `sparsentv`, three heuristic sieves which perform the enumeration in any dimension and level.

4. Sieve algorithms in higher dimensions

Using transition-vectors implies the sieve enumerations are exhaustive. Since completeness is not the main target of `globalntv`, `localntv` and `sparsentv`, the vectors used in Step (2) of Section 3, called here *nearly-transition-vectors*, will be weakened by removing from Definition 3.2 the strong condition about $\boldsymbol{d}[k]$.

Definition 4.1 (nearly-transition-vector). Let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space. A k-nearly-transition-vector is an element $\boldsymbol{v} \neq \boldsymbol{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in the intersection

of Λ and the t-extended search space $\mathcal{H}_k$, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the last $t-1-k$ coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is larger than $\boldsymbol{c}[k]$.[2]

The three generic sieve algorithms will take place in a general framework, described by allowing the report of duplicated elements for simplicity in Algorithm 1. It is purposely vague, to be as general as possible: instantiation examples of Initialization, Step (c) and Step (d) will be given in the following.

The addition of a possible nearly-transition-vector (Step (c)) is likewise performed for all the three sieve algorithms. Like the addition of a 2-nearly-transition-vector in the space sieve [14], a loop iterates the list of k-nearly-transition-vectors, beforehand sorted by increasing coordinate k (see Section 4C). We also choose to use the same fall-back strategy (Step (d)); this choice is justified in Section 4B. Therefore, the difference between the three sieve algorithms only comes from the initialization processes, described in Section 4A.

4A. ***Initializations.*** To define the three initialization processes, we introduce two new notions: the *shape* of the nearly-transition-vectors and the *skew-small-vectors*.

4A1. *Preliminaries.* Even if the three initialization processes are different, the shapes of the nearly-transition-vectors are the same. The shape represents the expected magnitude of the coefficients of the nearly-transition-vectors with respect to a search space $\mathcal{H}$ and $\Lambda_{\mathfrak{QR}}$. In this paragraph, the $O(j)$ notation will denote a value smaller than or almost equal to j. Let us recall the shape of the transition-vectors of the ℓ-level sieve algorithms in three dimensions. Let I_i be the length of the interval $[H_i^m, H_i^M)$. When $\ell = 0$, the shape is equal to $(O(r), O(1), O(1))$; the one for $\ell = 1$ is $(O(I_0), O(r/I_0), O(1))$; the one for $\ell = 2$ is $(O(I_0), O(I_1), O(r/(I_0 I_1)))$. This shape is generalized, as $(I_0, I_1, \ldots, I_{\ell-1}, r/(I_0 \times I_1 \times \cdots \times I_{\ell-1}), 1, 1, \ldots, 1)$, given a level ℓ of a sieve algorithm and removing the $O(\cdot)$ for clarity.

The initialization processes of the three sieve algorithms do not ensure that the produced vectors are nearly-transition-vectors. They build skew-small-vectors, that are lattice vectors whose coefficients try to follow the shape. Even if Definition 4.2 does not capture it, skew-small-vectors are built to be almost nearly-transition-vectors: a k-skew-small-vector $\boldsymbol{v}$ is a k-nearly-transition-vector if $|\boldsymbol{v}[i]| < I_i$.

Definition 4.2 (skew-small-vector). Let k be in $[0, t)$. A k-skew-small-vector is an element $\boldsymbol{v} \neq \boldsymbol{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in Λ, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the last $t-1-k$ coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is larger than $\boldsymbol{c}[k]$.

4A2. *Three initialization processes.* The three initialization processes try to generate a large number of nearly-transition-vectors, given the level ℓ of the sieve algorithms. They begin by building a basis $\mathcal{B}$ of $\Lambda_{\mathfrak{QR}}$ whose basis vectors are skew-small-vectors. Nearly-transition-vectors are afterwards built thanks to small linear combination of the basis vectors. The major difference between `globalntv` on the one hand, and `localntv` and `sparsentv` on the other, is in the coefficients of the k-skew-small-vectors,

[2]Note that transition vectors of [14, Definition 5] are 2-nearly-transition-vectors.

Initialization: Call a procedure that returns nearly-transition-vectors with respect to a search space $\mathcal{H}$ and a lattice $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ described as in (1).

Set $\boldsymbol{c}$ to $\mathbf{0}$ and k to $t-1$.

Enumeration:

(1) While $\boldsymbol{c}[k] < H_k^M$:
   (a) Report $\boldsymbol{c}$.
   (b) If $k > 0$, call this enumeration procedure recursively with inputs $\boldsymbol{c}$ and $k-1$.
   (c) Find a k-nearly-transition-vector $\boldsymbol{v}$ from the one computed during Initialization, such that adding $\boldsymbol{v}$ to $\boldsymbol{c}$ lands in the extended search space $\mathcal{H}_{k-1}$ and $\boldsymbol{c}[k]$ is the smallest possible.
   (d) If there does not exist such a k-nearly-transition-vector $\boldsymbol{v}$, call a *fall-back strategy* that tries to produce a new element $\boldsymbol{c}$ in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$, and therefore a new k-nearly-transition-vector.

(2) Recover $\boldsymbol{c}$ as it was when the procedure was called.

(3) While $\boldsymbol{c}[k] \geq H_k^m$, perform Steps (a)–(d) by considering $\boldsymbol{c} - \boldsymbol{v}$ instead of $\boldsymbol{c} + \boldsymbol{v}$.

Algorithm 1. Framework for `globalntv`, `localntv` and `sparsentv`.

where $k > \ell$. In `localntv` and `sparsentv`, the coordinate k is enforced to 1, and even to 0 for the coordinates $\ell + 1$ to $k - 1$ in `sparsentv`. This comes from a crude interpretation of the magnitude of the coefficients given by the shape. To build the k-skew-small-vectors, where $k \leq \ell$ for `localntv` and `sparsentv` or all of them for `globalntv`, the initialization processes compute a skew basis of a (sub)lattice, which is a basis formed by skew-small-vectors. The basis $\mathcal{B}$ is built thanks to

- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{t-1}}\}$ for `globalntv`;
- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ followed by, for k in $[\ell+1, t)$, a reduction of $\boldsymbol{b_k}$ by its closest vector in $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ for `localntv`;
- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ followed by, for k in $[\ell+1, t)$, a reduction of $\boldsymbol{b_k}$ by its closest vector in $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ for `sparsentv`.

To build possible nearly-transition-vectors, linear combinations of the skew basis vectors are performed, as well as computations of some vectors close to $\boldsymbol{b_k}$ in the corresponding sublattice instead of one for `localntv` and `sparsentv`. The patterns of the skew-small-vectors produced by the different initializations follow necessarily the ones reported in Table 3. Note that, when $\ell = t - 2$, `localntv` and `sparsentv` have the same initialization processes. When $\ell = t - 1$, the three initialization processes are the same.

4B. ***A common fall-back strategy.*** At this step, all the additions to $\boldsymbol{c}$ in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$ of a k-nearly-transition-vector fail to land in $\mathcal{H}_{k-1}$. The additions of $\boldsymbol{v}$, a k-skew-small-vector, are necessarily out of $\mathcal{H}_{k-1}$. Since no k-skew-small-vector makes it possible to stay in $\mathcal{H}_{k-1}$, a potential k-nearly-transition-vector must have some smaller coordinates. Vectors close to $\boldsymbol{c} + \boldsymbol{v}$ in the sublattice formed by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ may

k	`globalntv`	`localntv`	`sparsentv`
0	$(>0,0,0,0,0)$	$(>0,0,0,0,0)$	$(>0,0,0,0,0)$
1	$(\cdot,>0,0,0,0)$	$(\cdot,>0,0,0,0)$	$(\cdot,>0,0,0,0)$
2	$(\cdot,\cdot,>0,0,0)$	$(\cdot,\cdot,>0,0,0)$	$(\cdot,\cdot,>0,0,0)$
3	$(\cdot,\cdot,\cdot,>0,0)$	$(\cdot,\cdot,\cdot,1,0)$	$(\cdot,\cdot,\cdot,1,0)$
4	$(\cdot,\cdot,\cdot,\cdot,>0)$	$(\cdot,\cdot,\cdot,\cdot,1)$	$(\cdot,\cdot,\cdot,0,1)$

Table 3. Patterns of the k-skew-small-vectors, where $\ell = 2$ and $t = 5$.

make it possible from $\boldsymbol{c}+\boldsymbol{v}$ to obtain such a k-nearly-transition-vector. Let $\boldsymbol{e}$ be such a vector; subtracting $\boldsymbol{e}$ from $\boldsymbol{c}+\boldsymbol{v}$ will shrink the k first coefficients of $\boldsymbol{c}+\boldsymbol{v}$. If $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in the search space, $\boldsymbol{v}-\boldsymbol{e}$ is a new k-nearly-transition-vector. If not, set $\boldsymbol{c}$ to $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ and rerun this procedure, until $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in $\mathcal{H}$ or its coordinate k is larger than H_k^M. The different steps of this fall-back strategy are, for $\boldsymbol{c}$ in $\Lambda_{\mathfrak{QR}} \cap \mathcal{H}$ and k in $[0, t)$:

(1) While $\boldsymbol{c}[k] < H_k^M$:
  (a) For all k-skew-small-vectors $\boldsymbol{v}$:
    (i) Compute some vectors close to $\boldsymbol{c}+\boldsymbol{v}$ in the sublattice generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ and store them in the list E.
    (ii) For all $\boldsymbol{e}$ in E, return $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ if $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ is in $\mathcal{H}$.
  (b) Set $\boldsymbol{c}$ to one of the vectors $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ computed previously.
(2) Return fail.

If this procedure does not fail, the new element in $\mathcal{H}$ is the output of this procedure and $\boldsymbol{v}-\boldsymbol{e}$ is the new k-nearly-transition-vector, computed by the difference between the output and the input vectors of the fall-back procedure and inserted in the lists of k-nearly-transition-vectors and k-skew-small-vectors for further use.

This fall-back strategy is costly since it requires solving multiple closest vector problems in Step (ai), iterating all the k-skew-small-vectors and looping while H_k^M is not reached. The condition to use such a strategy must therefore be carefully studied. If $k \leq \ell$, the average number of elements with the same last $t-k-1$ coordinates is equal to 1, from the Definition 3.1 of the level. If no precomputed k-nearly-transition-vectors allow one find a new element in $\mathcal{H}$, then, most likely, there do not exist such elements. However, if $k > \ell$, there are generally more chances that such an element exists. The fall-back strategy is therefore applied only when $k > \ell$. This condition must be studied a little bit more carefully. If $\ell = t-1$, the first $t-1$ coordinates of $\boldsymbol{c}+\boldsymbol{v}$ out of $\mathcal{H}$ must be shrunk, where $\boldsymbol{v}$ is a ℓ-skew-small-vector. Therefore, when $k = t-1$, the close vector $\boldsymbol{e}$ is a linear combination of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{t-2}}\}$. Since this strategy allows one to modify the maximal number of coordinates without changing the last nonzero one, the strategy allows one to increase the chance of finding a new element. Another strategy is proposed in Section 4D, but is specific to `sparsentv`.

4C. ***Formal algorithms.*** The pseudocode of the addition of a nearly-transition-vector and the fall-back strategy are given respectively in Function `add` and in Function `fbadd`. They return an element in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$ or an element out of $\mathcal{H}$ to stop the enumeration of a subset of $\mathcal{H}$. The lists T and S consist of t lists containing respectively nearly-transition-vectors and skew-small-vectors (e.g., k-nearly-transition-vectors are stored in $T[k]$). Each list $T[k]$ and $S[k]$ is sorted by increasing coordinate k. Given an element $\boldsymbol{c}$ of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and an integer i, the function `CVA` (close vectors around a targeted element) returns a list of some lattice vectors close to $\boldsymbol{c}$ in the sublattice of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_i}\}$.

```
FUNC. add(c, k, H, T, S, Λ_QR, ℓ)
for v ∈ T[k] do
    if c + v ∈ H_{k−1} then
        return c + v;
if k > ℓ or k = t − 1 then
    e ← fbadd(c, k, H, S, Λ_QR);
    if e ∈ H then
        T[k] ← T[k] ∪ {e − c};
        S[k] ← S[k] ∪ {e − c};
    c ← e;
else
    c ← (H_0^M, H_1^M, ..., H_{t−1}^M);        // ∉ H
return c;
```

```
FUNC. fbadd(c, k, H, S, Λ_QR)
while c[k] < H_k^M do
    L ← ∅;
    for v ∈ S[k] do
        E ← CVA(c + v, k − 1, Λ_QR);
        for e ∈ E do
            if c + v − e ∈ H then
                return c + v − e;
            L ← L ∪ {c + v − e};
    set c to an element of L;
return c;                                      // ∉ H
```

4D. ***A specific fall-back strategy.*** Unlike the previous fall-back strategy, we describe here a specific one which allows one to recover all the sieve algorithms of Section 3. This specific fall-back strategy is designed for `sparsentv` by exploiting the specific patterns of the skew-small-vectors of `sparsentv`. It can be more costly but can report a larger number of elements. To completely recover exhaustive sieve algorithms, the k-skew-small-vectors used in the sieve algorithms must have their coordinate k equal to 1, when $k > \ell$.

When the fall-back strategy is called, the coefficients of $\boldsymbol{c}+\boldsymbol{v}$, where $\boldsymbol{c}$ is in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$ and $\boldsymbol{v}$ is a k-skew-small-vector, are shrunk with vectors close to $\boldsymbol{c}+\boldsymbol{v}$ in the sublattice generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ instead of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$, to keep unchanged the coordinates $\ell+1$ to $t-1$ of $\boldsymbol{c}+\boldsymbol{v}$. Let $\boldsymbol{e}$ be a vector subtracted from $\boldsymbol{c}+\boldsymbol{v}$ to shrink its coefficients. If $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in $\mathcal{H}$, a new element in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$ is found, as well as a new k-nearly-transition-vector.

If $k > \ell + 1$, the coordinates $\ell + 1$ to $k - 1$ of $\boldsymbol{c}$ have not been modified, and therefore, some cuboids of dimension $\ell + 1$ were not explored to try to find a new starting point: to explore them, this procedure must be called with inputs one of the vectors generated previously and $k - 1$. If all the recursions fail to find a new element in the intersection of the lattice and the search space, $\boldsymbol{c}$ is set to $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ and this procedure is redone with inputs $\boldsymbol{c}$ and k, until a generated element fits in $\mathcal{H}$ or its coordinate k is larger

than H_k^M. The different steps of this generation are the same as the ones described in Section 4B, except that after Step (b), the following instruction is added:

(1) While $\boldsymbol{c_t}[k] < H_k^M$:

⋮

(c) If $k-1 > \ell$, use this fall-back procedure (additive or subtractive case) with $\boldsymbol{c}$ and $k-1$ as inputs and return the result if it does not fail.

(2) Return fail.

5. Analyses of the generic sieves

Practical generic sieve algorithms are of two types: exhaustive for the levels $\ell = 0$ and $\ell = 1$, and heuristic for all levels.[3] For levels $\ell = 0$ and $\ell = 1$, using heuristic algorithms makes almost no sense, since generally, the exhaustive algorithms are optimal in term of running time. For larger levels, the practical gain obtained by using the space sieve lets us expect an improvement since exhaustive sieves are not adapted to such levels. However, heuristic sieves do not ensure completeness of the enumeration: if substantially many relations are not reported, the time per relation can negatively be impacted and can eventually be worse than with exhaustive sieves.

To evaluate the practicability of the three new sieve algorithms, we analyze them thanks to a Sage implementation of the three sieves named `ntv.sage` (provided in CADO-NFS), mainly implemented to test the accuracy of the enumeration processes; see Section 5A. Even if the implementation is not optimized to test running time, we can extrapolate some tendencies about the efficiency of the sieves; see Section 5B. The practical experiments were done on random lattices[4] having the shape of (1), whose volume is adapted to fit for the tested levels.

5A. ***Accuracy.*** The quality criteria to test accuracy reported in Table 4 are

- the number of produced skew-small-vectors, adjusted thanks to the number of the small linear combinations and close vectors,
- the number of iterations of the while loop in the fall-back strategy and
- the relative error between the expected number of elements to be enumerated ($\#\mathcal{H}/r$) and the number of reported elements.

The relative error informs about the accuracy of the algorithm. A large relative error likely means that the nearly-transition-vectors have coordinates that are too large. A few more linear combinations during the initialization may solve this problem. The criterion about the fall-back strategy informs about the

[3]Combining the 3-dimensional lattice sieve [19] and Section 4D may lead to obtaining a 2-level exhaustive generic sieve algorithm, but we did not manage to fully implement the 3-dimensional lattice sieve.

[4]From the point of view of a practical sieving procedure, lattices describing ideals of the same or different factor bases, or random lattices, are treated similarly.

	`globalntv` (ℓ=2)				`localntv` (ℓ=2)				`globalntv` (ℓ=3)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
#ssvs	40				41				40			
#fbs	0	2.0	61	3.1	0	3.0	61	4.3	0	12.0	65	20.0
rel. err.	0.0	2.6	95.7	10.1	0.0	1.2	96.7	5.8	0.0	0.0	75.0	2.0

(A) Experiments on 2^{14} lattices where $\mathcal{H} = [-2^6, 2^6)^3 \times [0, 2^6)$ ($t = 4$, $\#\mathcal{H} = 2^{27}$).

	`globalntv` (ℓ=2)				`localntv` (ℓ=2)				`sparsentv` (ℓ=2)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
#ssvs	364				69				37			
#fbs	0	5.0	712	18.3	0	9.0	591	20.0	0	13.0	332	22.0
rel. err.	0.0	1.5	36.1	6.4	0.0	1.6	50.0	5.6	0.0	2.0	49.0	5.9

(B) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

	`globalntv` (ℓ=3)				`localntv` (ℓ=3)				`sparsentv` (ℓ=3)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
#ssvs	364				88				72			
#fbs	0	8.0	142	13.3	0	12.0	186	16.8	0	14.0	161	18.1
rel. err.	0.0	2.7	54.4	7.7	0.0	3.3	47.7	6.9	0.0	3.2	48.8	6.8

(C) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

	`globalntv` (ℓ=4)				`localntv` (ℓ=4)				`globalntv` (ℓ=5)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
#ssvs	364				153				364			
#fbs	0	1.0	10	1.8	0	3.0	10	3.3	0	8.5	17	8.3
rel. err.	0.0	6.4	60	11.3	0.0	5.2	52.9	9.8	0.0	0.0	66.7	2.0

(D) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

Table 4. Experiments on the three sieves: "#ssvs", "#fbs" and "rel. err." correspond to the criteria listed in Section 5A.

global effort on discovering new nearly-transition-vectors or stopping regularly the enumeration process, as the number of generated skew-small-vectors about the global effort on the initialization. The combination of these three criteria is needed since, e.g., generating a huge amount of skew-small-vectors will decrease quantitatively the two other criteria by putting solely too much effort on the initialization.

Since the patterns of the skew-small-vectors of `localntv` and `sparsentv` are constrained, their relative errors are expected to be better (i.e., smaller) than the one with `globalntv`. Since the initialization is less under control with `globalntv`, the number of skew-small-vectors may be often (much) larger for `globalntv`; however, the number of calls to the fall-back strategy is expected to be lower.

The accuracy of the algorithms seems more than sufficient for the majority of the lattices, both in four and six dimensions. The maximal values of all the tables can be impressive, but occur only for a sufficiently small number of skewed lattices; since the enumeration in such lattices may be costly, it can be better to avoid them or at least, to be not too accurate.

In four dimensions, the accuracy is combined with a reasonable number of produced skew-small-vectors. The criteria do not help to determine which of the 2-level `localntv` and `globalntv` is the most suitable algorithm. The running time estimations may help to decide. At level $\ell = 3$, the number of calls to the fall-back strategy can be an issue but may be under control in a careful implementation.

The situation is mitigated in dimension 6. Except for the 2-level `sparsentv`, the number of skew-small-vectors is huge, which disqualifies with this setting all the sieves at any level. In addition, the number of calls to the fall-back strategy at levels $\ell = 2$ and $\ell = 3$ indicates that the produced nearly-transition-vectors are of poor quality. If dimension-6 sieving were feasible, it would need more investigation; however, using cuboid search spaces is probably a constraint that implies a hardness, or even an impossibility, for the sieving process. In addition, the initialization of the norms in higher dimensions implemented in CADO-NFS [43] is actually too slow for dimensions larger than six because of preserving a relative accuracy. It confirms the hardness of the relation collection above dimension 4.

5B. ***Running time.*** From the previous section, only 4-dimensional sieving seems to be an option. We compare, at levels $\ell = 2$ and $\ell = 3$, the new sieves with the state-of-the-art sieve algorithms and also between themselves.

Comparison with the plane sieve. The 2-level `globalntv` and `localntv` are compared with the most efficient existing sieve algorithm, which is the (generalized) plane sieve. Our implementation of the plane sieve is however a bit incomplete: we implement the fall-back strategy of Section 4D without enforcing the coordinate k of the k-skew-small-vectors to be equal to 1. This implementation may be a bit faster than a complete plane sieve. On 2^{10} lattices, `globalntv` and `localntv` are faster than our generalized plane sieve, with `localntv` slightly faster than `globalntv`. Since the accuracy of the two heuristic sieve algorithms is quite good, both sieves must be considered as an alternative to the plane sieve.

Comparison of the new sieves. The 3-level `globalntv` is also compared with the 2-level `globalntv` and `localntv` on 2^{10} lattices. Unlike the previous comparisons, the results can be puzzling. Indeed, for lattices where the 3-level `globalntv` is expected to be efficient, the 2-level `localntv` is less than 1.5 times faster. Furthermore, the 2-level `localntv` is more than 3 times faster than the 2-level `globalntv`. Before explaining these results, we first remark that, in this situation, the three studied sieve algorithms share the same condition to use or not the fall-back strategy. The second remark comes from a detail of our implementation. Since accuracy is our main concern, Step (b) of the fall-back strategy in Section 4B sets $\boldsymbol{c}$ to one of the computed elements with the smallest coordinate k (i.e., the first element, since the list of k-nearly-transition-vectors is sorted by increasing coordinate k).

The 2-level `globalntv` and `localntv` produce more or less the same nearly-transition-vectors, despite having differently produced skew-small-vectors. The 3-skew-small-vectors are less numerous and

have smaller coordinates with `localntv` than with `globalntv`. Then, if the for loop on the k-skew-small-vectors (Step 1(a)i) fails to find an element in $\mathcal{H}$ in both sieves, and if the coordinate k of the first k-skew-small-vectors is the same for both sieves (these two situations often occur), `localntv` is faster than `globalntv`.

Between the 3-level `globalntv` and the 2-level `localntv`, the situation shares some of the observations made previously. However, this time, `globalntv` produces nearly-transition-vectors and skew-small-vectors of better quality than `localntv`: in some cases, `globalntv` is faster than `localntv`, but if the situations become the same as in the previous analysis, `localntv` stays faster. We believe that a careful study of the different parts (especially how the linear combinations can produce useful vectors during the initialization of `globalntv` specialized in dimension 4) of the algorithms will lead to an efficient implementation of the 3-level `globalntv`.

6. Conclusion

In this article we propose algorithms to sieve in any dimension in the intersection of a lattice and a cuboid, which is one of the challenges we list to have a practical implementation of the $\mathrm{NFS}_{>1}$ algorithms. These algorithms allow us to report a large portion of the elements in the intersection faster than the previous generic sieve algorithms. We provide a reference implementation of these algorithms, allowing us to highlight their advantages and drawbacks for the accuracy and efficiency of the enumeration, and demonstrate the practicability of these sieves for dimension 4, and the hardness of sieving in dimension 6 and above.

In the near future, we plan to integrate these algorithms, specialized in dimension 4, in the existing implementations of NFS_1 in CADO-NFS [43] and extend it to $\mathrm{NFS}_{>1}$. It will help key size estimations for pairings [30; 3]. However, since a practical computation of the relation collection with $\mathrm{NFS}_{>1}$ will be possible only with good polynomials f_0 and f_1, we also plan to study quality criteria for such NFS algorithms. Further work includes also enumeration in noncuboid search space.

Acknowledgments

The author is grateful to Pierrick Gaudry and Marion Videau for numerous discussions and reviews of preliminary versions of this work, as well as Aurore Guillevic and Shashank Singh for numerous discussions about NFS. He also thanks Damien Stehlé and the referees whose remarks helped to improve the presentation of his results.

References

[1] Shi Bai, Cyril Bouvier, Alexander Kruppa, and Paul Zimmermann, *Better polynomials for GNFS*, Math. Comp. **85** (2016), no. 298, 861–873. MR 3434885

[2] Razvan Barbulescu, *Algorithmes de logarithmes discrets dans les corps finis*, Ph.D. thesis, Université de Lorraine, 2013.

[3] Razvan Barbulescu and Sylvain Duquesne, *Updating key size estimations for pairings*, J. Cryptology (2018).

[4] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain, *Improving NFS for the discrete logarithm problem in non-prime finite fields*, Advances in cryptology—EUROCRYPT 2015, I, Lecture Notes in Comput. Sci., no. 9056, Springer, 2015, pp. 129–155. MR 3344923

[5] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung, *The tower number field sieve*, Advances in cryptology—ASIACRYPT 2015, II, Lecture Notes in Comput. Sci., no. 9453, Springer, 2015, pp. 31–55. MR 3487762

[6] Yuval Bistritz and Alexander Lifshitz, *Bounds for resultants of univariate and bivariate polynomials*, Linear Algebra Appl. **432** (2010), no. 8, 1995–2005. MR 2599838

[7] Fabrice Boudot, *On improving integer factorization and discrete logarithm computation using partial triangulation*, Cryptology ePrint Archive, report 2017/758, 2017.

[8] J. P. Buhler, H. W. Lenstra, Jr., and Carl Pomerance, *Factoring integers with the number field sieve*, The development of the number field sieve, Lecture Notes in Math., no. 1554, Springer, 1993, pp. 50–94. MR 1321221

[9] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, 2000.

[10] Don Coppersmith, *Solving homogeneous linear equations over* GF(2) *via block Wiedemann algorithm*, Math. Comp. **62** (1994), no. 205, 333–350. MR 1192970

[11] Jens Franke and Thorsten Kleinjung, *Continued fractions and lattice sieving*, conference paper, 2005.

[12] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), no. 2, 224–280. MR 2578668

[13] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé, *A kilobit hidden SNFS discrete logarithm computation*, Advances in cryptology—EUROCRYPT 2017, I, Lecture Notes in Comput. Sci., no. 10210, Springer, 2017, pp. 202–231. MR 3652104

[14] Pierrick Gaudry, Laurent Grémy, and Marion Videau, *Collecting relations for the number field sieve in* GF(p^6), LMS J. Comput. Math. **19** (2016), no. suppl. A, 332–350. MR 3540964

[15] Jack E. Graver, *On the foundations of linear and integer linear programming, I*, Math. Programming **9** (1975), no. 2, 207–226. MR 0386673

[16] Laurent Grémy, Aurore Guillevic, François Morain, and Emmanuel Thomé, *Computing discrete logarithms in* $\mathbb{F}(p^6)$, Selected Areas in Cryptography—SAC 2017, Lecture Notes in Comput. Sci., no. 10719, Springer, 2018, pp. 85–105.

[17] Aurore Guillevic, *Faster individual discrete logarithms with the QPA and NFS variants*, Math. Comp. (2018).

[18] Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, and Tsuyoshi Takagi, *An experiment of number field sieve for discrete logarithm problem over* GF(p^{12}), Number theory and cryptography, Lecture Notes in Comput. Sci., no. 8260, Springer, 2013, pp. 108–120. MR 3160838

[19] ———, *A construction of 3-dimensional lattice sieve for number field sieve over* $\mathbb{F}_{p^n}$, Cryptology ePrint Archive, report 2015/1179, 2015.

[20] 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. Comp. **72** (2003), no. 242, 953–967. MR 1954978

[21] Antoine Joux, Reynald Lercier, Nigel Smart, and Frederik Vercauteren, *The number field sieve in the medium prime case*, Advances in cryptology—CRYPTO 2006, Lecture Notes in Comput. Sci., no. 4117, Springer, 2006, pp. 326–344. MR 2422170

[22] Antoine Joux and Cécile Pierrot, *Nearly sparse linear algebra and application to discrete logarithms computations*, Contemporary developments in finite fields and applications, World Sci. Publ., Hackensack, NJ, 2016, pp. 119–144. MR 3587261

[23] Taechan Kim and Razvan Barbulescu, *Extended tower number field sieve: a new complexity for the medium prime case*, Advances in cryptology—CRYPTO 2016, I, Lecture Notes in Comput. Sci., no. 9814, Springer, 2016, pp. 543–571. MR 3565295

[24] Taechan Kim and Jinhyuck Jeong, *Extended tower number field sieve with application to finite fields of arbitrary composite extension degree*, Public-key cryptography—PKC 2017, I, Lecture Notes in Comput. Sci., no. 10174, Springer, 2017, pp. 388–408. MR 3649119

[25] Thorsten Kleinjung, *On polynomial selection for the general number field sieve*, Math. Comp. **75** (2006), no. 256, 2037–2047. MR 2249770

[26] Thorsten Kleinjung, *Polynomial selection*, slides presented at the CADO workshop on integer factorization, 2008.

[27] Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, and Colin Stahlke, *Computation of a 768-bit prime field discrete logarithm*, Advances in cryptology—EUROCRYPT 2017, I, Lecture Notes in Comput. Sci., no. 10210, Springer, 2017, pp. 185–201. MR 3652103

[28] Arjen K. Lenstra, *General purpose integer factoring*, Topics in computational number theory inspired by Peter L. Montgomery, Cambridge Univ. Press, 2017, pp. 116–160. MR 3753110

[29] Arjen K. Lenstra and Eric R. Verheul, *The XTR public key system*, Advances in cryptology—CRYPTO 2000, Lecture Notes in Comput. Sci., no. 1880, Springer, 2000, pp. 1–19. MR 1850033

[30] Alfred Menezes, Palash Sarkar, and Shashank Singh, *Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography*, Paradigms in cryptology—MYCRYPT 2016: malicious and exploratory cryptology, Lecture Notes in Comput. Sci., no. 10311, Springer, 2017, pp. 83–108.

[31] B. Murphy, *Polynomial selection for the number field sieve integer factorisation algorithm*, Ph.D. thesis, The Australian National University, 1999.

[32] Shmuel Onn, *Theory and applications of n-fold integer programming*, Mixed integer nonlinear programming, IMA Vol. Math. Appl., no. 154, Springer, 2012, pp. 559–593. MR 3587645

[33] J. M. Pollard, *The lattice sieve*, The development of the number field sieve, Lecture Notes in Math., no. 1554, Springer, 1993, pp. 43–49. MR 1321220

[34] C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational methods in number theory, I, Math. Centre Tracts, no. 154, Math. Centrum, Amsterdam, 1982, pp. 89–139. MR 700260

[35] Carl Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), no. 12, 1473–1485. MR 1416721

[36] Karl Rubin and Alice Silverberg, *Torus-based cryptography*, Advances in cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., no. 2729, Springer, 2003, pp. 349–365. MR 2093203

[37] Palash Sarkar and Shashank Singh, *A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm*, Advances in cryptology—ASIACRYPT 2016, I, Lecture Notes in Comput. Sci., no. 10031, Springer, 2016, pp. 37–62. MR 3598073

[38] ———, *A generalisation of the conjugation method for polynomial selection for the extended tower number field sieve algorithm*, Cryptology ePrint Archive, report 2016/537, 2016.

[39] ———, *New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields*, Advances in Cryptology—EUROCRYPT 2016, Lecture Notes in Comput. Sci., no. 9665, Springer, 2016, pp. 429–458.

[40] ———, *Tower number field sieve variant of a recent polynomial selection method*, Cryptology ePrint Archive, report 2016/401, 2016.

[41] Oliver Schirokauer, *Discrete logarithms and local units*, Philos. Trans. Roy. Soc. London Ser. A **345** (1993), no. 1676, 409–423. MR 1253502

[42] ———, *Virtual logarithms*, J. Algorithms **57** (2005), no. 2, 140–147. MR 2177621

[43] The CADO-NFS Development Team, *CADO-NFS, an implementation of the number field sieve algorithm*, 2018.

[44] Pavol Zajac, *Discrete logarithm problem in degree six finite fields*, Ph.D. thesis, Slovak University of Technology, 2008.

[45] Yuqing Zhu, Jincheng Zhuang, Chang Lv, and Dongdai Lin, *Improvements on the individual logarithm step in extended tower number field sieve*, Cryptology ePrint Archive, report 2016/727, 2016.

Received 2 Mar 2018. Revised 18 May 2018.

LAURENT GRÉMY: laurent.gremy@inria.fr
Univ Lyon, CNRS, ENS de Lyon, Inria, Université Claude Bernard Lyon 1, LIP UMR 5668, F-69007, Lyon, France

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine