Threshold phenomena in random lattices and efficient reduction algorithms

Ali Akhavi
GREYC - Université de Caen, F-14032 Caen Cedex, France
ali.akhavi@info.unicaen.fr

Abstract. Two new lattice reduction algorithms are presented and analyzed. These algorithms, called the Schmidt reduction and the Gram reduction, are obtained by relaxing some of the constraints of the classical LLL algorithm. By analyzing the worst case behavior and the average case behavior in a tractable model, we prove that the new algorithms still produce "good" reduced basis while requiring fewer iterations on average. In addition, we provide empirical tests on random lattices coming from applications, that confirm our theoretical results about the *relative behavior* of the different reduction algorithms.

1 Introduction

A Euclidean lattice is the set of all integer linear combinations of p linearly independent vectors in $\mathbb{R}^n$. The vector space $\mathbb{R}^n$ is then called *the ambient space.* Any lattice can be generated by many bases (all of them of cardinality p). The lattice basis reduction problem aims to find bases with good Euclidean properties, that is sufficiently short vectors and almost orthogonal. The problem is old and there exist numerous notions of reduction; the most natural ones are due to Minkowski or to Korkhine–Zolotarev. For a general survey, see for example [7, 18]. Both of these reduction processes are "strong", since they build reduced bases with somehow best Euclidean properties. However, they are also computationally hard to find, since they demand that the first vector of the basis should be a shortest one in the lattice. It appears that finding such an element in a lattice is likely to be NP-hard [1, 20].

Fortunately, even approximate answers to the reduction problem have numerous theoretical and practical applications in computational number theory and cryptography: Factoring polynomials with rational coefficients [11], finding linear Diophantine approximations [9], breaking various cryptosystems [10, 14],[19] and integer linear programming [6, 12]. In 1982, Lenstra, Lenstra and Lovász [11] gave a powerful approximation reduction algorithm. It depends on a real approximation parameter $t \in]1, 2[$ and is called LLL(t). It begins with the Gram-Schmidt orthogonalizing process, then it aims to ensure, for each index $i, 1 \leq i \leq p-1$, a lower bound on the ratio between the lengths ℓ_i and ℓ_{i+1} of two successive orthogonalized vectors,

$$\frac{\ell_{i+1}}{\ell_i} \geq s \qquad \text{with} \quad s^2 = \frac{1}{t^2} - \frac{1}{4} \leq \frac{3}{4}. \tag{1}$$

So, for reducing an n-dimensional lattice, it performs at least $n-1$ iterations. This celebrated algorithm seems difficult to analyze precisely, both in the worst–case and in average–case. The original paper [11] gives an upper bound for the number of iterations of LLL(t), which is polynomial in the data size. When given p input vectors of $\mathbb{R}^n$ of length at most M, the data size is $O(np \log M)$ and the upper bound is $p^2 \log_t M + p$. Daudé and Vallée [4] exhibited an upper bound for the average number of iterations (in a simple natural model) which asymptotically equals $(p^2/2) \log_t n + p$.

There is already a wide number of variations around the LLL algorithm (due for instance to Kannan or Schnorr [6, 13]) whose goal is to find lattice bases with sharper Euclidean properties than the original LLL algorithm.

Here, we choose the other direction, and we present two new variations around the LLL–reduction that are a priori weaker than the usual LLL reduction. They are called Schmidt–reduction and Gram–reduction. As for the LLL-reduction, they depend both on the parameter s. The Gram reduction also depends on another parameter γ. When $\gamma = 0$, the Gram–reduction coincides with the LLL reduction. Our algorithms are modifications of the LLL algorithm; they have exactly the same structure but they are based on different and weaker tests on the ratio between the lengths of orthogonalized vectors. Our purpose is twofold. On one hand, we propose more time–efficient reductions for lattices of high dimension. Although the new reduced bases are less sharp, they can play the same rôle as the Lovász-reduced ones in most of the applications, and they are obtained faster. On the other hand, the new algorithms are easier to analyze precisely so that the randomness and efficiency issues are much better understood.

Plan of the paper. In Section 2, we define the new reductions and we compare them to the LLL reduction: We give the Euclidean qualities of any reduced basis and the worst-case complexity of the reduction algorithms. Section 3 presents the main tools of the average–analysis in a tractable model. In Section 4, we show a general threshold phenomenon for the ratios of lengths of two different orthogonalized vectors and we compare the different reduction processes on random lattices. In Section 5, we report empirical tests on random lattices coming from applications: the new reduction algorithms remain more time–efficient and their outputs are still strong enough to be useful in applications.

Summary of results.

(a) First, we show that our reduced bases have always Euclidean properties similar to the LLL reduced ones. In particular, the shortest vector is at most $(1/s)^{n-1}$ times longer than a shortest element in the lattice. Observe that most of applications use only the first vector of the reduced basis.

(b) For the worst–case number of iterations, we show for all the reduction algorithms, the same upper bound as for the LLL algorithm. So, we cannot distinguish between these algorithms by a worst–case analysis.

Then, we compare these reductions by means of average–case analysis. We adopt a tractable probabilistic model, where the p vectors of the input basis are chosen uniformly and independently in the unit ball of $\mathbb{R}^n$. For the average analysis, we use various tools: We begin with the result due to Daudé and Vallée [4] about the distribution function of the length ℓ_a of the a-th orthogonalized vector associated with random bases. Then, we generalize a method due to Laplace to the two–dimensional–case and we apply this machinery to study the distribution function of the ratio ℓ_b/ℓ_a between the lengths of two different orthogonalized vectors. More precisely, we choose for a and b two affine functions of the dimension n of the ambient space:

Definition 1. For θ any real constant in $[0,1]$, and r any integer constant, the quantity $f(n) := \theta n + r$ is called *an affine index* (or simply *an index*) iff it is an element of $\{1, ..., n\}$. Moreover, such an index is called *a beginning index* iff the slope θ satisfies $\theta < 1$. It is called *an ending index* iff the slope θ satisfies $\theta = 1$.

We consider the asymptotics of the distribution function of the ratio ℓ_b/ℓ_a for $n \to \infty$ and when $a := \alpha n + i$, $b := \beta n + j$ are two indexes. By "almost surely", we mean that the probability tends exponentially to 1 with the dimension n. We exhibit some quite different phenomena according to the position of the pair (a, b) with respect to the dimension n of the ambient space $\mathbb{R}^n$.

(c) For a pair (a, b) of beginning indexes, the distribution function of ℓ_b/ℓ_a presents a threshold phenomenon that is of independent interest. More precisely, given two real constants α and β in $[0, 1[$, and two integer constants i and j, the probability

$$\Pr\{\ell_{\beta n+j}/\ell_{\alpha n+i} < v\}$$

follows a 0–1 law when n tends to infinity and the jump happens when v equals $\sqrt{1-\beta}/\sqrt{1-\alpha}$. Then, for any fixed s, we exhibit $\omega_0(s) < 1$ such that, when the ambient space is of sufficiently high dimension n, any random input of dimension $p := \omega n$ with $\omega < \omega_0(s)$ is almost surely reduced after $p-1$ iterations (in the sense of all the previous reductions). Furthermore, we show that the new algorithms, are quite efficient, even in the most difficult case of the full dimensional lattices $(p = n)$, since the numbers K_S and K_G of iterations of the Schmidt and the Gram algorithms are almost surely $n-1$: For any $\varepsilon > 0$, there exists N such that for any $n > N$,

$$\Pr\{K_S = n-1\} \geq 1 - s^{(1-\varepsilon)n} \quad ; \quad \Pr\{K_G = n-1\} \geq 1 - s^{(1-\varepsilon)n^\gamma}.$$

(d) On the contrary, for a pair (a, b) of ending indexes the distribution function of ℓ_b/ℓ_a does not present a threshold phenomenon anymore. More precisely, given two positive integer constants i and j, the probability

$$\Pr\{\ell_{n-j}/\ell_{n-i} < v\}$$

admits a limit that is a continuous function of v. Thus, the LLL algorithm is much less time–efficient, since we show that the number K_L of iterations of the LLL algorithm is strictly greater then $n-1$, with a non–negligeable probability,

$$\Pr\{K_L > n-1\} > 1/\sqrt{1+(1/s)^2}.$$

For the average number of iterations of the LLL algorithm, the only known upper–bound remains $n^2 \log_t n + n$ [4].

2 New reductions and worst-case analysis

First, we recall how the Euclidean properties of a basis are usually evaluated in lattice theory. Then, we define two new reductions: For s a real parameter defined by 1, and $\gamma \in]0, 1]$ a fixed real, we introduce the (s, γ)-Gram reduction and the s-Schmidt reduction. We compare all these reductions from two points of view, the Euclidean properties of the output basis, and the worst-case computational complexity of the algorithms. We obtain the results $(a), (b)$ of the introduction.

2.1 Two measures of quality

Let $\mathbb{R}^n$ be endowed with the usual scalar product $\langle\ ,\ \rangle$ and Euclidean length $|u| = \langle u, u\rangle^{1/2}$. A lattice of $\mathbb{R}^n$ is the set of all integer linear combinations of a set of linearly independent vectors. Generally it is given by one of its basis $(b_1, b_2, \ldots, b_p)$ and the number p is the dimension of the lattice. So, if M is the maximum length of the vectors b_i, the data-size is $(np \log M)$. In a lattice, there exist some invariant quantities that does not depend on the choice of a basis. Among these invariants, the n *successive minima* Λ_i are defined as follows: Λ_i is the smallest positive number t so that there exist in the lattice, i independent vectors of lengths at most t. So, Λ_1 is the length of a shortest vector.

Intuitively, a reduced basis of a lattice consists of short vectors or equivalently it is nearly orthogonal. The shortness of the vectors is measured by *the length defects*. The i-th length defect $\mu_i(b)$ compares $|b_i|$ to the i-th minimum Λ_i,

$$\mu_i(b) = |b_i|/\Lambda_i.$$

All the reduction algorithms begin with the usual Gram-Schmidt orthogonalization process, which associates to a basis $b = (b_1, b_2, \ldots, b_p)$ an orthogonal basis $b^* = (b_1^*, b_2^*, \ldots, b_p^*)$ and a triangular matrix $(m) = (m_{ij})$ that expresses system b into system b^*. The vector b_1^* equals b_1 and for $i \geq 2$, b_i^* is the component of b_i orthogonal to the vector subspace spanned by $b_1, \ldots, b_{i-1}$:

$b_1^* = b_1$, and $b_i^* = b_i - \sum_{j<i} m_{ij} b_j^*$, where $m_{ij} = \langle b_i, b_j^*\rangle / |b_j^*|^2$, for $j < i$.

It is clear that $m_{ij} = 0$ for $i < j$ and $m_{ii} = 1$.

The length ℓ_i of the vector b_i^* does play an important role in the sequel. The ratio $\ell_i/|b_i|$ is the sinus of the angle between b_i and the vector space spanned by $b_1, \ldots, b_{i-1}$. So, a nearly orthogonal basis, has all its ratios $\ell_i/|b_i|$ near to 1 and the *orthogonality defect* $\rho(b)$ measures the "nearly orthogonality" for b,

$$\rho(b) = \prod_{i=1}^{p} |b_i|/\ell_i. \tag{2}$$

$$\text{A basis } b \text{ is called } \textit{size-reduced} \text{ if } |m_{ij}| \leq 1/2, \text{ for } 1 \leq j < i \leq p. \tag{3}$$

Size-reduction is an easy tool to shorten a basis, since there is a simple algorithm that obtains a size-reduced basis from any basis, by integral translations of each b_i parallely to the previous b_j $(j < i)$. But size-reduction alone does not guarantee the usual quality needed for a reduced basis.

2.2 Concepts of reduction

Definition 2. Let t, s be two real parameters related by (1). Given a basis $b = (b_1, b_2, \ldots, b_p)$ of a lattice L and for an index i, $1 \leq i \leq p-1$, we consider

$$\text{the } t\text{-Lovász condition :}\quad \left(\ell_{i+1}^2 + m^2{}_{i+1,i}\ell_i^2\right)/\ell_i^2 \;\geq\; 1/t^2 \tag{4}$$

$$\text{the } s\text{-Siegel condition :}\quad \ell_{i+1}/\ell_i \;\geq\; s \tag{5}$$

$$\text{the } s\text{-Schmidt condition :}\quad \ell_{i+1}/\ell_1 \;\geq\; s^i \tag{6}$$

$$\text{the } (s,\gamma)\text{-Gram condition :}\quad (6) \text{ and } \ell_{i+1}/\ell_i \;\geq\; s^{i^\gamma}, \text{ with } 0 < \gamma \leq 1 \tag{7}$$

Let $\mathcal{C}_i$ be one of the above conditions, for a fixed index i. The basis b is called $\mathcal{C}$-reduced if it is size-reduced and if it satisfies the $\mathcal{C}_i$ condition, for all indexes i, $1 \leq i \leq p-1$.

The condition (4) is introduced by Lovász [11] and it is used in the original LLL algorithm. The s-Siegel condition is an immediate consequence of together (4) and size-reduction (3); it is in fact, always used rather than the t-Lovász condition and in the sequel we will often do so. An average study of ratios (ℓ_{i+1}/ℓ_i) shows that they have all 1 as mean values, but their variances increase with the index i. When i is closed to n, the ratios are very dispersed. So that, the s-Siegel conditions are more and more difficult to satisfy and it is reasonable to fix a lower bound for (ℓ_{i+1}/ℓ_i) that decreases with the index i. We introduce here the (s, γ)-Gram condition that takes in consideration the previous remark and is exactly the classical s-Siegel condition, as $\gamma = 0$. The s-Schmidt condition[1] is the less sharp introduced here. The s-Schmidt and s-Siegel conditions can not be compared, for a fixed index i. However, if the whole basis is $s-$Siegel reduced, then it is also $s-$Schmidt reduced. The next lemma compares more *locally* the above conditions; it is useful to study the computational complexity of the reduction algorithms.

Lemma 3. *Let t, s two parameters related by (1). Let $(b_1, \ldots, b_p)$ be a basis and $i \in \{1, \ldots, p\}$ a fixed index.*

1. *If the s-Siegel condition is not satisfied and $|m_{i+1,i}| \leq 1/2$, then the t-Lovász condition is not satisfied either.*
2. *If the (s, γ)-Gram condition is not satisfied, neither is the s-Siegel condition. Conversely, the choice of $\gamma = 0$ in the (s, γ)-Gram reduction leads exactly to the s-Siegel reduction.*
3. *If the s-Schmidt condition is satisfied for the index i, but not for the index $i+1$, then the s-Siegel is not satisfied for the index $i+1$ either.*

2.3 Comparing the quality of reduced bases

The next theorem shows that the s-Schmidt reduction provides only a short vector of the lattice. For the three other reductions, all vectors of the reduced bases are short and the basis is nearly orthogonal. For the proof, see [2].

Theorem 4. *Let $b = (b_1, \ldots, b_p)$ be a basis of a lattice.*

1. *If b is s-Schmidt reduced, then its first length defect is bounded from above:*
$$\mu_1(b) \leq (1/s)^{(p-1)}. \tag{8}$$
2. *If b is (s, γ)-Gram reduced, then its first length defect is upper bounded as in (8). All the other lengths defects and the orthogonality defect are also bounded from above:*
$$\mu_i(b) \leq (1/s)^{(p-1)^{1+\gamma}}, \text{ for all } i \in \{2, ..., p\} \quad \text{and} \quad \rho(b) \leq (1/s)^{(p^{2+\gamma})/(2+\gamma)}.$$

2.4 Comparing reduction algorithms

Let us consider the generic $\mathcal{C}$-reduction algorithm, where $\mathcal{C}$ is one of the conditions introduced in Definition 2.

[1] The Schönhage's semi–reduction [16] is not too far from our Schmidt reduction.

The $\mathcal{C}$-reduction algorithm:

Input: A basis $(b_1, \ldots, b_p)$ of a lattice L.
Output: A $\mathcal{C}$-reduced basis b of the lattice L.
Initialization: Compute the orthogonalized system b^* and the matrix m.
$\mathbf{i := 1}$;
While $\mathbf{i < p}$ **do**
  $b_{i+1} := b_{i+1} - \lfloor m_{i+1,i} \rceil b_i$ ($\lfloor x \rceil$ is the integer nearest to x).
  Test the $\mathcal{C}_i$ condition.
    If true, make $(b_1, \ldots, b_{i+1})$ size-reduced by translations; **set** $\mathbf{i := i + 1}$;
    If false, swap b_i and b_{i+1}; update b^* and m; if $i \neq 1$ then **set** $\mathbf{i := i - 1}$;

During an execution, the index i varies in $\{1, \ldots, n\}$. When i equals some $k \in \{1, \ldots, p-1\}$, the beginning lattice generated by $(b_1, \ldots, b_k)$ is already reduced. Then, the $\mathcal{C}_k$ condition is tested. If the test is positive, size-reduction is performed and the beginning lattice generated by $(b_1, \ldots, b_{k+1})$ is reduced. So, i is incremented. Otherwise, the vectors b_k and b_{k+1} are swapped. At this moment, nothing guarantees that $(b_1, \ldots, b_k)$ "remains" reduced. So, i is decremented. The algorithm updates b^* and m, translates the new b_k in the direction of b_{k-1} and tests the $\mathcal{C}_{k-1}$ condition. Thus, the index i may fall down to 1. Finally, when i equals p, the whole basis is reduced and the algorithm terminates. The following Theorem shows that the $\mathcal{C}$-reduction algorithm terminates always and performs a polynomial number of iterations. However, this worst–case analysis does not distinguish between the four previous reduction algorithms.

Theorem 5. *Let s and t be real parameters related by (1), $\mathcal{C}$ one of the four conditions of Definition 2, and $(b_1, b_2, \ldots, b_p)$ any integer input basis. The maximum number K of iterations of the generic $\mathcal{C}$-reduction satisfies*

$$K \leq p(p-1) \log_t M + p - 1, \quad \textit{where} \quad M := \max_{i \in \{1, \ldots, p\}} |b_i|.$$

Sketch of proof. When $\mathcal{C}$ denotes the t-Lovász condition, the original proof of [11] is based on the decrease of the integer quantity

$$D := \prod_{i=1}^{p-1} \prod_{j=1}^{i} \ell_j^2,$$

by the factor $(1/t^2)$, whenever a test is negative. When $\mathcal{C}$ is another condition, a negative test for an index i means that $(b_1, \ldots, b_{i-1})$ is $\mathcal{C}$-reduced, whereas $(b_1, \ldots, b_i)$ is not. So, by Lemma 3, the t-Lovász test would be negative either.

3 The lengths ℓ_i in the probabilistic model and the Laplace method

First, we define the probabilistic model. Then we give various tools that we use on the average–analysis of the next Section. We begin with the result due to Daudé and Vallée [4] about the distribution function of the length ℓ_a of the $a-th$ orthogonalized vector associated with random bases. Then, we generalize a method due to Laplace for evaluating asymptotics for integrals, to the two–dimensional–case.

3.1 The probabilistic model

All the previous reduction algorithms act in the same way on a basis and on its transformed by a homothety. On the other hand, choosing a continuous model makes it possible to use powerful mathematical tools. All these reasons legitimate working with bases of length less than 1. The most natural and simplest model is thus the uniform model over all legal inputs to the reduction algorithms. So, in our analysis, the input vectors $b_1, b_2, \ldots, b_p$, $(p \leq n)$ are chosen independently and uniformly inside the unit ball $\mathcal{B}_n$ of $\mathbb{R}^n$. Clearly, they form almost surely an independent system, called a random basis (p-dimensional). The lattice that it generates is called a random lattice. It is full–dimensional if $p = n$. Classical methods (see Section 3 in [4]) generalize our results on a discrete model .

3.2 The distribution of variables ℓ_i

Under the uniform model, Daudé and Vallée showed that the squares of the lengths of ℓ_i's follow a Beta law (Corollary of the next Theorem). Before describing the result, we recall some usual definitions. For $u \in [0,1]$ and two reals p and q, the random variable X of the interval $[0,1]$ follows the Beta law of parameters p and q if its distribution function satisfies

$$\Pr\{X \leq u\} = \frac{\int_0^u x^{p-1}\,(1-x)^{q-1}\,dx}{\int_0^1 x^{p-1}\,(1-x)^{q-1}\,dx}.$$

The numerator is called an *incomplete Beta integral* and denoted $B(p,q,u)$. The normalization coefficient (the denominator) is simply a *Beta integral* $B(p,q)$ [21]. The next theorem describes the density of the random variables ℓ_i. It plays a central rôle in our probabilistic analysis.

Theorem 6. *[4] If the vectors $b_1, b_2, \ldots, b_p$ are independently and uniformly distributed inside the unit ball $\mathcal{B}_n$ of $\mathbb{R}^n$, then the lengths ℓ_i of their orthogonalized vectors are independent variables. The density $f_{i,n}(u)$ of ℓ_i on the interval $[0,1]$ is given by*

$$f_{i,n}(u) = \frac{2}{B(\frac{n-i+1}{2}, \frac{i+1}{2})} u^{n-i}(1-u^2)^{\frac{i-1}{2}}.$$

All previous reduction algorithms deal with ratios of the form $\dfrac{\ell_b}{\ell_a}$. In the sequel,

$$a(n) := \alpha n + i \quad \text{and} \quad b(n) := \beta n + j, \tag{9}$$

are always affine indexes (Definition 1). We look for asymptotic equivalents for the distribution function

$$G_{n,a,b}(v) := \Pr\{\ell_{b(n)}/\ell_{a(n)} < v\}$$

of ratios ℓ_b/ℓ_a. When $a(n) \neq b(n)$, the previous Theorem shows that $\ell_{b(n)}$ and $\ell_{a(n)}$ are independent variables and gives their density. So, the density $f_{n,a,b}(x,y)$ of the couple $(\ell_{a(n)}, \ell_{b(n)})$ satisfies $f_{n,a,b}(x,y) = f_{n,a}(x) f_{n,b}(y)$. The exact expression of $G_{n,a,b}(v)$ involves the polygon $\Delta(v)$ and $\Delta(\infty)$

$$\Delta(v) = \{(x,y) \in [0,1]^2 : y/x < v\} \quad \text{and} \quad \Delta(\infty) = [0,1]^2, \tag{10}$$

and is expressed as a ratio of two generic integrals,

$$G(v) = \frac{I_n(v)}{I_n(\infty)}, \quad \text{where} \quad I_n(v) := \int_{\Delta(v)} g(x,y) e^{nh(x,y)} dxdy, \tag{11}$$

$$\text{with} \quad g(x,y) = (1-x^2)^{\frac{i-1}{2}}\, x^{-i}\, (1-y^2)^{\frac{j-1}{2}}\, y^{-j}, \quad \text{and} \tag{12}$$

$$h(x,y) = (\alpha/2)\ln(1-x^2) + (\beta/2)\ln(1-y^2) + (1-\alpha)\ln(x) + (1-\beta)\ln(y). \tag{13}$$

An appropriate way to study the asymptotic behaviors of integrals such $I(v)$ and $I(\infty)$ is the Laplace method (see for example [3, 5, 17]). The next subsection first explains the Laplace's idea. Then we generalize the Laplace method for g and h functions of two variables, and the integration domain, a polygon.

3.3 The Laplace method for integrals

Let us consider the convergent integral $\quad I_n = \int_\Delta F(x,n)dx.$
It often happens that the graph of $F(x,n)$, considered as a function of x, has somewhere a sharp peak, and that the contribution of a neighborhood of the peak is almost equal to the whole integral, when n is large. Then we can try to approximate F in that neighborhood by simpler functions, for which the integral can be evaluated. The advantage is that we need only a local approximation for F. This idea is due to Laplace and it is often used to find the asymptotic behavior of simple integrals. For our needs, we have to generalize Laplace's idea for double integrals that appear in (11): the integration domain Δ is always a convex plan polygon and the functions g and h satisfy some strong assumptions. For a more precise version and for the proof, see [2].

Proposition 7. *Let Δ be a polygon and I_n a sequence of absolutely convergent integrals*

$$I_n = \int_\Delta g(x,y)e^{nh(x,y)}\, dxdy, \quad \textit{where}$$

(a) the function h has an absolute and strict maximum on Δ, say at (x_0, y_0),
(b) there are two linear forms X and Y of variables $(x - x_0, y - y_0)$ such that near (x_0, y_0) and inside Δ, the functions h and g are approximated as follows

$$h(x,y) - h(x_0,y_0) = \Theta\left(H_1(X) + H_2(Y)\right), \qquad \textit{when } (x,y) \longrightarrow (x_0,y_0), \tag{14}$$

where H_1, H_2 are one–variable polynomials of low degrees[2] $\rho \geq 1$ and $\sigma \geq 1$.

$$g(x,y) \sim CX^\lambda\, Y^\mu, \qquad \textit{when } (x,y) \longrightarrow (x_0,y_0). \tag{15}$$

where $C \neq 0$, $\lambda > -1$ and $\mu > -1$ are real constants.

Then when n is large, $\quad I_n = \Theta\left(e^{nh(x_0,y_0)}\, n^{-\frac{\lambda+1}{\rho} - \frac{\mu+1}{\sigma}}\right).$

Remarks **1.** If the maximum (x_0, y_0) is inside the polygon Δ and not on its boundary, then λ and μ are positive even integers. If the maximum (x_0, y_0) is on the boundary but not at a vertex of the polygon Δ, then $Y = 0$, introduced in (b), is the equation of the polygon side that contains (x_0, y_0) and λ is a positive

---

[2] The low degree of a polynomial $\sum_{i=0}^{r} a_i X^i$ is the minimal index i such that $a_i \neq 0$.

and even integer. If the maximum (x_0, y_0) is at a vertex of the polygon $\Delta(v)$, then $X = 0, Y = 0$ are the equations of the two polygon sides containing (x_0, y_0).
2. We need the following quite particular case in Theorem 8: If
(i) the maximum (x_0, y_0) is at a vertex of the polygon Δ and v denotes the tangent of the angle of Δ at its vertex (x_0, y_0) which is acute,
(ii) the linear forms X and Y equal $X := x - x_0$, $Y =: y - y_0$ and they may not correspond to the polygon sides' directions,
(iii) in (14), $H_1(X) = H_2(X) = -AX^2$, with $A < 0$, then when n is large,

$$I_n \sim \frac{C}{4}\, B\left(\frac{\lambda+1}{2}, \frac{\mu+1}{2}, \frac{v^2}{1+v^2}\right)\, \Gamma(\frac{\lambda+\mu+2}{2})\, e^{nh(x_0,y_0)} \left(\frac{1}{An}\right)^{\frac{\lambda+\mu+2}{2}} . \quad (16)$$

4 From ratios ℓ_b/ℓ_a to the reduction algorithms

We apply here the machinery developed in the last Section for studying the asymptotic distribution function of the ratio ℓ_b/ℓ_a between the lengths of two different orthogonalized vectors. More precisely, when n denotes the dimension n of the ambient space $\mathbb{R}^n$, $a(n)$ and $b(n)$ are two affine indexes , as defined by (9). Theorem 8 exhibits some quite different phenomena according to the position of the pair (a, b) with respect to n.
Then we differentiate the behaviors of the previous reduction algorithms (Theorem 9). The reduction algorithms operate always on a random basis $(b_1, \ldots, b_p)$, $(p \le n)$. When using the term "almost surely", we mean that the probability tends exponentially to 1 with the dimension n. In this section, we prove the points $(c), (d)$ of the Introduction.

4.1 Asymptotic behavior of $G_{n,a,b}(v)$

Proposition 7 shows that the asymptotic behaviors of integrals $I_n(v)$ and $I_n(\infty)$ that are involved in $G_{n,a,b}(v)$'s expression (11) depend strongly on the maximum of the function h (13) on the integration domain. The function h has a strict and global maximum on $\Delta(\infty) = [0,1]^2$, at $(\sqrt{1-\alpha}, \sqrt{1-\beta})$. Three different behaviors arise according to the relative positions of this point and $\Delta(v)$:
1. The point $(\sqrt{1-\alpha}, \sqrt{1-\beta})$ is not in $\Delta(v)$. Then, one shows easily that the function h has a global and strict maximum on $\Delta(v)$, which is on the boundary $y = vx$, say at $(\xi, v\xi)$. Since $\Delta(\infty)$ contains strictly $\Delta(v)$, clearly, $D_{\alpha,\beta,v} := \exp\left(h(\xi, v\xi) - h(\sqrt{1-\alpha}, \sqrt{1-\beta})\right) < 1$. Then, Proposition 7 gives equivalents for $I(v)$ and $I(\infty)$. Thus, the distribution function tends exponentially to 0 with n. More precisely, there are two constants $D_{\alpha,\beta,v} < 1$ and $f_{(i,j)}$, such that

$$G_{n,a,b}(v) \sim \Theta\left((D_{\alpha,\beta,v})^n \;\; n^{\,f_{(i,j)}}\right).$$

2. The point $(\sqrt{1-\alpha}, \sqrt{1-\beta})$ is inside $\Delta(v)$, but not in its boundary $y = vx$. So, the function h has the same maximum on $\Delta(v)$ and on $\Delta(\infty)$. Moreover, the maximum $(\sqrt{1-\alpha}, \sqrt{1-\beta})$ has *the same neighborhood* as an element of $\Delta(v)$ and as an element of $\Delta(\infty)$. By Proposition 7, $I(v)$ and $I(\infty)$ have the same equivalents and the distribution function tends to 1 with n. Further, since $G_{n,a,b}(v) = 1 - G_{n,b,a}(1/v)$, the convergence is exponential,

$$1 - G_{n,a,b}(v) \sim \Theta\left(\left(D_{\beta,\alpha,\frac{1}{v}}\right)^n \; n^{f(j,i)}\right).$$

3. The point $(\sqrt{1-\alpha}, \sqrt{1-\beta})$ is on the boundary $y = vx$ of $\Delta(v)$. The function h has the same maximum on $\Delta(v)$ and on $\Delta(\infty)$. But the point $(\sqrt{1-\alpha}, \sqrt{1-\beta})$ has not the *the same neighborhood* as an element of $\Delta(v)$ and as an element of $\Delta(\infty)$. Then, it arrises from (16) that for any fixed v, the distribution function $G(v)$ tends to a constant, strictly in $]0,1[$.

Theorem 8. *Let the vectors $b_1, b_2, \ldots, b_n$ be independently and uniformly distributed inside the unit ball $\mathcal{B}_n$ of $\mathbb{R}^n$, and let ℓ_a denote the length of the a-th orthogonalized vector.*

(i) If $a(n) := \alpha n + i$, $b(n) := \beta n + j$ are beginning indexes, i.e.$(\alpha, \beta) \in [0,1[^2$, then the distribution function $G(v)$ of the ratio ℓ_b/ℓ_a follows asymptotically and exponentially with n, a 0–1 law. The jump is at $(\sqrt{1-\alpha}, \sqrt{1-\beta})$.

(ii) If $a(n) := n - i$, $b(n) := n - j$, i.e. $\alpha = \beta = 1$ and i, j are two positive integer constants, then the asymptotic distribution function of ℓ_b/ℓ_a does not follow a 0–1 law, but variates continuously *with i, j and v, in $]0,1[$:*

$$\Pr\{\frac{\ell_{n-j}}{\ell_{n-i}} < v\} \to \frac{B\left(\frac{j+1}{2}, \frac{i+1}{2}, \frac{v^2}{1+v^2}\right)}{B\left(\frac{j+1}{2}, \frac{i+1}{2}\right)}, \quad \textit{when } n \to \infty. \tag{17}$$

4.2 Satisfying the $\mathcal{C}$ condition for a fixed index

Theorem 8 shows that for any beginning index, a random lattice satisfies any $\mathcal{C}$ condition of Definition 2. In short, for the random bases of the uniform model the "serious" reduction problems occur for the ending indexes. Considering such indexes, we classify the previous reductions in two groups: First, the s-Schmidt and (s,γ)-Gram conditions are almost surely satisfied even for an ending index, by (i) of Theorem 8. Second, the s-Siegel and t-Lovász conditions are not, by (ii) of Theorem 8.

4.3 Full–dimensional random lattices in $\mathbb{R}^n$

Here, we confirm the separation in two groups, that we made in (4.2) for the behaviors of different reduction algorithms previously introduced.

First, let $\mathcal{C}$ denote the s-Schmidt or the (s,γ)-Gram condition. The previous paragraph showed that for any index $i \in \{1, \ldots, n\}$, $\mathcal{C}_i$ is almost surely satisfied. The next Theorem makes precise that the conditions are almost surely satisfied *all together*. So, all the tests $\mathcal{C}_i$ are positive and the number of iterations equals $n-1$. In other words, almost surely, the $\mathcal{C}$–reduction algorithm just size-reduce the input basis and verify that the tests are fulfilled. The proof [2] is technical (particularly for the Gram reduction) and is based once more on the Laplace's idea for evaluating asymptotic behavior of *sums*.

Second, the s-Siegel (or the t-Lovász) reduction. If a random basis is reduced, in particular the last Siegel condition is satisfied. By the relation (17), we find the asymptotic probability that last s-Siegel condition is not satisfied and thus we give a lower bound for the probability that a random lattice is not Siegel reduced. Equivalently during an execution of the Siegel reduction algorithm, the index i is decremented at least once, with a non–negligible probability.

Theorem 9. *Let K_L, K_G, K_S denote the numbers of iterations of the s-Siegel, (s,γ)-Gram and s-Schmidt reduction, when they operate on a random full-dimensional basis. For any $0 < \varepsilon < 1$, there exists N (which depends also on γ in (s,γ)-Gram reduction), such that for $n > N$,*

$$\Pr\{K_L > n-1\} \geq 1/\sqrt{1+(1/s)^2} \tag{18}$$

$$\Pr\{K_G = n-1\} \geq 1 - s^{(1-\varepsilon)n^\gamma} \tag{19}$$

$$\Pr\{K_S = n-1\} \geq 1 - s^{(1-\varepsilon)n} \tag{20}$$

4.4 Lattices of low dimension in $\mathbb{R}^n$.

For any real parameter s, $0 < s < 1$, let $\omega_0(s)$ be the greatest real satisfying

$$s^2 < (1-\omega)\omega^{\frac{\omega}{1-\omega}}$$

By using similar methods (and in a simpler way) as in the proof of (19) and (20), we show that the number of iterations of the $s-$Siegel algorithm when it works on random input of dimension $p := \omega n$ with $\omega < \omega_0(s)$ is almost surely $p-1$. Comparing this result with (18) shows, in particular, the importance of the ratio between the dimensions of the input basis and the ambient space on the average behavior of the reduction process.

5 Statistical evaluations

The previous analysis shows that for random inputs of the uniform model, the new reduced bases are obtained faster. Several questions remain in practice.
(1) Is the output basis of the LLL algorithm of much better quality?
(2) We showed that, very probably, the number of iterations of the classical LLL algorithm is strictly greater than $n-1$ (the minimum possible). On the other hand, the only bound established for the average number of iterations of the LLL algorithm is $n^2 \log n$ [4]. Is, in practice, the t-Lovász reduced basis much more slowly to be obtained, in comparison with the new reduced bases?
(3) The uniform model is a tractable one for a mathematical average analysis. But in usual applications of lattice reduction, the lattices are not really of the uniform model. Are the new reduced bases obtained still faster with random inputs coming from applications?
Our next experimental study gives an insight to the answers of these questions. For every model considered, we report experimental mean values obtained with 20 random inputs. For each model, we provide three tables. The first table shows the average number of iterations of the different reduction algorithms. The second table gives the n-th root of the orthogonality defect of different output bases. (the first line corresponds to the input basis). The third table describes the ratio

between the lengths of the shortest output vector of the new reduction algorithms and the classical LLL algorithm. For the approximation parameters (s or t), we generally use the usual values $t^2 = 4/3$ ($s^2 = 1/2$), unless for the last row of each Table, where the optimal Schmidt algorithm is considered ($s^2 = 3/4$).

5.1 Experimentations on the uniform model

Table 1 first largely confirms our average analysis. To generate such random integer inputs we use ideas of Knuth and Brent[8]. Then, the number of iterations of the new reduction algorithms is always the minimum possible for lattices of dimension greater than 20. Moreover, the output bases of the LLL algorithm is not of better quality than the new reduced bases, while it requires much more iterations to be obtained. In other words, on random inputs of the uniform model, the LLL algorithm demands a non negligeable number of iterations to build a basis of similar quality than its input. Contrarily, the new algorithms, immediately detect, the acceptable quality of such an input.

dim	10	20	30	40	10	20	30	40	10	20	30	40
LLL	59.8	132.7	149.8	191.4	1.20	1.54	1.71	1.82	1	1	1	1
Gr/Sch	9.4	19	29	39	1.42	1.69	1.71	1.77	1.04	1.07	1.00	1.00
Sch opt	22.9	19.8	29	39	1.33	1.69	1.71	1.77	1.04	1.07	1.00	1.00

Table 1. Comparison between the number of iterations and the quality of the output bases on random inputs of *the uniform model*. The input vectors are of length at most 2^{dim}, where dim is the dimension of the input. On the right , we report the number of iterations, on the middle the n-th root of the orthogonality defect, and on the left the ratio of lengths of the shortest output vector (reference: LLL)

5.2 Experimentations in the "SubsetSum" model

Given $a_1, \ldots, a_n, M$, consider the basis $(b_1, \ldots, b_{n+1})$ of $\mathbb{Z}^{n+2}$ formed with the rows of the following matrix:

$$\begin{pmatrix} 2\,0\,0\,.\,.\,.\,na_1\,0 \\ 0\,2\,0\,.\,.\,.\,na_2\,0 \\ .\,.\,.\,.\,.\,.\,.\quad.\quad. \\ .\,.\,.\,.\,.\,2\,na_n\,0 \\ 1\,1\,.\,.\,.\,1\,nM\,1 \end{pmatrix}.$$

Lattices generated by such a basis are used by Schnorr and Euchner [15] to solve almost all subset sum problems. Moreover, lattices of similar shape are used in many other applications [19]. Here, our results are obtained from 20 random inputs of the "SubsetSum" model, generated as follows: Pick random numbers $a_1, \ldots, a_n$ in the interval $[1, 2^n]$, pick a random set $I \subset \{1, \ldots, n\}$ and put $M = \sum_{i \in I} a_i$. (The choice of a_i in the interval $[1, 2^n]$ lead us to deal with lattices of density 1, which are the most difficult in cryptographical applications.)

Number of iterations										
dim	10	20	30	40	50	60	80	90	100	110
LLL	140	449	782	1131	1775	1763	2163	2266	2363	2600
Sch	29.9	75.1	137	208	279	340	462	483	500	596
Gram	36	87	148	218	286	372	813	951	1115	1363
Sch opt	62	144	254	393	542	614	737	758	779	810
n-th root of the orthogonality defect										
rand	$1.1e3$	$2e6$	$0.2e9$	$4.3e12$	$5e15$	$6.6e18$	$8.9e24$	$1e28$	$1.2e31$	$1.4e34$
LLL	1.2	1.6	2.1	2.8	3	3.3	3.8	3.8	4.2	4.1
Sch	2.3	5.9	10	18	31	54	64	48	38	35
Gram	2	4.3	8.6	16	28	31	19	19	20	19
Sch opt	1.5	2.6	4	6.3	8.3	7.3	9	8.3	10	9.9
Ratio between the lenghts of the shortest output vectors (reference LLL)										
Sch	1.4	2.4	2.7	4.2	6.5	5.4	5.7	6.4	5.4	3.8
Gram	1.4	2	2.6	3.9	5.9	5.4	2.6	3.8	3.5	3.4
Sch opt	1.1	1.4	1.6	1.6	1.9	1.7	1.8	1.7	1.7	2.1

Table 2. Comparison between the number of iterations and the quality of the output bases on random inputs of *the Subset Sum model* of density 1.

Table 2 shows that the new reduced basis are obtained steel quite faster, while on average, they remain of a similar quality. Let us point out in particular, the optimal Schmidt algorithm which obtains an output vector at most twice longer than the the shortest output vector of the classical LLL algorithm, after a number of iterations that is on average three times less.

6 Conclusion

We have presented and analyzed two efficient variations of the LLL algorithm.

From a theoretical point of view, we have exhibited several threshold phenomena in random lattices of the uniform model: (1) The distribution function of ℓ_b/ℓ_a, when a and b are beginning indexes, which follows asymptotically a 0–1 law (2) the gap that occurs in the behaviors of these distribution functions as (a, b) becomes a pair of ending indexes, (3) the gap between the reduction probabilities of a random input for (s, γ)-Gram reduction ($\gamma > 0$) and s-Siegel reduction (which coincides with (s, γ)-Gram, with $\gamma = 0$).

From a practical point of view, empirical tests of Section 5 show that our new reductions are quite interesting. They provide some new tools for lattice reduction and can be very useful to build up an algorithmic strategy of reduction.

Acknowledgments. This work is part of my Ph.D. thesis [2]. I thank Brigitte Vallée, who is my thesis advisor, for regular helpful discussions. Many thanks to her and to Philippe Flajolet for their encouragement and for their help to improve the paper.

References

1. Ajtai, M. The shortest vector problem in L_2 is NP-hard for randomized reduction. *Elect. Colloq. on Comput. Compl.* (1997). (http://www.eccc.unitrier.de/eccc).
2. Akhavi, A. *Analyse comprative d'algorithmes de réduction sur les réseaux aléatoires.* PhD thesis, Université de Caen, 1999.
3. Bender, C., and Orzag, S. *Advanced Mathematical Methods for Scientists and Engineers.* MacGraw-Hill, New York, 1978.
4. Daudé, H., and Vallée, B. An upper bound on the average number of iterations of the LLL algorithm. *Theoretical Computer Science 123* (1994), 95–115.
5. De Bruijn, N. G. *Asymptotic methods in Analysis.* Dover, New York, 1981.
6. Kannan, R. Improved algorithm for integer programming and related lattice problems. In *15th ACM Symp. on Theory of Computing* (1983), pp. 193–206.
7. Kannan, R. Algorithmic geometry of numbers. *Ann. Rev. Comput. Sci. 2* (1987), 231–267.
8. Knuth, D. E. *The Art of Computer Programming*, 2nd ed., vol. 2: Seminumerical Algorithms. Addison-Wesley, 1981.
9. Lagarias, J. C. The computational complexity of simultaneous diophantine approximation problems. In *23rd IEEE Symp. on Found. of Comput. Sci.* (1982), pp. 32–39.
10. Lagarias, J. C. Solving low-density subset problems. In *IEEE Symp. on Found. of Comput. Sci.* (1983).
11. Lenstra, A. K., Lenstra, H. W., and Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann. 261* (1982), 513–534.
12. Lenstra, H. Integer programming with a fixed number of variables. *Math. Oper. Res. 8* (1983), 538–548.
13. Schnorr, C. P. A hierarchy of polynomial time lattice basis reduction algorithm. *Theoretical Computer Science 53* (1987), 201–224.
14. Schnorr, C. P. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In *Eurocrypt* (1995).
15. Schnorr, C. P., and Euchner, M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In *Proceedings of the FCT'91 (Altenhof, Germany), LNCS 529* (1991), Springer, pp. 68–85.
16. Schönhage, A. Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. In *Lect. Notes Comput. Sci.* (1984), vol. 172, pp. 436–447.
17. Sedgewick, R., and Flajolet, P. *An Introduction to the Analysis of Algorithms.* Addison-Wesley Publishing Company, 1996.
18. Vallée, B. Un problème central en géométrie algorithmique des nombres: la réduction des réseaux. Autour de l'algorithme LLL. *Informatique Théorique et Applications 3* (1989), 345–376.
19. Vallée, B., Girault, M., and Toffin, P. How to break Okamoto's cryptosystem by reducing lattice bases. In *Proceedings of Eurocrypt* (1988).
20. van Emde Boas, P. Another NP-complete problem and the complexity of finding short vectors in a lattice. *Rep. 81-04 Math. Inst. Univ. Amsterdam* (1981).
21. Whittaker, E., and Watson, G. *A course of Modern Analysis*, 4th ed. Cambridge University Press, Cambridge (England), 1927. reprinted 1973.