

A Measure Version of Gaussian Heuristic

Hao Chen *

May 3, 2016

Abstract

Most applicable lattice reduction algorithms used in practice are BKZ (Block-Korkine-Zolotarev) type algorithms as the blockwise generalizations of the LLL algorithm (Lenstra-Lenstra-Lovasz). Its original version was proposed by Schnorr and Euchner in 1991. The quality of reduced lattice bases is measured by the Hermitian factor $\frac{\|\mathbf{b}_1\|}{\text{vol}(\mathbf{L})^{1/d}}$ and the d -th root of this factor which is called root Hermitian factor. In Asiacrypt 2011 paper Y. Chen and Phong Q. Nguyen used BKZ with extreme pruning enumeration subroutine to handle the large block size lattice reduction with the purpose that the better root Hermitian factors can be expected. This BKZ 2.0 algorithm has been served as a base stone for the security evaluation of recent lattice-based cryptosystems such as fully homomorphic encryption and cryptographic multilinear mappings. In this paper we propose a measure version of Gaussian heuristic. This is a strict mathematical proven theorem. It can be used to give a strict mathematical proof for conjectured or simulated root Hermitian factors in BKZ 2.0 type algorithms and BKZ or slide reduction with large block-sizes. The theoretical analysis of these heuristic assumptions in the simulator of BKZ 2.0 type algorithms are also given.

Keywords: Lattice Reduction, Hermitian Invariant, BKZ, Slide Reduction, Root Hermitian Factor

1 Introduction

A lattice \mathbf{L} is a discrete subgroup in \mathbf{R}^d generated by d linear independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_d$ over the ring of integers, where $\mathbf{L} := \{a_1\mathbf{b}_1 + \dots + a_d\mathbf{b}_d :$

*Hao Chen is with the Department of Mathematics, School of Sciences, Hangzhou Dianzi University, Hangzhou, Zhejiang Province, 310018, China, haochen@hdu.edu.cn. This research is supported by NSFC Grants 11371138 and 11531002.

$a_1 \in \mathbf{Z}, \dots, a_d \in \mathbf{Z}$. The volume $vol(\mathbf{L})$ of this lattice \mathbf{L} is $\sqrt{\det(\mathbf{B} \cdot \mathbf{B}^T)}$, where $\mathbf{B} := (b_{ij})$ is the $d \times d$ generator matrix of this lattice, where $\mathbf{b}_i = (b_{i1}, \dots, b_{id}) \in \mathbf{R}^d$, $i = 1, \dots, d$, are the basis of this lattice. The dual lattice $\mathbf{L}^* := \{\mathbf{x} \in \mathbf{R}^d : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbf{Z}, \forall \mathbf{y} \in \mathbf{L}\}$. The length of the shortest non-zero lattice vector is denoted by $\lambda_1(\mathbf{L})$. The Hermitian invariant of this lattice \mathbf{L} is $\gamma_d(\mathbf{L}) = \frac{\lambda_1(\mathbf{L})^2}{vol(\mathbf{L})^{2/d}}$, which is closely related to the center density $\delta_d(\mathbf{L}) = \frac{(\lambda_1(\mathbf{L})/2)^d}{vol(\mathbf{L})} = \frac{\gamma_d(\mathbf{L})^{d/2}}{2^d}$ of the sphere packing from this lattice \mathbf{L} ([9, 30]). The supremum γ_d of $\gamma_d(\mathbf{L})$'s of all d dimensional lattices is called the d -dimensional Hermitian constant. Sometimes we use $L(\mathbf{x}_1, \dots, \mathbf{x}_m)$ to denote the lattice generated by vectors $\mathbf{x}_1, \dots, \mathbf{x}_m$.

From Minkowski's first theorem ([37]) we have $\frac{\lambda_1(\mathbf{L})}{vol(\mathbf{L})^{1/d}} \leq 2(\frac{1}{vol(\mathbf{B}_d)})^{1/d}$, where \mathbf{B}_d is the d dimensional unit hyper-ball and it is well-known $vol(\mathbf{B}_d) = \frac{(\pi)^{d/2}}{\Gamma(1+\frac{d}{2})}$. Hence $\gamma_d \leq 1 + \frac{d}{4}$ ([9, 37]). From Gaussian Heuristic $\frac{\lambda_1(\mathbf{L})}{vol(\mathbf{L})^{1/d}} \approx (\frac{1}{vol(\mathbf{B}_d)})^{1/d} = \frac{\Gamma(1+\frac{d}{2})^{1/d}}{\sqrt{\pi}} \approx \sqrt{\frac{d}{2\pi e}}$ ([4, 37, 13]). Here $GH(\mathbf{L}) = (\frac{1}{vol(\mathbf{B}_k)})^{1/k} vol(\mathbf{L})^{1/k}$ is the Gaussian Heuristic of the lattice. We denote $GH(k) = (\frac{1}{vol(\mathbf{B}_k)})^{1/k}$ as in [33].

Lattice reduction algorithms are used to find a "relatively short" lattice basis from an arbitrary given lattice basis. For example, Lagrange's algorithm (also attributed to Gauss, see [23] [15]) can be used to find the two minima of a dimension 2 lattice. Actually if $\mathbf{b}_1, \mathbf{b}_2$ is a lattice basis of a 2 dimensional lattice \mathbf{L} satisfying $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ and $\frac{\langle \mathbf{b}_2, \mathbf{b}_1 \rangle}{\|\mathbf{b}_1\|^2} \leq \frac{1}{2}$, then $\lambda_1(\mathbf{L}) = \|\mathbf{b}_1\|$, $\lambda_2(\mathbf{L}) = \|\mathbf{b}_2\|$ ([37]). However when the dimensions increase to 5 the situation is quite different ([30]).

The LLL algorithm [25] was proposed in 1982 and this has led to new development of reduction theory and lattice-based cryptanalysis ([38]). The block generalization of the LLL algorithm due to C.P. Schnorr and Euchner ([39, 43, 40, 41]) has been widely used in practice to get some block-HKZ reduced lattice bases. Lattice reduction has been played an essentially important role in lattice-based cryptanalysis ([38]) and lattice-based cryptography ([32, 34]). A much stronger version BKZ 2.0 by Y. Chen and Phong Q. Nguyen [7] was given in 2011-2013, with the enumeration with extreme pruning employed as sub-routine such that large block size k can be implemented. This BKZ 2.0 served as a base stone for the security evaluation of recent lattice-based cryptosystems ([27, 2, 26, 46]).

2 Preliminaries and our contribution

Lattice space. The space of all d dimensional lattices $\mathbf{X}_d = SL_d(\mathbf{R})/SL_d(\mathbf{Z})$ has a natural (normalized) $SL_d(\mathbf{Z})$ invariant measure μ_d satisfying $\mu_d(\mathbf{X}_d) = 1$ ([4, 36]).

Gram-Schmidt orthogonalization. Let $\mathbf{b}_1, \dots, \mathbf{b}_d$ be a basis of a dimension d lattice $\mathbf{L} \subset \mathbf{R}^d$, let π_i denote the orthogonal projection from \mathbf{R}^d to the orthogonal supplement of the linear span of $\mathbf{b}_1, \dots, \mathbf{b}_{i-1}$. The Gram-Schmidt orthogonalization is the orthogonal base $\mathbf{b}_1^*, \dots, \mathbf{b}_d^*$ of \mathbf{R}^d , recursively, $\mathbf{b}_1^* = \mathbf{b}_1, \mathbf{b}_2^* = \pi_2(\mathbf{b}_2), \dots, \mathbf{b}_i^* = \pi_i(\mathbf{b}_i)$. Equivalently we have $\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$ where $\mu_{i,j} = \frac{\langle \mathbf{b}_j, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_j^*\|^2}$, for $1 \leq j < i \leq d$.

We have $\lambda_i(\mathbf{L}) \geq \min_{i \leq j \leq d} \|\mathbf{b}_j^*\|$ and $\frac{\mathbf{b}_i}{\|\mathbf{b}_i\|^2} \in (\pi_j(L(\mathbf{b}_1, \dots, \mathbf{b}_i)))^*$ for any $j \in \{1, \dots, i\}$ ([37]).

If $\mu_{i,j} \leq \frac{1}{2}$, the basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ is called size-reduced. This reduction is easy with suitable substituting \mathbf{b}_i by $\mathbf{b}_i - \lceil \mu_{i,j} \rceil \mathbf{b}_j$.

HKZ (Hermitian-Korkine-Zolotarev) reduced basis. If a basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ is sized-reduced and $\mathbf{b}_i^* = \lambda_i(\pi_i(\mathbf{L}))$ for all $1 \leq i \leq d$, it is called HKZ-reduced. A HKZ reduction needs the SVP oracle and its running time is exponential. We have $\frac{4}{i+3} \leq \left(\frac{\|\mathbf{b}_i\|}{\lambda_i(\mathbf{L})}\right)^2 \leq \frac{i+3}{4}$ for $1 \leq i \leq d$, if $\mathbf{b}_1, \dots, \mathbf{b}_d$ is a HKZ-deduced basis of a d dimensional lattice \mathbf{L} ([24, 37]).

The LLL algorithm. A basis of a lattice satisfies the δ Lovasz condition for a constant $\delta \in [\frac{1}{4}, 1]$, if for all $1 \leq i \leq d$, $\delta \|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^* + \mu_{i+1,i} \mathbf{b}_i^*\|^2 = \|\pi_i(\mathbf{b}_{i+1}^*)\|^2$ or equivalently $(\delta - \frac{1}{4}) \|\mathbf{b}_i^*\|^2 \leq (\delta - \mu_{i+1,i}) \|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$. A sized reduced basis satisfying the Lovasz condition is called LLL reduced. The famous LLL algorithm [25] can be used to get a LLL reduced basis ($\delta < 1$) from a given lattice basis within polynomial time of the size of the input basis.

Enumeration and enumeration with extreme pruning The enumeration algorithm was considered in the middle of 1980's by U. Fincke and M. Phost [10] and R. Kannan [22]. It can be used to find the shortest non-zero lattice vectors $\mathbf{x} \in \mathbf{L}$ satisfying $\|\mathbf{x}\| \leq R$. If $\mathbf{b}_1, \dots, \mathbf{b}_d$ is a basis of this d dimensional lattice \mathbf{L} , from Gram-Schmidt orthogonalization, $\mathbf{x} = x_1 \mathbf{d}_1 + \dots + x_d \mathbf{b}_d = (x_1 + \mu_{2,1} x_2 + \dots + \mu_{d,1} x_d) \mathbf{b}_1^* + \dots + (x_j +$

$\sum_{i>j}\mu_{j,i}x_i)\mathbf{b}_j^* + \dots + x_d\mathbf{b}_d^*$. Thus recursively

$$|(x_j + \sum_{i>j}\mu_{i,j}x_i)| \leq \frac{\sqrt{R^2 - \sum_{k>j}(x_k + \sum_{i>k}\mu_{i,k}x_i)^2\|\mathbf{b}_k^*\|^2}}{\|\mathbf{b}_j^*\|}$$

. Then from $\mathbf{x}_d \in \mathbf{Z} \cap [-\frac{R}{\|\mathbf{b}_d\|}, \frac{R}{\|\mathbf{b}_d\|}]$ we have recursively

$$x_j \in \mathbf{Z} \cap [-\frac{\sqrt{R^2 - \sum_{k>j}(x_k + \sum_{i>k}\mu_{i,k}x_i)^2\|\mathbf{b}_k^*\|^2}}{\|\mathbf{b}_j^*\|} - \sum_{i>j}\mu_{i,j}x_i,$$

$$\frac{\sqrt{R^2 - \sum_{k>j}(x_k + \sum_{i>k}\mu_{i,k}x_i)^2\|\mathbf{b}_k^*\|^2}}{\|\mathbf{b}_j^*\|} - \sum_{i>j}\mu_{i,j}x_i]$$

. From this process of enumeration we can find the desirable \mathbf{x} .

The complexity of enumeration is $\sum_{k=1}^d \mathbf{N}_k$ where \mathbf{N}_k is the number of lattice points $|\pi_k(\mathbf{L}) \cap \mathbf{B}_k(R)|$ where $\mathbf{B}_k(R)$ is the ball centered at the origin with the radius R . From Gauss heuristic and Sterling formula we have (see [14, 20])

$$\mathbf{N}_k \approx 2^{O(d)} \frac{R^{d-k+1}}{(d-k+1)^{\frac{d-k+1}{2}} \prod_{j=k}^d \|\mathbf{b}_j^*\|}$$

It is obvious that the complexity of this enumeration algorithm depends on the choices of R and the ratios $\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_i^*\|}$. When the basis is quasi-HKZ, that is, $\pi_1(\mathbf{b}_2), \dots, \pi_1(\mathbf{b}_d)$ is HKZ reduced for the lattice $\pi_1(\mathbf{L})$, an upper bound $d^{\frac{d}{2\epsilon} + o(d)}$ for the complexity can be proved ([20]). A heuristic lower bound $d^{\frac{d}{8} + o(d)}$ was given in [37]. Practically only LLL-reduction on the basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ is pre-processed. Though the theoretical upper bound of the enumeration complexity in this case is $d^{O(d^2)}$ the experiments showed that the enumeration process is fast ([14, 37]).

The enumeration with pruning was first considered by Schnorr et al and revisited by Gama, Nguyen and Regev in [14] in 2010. In the above enumeration process we can start from $\mathbf{x}_d \in \mathbf{Z} \cap [-\frac{RR_d}{\|\mathbf{b}_d\|}, \frac{RR_d}{\|\mathbf{b}_d\|}]$ and recursively

$$x_j \in \mathbf{Z} \cap [-\frac{\sqrt{R^2 R_j^2 - \sum_{k>j}(x_k + \sum_{i>k}\mu_{i,k}x_i)^2\|\mathbf{b}_k^*\|^2}}{\|\mathbf{b}_j^*\|} - \sum_{i>j}\mu_{i,j}x_i,$$

$$\frac{\sqrt{R^2 R_j^2 - \sum_{k>j} (x_k + \sum_{i>k} \mu_{i,k} x_i)^2 \|\mathbf{b}_k^*\|^2}}{\|\mathbf{b}_j^*\|} - \sum_{i>j} \mu_{i,j} x_i]$$

, where R_d, R_{d-1}, \dots, R_1 are positive real numbers satisfying $0 < R_j < 1$ for $j = d, \dots, 1$. That is during the enumeration process some nodes in the enumeration tree are pruned. A success possibility p_{succ} that the desired \mathbf{x} can be found during this enumeration process is calculated in [14] under some reasonable heuristic hypotheses. The point here is the setting of suitable pruning coefficients R_d, \dots, R_1 such that a success probability $p > p_0$ can be satisfied.

The enumeration with extreme pruning is a process that with relatively easy pruning coefficients and a small success probability the enumeration is executed several times for randomized input lattice bases. For a randomized input lattice basis, do LLL reduction and then do the enumeration with these pruning coefficients. From the experiments in [14] it is quite effective to 110 dimensional hard knapsack lattices with high densities. Exponential speedups can be achieved by enumeration with pruning.

For the pruning in BDD (bounded distance decoding) solver via nearest plane algorithm and their applications in the security evaluation we refer to [28].

Blockwise HKZ reduced basis. A lattice basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ is called block-Korkine-Zolotarev reduced with block size k (k -HKZ reduced) if for any $i \leq d - k + 1$, the basis $\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_{i+k-1})$ is HKZ reduced basis of the k dimensional lattice $\pi_i(L(\mathbf{b}_i, \dots, \mathbf{b}_{i+k-1}))$. It is called block- $2k$ -reduced if for any $i \leq \lfloor d/k \rfloor - 2$, the basis $\pi_{ik+1}(\mathbf{b}_{ik+1}), \dots, \pi_{ik+1}(\mathbf{b}_{(i+2)k})$ (or $\pi_{ik+1}(\mathbf{b}_{ik+1}), \dots, \pi_{ik+1}(\mathbf{b}_d)$) is HKZ reduced ([39, 19]).

Any $2k$ -HKZ reduced basis is block- $2k$ -reduced and any block- $2k$ -HKZ-reduced basis is k -HKZ reduced. For Schnorr's block reduction algorithms we refer to [39, 43], the most used algorithm in practice is the BKZ in [40, 41]. In [13] the quality of the output block reduced bases of BKZ was experimentally assessed. In [7] a BKZ with extreme pruning enumeration algorithm was given so that the blockwise reduction with large block size reduction can be handled.

Schnorr’s constants. The Schnorr constant α_k and β_k were defined to measure the quality of block- $2k$ KZ reduced basis ([39, 43]). For a HKZ reduced basis $\mathbf{b}_1, \dots, \mathbf{b}_{2k}$ of a dimension $2k$ lattice \mathbf{L} , $\beta_k(\mathbf{L}) = (\frac{\|\mathbf{b}_1^*\| \dots \|\mathbf{b}_k^*\|}{\|\mathbf{b}_{k+1}^*\| \dots \|\mathbf{b}_{2k}^*\|})^{2/k}$ and $\beta_k = \max_{\forall \mathbf{L}, \forall \text{HKZ}} \beta_k$. $\alpha_k = \max_{\forall \text{HKZ} \mathbf{b}_i} \frac{\|\mathbf{b}_1\|^2}{\|\mathbf{b}_k^*\|^2}$ for all HKZ bases $\mathbf{b}_1, \dots, \mathbf{b}_k$ of all k dimensional lattices. The presently known best upper and lower bounds for the Schnorr constant are $k^{\log k} \leq \alpha_k \leq k^{\frac{\log k}{2} + O(1)}$ and $\frac{k}{12} \leq \beta_k \leq (1 + \frac{k}{2})^{2 \ln 2 + \frac{1}{k}}$ ([11, 19]). We refer to [6, 19] for the analysis of the Schnorr constant, the worst-cases of HKZ bases and block-Korkine-Zolotarev reduced bases.

Geometric series assumption. From experiments, the Gram-Schmidt norms $\mathbf{b}_1^*, \dots, \mathbf{b}_d^*$ after sufficient reduction often satisfy $\frac{\|\mathbf{b}_{i+1}^*\|}{\|\mathbf{b}_i^*\|} \approx q$ except the final several indices where $q \in [\frac{3}{4}, 1)$ ([43, 42, 13]). This is called the Geometric series assumption (GSA) in [42].

LLL and BKZ at average. The experiments in [13] assessed the Hermitian factor $\frac{\|\mathbf{b}_1\|}{\text{vol}(\mathbf{L})^{1/d}}$. In [13], $h^{1/d} = c$ is called Hermitian factor constant and later this has been called root Hermitian factor widely in the literature ([35, 1, 2, 26, 46]). It was checked the root Hermitian factors converge when d grows to large ([13], Figure 5). It was also checked the effect of the LLL algorithm and the BKZ-20, BKZ-28 algorithms on some lattices (see Table 1 below, as listed in Table 1 in [13]).

Table 1 Root Hermitian factors for LLL and small block BKZ

algorithm	LLL	BKZ-20	BKZ-28	DEEP-50
c	1.0219	1.0128	1.0109	1.011
theory	1.0754	1.0337	1.0282	1.0754

Slide reduction algorithm and self-dual BKZ. We refer slide reduction to [12] and [37]. Originally it was reported that the slide reduction is outperformed by BKZ. In [33] experimental results about the quality of reduced basis by slide reduction was given and it was reported they are quite good when the blocksize is bigger than 50. A new version of BKZ called self-dual BKZ with enumerations on both projected lattices and projected dual lattices was proposed in [33]. The related Hermitian factor and root Hermitian factor were analysed under the assumption of Gaussian heuristic.

BKZ and BKZ 2.0 algorithms. BKZ algorithms (with the Schnorr et al version of enumeration pruning as a sub-routine) were implemented in Number Theory library [45]. In [21] a variant of BKZ ([40, 41]) algorithm and a strict theoretical analysis of its running time was given. A terminating condition was introduced which aborts BKZ within a small number of tours to enumeration. The upper bound from theoretic analysis is Hermitian factor $h = 2(\nu_k)^{\frac{d-1}{2(k-1)} + \frac{3}{2}}$. Here $\nu_k = \max\{\gamma_1, \dots, \gamma_k\}$ is the maximum of Hermitian's constants within dimension k .

A much stronger version BKZ 2.0 by Y. Chen and Phong Q. Nguyen [7] was given in 2011-2013, with the enumeration with extreme pruning employed as sub-routine such that large block size k can be implemented. It executes a LLL reduction on the input basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ and then run small block size BKZ for each projected lattice $\pi_j(\mathbf{L}(\mathbf{b}_j, \dots, \mathbf{b}_{j+k-1}))$ for $j = 1, \dots, d - k + 1$ before goto the enumeration with extreme pruning. Then run enumeration with extreme pruning for the projected lattices $\pi_j(\mathbf{L}(\mathbf{b}_j, \dots, \mathbf{b}_{j+k-1}))$ for $j = 1, \dots, d - k + 1$ to find $(v_j, \dots, v_{j+k-1}) \in \mathbf{Z}^{j-k+1}$ such that $\pi_j(\sum_{i=j}^{j+k-1} v_i \mathbf{b}_i)$ is a lattice vector with the length equal to $\lambda_1(\pi_j(\mathbf{L}(\mathbf{b}_j, \dots, \mathbf{b}_{j+k-1})))$. The algorithm inserts the lattice vector $\sum_{i=j}^{j+k-1} v_i \mathbf{b}_i$ between \mathbf{b}_{j-1} and \mathbf{b}_j . The LLL algorithm and some BKZ- k algorithms before the enumeration subroutine are needed. The algorithm execute several rounds of the above process. In order to reduce the time of enumeration with extreme pruning several BKZ with block size 50 and 60 are often executed on local blocks. The terminating condition in [21] was used to abort the algorithm.

This BKZ 2.0 served as a base stone for the security evaluation of recent lattice-based cryptosystems ([27, 2, 26, 46, 33]). As described in [1] Section 3.2, the Gaussian heuristic $R = \sqrt{1.1}(\frac{1}{\text{vol}(\mathbf{B}_k)})^{1/k} = 1.0488(\frac{1}{\text{vol}(\mathbf{B}_k)})^{1/k}$ was used as the bound of the enumeration with extreme pruning ([7], section 4.3). We refer to [8, 2] for the detailed description of BKZ 2.0 and the estimated time needed to get sufficiently good root Hermitian factor ([21, 2], see page 9 [2]). In [1] an optimization of BKZ 2.0 was given.

Conjectured and simulated root Hermitian factor. In [7] the root Hermitian factors for large block sizes were conjectured from a simulation algorithm of Gram-Schmidt sequences $(\|\mathbf{b}_1^*\|, \|\mathbf{b}_2^*\|, \dots, \|\mathbf{b}_d^*\|)$. Some estimations for root Hermitian factors and time needed to achieve them have been studied in [46, 26, 2, 33] for security evaluation of and the hard-

ness of lattice and LWE computation problems. The limit of root Hermitian factors when the lattice dimensions go to infinity was argued in [8] (also see page 8 of [2]). Assuming Gaussian heuristic and geometric series assumption the limit of root Hermitian factors of a basis after BKZ 2.0 type reduction when the dimensions of the lattices tends to the infinity was analysed in [8] (page 95-96 of [8] and also see page 8 of [2]), $\lim_{d \rightarrow \infty} c_{d, BKZ2.0} = \left(\frac{1}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}} \approx \left(\frac{k}{2\pi e} (\pi k)^{\frac{1}{k}}\right)^{\frac{1}{2(k-1)}}$. In [33] the root of Hermitian factor of block-size k $c_k = GH(k)^{\frac{1}{k-1}}$ was proved under the Gaussian heuristic ([33], page 15, Corollary 1).

The following table is Table 4.1 in page 96 of [8].

Table 2 Limits of the root Hermitian factors for block size $50 \leq k \leq 1000$

k	50	60	70	80	90	100	110
$\lim c_{BKZ2.0}$	1.0121	1.0115	1.0108	1.0103	1.0097	1.0093	1.0088
k	120	130	140	150	160	170	180
$\lim c_{BKZ2.0}$	1.0084	1.0081	1.0078	1.0075	1.0072	1.0067	1.0065
k	190	200	210	220	230	240	250
$\lim c_{BKZ2.0}$	1.0065	1.0063	1.0061	1.0059	1.0058	1.0056	1.0055
k	300	400	500	600	700	800	1000
$\lim c_{BKZ2.0}$	1.0048	1.0040	1.0034	1.0030	1.0027	1.0024	1.0020

Our Contribution. We will give theoretical explain for the behaviour of the root Hermitian factors from the distribution of Hermitian invariants on the lattice space \mathbf{X}_d .

A measure version of Gaussian Heuristic: In section 2 we give a measure version of Gaussian heuristic which estimates the measure of the set of lattices having their $\lambda_1(\mathbf{L}) \approx GH(\mathbf{L})$. Then it is clear that above 95 percent of lattices of the dimension $d \geq 86$ satisfy $0.952GH(\mathbf{L}) \leq \lambda_1(\mathbf{L}) \leq 1.067GH(\mathbf{L})$ from this measure version of Gaussian heuristic. In the simulation algorithm in section 6.1 of [7], they assumed that $\lambda_1(\mathbf{L}) = GH(\mathbf{L})$ for all projected lattices of suitable large dimensions during the reduction process, based on the intuition that almost all lattices of suitable large dimensions are "random". Our results give a theoretical explain of their this assumption.

Theoretical analysis for root Hermitian factors: When the blocksize is large, these root Hermitian factors were conjectured as in the above Table 2

from a simulation algorithm in [7] section 6.1, 6.2 and the theoretical analysis described above (see page 93-96 of [8], page 15 of [33]). From the measure version of Gaussian heuristic and under geometric series assumption we give a theoretical proof of these root Hermitian factors (see section 3.3). Actually it is more suitable to argue that they are in some ranges around $GH(k)^{\frac{1}{k-1}}$. In this way some information that the root Hermitian factor that a BKZ 2.0 type algorithm or a slide reduction with this block size cannot achieve can be given (as remarked in the Conclusion and Future Work of [33]).

Combining with Micciancio-Walter's Self-Dual BKZ. The basic assumption in Section 5 of [33] is that every lattice that is passed to the SVP oracle during the self-dual BKZ satisfies the Gaussian heuristic. We can say that with the probability at least $(0.95)^U$, where U is the number of k dimensional lattices passed to the SVP oracle during the self-dual BKZ in [33], all results in Section 5 of [33] including the argument for GSA are true in the sense that $\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{i+1}^*\|}$'s are within a small range around $GH(k)^{\frac{1}{k-1}}$, because the argument there can be strictly based on the proven measure version of Gaussian heuristic.

3 A measure version of Gaussian heuristic

The following Siegal's mean value theorem has pioneered the research about the average behaviour of lattice invariants ([44, 18]).

Siegal's mean value theorem. *Let f be a Riemann integrable function on \mathbf{R}^d , then $\int_{\mathbf{X}_d} \sum_{\mathbf{v} \in \mathbf{L}-\mathbf{0}} f(\mathbf{v}) d\mu_d = \int_{\mathbf{R}^d} f dx$.*

G. A. Margulis proved the following random Minkowski theorem [29].

Theorem 3.1 (Margulis 2011) *Let m be the Borel measure on \mathbf{R}^d , there exists a constant C_d only depending on d such that for any measurable set $\mathbf{A} \subset \mathbf{R}^d$, $\mu_d(\{\mathbf{L} \in \mathbf{X}_d : \mathbf{L} \cap \mathbf{A} = \emptyset\}) \leq \frac{C_d}{m(\mathbf{A})}$. Here $C_d = 8 \frac{\zeta(d)}{\zeta(d-1)}$.*

We have the following version of Gaussian Heuristic from Margulis Theorem and Siegal's mean value theorem.

Theorem 3.2 (measure version of Gaussian Heuristic) *For any big positive real constant x $\mu_d\{\mathbf{L} \in \mathbf{X}_d : \lambda_1(\mathbf{L}) \leq (\frac{x}{\text{vol}(\mathbf{B}_d)})^{1/d}\} \geq 1 - \frac{C_d}{x}$.*

any small positive real constant $x' < 1$, $\mu_d\{\mathbf{L} \in \mathbf{X}_d : \lambda_1(\mathbf{L}) \geq (\frac{x'}{\text{vol}(\mathbf{B}_d)})^{1/d}\} \geq 1 - \frac{x'}{2}$. Thus we have

$$\mu_d\{\mathbf{L} \in \mathbf{X}_d : (\frac{x}{\text{vol}(\mathbf{B}_d)})^{1/d} \geq \lambda_1(\mathbf{L}) \geq (\frac{x'}{\text{vol}(\mathbf{B}_d)})^{1/d}\} \geq 1 - \frac{C_d}{x} - \frac{x'}{2}$$

For example when the dimension $d \geq 117$, then above 95 percent of lattices of dimension d has their lengths of shortest non-zero lattice vectors in the range $0.97(\frac{1}{\text{vol}(\mathbf{B}_d)})^{1/d} \leq \lambda_1 \leq 1.0488(\frac{1}{\text{vol}(\mathbf{B}_d)})^{1/d}$.

4 Analysis

4.1 Gaussian Heuristic in lattice challenge

In lattice challenge including random (Goldstein-Mayer) lattices and ideal lattices ([47]), the length of the targeted lattice vector is required within $1.05GH$. Since $(1.05)^d > 256$ when $d \geq 115$ above 95 percent lattices of dimension $d \geq 115$ satisfy $\lambda_1(\mathbf{L}) \leq 1.05GH(\mathbf{L})$ from Theorem 2.4, this requirement is quite reasonable. Actually above 99 percent of lattice of dimensions $d \geq 140$ satisfy $\lambda_1(\mathbf{L}) \leq 1.05GH(\mathbf{L})$. Hence we suggest the requirement $1.022933673GH$ when $d \geq 300$ and $1.0001219828GH$ when $d \geq 400$ in ideal lattice challenge, since above 99 percent of lattices satisfy this requirement.

4.2 Gaussian Heuristic in BKZ 2.0 and progressive BKZ

In enumeration sub-routine of BKZ 2.0 [7, 8] $\sqrt{1.1}GH$ of the projected block lattices was used. More importantly in the simulation algorithm to estimate the root Hermitian factors in section 6.1 of [7] $\lambda_1 = GH$ for the projected block lattices was used when the block size is large. As explained in section 6.1 of [7], the intuition is in the large block size case most lattices are considered as "random" lattices so that Gaussian Heuristic can be used. From the following proposition we give a theoretical ground for their intuition and experimental observation.

Proposition 4.1. *Above 95.30419355... percent of lattices of the dimension $k \geq 86$ satisfy $(0.147)^{1/k}GH(\mathbf{L}) \leq \lambda_1(\mathbf{L}) \leq (256)^{1/k}GH(\mathbf{L})$.*

Proof. It is direct from Theorem 3.2.

In the following table we listed the ranges in the above proposition.

Table 3 Ranges of λ_1 for most lattices of the dimension k

k	86	117	132	168	216	286
$\frac{\lambda_1}{GH}$	0.952-1.067	0.964-1.0485	0.969-1.043	0.975-1.034	0.98-1.026	0.985-1.0196
fraction	0.953	0.953	0.953	0.953	0.953	0.953

In section 3.1 of [1] modified Gaussian heuristic constants τ_i for dimensions $i \leq 50$ as in Fig 2 in page 9 of [1] were used for more explicit simulator. We suggest $\tau_i = (256)^{\frac{1}{i}}$ from our measure version of Gaussian heuristic since above 95 percent lattices in \mathbf{X}_i satisfying $\frac{\lambda_1(\mathbf{L})}{GH(\mathbf{L})} \leq (256)^{1/i}$.

4.3 Combining with Micciancio-Walter self dual BKZ

Combining the measure version of Gaussian heuristic and the Corollary 2 in page 15 of [33] we have the following result which guarantee the geometric series assumption is correct under certain probability.

Corollary 4.1 *With the probability $(0.95)^U$ where U is the number of the k dimensional lattices passed to the SVP oracle in the self-dual BKZ algorithm in [33], the reduced lattice basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ satisfy $\|\mathbf{b}_i^*\|$ is in the small range $[0.99858739 \dots GH(k)^{\frac{d+1-2i}{2(k-1)}} \text{vol}(\mathbf{L})^{1/d}, 1.00040865829 \dots GH(k)^{\frac{d+1-2i}{2(k-1)}} \text{vol}(\mathbf{L})^{1/d}]$ for $i \leq d - k$.*

4.4 The conjectured and simulated root Hermitian factors

The root Hermitian factor of BKZ 2.0 algorithm has played a fundamental role in the security evaluation of lattice-based cryptography and the hardness of LWE problems ([35, 2, 46, 26]). They are extrapolated from the simulation algorithm and theoretical analysis in [7, 8] (see [35, 46, 26, 2]). Here we give a theoretical proof of root of Hermitian factors of BKZ 2.0 with large block sizes from our measure version of Gaussian heuristic.

Theorem 4.1. *Under the Geometric series assumption, the root Hermitian factors of above 95 percent of lattices when the blocksize $k \geq 117$ satisfy*

that they are with in $[0.99858739\dots GH(k)^{\frac{1}{k-1}}, 1.00040865829\dots GH(k)^{\frac{1}{k-1}}]$.

Proof. If we assume that the lattice basis of the projected lattice $\mathbf{L}_{j,k} = \pi_j(\mathbf{L}(\mathbf{b}_j, \dots, \mathbf{b}_{j+k-1}))$ reduced by BKZ 2.0 satisfies the some Geometric Series Assumption, that is, $\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_{i+1}\|} = q$ where q is a constant. Then its Hermitian invariant is $\gamma_k(\mathbf{L}_{j,k}) = \frac{\|\mathbf{b}_j^*\|^2}{(\prod_{i=j}^{j+k-1} \|\mathbf{b}_i^*\|)^{2/k}} \approx \frac{q^{2(k-1)} \|\mathbf{b}_{j+k-1}^*\|^2}{q^{k-1} \|\mathbf{b}_{j+k-1}^*\|^2} = q^{k-1}$. From the measure version of Gaussian heuristic (Theorem 3.2) the subset in \mathbf{X}_k of the lattices satisfying

$$\left(\frac{x'}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}} \leq q \leq \left(\frac{x}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}}$$

has the measure $1 - \frac{C_k}{x} - \frac{x'}{2}$. As in Proposition 3.1 we take $x' = 0.147$ and $x = 256$. In the following Table 8 we will give the range of q . Since $\left(\frac{256}{0.147}\right)^{1/k(k-1)}$ is very close to 1 when $k \geq 120$, we can take $q \approx \left(\frac{256}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}}$.

1) *From Margulis's Theorem.* We set $x = 256$ in Theorem 3.1, then the fraction of lattices with their Hermitian invariants smaller than $\left(\frac{256}{\text{vol}(\mathbf{B}_k)}\right)^{2/k}$ is at least 95 percent. In Table 4 we list upper bounds $\left(\frac{256}{\text{vol}(\mathbf{B}_k)}\right)^{1/k(k-1)}$ for root Hermitian factors.

Table 4 Expected root Hermitian factors c for large block size k when $x = 256$

k	86	106	132	168	216	286
c	1.011	1.00954	1.00886	1.00728	1.00627	1.00527
fraction	0.95	0.95	0.95	0.95	0.95	0.95
k	300	320	380	400	420	486
c	1.0049	1.00469	1.00416	1.00388	1.003497	1.00527
fraction	0.95	0.95	0.95	0.95	0.95	0.95

2) *From the measure version of Gaussian heuristic and GSA.* Comparing with Table 2 ([8] Table 4.1) we have the following table 6, fractions are also listed. The root of Hermitian factors are computed in the range

$$\left(\frac{x'}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}} \leq q \leq \left(\frac{x}{\text{vol}(\mathbf{B}_k)}\right)^{\frac{1}{k(k-1)}}$$

. We set $x' = 0.147$ and $x = 256$. We also list the root Hermitian factors for BKZ with small block sizes in Table 5.

Table 5 The root Hermitian factors for block size $16 \leq k \leq 48$

k	16	18	20	22	24
q	0.998-1.031	1.0019-1.027	1.0045-1.025	1.00649-1.0289	1.0078-1.022
fraction	0.953	0.953	0.953	0.953	0.953
k	26	28	30	32	34
q	1.0088-1.02	1.0096-1.019	1.0101-1.01888	1.0105-1.0182	1.0108-1.0176
fraction	0.953	0.953	0.953	0.953	0.953
k	36	38	40	44	48
q	1.011-1.017	1.0112-1.0166	1.0113-1.0161	1.01135-1.0154	1.01131-1.0147
fraction	0.953	0.953	0.953	0.953	0.953

Table 6 The root Hermitian factors for block size $50 \leq k \leq 1100$

k	50	60	70	80	90
q	1.011-1.0141	1.010-1.013	1.01-1.012	1.009-1.011	1.0094-1.01
fraction	0.953	0.953	0.953	0.953	0.953
k	100	110	120	130	140
q	1.0090-1.0098	1.0086-1.0092	1.0082-1.0088	1.0079-1.0084	1.0076-1.0080
fraction	0.953	0.953	0.953	0.953	0.953
k	150	160	170	180	190
q	1.0073-1.0077	1.0071-1.0074	1.0068-1.0071	1.0066-1.0068	1.0064-1.0066
fraction	0.953	0.953	0.953	0.953	0.953
k	200	210	220	230	240
q	1.0062-1.0064	1.0060-1.0062	1.0058-1.0060	1.0057-1.0058	1.0055-1.0056
fraction	0.953	0.953	0.953	0.953	0.953
k	250	300	400	500	600
q	1.0054-1.0055	1.0048-1.0049	1.00397-1.004	1.00339-1.0034	1.00298-1.003
fraction	0.953	0.953	0.953	0.953	0.953
k	700	800	900	1000	1100
q	1.00267	1.00242	1.00222	1.002048	1.0018-1.0019
fraction	0.953	0.953	0.953	0.953	0.953

When the block size is 70, our range of root Hermitian factor is [1.0104378, 1.01200017...], notice that the ranges of root Hermitian factors from experimental results about BKZ2.0, Slide reduction and Self-Dual BKZ algorithms

in [33] page 31 are smaller than ours. From our theoretical analysis, when the block size is 70, root Hermitian factor 1.0104378 seems impossible, and the root Hermitian factor 1.01200017 is possible.

5 Concluding remark: What root Hermitian factor can not be achieved?

Gaussian heuristic is widely used in lattice reduction algorithms and enumeration as a prediction of the length of shortest vectors of lattices. Our measure version of Gaussian heuristic gives an strict proven theorem such that this heuristic can be used strictly. Its basic meaning is when the dimension is large, almost all lattices satisfy this heuristic. Hence the root Hermitian factor of BKZ 2.0 type algorithms and slide reduction with large block size can be proved are within a small range around $GH(k)^{\frac{1}{k-1}}$.

In [33] section 8 the authors wrote”...we need to find a way to translate this to a root Hermitian factor that is unlikely to be achieved by lattice reduction...”, since the root Hermitian factor which can not be achieved is essentially important to the security evaluation of lattice-based cryptosystems ([27, 2, 26, 46, 33]). From Table 6 and our measure version of Gaussian heuristic we can say that when the block size $k = 100$ is used, it seems that the root Hermitian factor 1.0098 is possible and the root Hermitian factor smaller than 1.0090. is unlikely possible, since the probability that local projected lattices of dimension 100 have smaller Hermitian invariant is very small.

References

- [1] Y. Aono, Y.Wang, T.Hayashi and T. Takagi, Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator, Eurocrypt 2016.
- [2] M. R. Albrecht, R. Player and S. Scott, On the concrete hardness of learning with errors, Journal of Mathematical Cryptology, **9**, 169-203, 2015.

- [3] M. Ajtai, The shortest vector problem in L_2 is NP-hard for randomized reduction, STOC 1998, 10-19.
- [4] M. Ajtai, Random lattices and a conjectured 0-1 law about their polynomial time computable properties, FOCS 2002, 13-39.
- [5] M. Ajtai, The worst-case behaviour of Schnorr's algorithm approximating the shortest nonzero vector in a lattice, 396-406, STOC 2003.
- [6] M. Ajtai, Optimal lower bounds for the Korkine-Zolotareff parameters of a lattice and for Schnorr's algorithm for the shortest vector problem, 21-51, STOC 2008.
- [7] Y. Chen and Phong Q. Nguyen, BKZ2.0: Better lattice security estimates, 1-20, Asiacrypt 2011, full version, <http://www.di.ens.fr/~ychen/research/>
- [8] Y. Chen, Ph.D These, <http://www.di.ens.fr/~ychen/research/>
- [9] J.H. Conway and N.J.A. Sloane, Sphere packings, lattice and groups, Grundlehren 290, third Edition, Springer, 1999.
- [10] U. Fincke and M. Phost, A procedure for determining algebraic integers of given norm, EUROCAL, LNCS 162, 194-202, 1983.
- [11] N. Gama, N. Howgrave-Graham, H. Koy and P.Q. Nguyen, Rankin constant and blockwise lattice reduction, 112-130, Crypto 2006.
- [12] N. Gama and Phong Q. Nguyen, Finding short lattice vectors within Mordell's inequality, STOC 2008.
- [13] N. Gama and Phong Q. Nguyen, Predicting lattice reductions, 31-51, Eurocrypt 2008.
- [14] N. Gama, Phong Q. Nguyen and O. Regev, Lattice enumeration using extreme pruning, Eurocrypt 2010, 257-278., 2010.
- [15] C. Gauss, Disquisitiones Arithmeticae, 1801.
- [16] C. Gentry, Fully homomorphic encryption using ideal lattices, STOC 2009, 167-178.
- [17] S. Garg, C. Garg and S. Halevi, Candidate multilinear maps from ideal lattices, Eurocrypt 2013, 1-17.

- [18] P. M. Gruber, *Convex and discrete geometry*, Grundlehren 336, Springer 2007.
- [19] G. Hanrot and D. Stehle, Worst-case Hermitian-Korkine-Zolotarev reduced lattice bases, Nov.2007, INRIA report, CoRR. abs/0801.3331,2008.
- [20] G. Hanrot, X. Pujol and D. Stehle, Algorithms for shortest and closest lattice vector problems, invited contribution, IWCC 2011.
- [21] G. Hanrot, X. Pujol and D. Stehle, Analyzing blockwise lattice algorithms using dynamic systems, 447-464, Cryoto 2011.
- [22] R. Kannan, Improved algorithms for integer programming and related lattice problems, STOC 1983, 99-108, 1983.
- [23] L. Lagrange, *Recherches d'arithmetique*, em *Nouv. Mem. Acad.* 1773.
- [24] J. C. Lagarias, H. W. Lenstra and C. P. Schnorr, Korkine-Zolotarev bases and successive minimas of a lattice and its reciprocal lattice, *Combinatorica*, **10**, 333-348, 1990.
- [25] A.K.Lenstra, H.W. Lenstra and L.Lovasz, Factoring polynomials with rational coefficients, *Math. Ann.*, **261**, 513-524, 1982.
- [26] T. Lepoint and M. Naehrig, A comparison of the homomorphic encryption schemes FV and YASHE, *Africacrypt 2014*, LNCS 8469, 318-335, 2014.
- [27] R. Lindner and C. Peikert, Better key sizes (and attacks) for LWE-based encryption, *CT-RSA*, 2011, LNCS 6558, 319-339, 2011.
- [28] M. Liu and Phong Q. Nguyen, Solving BDD by enumeration, *CT-RSA*, 2013, LNCS 7779,293-309, 2013.
- [29] G. A. Margulis, Random Minkowski theorem, *Probl. Peredachi Inf.*, **47**, 104-108, 2011.
- [30] J. Martinet, *Perfect lattices in Euclid spaces*, Grundlehren 327, Springer 2003.
- [31] D. Micciancio and S. Goldwasser, *Complexity of lattice problems, A cryptographic perspective*, Kluwer Academic Publishers.

- [32] D. Micciancio and O. Regev, Lattice-based cryptography, Book chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008).
- [33] D. Micciancio and M. Walter, Practical, predictable lattice basis reduction, Eurocrypt 2016.
- [34] C. Peikert, Survey on lattice-based cryptography, 2015.
- [35] T. Plantard and M. Schneider, Creating a challenge for ideal lattices, iacr preprint 2013/039, 2013.
- [36] Phong Q. Nguyen and D. Stehle, LLL on the average, 238-256, ANTS 2006.
- [37] Phong Q. Nguyen, Hermitian constant and lattice reductions, 19-70, The LLL algorithm, Edited by Phong Q. Nguyen and B. Vallee, Springer, 2009.
- [38] Phong Q. Nguyen and B. Vallee (Editors), The LLL algorithm, Springer 2009.
- [39] C. P. Schnorr, A hierarchy of polynomial time lattice basis reduction algorithms, Theoretical Computer Science, **53**, 201-234, 1987.
- [40] C. P. Schnorr and M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, 68-85, Proc. 1991 Symposium on the Fundamentals of Computation Theory, LNCS 529, 1991.
- [41] C. P. Schnorr and M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, Mathematical Programming, **66**, 181-199, 1994.
- [42] C. P. Schnorr, Lattice reduction by random sampling and birthday methods, STACS, LNCS 2607, 145-150, 2003.
- [43] C. P. Schnorr, Progress on LLL and lattice reduction, The LLL algorithm, Edited by Phong Q. Nguyen and B. Vallee, 145-170, Springer 2009.
- [44] C. L. Siegel, A mean value theorem in geometry of numbers, Annals of Math., **46**, 340-347, 1945.

- [45] V. Shoup, Number Theory C++ library (NTL),
<http://www.shoup.net/ntl/>.
- [46] J. van de Pol and N. Smart, Estimating key sizes for high dimensional lattice-based systems, IMACC2013, Edited by M.Stam, LNCS 8308, 290-303, 2013.
- [47] <http://latticechallenge.org>.