Worst-Case Hermite-Korkine-Zolotarev Reduced Lattice Bases

Guillaume Hanrot, Damien Stehlé

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Worst-Case Hermite-Korkine-Zolotarev Reduced Lattice Bases

Guillaume Hanrot — Damien Stehlé

N° 6422

Novembre 2007

Thème SYM

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--6422--FR+ENG

Worst-Case Hermite-Korkine-Zolotarev Reduced Lattice Bases

Guillaume Hanrot, Damien Stehlé*

Thème SYM — Systèmes symboliques
Projets Cacao et Arénaire

Rapport de recherche n° 6422 — Novembre 2007 — 25 pages

Abstract: The Hermite-Korkine-Zolotarev reduction plays a central role in strong lattice reduction algorithms. By building upon a technique introduced by Ajtai, we show the existence of Hermite-Korkine-Zolotarev reduced bases that are arguably least reduced. We prove that for such bases, Kannan's algorithm solving the shortest lattice vector problem requires $d^{\frac{d}{2e}(1+o(1))}$ bit operations in dimension d. This matches the best complexity upper bound known for this algorithm. These bases also provide lower bounds on Schnorr's constants α_d and β_d that are essentially equal to the best upper bounds. Finally, we also show the existence of particularly bad bases for Schnorr's hierarchy of reductions.

Key-words: Lattice basis reduction, shortest vector problem, HKZ-reduction, BKZ-reduction

* CNRS and Université de Lyon / ÉNS Lyon / LIP, 46 allée d'Italie, 69364 Lyon Cedex 07, France.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy (France)
Téléphone : +33 3 83 59 30 00 — Télécopie : +33 3 83 27 83 19

Bases Hermite-Korkine-Zolotarev réduites “pires cas”.

Résumé : La réduction d’Hermite-Korkine-Zolotarev joue un rôle central dans les algorithmes de réduction forte des réseaux. En utilisant une technique due à Ajtai, nous prouvons l’existence de bases Hermite-Korkine-Zolotarev réduites qui sont les plus mal réduites possible. Pour de telles bases, l’algorithme de Kannan pour la résolution du problème du vecteur le plus court nécessite $d^{\frac{d}{2e}(1+o(1))}$ opérations élémentaires en dimension d, ce qui coïncide avec la meilleure borne supérieure connue pour sa complexité. Ces bases fournissent également des bornes inférieures pour les constantes de Schnorr α_d et β_d, qui coïncident là encore avec les meilleures bornes supérieures connues. Enfin, nous montrons l’existence de mauvaises bases réduites pour les algorithmes de la hiérarchie de Schnorr.

Mots-clés : Réduction des réseaux, problème du vecteur le plus court, réduction HKZ, réduction BKZ

1 Introduction

A *lattice* L is a discrete subgroup of a euclidean space $\mathbb{R}^n$. Such an object can always be written as the set of integer linear relations of some linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d \in \mathbb{R}^n$. The $\boldsymbol{b}_i$'s form a *basis* of L. Such a representation is not unique, but all bases share the same cardinality d, called the lattice *dimension*. Another lattice invariant is the so-called lattice *volume* $\det(L)$, which is defined as the geometric d-dimensional volume of any parallelepiped $\mathcal{P}(\boldsymbol{b}_i) = \{\sum_i y_i \boldsymbol{b}_i, y_i \in [0,1]\}$ spanned by a lattice basis $(\boldsymbol{b}_i)_i$. When $d \geq 2$, a given lattice has an infinity of bases, related to one another by unimodular transformations. Some bases are better than others, in particular under the light of applications such as algorithmic number theory [5] and cryptography [15, 13]. In these applications, one is mostly interested in lattice bases made of rather short and rather orthogonal vectors. Such bases are called *reduced*. One often distinguishes between reductions that are rather weak but can be computing efficiently and reductions that are strong but that require a much larger amount of computational resources. The main reduction of the first family is the celebrated LLL-reduction [12], whereas the most famous one in the second family is the Hermite-Korkine-Zolotarev reduction (HKZ for short). There exist compromises between LLL and HKZ reductions, such as Schnorr's Block-Korkine-Zolotarev (BKZ) reductions [19] depending on a parameter k: the 2-BKZ reduction is essentially the LLL reduction whereas the d-BKZ reduction is exactly the HKZ reduction. Other compromises have been considered in [19, 18, 7].

From the algorithmic point of view, LLL-reduction can be reached in time polynomial in the lattice dimension. The other parameters, such as the dimension of the embedding space and the bit-size of the initial vectors are of small interest here since all the described algorithms have polynomial complexities with respect to them. On the other extreme, there are two main algorithms to compute an HKZ-reduced basis. The first one is due to Kannan [11] and was improved by Helfrich and Schnorr [9, 19]. Its complexity has been revised downwards by Hanrot and Stehlé [8] who proved a $d^{\frac{d}{2\mathrm{e}}(1+o(1))}$ upper bound. The other algorithm is due to Ajtai, Kumar and Sivakumar [2] and its complexity upper bound was re-assessed recently by Nguyen and Vidick [16]: its cost is provably bounded by $2^{5.9 \cdot d}$. The latter algorithm has a much better asymptotic complexity upper bound than Kannan's. However, it suffers from two drawbacks: firstly, it requires an exponential space whereas Kannan's space requirement is polynomial; secondly, it is probabilistic in the sense that there is a tiny probability that the computed basis is not HKZ-reduced, whereas Kannan's algorithm is deterministic. In practice, for manageable problem sizes, it seems that adaptations of Kannan's algorithm still outperform the algorithm of Ajtai, Kumar and Sivakumar. One of the results of the present paper is to provide a worst-case complexity lower bound to Kannan's algorithm which is essentially the same as the $d^{\frac{d}{2\mathrm{e}}(1+o(1))}$ complexity upper bound: it proves that from the worst-case point of view, Kannan's algorithm is asymptotically worse that the one of Ajtai, Kumar and Sivakumar. In the compromises between LLL and HKZ-reductions, an algorithm computing HKZ-reduced bases (either Kannan's or the one of Ajtai, Kumar and Sivakumar) is used on k-dimensional bases, where k is the parameter of the compromise. When k is greater than $c \log d$ for some constant c, the complexities of the compromise algorithms are $k^{O(k)}$ or $2^{O(k)}$ depending on the chosen HKZ-reduction algorithm.

The main result of the present paper is to prove the existence of HKZ-reduced bases which are arguably least reduced possible. These bases are good corner cases for strong lattice reductions. We prove that given them as input, Kannan's algorithm costs at least $d^{\frac{d}{2e}(1+o(1))}$ binary operations in dimension d, thus completing the worst-case analysis of Kannan's algorithm. This proves that the Ajtai-Kumar-Sivakumar algorithm is strictly better than Kannan's from the worst-case asymptotic time complexity perspective. These lattice bases also provide lower bounds on Schnorr's constants α_k and β_k which play a central role to estimate the quality of Schnorr's hierarchies of reductions. As a by-product, we improve the best known upper bound for α_k, and the lower and upper bounds essentially match. Our lower bound on β_k match its best known upper bound, provided by [7]. This gives weight to the fact that the primal-dual reduction therein may be better than Schnorr's classical hierarchy. Finally, we provide lattice bases that are particularly bad for Schnorr's hierarchy of reduction algorithms.

To achieve these results, we simplify and build upon a technique introduced by Ajtai in [1] to show lower bounds on Schnorr's constants α_k and β_k. These lower bounds were of the same orders of magnitude as the best upper bounds, but with undetermined constants in the exponents. It consists in building random lattice bases that are HKZ-reduced with non-zero probability and such that the quantities under investigation (e.g., Schnorr's constants) are close to the best known upper bounds. The random lattice bases are built from their Gram-Schmidt orthogonalisations.

ROAD-MAP. In Section 2 we provide the background that is necessary to the understanding to the rest of the article. In Section 3 we simplify Ajtai's method to generate lattice bases. We use it first in Section 4 to show the existence of worst-case HKZ-reduced bases with respect to the orthogonality of the basis vectors. Using these bases, we provide lower bounds to the worst-case cost of Kannan's algorithm and to Schnorr's constants α_k and β_k, in Section 5. We use Ajtai's technique a second time in Section 6 to build lattice bases that are particularly bad for Schnorr's hierarchy of reduction algorithms. Finally, in Section 7, we draw a list of possible natural extensions of our work.

NOTATION. If y is a real number, we let $\lfloor y \rceil$ denote its closest integer (with any rule for the ambiguous cases), and we define $\{y\} = y - \lfloor y \rceil$. If $a \leq b$, we let $[\![a, b]\!]$ denote the set of integers belonging to the interval $[a, b]$. All logarithms used are in basis e. Finally, for x a real number, we define $(x)_+ := \max(x, 0)$.

2 Background on Lattices

We refer to [4] for a complete introduction to lattices.

Gram-Schmidt orthogonalisation. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ be linearly independent vectors. We define $\boldsymbol{b}_i^* = \boldsymbol{b}_i - \sum_{j<i} \mu_{i,j} \boldsymbol{b}_j^*$ with $\mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2}$. The $\boldsymbol{b}_i^*$'s are orthogonal and, for any i, we have that the linear span of the $\boldsymbol{b}_j^*$'s for $j \leq i$ is exactly the span of the $\boldsymbol{b}_j$'s for $j \leq i$. If $j \leq i$, we denote by $\boldsymbol{b}_i(j)$ the projection of $\boldsymbol{b}_i$ orthogonally to the vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1}$. We have $\boldsymbol{b}_i(j) = \boldsymbol{b}_i^* + \sum_{k=j}^{i-1} \mu_{i,k} \boldsymbol{b}_k^*$.

Minkowski's inequality. For all integer $d \geq 1$, there exists a constant γ_d, called *Hermite's constant*, such that for any d-dimensional lattice L there exists a non-zero vector $\boldsymbol{b} \in L$ with $\|\boldsymbol{b}\| \leq \gamma_d^{1/2} \cdot (\det L)^{\frac{1}{d}}$. The latter relation is known as *Minkowski's inequality*. Hermite's constant satisfies $\gamma_d \leq d$. Asymptotically, one has $\frac{1.744d}{2\pi \mathrm{e}}(1+o(1)) \geq \gamma_d \geq \frac{d}{2\pi \mathrm{e}}(1+o(1))$ (see [10] for the upper bound). We define the *minimum* of a lattice L as the length of a shortest non-zero vector, and we let it be denoted by $\lambda(L)$. Minkowski's inequality can be easily restated in terms of the Gram-Schmidt orthogonalisation of any basis $(\boldsymbol{b}_i)_i$ of L since $\det(L) = \prod_i \|\boldsymbol{b}_i^*\|$:

$$\lambda(L) \leq \sqrt{d} \cdot \left(\prod_{i=1}^{d} \|b_i^*\| \right)^{\frac{1}{d}}.$$

Hermite-Korkine-Zolotarev reduction. A basis $(\boldsymbol{b}_i)_i$ of a lattice L is said to be *HKZ-reduced* if its first vector reaches the minimum of L and if orthogonally to $\boldsymbol{b}_1$ the other $\boldsymbol{b}_i$'s are themselves HKZ-reduced. This implies that for any i we have $\|\boldsymbol{b}_i^*\| \leq \sqrt{d-i+1} \cdot \left(\prod_{j=i}^{d} \|\boldsymbol{b}_j^*\| \right)^{\frac{1}{d-i+1}}$. We call these $d-1$ inequalities the *primary Minkowski inequalities*. Many other Minkowski-type inequalities are satisfied by an HKZ-reduced basis since the HKZ-reducedness of $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ implies the HKZ-reducedness of any basis $(\boldsymbol{b}_i(i), \ldots, \boldsymbol{b}_j(i))$ for any $i \leq j$.

Schnorr's hierarchies of reductions. A basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ is called *Block-Korkine-Zolotarev reduced* with block-size k (k-BKZ for short) if for any $i \leq d-k+1$ the k-dimensional basis $(\boldsymbol{b}_i(i), \ldots, \boldsymbol{b}_{i+k-1}(i))$ is HKZ-reduced. This reduction was initially called k-reduction in [19]. Schnorr also introduced the block-$2k$-reduction: a basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ is block-$2k$-reduced if for any $i \leq \lceil d/k \rceil - 2$, the basis $(\boldsymbol{b}_{ik+1}(ik+1), \ldots, \boldsymbol{b}_j(ik+1))$ with $j = \min(d, (i+2)k)$ is HKZ-reduced. Any $2k$-BKZ-reduced basis is block-$2k$-reduced and any block-$2k$-reduced basis is k-BKZ-reduced. In the following, we will concentrate on the BKZ hierarchy of reductions.

Schnorr's constants. In order to analyze the quality of the k-BKZ and block-$2k$ reductions, Schnorr introduced the constants

$$\alpha_k = \max_{(\boldsymbol{b}_i)_{i \leq k} \text{HKZ-reduced}} \frac{\|\boldsymbol{b}_1\|^2}{\|\boldsymbol{b}_k^*\|^2} \quad \text{and} \quad \beta_k = \max_{(\boldsymbol{b}_i)_{i \leq 2k} \text{HKZ-reduced}} \left(\frac{\prod_{i \leq k} \|\boldsymbol{b}_i^*\|^2}{\prod_{i > k} \|\boldsymbol{b}_i^*\|^2} \right)^{\frac{1}{k}}.$$

The best known upper bounds on α_k and β_k are $k^{1+\log k}$ and $\frac{1}{10}k^{2\log 2}$ (see [19, 7]). We will improve the upper bound on α_k in Section 5. Any k-BKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ of a lattice L satisfies $\|\boldsymbol{b}_1\| \leq \min\left(k^{\frac{d-1}{k-1}}, \alpha_k^{\frac{d-1}{k-1}-1} \right) \lambda(L)$. Ajtai [1] showed that $\alpha_k \geq k^{c \log k}$ for some constant c, so that the first upper bound is stronger than the second one. Furthermore, every block-$2k$-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{mk})$ of a lattice L satisfies $\|\boldsymbol{b}_1\| \leq \sqrt{k}\sqrt{\beta_k}^{m-1}\lambda(L)$ (see [19, 20]).

3 Ajtai's Drawing of HKZ-Reduced Bases

Consider a dimension $d > 0$ and a function $f : [\![1, d]\!] \to \mathbb{R}^+ \setminus \{0\}$. By generalising an argument due to Ajtai [1], we prove that one can build a d-dimensional lattice basis which is HKZ-reduced and such that $\|\boldsymbol{b}_i^*\| = f(i)$, under a "Minkowski-type" condition for the values of f.

Theorem 1 *Let $d > 0$ and $f : [\![1, d]\!] \to \mathbb{R}^+ \setminus \{0\}$. Assume that for any $j \leq d$, one has*

$$\sum_{i=1}^{j-1} \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)}\right) < 1.$$

Then there exists an HKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ with $\|\boldsymbol{b}_i^*\| = f(i)$.

The condition above might seem intricate at first glance, though it is in fact fairly natural. The term $(j-i)^{-\frac{j-i}{2}} \prod_{k=i}^{j} \frac{f(i)}{f(k)}$ resembles Minkowski's inequality. It is natural that it should occur for all (i, j), since for an HKZ-reduced basis Minkowski's inequality is satisfied for all bases $(\boldsymbol{b}_i(i), \ldots, \boldsymbol{b}_j(i))$. Another way of stating this is that a necessary condition for a basis to be HKZ-reduced would be

$$\forall j \leq d,\ \sum_{i=1}^{j-1} (4\gamma_{j-i+1})^{-\frac{j-i}{2}} \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)}\right) < 1.$$

This is merely a restatement of the fact that, since Minkowski's inequality is verified for any pair (i, j), the i-th term is at most $2^{-(j-i)}$, so that the sum is < 1. In view of the fact that asymptotically $\gamma_d \leq \frac{1.744d}{2\pi \mathrm{e}}(1 + o(1))$, we see that we are not far from an optimal condition.

Lemma 1 is the core of the proof of Theorem 1. It bounds the probability that when a random basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ is built appropriately, any lattice vector $\sum_i x_i \boldsymbol{b}_i$ with $x_d \neq 0$ will be longer than $\boldsymbol{b}_1$.

Lemma 1 *Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{d-1})$ be a lattice basis and let $\boldsymbol{b}_d$ be a random vector. We suppose that:*

1. *For any $i \leq d$, we have $\|\boldsymbol{b}_i^*\| = f(i)$.*
2. *The $\mu_{d,i}$'s for $i < d$ are independent random variables uniformly distributed in $[-1/2, 1/2]$.*

Let p be the probability that there exists $(x_1, \ldots, x_d)$ with $x_d \neq 0$ such that $\|\sum_i x_i \boldsymbol{b}_i\| \leq \|\boldsymbol{b}_1\|$. Then:

$$p \leq \left(\frac{2\pi \mathrm{e}}{d-1}\right)^{\frac{d-1}{2}} \sum_{x>0} \left(1 - \left(\frac{x f(d)}{f(1)}\right)^2\right)_+^{\frac{d-1}{2}} \left(\prod_{i<d} \frac{f(1)}{f(i)}\right).$$

Proof. Wlog we can assume $x_d > 0$. We can write

$$\sum_{i \leq d} x_i \boldsymbol{b}_i = \sum_{i \leq d} \left(x_i + \sum_{j=i+1}^{d} \mu_{j,i} x_j\right) \boldsymbol{b}_i^*.$$

For $i \leq d$, we define $u_i = x_i + \left\lfloor \sum_{j=i+1}^{d} \mu_{j,i} x_j \right\rceil$ and $\delta_i = \left\{ \sum_{j=i+1}^{d} \mu_{j,i} x_j \right\}$. Notice that $\delta_i = \left\{ \mu_{d,i} x_d + \sum_{j=i+1}^{d-1} \mu_{j,i} x_j \right\}$ is made of a random term ($\mu_{d,i} x_d$) and a constant term ($\sum_{j=i+1}^{d-1} \mu_{j,i} x_j$). Since $x_d \neq 0$ and since the $\mu_{d,i}$'s are distributed independently and uniformly in $[-1/2, 1/2]$, the

same holds for the δ_i's (for each fixed choice of $(x_1, \ldots, x_d)$). The event defining p can thus be rewritten as

$$\exists u_d \in \mathbb{Z}_{>0},\ \exists (u_1, \ldots, u_{d-1}) \in \mathbb{Z}^{d-1},\ \sum_{i<d} (u_i + \delta_i)^2 f(i)^2 \leq f(1)^2 - u_d^2 f(d)^2.$$

The probability of this event is 0 if $f(1)^2 - u_d^2 f(d)^2 < 0$. We shall thus assume in the sequel that $0 < u_d \leq f(1)/f(d)$. The probability p is then bounded by

$$\sum_{u_d \in \mathbb{Z} \setminus \{0\}} \sum_{(u_1, \ldots, u_{d-1}) \in \mathbb{Z}^{d-1}} \Pr\left(\sum_{i<d} (u_i + \delta_i)^2 f(i)^2 \leq f(1)^2 - u_d^2 f(d)^2 \right).$$

Let $c > 0$ be an arbitrary constant. We can estimate the last upper bound by using the inequality

$$\Pr\left(\sum_{i<d} (u_i + \delta_i)^2 f(i)^2 \leq f(1)^2 - u_d^2 f(d)^2 \right) \leq \int_{\boldsymbol{\delta} \in \left[-\frac{1}{2}, \frac{1}{2}\right]^{d-1}} \exp\left(c - c \frac{\sum_{i<d} (u_i + \delta_i)^2 f(i)^2}{f(1)^2 - u_d^2 f(d)^2} \right) d\boldsymbol{\delta}.$$

Summing over the u_i's, we obtain the estimate

$$\begin{aligned}
\sum_{\boldsymbol{u} \in \mathbb{Z}^{d-1}} \int_{\boldsymbol{\delta} \in \left[-\frac{1}{2}, \frac{1}{2}\right]^{d-1}} \exp\left(c - c \frac{\sum_{i<d} (u_i + \delta_i)^2 f(i)^2}{f(1)^2 - u_d^2 f(d)^2} \right) d\boldsymbol{\delta} \quad &= \\
&\int_{\mathbb{R}^{d-1}} \exp\left(c - c \frac{\sum_{i<d} \delta_i^2 f(i)^2}{f(1)^2 - u_d^2 f(d)^2} \right) d\boldsymbol{\delta} \\
&= \mathrm{e}^c \prod_{i<d} \int_{\mathbb{R}} \exp\left(-c \frac{\delta_i^2 f(i)^2}{f(1)^2 - u_d^2 f(d)^2} \right) d\delta_i \\
&= \mathrm{e}^c \left(\frac{\pi}{c} \right)^{\frac{d-1}{2}} \left(1 - \left(\frac{u_d f(d)}{f(1)} \right)^2 \right)^{\frac{d-1}{2}} \prod_{i<d} \frac{f(1)}{f(i)}.
\end{aligned}$$

Taking $c = (d-1)/2$ and summing over $x_d = u_d > 0$ yields the bound that we claimed. Recall that the terms corresponding to $u_d > f(1)/f(d)$ do not contribute. □

We now proceed to prove Theorem 1. We build the basis iteratively, starting with $\boldsymbol{b}_1$, chosen arbitrarily with $\|\boldsymbol{b}_1\| = f(1)$. Assume now that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1}$ have already been chosen with $\|\boldsymbol{b}_i^*\| = f(i)$ for $i < j$ and that they are HKZ-reduced. We choose $\boldsymbol{b}_j$ as $\boldsymbol{b}_j^* + \sum_{k<j} \mu_{j,k} \boldsymbol{b}_k^*$ such that $\|\boldsymbol{b}_j^*\| = f(j)$ and the random variables $(\mu_{j,k})_{k<j}$ are chosen uniformly and independently in $[-1/2, 1/2]$. Let $p_{i,j}$ be the probability that the vector $\boldsymbol{b}_i^*$ is not a shortest non-zero vector of $L(\boldsymbol{b}_i(i), \ldots, \boldsymbol{b}_j(i))$. This means that there exist integers $(x_i, \ldots, x_j)$ such that

$$\left\| \sum_{k=i}^{j} x_k \boldsymbol{b}_k(i) \right\| < \|\boldsymbol{b}_i^*\|.$$

Since $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1})$ is HKZ-reduced, so is $(\boldsymbol{b}_i(i), \ldots, \boldsymbol{b}_j(i))$ and thus we must have $x_j \neq 0$. Lemma 1 gives us

$$\begin{aligned} p_{i,j} &\leq \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \sum_{x>0} \left(1 - \left(\frac{xf(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j-1} \frac{f(i)}{f(k)}\right) \\ &\leq \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \left(\frac{f(i)}{f(j)}\right) \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j-1} \frac{f(i)}{f(k)}\right) \\ &\leq \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)}\right). \end{aligned}$$

We conclude the proof by observing that the probability of non-HKZ-reducedness of $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j)$ is at most $\sum_{i<j} p_{i,j}$. By hypothesis, this quantity is < 1. Overall, this means that there exist $\mu_{i,j}$'s such that $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j)$ is HKZ-reduced. □

The proof of the lemma and the derivation of the theorem may not seem tight. For instance, summing over all possible $(u_1, \ldots, u_d)$ might seem pessimistic in the proof of the lemma. We do not know how to improve the argument apart from the x_d part, for which, when $j - i$ is large, the term

$$\sum_{x>0} \left(1 - \left(x\frac{f(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}}$$

could be interpreted as a Riemann sum corresponding to the integral

$$\frac{f(i)}{f(j)} \cdot \int_0^{\pi/2} \sin^{j-i+1} x \, \mathrm{d}x \approx \frac{f(i)}{f(j)} \cdot \sqrt{\frac{\pi}{2(j-i+1)}}.$$

Notice however that if one uses the same technique to look for vectors of lengths smaller than $\sqrt{c \cdot d} \cdot \left(\prod_{i<d} f(i)\right)^{\frac{1}{d}}$ instead of $f(1)$, one finds that there exists a lattice where there is no vector shorter than this length (with $x_d \neq 0$) as soon as $c < \frac{1}{2\pi \mathrm{e}}$. We thus recover, up to the restriction $x_d \neq 0$, the asymptotic lower bound on Hermite's constant. As a consequence, it seems that the main hope of improvement would be to replace the sum (in the proof of the theorem) by a maximum, or something intermediate. Replacing by a maximum seems quite difficult. It would require to prove that, if vectors of lengths $\leq \|\boldsymbol{b}_1\|$ exist, then one of them has $x_d \neq 0$, at least almost surely. A deeper understanding of that kind of phenomenon would allow one to obtain refined versions of Theorem 1.

4 Worst-Case HKZ-reduced Bases

This section is devoted to the construction of an explicit function f satisfying the conditions of Theorem 1 as tightly as possible. In order to make explicit the fact that f depends on the underlying dimension d, we shall write f_d instead of f. Note that though $f(i)$ will depend on d,

this will not be the case for $f(d-i)$. Suppose that the basis $(\boldsymbol{b}_i)_i$ is HKZ-reduced. Then f_d must satisfy Minkowski-type inequalities, namely:

$$\forall i < j,\ f_d(i) \leq \sqrt{\gamma_{j-i+1}} \cdot \left(\prod_{k=i}^{j} f_d(k) \right)^{\frac{1}{j-i+1}}.$$

We choose f_d according to the strongest of those conditions, namely those we called the primary Minkowski inequalities, i.e., with $j = d$. It is known (see [17] for example) that this set of conditions does not suffice for an HKZ-reduced basis to exist. We thus expect to have to relax somehow these constraints. We will also replace the Hermite constant (known only for $d \leq 8$ and $d = 24$) by a more explicit term. For these reasons, we introduce

$$f_{\psi,d}(i) = \sqrt{\psi(d-i+1)} \cdot \left(\prod_{k=i}^{d} f_{\psi,d}(k) \right)^{\frac{1}{d-i+1}},$$

where ψ is be chosen in the sequel. This equation uniquely defines $f_{\psi,d}(i)$ for all i once we set $f_{\psi,d}(d) = 1$.

Theorem 2 *Let $\psi(x) = C \cdot x$ with $C = \exp(-6)$. Then, for all $1 \leq i < j \leq d$, we have*

$$(j-i+1)^{-\frac{j-i}{2}} \left(1 - \left(\frac{f_{\psi,d}(j)}{f_{\psi,d}(i)} \right)^2 \right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} \right) \leq \left(2\pi \mathrm{e} (\sqrt{\mathrm{e}}+1)^2 \right)^{-\frac{j-i}{2}}.$$

Thanks to Theorem 1, we obtain the following.

Corollary 1 *Let ψ be as in the previous theorem. There exist HKZ-reduced bases with*

$$\|\boldsymbol{b}_i^*\| = f_{\psi,d}(i) = \sqrt{d-i+1} \cdot \prod_{l=i+1}^{d} \left(C(d-l+2) \right)^{\frac{1}{2(d-l+1)}}.$$

Moreover, when $d-i$ grows to infinity, we have

$$\|\boldsymbol{b}_i^*\| = (d-i+1)^{\frac{1+\log C}{2}} \cdot \exp\left(\frac{\log^2(d-i+1)}{4} + O(1) \right).$$

The proof of the Theorem 2 follows from elementary analytical considerations. The elementary and somewhat technical nature of this proof leads us to postpone it to an appendix. It can be skipped without inconvenience for the general progression of the paper. We only give here an overview of the strategy.

First, we prove that $(j-i+1)^{-\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)} \right) < 1$. Then, in order to prove that the whole term is actually smaller than $\left(2\pi\mathrm{e}(\sqrt{\mathrm{e}}+1)^2\right)^{\frac{i-j}{2}}$, we need to consider four different cases. Let us write $a = d-i+1$ and $b = d-j+1$. This change of variables makes the problem independent of d.

- When a and b are very close, i.e., $a \geq b \geq a - 1.65\frac{a}{(\log a)^3}$, the term $(1 - (f(j)/f(i))^2)$ can be made arbitrarily small when a grows to infinity. For a large enough, this yields a sufficiently small exponential term.
- When a and b are not too close but not too far either, i.e., $a - 1.65\frac{a}{(\log a)^3} \geq b \geq \kappa a$ for any constant κ, the term $(j-i+1)^{-\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)}\right)$ is decreasing exponentially, at a rate which can be made arbitrarily large for a large enough (thanks to the "x" part of $\psi(x)$).
- When $a/b \to +\infty$, the "C" part of $\psi(x)$ provides an exponential term.
- Finally, for small a (the arguments used in the previous zones only work when a is large enough), we have to perform numerical computations to check that the inequality is indeed true.

Proof of the corollary. According to Theorem 2, we have

$$\begin{aligned}\sum_{i=1}^{j-1} \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f(i)}{f(k)}\right) &\leq \sum_{i=1}^{j-1} \left(\frac{j-i+1}{j-i}\right)^{\frac{j-i}{2}} \left(\sqrt{\mathrm{e}}+1\right)^{-(j-i)} \\ &< \sqrt{\mathrm{e}} \cdot \sum_{i \geq 1} (\sqrt{\mathrm{e}}+1)^{-i} = 1.\end{aligned}$$

The first part of the result follows from Theorem 1 and basic computations that are actually detailed in the appendix (Lemma 3). For the second part, note that our choice of ψ gives

$$2 \log f_{\psi,d}(i) = \log(d-i+1) + \sum_{l=i+1}^{d} \frac{\log C + \log(d-l+2)}{d-l+1}.$$

Suppose that $d - i \to +\infty$. We have

$$\begin{aligned}\left|\sum_{l=i+1}^{d} \frac{\log(d-l+2)}{d-l+1} - \int_i^d \frac{\log(d-x+1)}{d-x+1}\,\mathrm{d}x\right| &\leq \left|\sum_{l=i+1}^{d} \frac{\log(d-l+1)}{d-l+1} - \int_i^d \frac{\log(d-x+1)}{d-x+1}\,\mathrm{d}x\right| \\ &\quad + \sum_{l=i+1}^{d} \frac{1}{(d-l+1)^2}. \\ &\leq O(1) + \sum_{l=i+1}^{d} \int_{l-1}^{l} \left|\frac{\log(d-l+1)}{d-l+1} - \frac{\log(d-x+1)}{d-x+1}\right| \mathrm{d}x \\ &\leq O(1) + \sum_{l=i+1}^{d} \max_{x \in [l-1,l]} \frac{|1 - \log(d-x+1)|}{(d-x+1)^2} \;=\; O(1).\end{aligned}$$

Classically, we also have

$$\left|\sum_{l=i+1}^{d} \frac{\log C}{d-l+1} - \log(C) \cdot \log(d-i+1)\right| = O(1).$$

The result follows from the fact that $\int_i^d \frac{\log(d-x+1)}{d-x+1}\,\mathrm{d}x = \frac{\log^2(d-i+1)}{2}$. □

As a direct consequence of the Corollary, we also have

Corollary 2 *Let ψ be as in the previous theorem. There exist dual-HKZ-reduced bases with*

$$\|\boldsymbol{b}_i^*\| = f_{\psi,d}(i) = (\sqrt{d-i+1})^{-1} \cdot \prod_{l=i+1}^{d} (C(d-l+2))^{-\frac{1}{2(d-l+1)}}.$$

Moreover, when $d-i$ grows to infinity, we have

$$\|\boldsymbol{b}_i^*\| = (d-i+1)^{-\frac{1+\log C}{2}} \cdot \exp\left(-\frac{\log^2(d-i+1)}{4} + O(1)\right).$$

5 Lower Bounds Related to the HKZ-Reduction

The HKZ-reduced bases that we built in the previous section provide lower bounds to several quantities. It gives a lower bound on the complexity of Kannan's algorithm for computing a shortest non-zero vector [11] that matches the best known upper bound [8]. It also provides essentially optimal lower bounds to Schnorr's constants α_k and β_k.

5.1 Reminders on Kannan's Algorithm

A detailed description of Kannan's algorithm can be found in [19]. Its aim is to HKZ-reduce a given basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$. To do this, it first quasi-HKZ-reduces it, which means that $\|\boldsymbol{b}_1\| \leq 2\|\boldsymbol{b}_2^*\|$ and the basis $(\boldsymbol{b}_2(2), \ldots, \boldsymbol{b}_d(2))$ is HKZ-reduced. After this first step, it finds all solutions $(x_1, \ldots, x_d) \in \mathbb{Z}^d$ to the equation

$$\left\| \sum_{i=1}^{d} x_i \boldsymbol{b}_i \right\| \leq \|\boldsymbol{b}_1\|. \tag{1}$$

It keeps the shortest non-zero vector $\sum_{i=1}^{d} x_i \boldsymbol{b}_i$, which attains the lattice minimum, extends it into a lattice basis and HKZ-reduces the projection of the last $d-1$ vectors orthogonally to the first one.

The computationally dominant step is the second one, i.e., solving Equation (1). It is performed by enumerating all integer points within hyper-ellipsoids. Equation (1) implies that:

$$|x_d| \cdot \|\boldsymbol{b}_d^*\| \leq \|\boldsymbol{b}_1\|.$$

We consider all the possible integers x_d that satisfy this equation. For any of them, we consider the following equation, which also follows from Equation (1):

$$|x_{d-1} + \mu_{d,d-1} x_d| \cdot \|\boldsymbol{b}_{d-1}^*\| \leq \left(\|\boldsymbol{b}_1\|^2 - x_d \|\boldsymbol{b}_d^*\|^2\right)^{1/2}.$$

This gives a finite number of possibilities for the integer x_{d-1} to be explored.

Suppose that $(x_{i+1}, \ldots, x_d)$ have been chosen. We then consider the following consequence of Equation (1):

$$\left| x_i + \sum_{j>i} \mu_{j,i} x_j \right| \cdot \|\boldsymbol{b}_i^*\| \leq \left(\|\boldsymbol{b}_1\|^2 - \sum_{j>i} \left(x_j + \sum_{k>j} \mu_{k,j} x_k \right) \|\boldsymbol{b}_j^*\|^2 \right)^{1/2},$$

which gives a finite number of possibilities to be considered for the integer x_i.

Overall, Equation (1) is solved by enumerating all the integer points within the hyper-ellipsoids $\mathcal{E}_i = \left\{ (y_i, \ldots, y_d) \in \mathbb{R}^{d-i+1}, \| \sum_{j>i} y_j \boldsymbol{b}_j(i) \| \leq \|\boldsymbol{b}_1\| \right\}$.

5.2 On the cost of Kannan's algorithm

In this subsection, we provide a worst-case complexity lower bound to Kannan's algorithm by considering that the worst-case HKZ-reduced bases built in he previous section. For these, the first step of Kannan's algorithm has no effect, and we give a lower-bound to the cost of the second one by providing a lower bound to the sum of the cardinalities of the sets $\mathcal{E}_i \cap \mathbb{Z}^{d-i+1}$.

Lemma 2 *Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ be a lattice basis. The number of points enumerated by Kannan's algorithm is at least the sum of the number of integer points in each of the hyperellipsoids*

$$\mathcal{E}_i' = \left\{ (y_i, \ldots, y_d) \in (\mathbb{R} \setminus \{0\})^{d-i+1}, \sum_{j \geq i} y_j^2 \|\boldsymbol{b}_j^*\|^2 \leq \frac{4}{5} \|\boldsymbol{b}_1\|^2 \right\}.$$

Proof. Let $\phi : \mathbb{R}^{d-i+1} \to \mathbb{R}^{d-i+1}$ be defined by $\phi(y_i, \ldots, y_d) = (z_i, \ldots, z_d)$ such that $z_i = y_i - \left\lfloor \sum_{k>j} \mu_{k,j} z_j \right\rceil$. The function ϕ is injective. Indeed, $\phi(y_i, \ldots, y_d) = (z_i, \ldots, z_d)$ implies that $y_j = z_j + \left\lfloor \sum_{k>j} \mu_{k,j} z_j \right\rceil$, which means that $(z_i, \ldots, z_d)$ uniquely determines $(y_i, \ldots, y_d)$. Furthermore,

$$\sum_{j \geq i} z_j \boldsymbol{b}_j(i) = \sum_{j \geq i} \left(z_j + \sum_{k>j} \mu_{k,j} z_k \right) \boldsymbol{b}_j^* = \sum_{j \geq i} (y_j + \delta_j) \boldsymbol{b}_j^*,$$

for some $\delta_j \in [-1/2, 1/2]$. Hence, for $(y_i, \ldots, y_d) \in \mathcal{E}_i' \cap \mathbb{Z}^{d-i+1}$, the z_i's are integers and

$$\left\| \sum_{j \geq i} z_j \boldsymbol{b}_j(i) \right\| = \sum_{j \geq i} (y_j + \delta_j)^2 \|\boldsymbol{b}_j^*\|^2 \leq \sum_{j \geq i} \frac{5}{4} y_j^2 \|\boldsymbol{b}_j^*\|^2 \leq \|\boldsymbol{b}_1\|^2.$$

This implies that if $(y_i, \ldots, y_d) \in \mathcal{E}_i' \cap \mathbb{Z}^{d-i+1}$ then $\phi(y_i, \ldots, y_d) \in \mathcal{E}_i \cap \mathbb{Z}^{d-i+1}$ is indeed considered. □

We can now provide a lower bound to the cost of Kannan's algorithm. This lower bound is essentially the best possible, since it matches the upper bound of [8]. This also shows that the worst-case HKZ-reduced bases are worst-case inputs for Kannan's algorithm.

Theorem 3 *Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ be a lattice basis. Let i be such that $\|\boldsymbol{b}_j^*\| \leq \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}}$ for all $j \geq i$. Then, the number of points considered by Kannan's algorithm is at least*

$$2^{-d+i-1} \prod_{j \geq i} \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|}.$$

In particular, given as input the basis built in the previous section, Kannan's algorithm performs at least $d^{\frac{d}{2\mathrm{e}}(1+o(1))}$ operations.

Proof. The set $\mathcal{E}_i'$ contains the subset

$$\prod_{j \geq i}^{d} \left(\left[-\frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|}, \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|} \right] \setminus \{0\} \right).$$

This means that the cardinality of $\mathcal{E}_i' \cap \mathbb{Z}^{d-i+1}$ is greater than

$$\prod_{j \geq i} \left(2 \left\lfloor \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|} \right\rfloor - 1 \right) \geq \prod_{j \geq i} \left(2\frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|} - \frac{3}{2} \right) \geq \frac{1}{2^{d-i+1}} \prod_{j \geq i}^{d} \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}\|\boldsymbol{b}_j^*\|}.$$

This proves the first part of the theorem. It remains to evaluate this quantity for the basis built in the previous section. For this basis, we have, for any $i \leq d$,

$$\prod_{j \geq i} \frac{\|\boldsymbol{b}_i^*\|}{\|\boldsymbol{b}_j^*\|} = (\sqrt{C(d-i+1)})^{d-i+1}.$$

As a consequence, the number of operations performed by Kannan's algorithm given this basis as input is greater than

$$\left(\frac{C(d-i+1)}{4d} \right)^{\frac{d-i+1}{2}} \cdot \left(\frac{\|\boldsymbol{b}_1\|}{\|\boldsymbol{b}_i^*\|} \right)^{d-i+1},$$

for any i such that $\|\boldsymbol{b}_j^*\| \leq \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}}$ for $j \geq i$. We choose $i = \left\lfloor d\left(1 - \frac{1}{\mathrm{e}}\right) + \alpha \frac{d}{\log d} \right\rceil$, for some α to be fixed later. Let $j \geq i$. According to Corollary 1, if $d - j \to +\infty$, we have

$$\begin{aligned}
2\log\frac{\|\boldsymbol{b}_j^*\|}{\|\boldsymbol{b}_1\|} &= \frac{\log^2(d-j+1) - \log^2 d}{2} + (1+\log C)\left(\log(d-j+1) - \log d\right) + O(1) \\
&\leq \log\frac{d-j+1}{d}\left(\log d + 1 + \log C\right) + O(1) \\
&\leq \log\frac{d-i+1}{d}\left(\log d + 1 + \log C\right) + O(1) \\
&\leq \log\left(\frac{1}{\mathrm{e}} - \frac{\alpha}{\log d} + O\left(\frac{1}{d}\right)\right)\left(\log d + 1 + \log C\right) + O(1) \\
&\leq -\log d - \alpha\mathrm{e} + O(1).
\end{aligned}$$

For α and d large enough, we shall indeed have $\|\boldsymbol{b}_j^*\| \leq \frac{\|\boldsymbol{b}_1\|}{\sqrt{d}}$ for any $j \geq i$. Hence, since for this value of i we have $\left(\frac{\sqrt{d-i+1}}{\sqrt{d}}\right)^{d-i+1} = 2^{-O(d)}$ and $\left(\frac{\|\boldsymbol{b}_1\|}{\|\boldsymbol{b}_i^*\|}\right)^{d-i+1} = d^{\frac{d}{2\mathrm{e}}}/2^{O(d)}$, the lower bound becomes $d^{\frac{d}{2\mathrm{e}}}/2^{O(d)}$, which concludes the proof of the theorem. □

5.3 On Schnorr's Constants

First of all, we improve the best known upper bound for α_k from $k^{\log k+1}$ to $k^{\frac{\log k}{2}+O(1)}$. We will see below that this improved upper bound is essentially the best possible.

Theorem 4 *Let $k \geq 2$. Then $\alpha_k \leq k^{\frac{\log k}{2}+O(1)}$.*

Proof. Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k)$ be an HKZ-reduced basis. For any i, we have

$$\|\boldsymbol{b}_i^*\|^{k-i} \leq \sqrt{k-i+1}^{k-i+1} \prod_{j>i} \|\boldsymbol{b}_j^*\|$$

Let the sequence u_i be defined by $u_k = \|\boldsymbol{b}_k^*\|$ and $u_i^{k-i} = \sqrt{k-i+1}^{k-i+1} \prod_{j>i} u_j$. Then the sequence u_i dominates the sequence $\|\boldsymbol{b}_i^*\|$. Moreover,

$$\frac{u_i}{u_{i+1}} = \frac{\sqrt{k-i+1}}{\sqrt{k-i}} \sqrt{k-i+1}^{\frac{1}{k-i}},$$

which implies that

$$\frac{\|\boldsymbol{b}_1\|}{\|\boldsymbol{b}_k^*\|} \leq \frac{u_1}{u_k} \leq \sqrt{k} \prod_{i<k} \sqrt{i}^{\frac{1}{i-1}} \leq O(1)\sqrt{k} k^{\frac{\log k}{4}}.$$

This concludes the proof. □

We now show that the new upper bound on α_k and the upper bound $\beta_k \leq \frac{1}{10} k^{2\log 2}$ are essentially the best possible. They are in particular essentially reached for the worst-case HKZ-reduced bases of the previous section.

Theorem 5 *Let $k \geq 2$. We have:*

$$\alpha_k = k^{\frac{\log k}{2}+O(1)} \text{ and } \beta_k = k^{2\log 2 + O\left(\frac{1}{\log k}\right)}.$$

Proof. Consider a worst-case k-dimensional HKZ-reduced basis as described in the previous section. We have $\|\boldsymbol{b}_k^*\| = 1$, and $\|\boldsymbol{b}_1\| = k^{\log k - O(1)}$ follows from Corollary 1.

Now, we consider a worst-case $2k$-dimensional HKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{2k})$ of a lattice L as described in the previous section. We have the following lower bounds:

$$\frac{\prod_{i\leq k} \|\boldsymbol{b}_i^*\|}{\prod_{i>k} \|\boldsymbol{b}_i^*\|} = \frac{\det(L)}{\prod_{i>k} \|\boldsymbol{b}_i^*\|^2} = \left(\frac{\sqrt{2k}}{\sqrt{k}} \frac{\|\boldsymbol{b}_1\|}{\|\boldsymbol{b}_{k+1}^*\|}\right)^{2k}.$$

Furthermore, $\left(\frac{\|\boldsymbol{b}_1\|}{\|\boldsymbol{b}_{k+1}^*\|}\right)^4 = \exp\left(\log^2(2k) - \log^2(k) + O(1)\right) = k^{2\log 2} \exp(O(1))$, as claimed. □

6 Difficult Bases for the BKZ Reductions

In this section, we build lattice bases that are k-BKZ reduced, but far from being fully HKZ-reduced. In the previous section, we showed lower bounds to Schnorr's constants appearing in the quality analysis of the hierarchies of reductions. Here we prove lower bounds on the quality itself. Note that the lower bounds that we obtain are of the same order of magnitude as the corresponding upper bounds, but the involved constants are smaller. This suggests that it may not be possible to combine worst cases for Schnorr's constants in order to build bad bases for the BKZ hierarchy of reductions and that better upper bounds may be proved by using an amortised analysis.

In the following, we fix a block-size k. The strategy used to prove the existence of the basis is almost the same as in Section 3. The sole difference is that when we add a new basis vector $\boldsymbol{b}_j$, we only require $(\boldsymbol{b}_{j-k+1}(j-k+1), \ldots, \boldsymbol{b}_j(j-k+1))$ to be HKZ-reduced instead of $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j)$. This modification provides us the following result.

Theorem 6 *Let $d > k$ and $f : [\![1, d]\!] \to \mathbb{R}^+ \setminus \{0\}$. Assume that for any $j \leq d$, one has*

$$\sum_{i=\max(j-k+1,1)}^{j-1} \left(\frac{2\pi \mathrm{e}}{j-i}\right)^{\frac{j-i}{2}} \left(1 - \left(\frac{f(j)}{f(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{l=i}^{j} \frac{f(i)}{f(l)}\right) < 1.$$

Then there exists a k-BKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ with $\|\boldsymbol{b}_i^*\| = f(i)$.

We now give a function f that fulfils the requirements of Theorem 6.

Corollary 3 *Let k be an integer and $c < 1$ be a constant such that*

$$\sum_{l=1}^{k-1} \left(\frac{4\pi \mathrm{e}}{lc} \sinh(-l \log c)\right)^{\frac{l}{2}} < 1.$$

Then, there exists a k-BKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ with $\|\boldsymbol{b}_i^*\| = c^i$.

Proof. Let $f(i) = c^i$ for any $i \leq d$. The condition of Theorem 6 becomes

$$\forall j \leq d, \sum_{i=\max(j-k+1,1)}^{j-1} \left(\frac{2\pi \mathrm{e}}{j-i}\left(1 - c^{2(j-i)}\right) c^{-(j-i+1)}\right)^{\frac{j-i}{2}} < 1,$$

or equivalently

$$\forall j \leq d, \sum_{l=1}^{\min(k-1,j-1)} \left(\frac{2\pi \mathrm{e}}{l}\left(1 - c^{2l}\right) c^{-(l+1)}\right)^{\frac{l}{2}} < 1.$$

Since $k < d$, this condition is equivalent to the one stated in the corollary. □

Using the corollary above, one can compute a suitable constant c for any given block-size. For $k = 2$, one can take $c = 0.972$, for $k = 3$, one can take $c = 0.985$ and for $k \leq 10$, one can take $c = 0.987$. The optimal value of c seems to grow very slowly with k. However, it does grow since for any fixed c, the general term of the sum tends to $+\infty$ when l grows to $+\infty$. We can also derive the following general result, as soon as the block-size is large enough:

Corollary 4 *Let $d > k > 8\pi\mathrm{e}$. There exists a k-BKZ-reduced basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d)$ of a lattice L with $\|\boldsymbol{b}_i^*\| = \left(\frac{8\pi\mathrm{e}}{k-1}\right)^{\frac{i}{k}}$. In particular, for any such basis, we have:*

$$\frac{\|\boldsymbol{b}_1\|}{\lambda(L)} \geq \sqrt{d}\left(\frac{k-1}{8\pi\mathrm{e}}\right)^{\frac{d-1}{2k}}.$$

Proof. Let $c = \left(\frac{8\pi\mathrm{e}}{k-1}\right)^{\frac{1}{k}}$ and $\phi : x \mapsto \frac{1}{x}\sinh(x\log c)$. We have that

$$\phi'(x) = -\frac{1}{x^2}\sinh(x\log c) + \frac{\log c}{x}\cosh(x\log c) = \frac{\cosh(x\log c)}{x^2}(-\tanh(x\log c) + x\log c).$$

Since $\tanh x \leq x$ for any $x < 0$, we have that the function ϕ decreases when $x < 0$. As a consequence, we obtain that for any $l < k$,

$$\frac{4\pi\mathrm{e}}{lc}\sinh(-l\log c) \leq \frac{2\pi\mathrm{e}}{(k-1)}c^{-k} \leq 1/4.$$

It follows that the condition of Theorem 6 is satisfied. It now remains to give a lower bound to $\|\boldsymbol{b}_1\|/\lambda(L)$. We have $\|\boldsymbol{b}_1\| = \left(\frac{8\pi\mathrm{e}}{k-1}\right)^{\frac{1}{k}}$ and Minkowski's theorem gives us that

$$\lambda(L) \leq \sqrt{d}\left(\prod_i \|\boldsymbol{b}_i^*\|\right)^{\frac{1}{d}} = \sqrt{d}\left(\frac{8\pi\mathrm{e}}{k-1}\right)^{\frac{d+1}{2k}}.$$

This directly provides the second claim of the theorem. □

By comparing to 1 the last term of the sum in Corollary 3, one sees that the following must hold:

$$(c^{-k} - c^{k+2}) \leq \frac{k-1}{2\pi\mathrm{e}}.$$

This means that, apart from replacing $8\pi\mathrm{e}$ by $2\pi\mathrm{e}$ in Corollary 4, one cannot hope for a much better constant by using our technique.

7 Concluding Remarks

We showed the existence of bases that are particularly bad from diverse perspectives related to strong lattice reductions and strong lattice reduction algorithms. A natural extension of our work would be to show how to generate such bases efficiently, for example by showing that the probabilities of obtaining bases of the desired properties can be made extremely close to 1. Another difficulty related to this goal will be to transfer the results from the continuous model, i.e., $\mathbb{R}^n$, to a discrete space, e.g., $\mathbb{Q}^n$ with a bound on denominators.

Our results allow to claim that some algorithms/reductions are better than others from the worst-case asymptotic complexity point of view. This only gives a new insight on what should be done in practice. It is well-known (see [14] about the LLL algorithm) that low-dimensional lattices may behave quite differently from predicted by the worst-case high-dimensional results.

Acknowledgements

This work was initiated during the July 2007 seminar "Explicit methods in Number Theory" at Mathematisches Forschungsinstitut Oberwolfach. The authors are grateful to the MFO for the great working conditions provided on this occasion. The authors would also like to thank Jacques Martinet for the interest he showed for a preliminary version of those results and for pointing [17]. The second author thanks John Cannon and the University of Sydney for having hosted him while some of the present work was completed.

References

[1] M. Ajtai. The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice. In *Proceedings of the 35th Symposium on the Theory of Computing (STOC 2003)*, pages 396–406. ACM Press, 2003.

[2] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the 33rd Symposium on the Theory of Computing (STOC 2001)*, pages 601–610. ACM Press, 2001.

[3] H. Brönnimann, G. Melquiond, and S. Pion. The design of the Boost interval arithmetic library. *Theoretical Computer Science*, 351:111–118, 2006.

[4] J. W. S. Cassels. *An Introduction to the Geometry of Numbers, 2nd edition*. Springer-Verlag, 1971.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory, 2nd edition*. Springer-Verlag, 1995.

[6] CRLibm, a library of correctly rounded elementary functions in double-precision. `http://lipforge.ens-lyon.fr/www/crlibm/`.

[7] N. Gama, N. Howgrave-Graham, H. Koy, and P. Nguyen. Rankin's constant and blockwise lattice reduction. In *Proceedings of Crypto 2006*, number 4117 in Lecture Notes in Computer Science, pages 112–130. Springer-Verlag, 2006.

[8] G. Hanrot and D. Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm (extended abstract). In *Proceedings of Crypto 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 170–186. Springer-Verlag, 2007.

[9] B. Helfrich. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases. *Theoretical Computer Science*, 41:125–139, 1985.

[10] A. Kabatyanskii and V. I. Levenshtein. Bounds for packings. on a sphere and in space. *Proulcmy Peredacha informatsü*, 14:1–17, 1978.

[11] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the 15th Symposium on the Theory of Computing (STOC 1983)*, pages 99–108. ACM Press, 1983.

[12] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:513–534, 1982.

[13] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective*. Kluwer Academic Press, 2002.

[14] P. Nguyen and D. Stehlé. LLL on the average. In *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)*, volume 4076 of *Lecture Notes in Computer Science*, pages 238–256. Springer-Verlag, 2006.

[15] P. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*, volume 2146 of *Lecture Notes in Computer Science*, pages 146–180. Springer-Verlag, 2001.

[16] P. Nguyen and T. Vidick. Sieve algorithms for the shortest vector problem are practical. Submitted.

[17] R. A. Pendavingh and S. H. M. van Zwam. New Korkin-Zolotarev inequalities. *SIAM Journal on Optimization*, 18(1):364–378, 2007.

[18] C. P. Schnorr. Progress on LLL and lattice reduction. In *Proceedings of the LLL+25 conference*. To appear.

[19] C. P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[20] C. P. Schnorr. Block reduced lattice bases and successive minima. *Combinatorics, Probability and Computing*, 3:507–533, 1994.

Proof of Theorem 2

This section is devoted to proving Theorem 2. Since $\exp(5) > 2\pi\mathrm{e}(\sqrt{\mathrm{e}}+1)^2$, it suffices to prove the following result.

Theorem 7 *Let $\psi(x) = C \cdot x$ with $C = \exp(-6)$. Then for all $1 \leq i < j \leq d$, we have*

$$(j-i+1)^{-\frac{j-i}{2}} \left(1 - \left(\frac{f_{\psi,d}(j)}{f_{\psi,d}(i)}\right)^2\right)_+^{\frac{j-i}{2}} \left(\prod_{k=i}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)}\right) \leq \exp\left(-\frac{5}{2}(j-i)\right),$$

where $f_{\psi,d}(d) = 1$ and $f_{\psi,d}(i) = \sqrt{\psi(d-i+1)} \cdot \left(\prod_{k=i}^{d} f_{\psi,d}(k)\right)^{\frac{1}{d-i+1}}$.

We shall work separately with the following two terms of the theorem:

$$\left(1 - \left(\frac{f_{\psi,d}(j)}{f_{\psi,d}(i)}\right)^2\right)_+^{\frac{j-i}{2}} \quad \text{and} \quad \left(\prod_{k=i}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)}\right).$$

We call these terms T_1 and T_2. Another notation that we use is $a = d - i + 1$ and $b = d - j + 1$, which is natural since the function $x \mapsto f(d - x + 1)$ does not depend on d. The domain of valid pairs (a, b) is $1 \leq b < a \leq d$.

Notice that if $j = d$, then we can use the definition of $f_{\psi,d}$, and by bounding T_1 by 1, we obtain the sufficient condition:

$$\sqrt{d - i + 1} \exp(-3(d - i + 1)) \leq \exp\left(-\frac{5}{2}(d - i)\right),$$

which is valid. In the following, we will assume that $j < d$.

Our proof is made of four main steps. The first step consists in simplifying the expressions of the terms T_1 and T_2. In the second step, we try to obtain the result without the first term, i.e., while bounding T_1 by 1. We reach this goal for $a \geq 158000$ along with $b \leq a - \frac{1.65}{\log^3 a}$. In the third step, we use T_2 to obtain the result for $a \geq 158000$ along with $b \geq a - \frac{1.65}{\log^3 a}$. Finally, we prove the result for $1 \leq b < a \leq 158000$ with an exhaustive check of the inequality to be satisfied.

7.1 Explicit Formulas

The results of this subsection remain correct for any function ψ.

Lemma 3 *The following holds for any $k > i$:*

$$\frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} = \sqrt{\frac{\psi(d - i + 1)}{\psi(d - k + 1)}} \cdot \prod_{\ell=i+1}^{k} \psi(d - \ell + 2)^{\frac{1}{2(d-\ell+1)}}.$$

Proof. We have

$$f_{\psi,d}(i)^{d-i} = \psi(d - i + 1)^{\frac{d-i+1}{2}} \cdot \prod_{k=i+1}^{d} f_{\psi,d}(k)$$

and

$$f_{\psi,d}(i + 1)^{d-i} = \psi(d - i)^{\frac{d-i}{2}} \cdot \prod_{k=i+1}^{d} f_{\psi,d}(k).$$

By taking the quotient, we obtain

$$\frac{f_{\psi,d}(i)}{f_{\psi,d}(i + 1)} = \sqrt{\frac{\psi(d - i + 1)}{\psi(d - i)}} \cdot \psi(d - i + 1)^{\frac{1}{2(d-i)}}.$$

The lemma follows by induction. □

The following lemma simplifies the expression of the term T_2.

Lemma 4 *The following holds for any $j > i$:*

$$\prod_{k=i+1}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} = \left(\prod_{l=i+1}^{j} \frac{\psi(d-i+1)\psi(d-l+2)}{\psi(d-l+1)(d-l+2)^{\frac{d-j}{d-l+1}}} \right)^{\frac{1}{2}}.$$

Proof. We have

$$\prod_{k=i+1}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} = \left(\prod_{k=i+1}^{d} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} \right) \cdot \left(\prod_{k=j+1}^{d} \frac{f_{\psi,d}(j)}{f_{\psi,d}(k)} \right)^{-1} \cdot \left(\frac{f_{\psi,d}(i)}{f_{\psi,d}(j)} \right)^{j-d}.$$

The first two terms can be made explicit by using the definition of $f_{\psi,d}$, and the last one has been studied in Lemma 3. We get:

$$\begin{aligned}
\prod_{k=i+1}^{j} \frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} &= \frac{\psi(d-i+1)^{\frac{d-i+1}{2}}}{\psi(d-j+1)^{\frac{d-j+1}{2}}} \cdot \left(\frac{\psi(d-i+1)}{\psi(d-j+1)} \right)^{\frac{j-d}{2}} \cdot \left(\prod_{l=i+1}^{j} \psi(d-l+2)^{\frac{j-d}{2(d-l+1)}} \right) \\
&= \frac{\psi(d-i+1)^{\frac{j-i+1}{2}}}{\psi(d-j+1)^{\frac{1}{2}}} \cdot \prod_{l=i+1}^{j} \psi(d-l+2)^{\frac{j-d}{2(d-l+1)}} \\
&= \left(\prod_{l=i+1}^{j} \frac{\psi(d-i+1)\psi(d-l+2)}{\psi(d-l+1)\psi(d-l+2)^{\frac{d-j}{(d-l+1)}}} \right)^{\frac{1}{2}},
\end{aligned}$$

as claimed. □

Note that by writing $a = d - i + 1$ and $b = d - j + 1$, the two lemmas above give us:

$$T_1 = \left(1 - \frac{\psi(b)}{\psi(a)} \prod_{l=b}^{a-1} \psi(l+1)^{-\frac{1}{l}} \right)_{+}^{\frac{a-b}{2}} \quad \text{and} \quad T_2 = \left(\prod_{l=b}^{a-1} \frac{\psi(a)\psi(l+1)}{\psi(l)\psi(l+1)^{\frac{b-1}{l}}} \right)^{\frac{1}{2}}.$$

7.2 Temptative Proof of Theorem 7 Without Using T_1

We consider the logarithm of $(j-i+1)^{-\frac{j-i}{2}} T_2$ and try to show that it is smaller than $-\frac{5}{2}(j-i)$. Thanks to Lemma 4, this is equivalent to showing that:

$$-(a-b)\log(a-b+1) + \sum_{l=b}^{a-1} \left(\log\psi(a) - \log\psi(l) + \log\psi(l+1)\left(1 - \frac{b-1}{l}\right) \right) \leq -5(a-b). \tag{2}$$

We first try to simplify the summand.

Lemma 5 *Let $b \geq 2$ be an integer. The function $x \in [b, a-1] \mapsto -\log x + \log(x+1)\left(1 - \frac{b-1}{x}\right)$ is increasing for $x \geq b$ if $b \geq 3$ and for $x \geq 4$ if $b = 2$.*

Proof. The derivative is $\frac{\log(x+1)(b-1)(x+1)-bx}{x^2(x+1)}$. It follows that the function under study is increasing as soon as $\left(1+\frac{1}{x}\right)\log(x+1) \geq \frac{b}{b-1}$. The result follows from the facts that $\frac{b}{b-1} \leq 2$, that $\frac{5}{4}\log 5 > 2$ and that $\frac{4}{3}\log 4 > \frac{3}{2}$. □

By using Lemma 5, we obtain an upper bound to T_2 if we had taken $\psi(x) = x$ instead of $\psi(x) = C \cdot x$.

Lemma 6 *The following holds for $a \geq 8$:*

$$\begin{aligned}\sum_{x=b}^{a-1} & \left(\log a - \log x + \log(x+1)\left(1-\frac{b-1}{x}\right)\right) \\ & \leq (a-b)\log(a-b+1) + (a-b)\left(\log\frac{a^2}{(a-1)(a-b+1)} - \frac{b-1}{a-1}\log a\right)\end{aligned}$$

Proof. When $b \geq 3$, the result follows directly from Lemma 5, by noticing that for all $x \in [b, a-1]$ we have

$$-\log x + \log(x+1)\left(1-\frac{b-1}{x}\right) \leq -\log(a-1) + \log(a)\frac{a-b}{a-1}.$$

Suppose now that $b = 2$. It can be checked numerically that the inequality holds for $a = 8$. Suppose now that $a > 8$. We have:

$$\begin{aligned}\sum_{x=b}^{a-1}\left(\log a - \log x + \log(x+1)\left(1-\frac{1}{x}\right)\right) &\leq 6\log 7 + 6\left(\log\frac{64}{49} - \frac{1}{7}\log 8\right) \\ &+ \sum_{x=8}^{a-1}\left(\log a - \log(a-1) + \log(a)\frac{a-b}{a-1}\right) \\ &= \sum_{x=2}^{a-1}\left(\log a - \log(a-1) + \log(a)\frac{a-b}{a-1}\right),\end{aligned}$$

which gives the result. □

Notice that Lemma 6 implies that T_2 with $\psi(x) = x$ instead of $C \cdot x$ already compensates the term "$(a-b)\log(a-b+1)$" of Equation (2). Indeed, the function $\theta : b \mapsto \log\frac{a^2}{(a-1)(a-b+1)} - \frac{b-1}{a-1}\log a$ is convex and

$$\theta(2) = 2\log\frac{a}{a-1} - \frac{\log a}{a-1} \text{ and } \theta(a-1) = \log\frac{a}{2(a-1)} + \frac{\log a}{a-1}.$$

Both $\theta(2)$ and $\theta(a-1)$, and thus all $\theta(x)$ for $x \in [2, a-1]$, are ≤ 0 for $a \geq 8$.

We now consider the left hand-side of Equation (2) with $\psi(x) = C \cdot x$.

Lemma 7 *Let $\alpha(a,b) = \log\frac{a}{(a-b)} - \frac{b-1}{a-1}\log a$ and $\beta(a,b) = 1 - \frac{b}{a-b}\log\frac{a}{b}$. For $a \geq 8$, we have:*

$$\begin{aligned}-(a-b)\log(a-b+1) &+ \sum_{l=b}^{a-1}\left(\log\psi(a) - \log\psi(l) + \log\psi(l+1)\left(1-\frac{b-1}{l}\right)\right) \\ &\leq (a-b)\left(\alpha(a,b) + \beta(a,b)\log C\right).\end{aligned}$$

Proof. First of all, we have:

$$-(a-b)\log(a-b+1) + \sum_{l=b}^{a-1} \left(\log a - \log l + \log(l+1) \left(1 - \frac{b-1}{l}\right)\right) \leq \alpha(a,b).$$

This follows from Lemma 6 and the fact that $(a-1)(a-b+1) \geq a(a-b)$. We now consider the terms depending on C. Since $\sum_{x=b+1}^{a} \frac{1}{x} \leq \log \frac{a}{b}$ and $\log C < 0$, we have:

$$\sum_{l=b}^{a-1} \left(\log(C) \left(1 - \frac{b-1}{l}\right)\right) \leq \log(C) \left(a - b - (b-1)\log\frac{a}{b}\right) \leq \log(C)\beta(a,b),$$

which gives the result. □

In the following, we study the function $(a,b) \mapsto \alpha(a,b) + \beta(a,b)\log C$. We would like to bound it by -5, be we will be able to do this only for a subset of all possible values of the pair (a,b).

Lemma 8 *Let $0 < \kappa < 1$ be a real constant and suppose that $a \geq 8$. The function $a \mapsto \alpha(a,\kappa a) + \beta(a,\kappa a)\log C$ decreases with respect to a.*

Proof. We have

$$\alpha(a,\kappa a) + \beta(a,\kappa a)\log C = -\log(1-\kappa) + \log C \left(1 + \frac{\kappa \log \kappa}{1-\kappa}\right) - \frac{(\kappa a - 1)\log a}{a-1}.$$

Hence,

$$\frac{\partial}{\partial a}\left(\alpha(a,\kappa a) + \log C \beta(a,\kappa a)\right) = \frac{-\kappa a^2 + a\log a(\kappa - 1) + (\kappa+1)a - 1}{a(a-1)^2}.$$

For the numerator to be negative, it suffices that $a \geq 1 + \frac{1}{\kappa}$ (then the term in a^2 is larger than the term in a) or that $a \geq \exp\left(\frac{\kappa+1}{1-\kappa}\right)$ (then the term in $a\log a$ is larger than the term in a). Since

$$\max_{\kappa \in [0,1]} \min\left(1 + \frac{1}{\kappa}, \exp\left(\frac{\kappa+1}{1-\kappa}\right)\right) \leq 6,$$

the result follows. □

In the results above, we did not need $C = \exp(-6)$. The only property we used about C was $\log C < 0$. In the sequel, we define $\tau(a,\kappa) = \alpha(a,\kappa a) - 6\beta(a,\kappa a)$. We are to prove that $\tau(a,\kappa) \leq -5$ as soon as κ is not very close to 1.

Lemma 9 *For any $a \geq 755$, the function $\kappa \mapsto \tau(a,\kappa)$ increases to a local maximum in $\left[0, \frac{1}{2}\right]$, then decreases to a local minimum in $\left[\frac{1}{2}, 1 - \frac{1}{2\log a}\right]$ and then increases.*

Proof. We first study

$$\frac{\partial^3}{\partial\kappa^3}\tau(a,\kappa) = \frac{20\kappa^2 + 10\kappa^3 + 6 - 36\kappa - 36\kappa^2\log\kappa}{(1-\kappa)^4\kappa^2}.$$

Using the fact that $\log\kappa \leq (\kappa-1) - (\kappa-1)^2/2 + (\kappa-1)^3/3$ for $\kappa \in [0,1]$, we find that the numerator can be lower bounded by a polynomial which is non-negative for $\kappa \in [0,1]$. As a consequence, $\tau'_\kappa(a,\kappa) = \frac{\partial}{\partial\kappa}\tau(a,\kappa)$ is a convex function with respect to $\kappa \in (0,1)$.

Notice now that $\tau'_\kappa(a,\kappa) = -6\log\kappa + o(\log\kappa) > 0$ for κ close to 0, that $\tau'_\kappa(a,1/2) = -10 + 24\log 2 - \frac{a\log a}{a-1} \leq 0$ for $a \geq 755$, and finally that

$$\begin{aligned}\tau'_\kappa\left(a, 1 - \frac{1}{2\log a}\right) &= -10\log a - 24\log\left(1 - \frac{1}{2\log a}\right)\log^2 a - \frac{a}{a-1}\log a \\ &\geq 2\log a - \frac{a}{a-1}\log a,\end{aligned}$$

which is clearly positive for $a \geq 3$. □

The following lemma provides the result claimed in Theorem 7 for $a \geq 158000$ and $b \leq a - 1.65\frac{a}{\log^3 a}$.

Lemma 10 *Suppose that $a \geq 158000$. Then, for all $\kappa \leq 1 - 1.65\frac{1}{\log^3 a}$, we have $\alpha(a,\kappa a) - 6\beta(a,\kappa a) \leq -5$.*

Proof. Let $a_0 = 158000$. We have $\tau'_\kappa(a_0, 0.08962) > 0 > \tau'_\kappa(a_0, 0.08963)$. Furthermore, for $\kappa \in [0.0937, 0.0938]$, we have

$$|\tau'_\kappa(a_0,\kappa)| \leq \max\left(|\tau'_\kappa(a_0,0.08962)|, |\tau'_\kappa(a_0,0.08963)|\right) \leq 3\cdot 10^{-4}.$$

Hence,

$$\max_{\kappa\in[0.08962,0.08963]} \tau(a_0,\kappa) \leq \tau(a_0,0.08962) + 3\cdot 10^{-9} < -5.$$

Thanks to Lemmas 8 and 9, we have, for $a \geq 158000$:

$$\max_{\kappa\in[0,1/2]} \left(\alpha(a,\kappa a) - 6\beta(a,\kappa a)\right) \leq -5.$$

Furthermore, since $\frac{1}{2\log a} \geq \frac{1.65}{\log(a)^3}$ and thanks to Lemma 9, we have, for any $a \geq 158000$:

$$\max_{\kappa\in\left[\frac{1}{2}, 1-\frac{1.65}{\log^3 a}\right]} \tau(a,\kappa) = \max\left(\tau\left(a,\frac{1}{2}\right), \tau\left(a, 1 - \frac{1.65}{\log^3 a}\right)\right).$$

Notice that

$$\tau\left(a, 1 - \frac{1.65}{\log^3 a}\right) \leq \alpha\left(a, a - \frac{1.65a}{\log^3 a}\right) = -\log 1.65 + 3\log\log a - \log a + \frac{a}{a-1}\frac{1.65}{(\log a)^2},$$

which is decreasing with respect to $a \geq 158000$. Moreover, for $a = 158000$, its value is below -5. As a consequence,

$$\max_{\kappa\in\left[\frac{1}{2}, 1-\frac{1.65}{\log^3 a}\right]} \tau(a,\kappa) \leq \max\left(\tau\left(a,\frac{1}{2}\right), -5\right) \leq -5.$$

□

7.3 Using T_1 When $b > a - \frac{1.65a}{(\log a)^3}$

This section ends the proof of Theorem 7 for $a \geq 158000$.

Lemma 11 *Assume that $\psi(x) = e^{-6} \cdot x$. Then, for $a > b \geq a - 1.65\frac{a}{(\log a)^3}$ and $a \geq a_1 \geq 1782$, we have*

$$1 - \left(\frac{f_{\psi,d}(d-b+1)}{f_{\psi,d}(d-a+1)}\right)^2 \leq 1 - \exp\left(-1.65\frac{\log a_1 - 5}{\log^3 a_1 - 1.65}\right).$$

Proof. According to Lemma 3, we have

$$\begin{aligned} -2\log\frac{f_{\psi,d}(d-b+1)}{f_{\psi,d}(d-a+1)} &= \log\left(\frac{a}{b}\right) + \sum_{l=b}^{a-1}\frac{-6+\log(l+1)}{l} \\ &\leq \frac{1.65}{\log^3 a - 1.65} + (a-b)\frac{-6+\log a}{b}, \\ &\leq 1.65\frac{\log a - 5}{(\log a)^3 - 1.65}. \end{aligned}$$

This upper bound decreases with respect to $a \geq 1782$. □

By using Lemma 10 and the fact that $\beta(a,b) \leq 0$, we see that the left hand side of Equation (2) is upper bounded, for $b \geq a - 1.65\frac{a}{(\log a)^3}$ and $a \geq a_1 \geq 1782$, by:

$$(a-b)\log\left(1 - \exp\left(-1.65\frac{\log a_1 - 5}{\log^3 a_1 - 1.65}\right)\right) \leq (a-b)\log\left(1.65\frac{\log a_1 - 5}{\log^3 a_1 - 1.65}\right),$$

and the constant in the right hand side is below -5 when $a_1 = 158000$.

7.4 Small Values of a

It only remains to prove Theorem 7 for small values of a. The following lemma was obtained numerically. In order to provide a reliable proof, we used the Boost interval arithmetic library [3] and CRlibm [6] as underlying floating-point libraries.

Lemma 12 *Let $\psi(x) = e^{-6} \cdot x$. For any $2 \leq b < a \leq 158000$, we have*

$$(j-i+1)^{-\frac{j-i}{2}}\left(1 - \left(\frac{f_{\psi,d}(j)}{f_{\psi,d}(i)}\right)^2\right)_+^{\frac{j-i}{2}} \cdot \prod_{k=i+1}^{j}\frac{f_{\psi,d}(i)}{f_{\psi,d}(k)} \leq \exp\left(-5\frac{j-i}{2}\right),$$

with $i = d-a+1$ and $j = d-b+1$.

7.5 Concluding Remarks

The value of $C = \exp(-6)$ is not optimal. Given the line of proof used above (obtaining a geometric decreasing of the general term of the sum in Theorem 1), the best value of C that one can expect is limited by the term corresponding to $j = d$, $i = d - 1$, for which we must have $(2\pi\mathrm{e}) \cdot (2C) \leq \frac{1}{(\sqrt{\mathrm{e}}+1)^2}$.

Note however that the probability p of Lemma 1 involved in our criterion can be computed more precisely for small dimensional lattices, thus improving the optimal value of C that can be reached.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399