A Complete Analysis of the BKZ Lattice Reduction Algorithm

Jianwei Li* and Phong Q. Nguyen**

Abstract. We present the first rigorous dynamic analysis of BKZ, the most widely used lattice reduction algorithm besides LLL: previous analyses were either heuristic or only applied to variants of BKZ. Namely, we provide guarantees on the quality of the current lattice basis during execution. Our analysis extends to a generic BKZ algorithm where the SVP-oracle is replaced by an approximate oracle and/or the basis update is not necessarily performed by LLL. Interestingly, it also provides quantitative improvements, such as better and simpler bounds for both the output quality and the running time. As an application, we observe that in certain approximation regimes, it is more efficient to use BKZ with an approximate rather than exact SVP-oracle.

Keywords: Lattice Reduction · BKZ · Dynamical Systems · Enumeration.

1 Introduction

Lattices are discrete subgroups of $\mathbb{R}^m$. A lattice L is represented by a *basis*, *i.e.* a set B of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$ such that L is equal to the set $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^n x_i \mathbf{b}_i, x_i \in \mathbb{Z}\}$ of all integer linear combinations of the $\mathbf{b}_i$'s. The integer n is the dimension or rank of L. Given a basis B of L, the goal of a lattice reduction algorithm is to find a better basis, ideally formed by short and nearly orthogonal vectors, which has numerous applications in mathematics and computer science.

The most widely used lattice reduction algorithm is also its simplest one: LLL [LLL82]. However, the quality of LLL is not sufficient for all applications, especially in cryptanalysis. This has led to the development of stronger blockwise reduction algorithms [Sch87,SE94,SH95,GHGKN06,GN08a,MW16,ALNS20,ABF+20], which generalize LLL using a special subroutine parameterized by an additional input parameter – the blocksize β – which impacts both the running time and the output quality: the higher β is, the slower the algorithm and the better the output basis.

The simplest such algorithm is the Blockwise Korkine-Zolotarev (BKZ) algorithm, published twenty-nine years ago by Schnorr and Euchner [SE94]. Commonly available in software libraries [FPL19,FPy19,ADH+19,Sho20], it has been used in many cryptanalyses and most lattice record computations [LR20,ADH+19]. Its importance has grown as lattice-based cryptography has emerged as the most popular candidate for post-quantum cryptography and homomorphic encryption: security estimates typically involve an assessment of the performances of BKZ. Yet, despite its simplicity, BKZ is still poorly understood from a theoretical point of view. In practice [CN11,AWHT16,BSW18,FPL19,FPy19,Sho20,LR20,ABF+20], except for small blocksizes, one usually stops its execution well before termination, without any rigorous worst-case guarantee on the output quality: Hanrot, Pujol and Stehlé published at CRYPTO '11 [HPS11] the first provable analysis, but only for a modified version of BKZ, noting that "*it does not seem easy to use (their) techniques to analyze*" BKZ. Instead, security estimates typically rely on Chen-Nguyen's heuristic modelization [CN11] of BKZ.

Interestingly, Hanrot *et al.* [HPS11] introduced the use of discrete dynamical systems to analyse blockwise reduction algorithms. All prior analyses mimicked the analysis of LLL itself, based on an always-decreasing potential function, but this type of analysis can only analyze the final reduced basis output by the algorithm, not the current basis during execution [LLL82].

Our Results. We obtain the first rigorous dynamic analysis of BKZ: previous analyses were either heuristic (like [CN11,BSW18]) or only applied to a specific variant of BKZ (like [HPS11]). Here, "dynamic" means that we provide guarantees on the quality of the current lattice basis during the execution of BKZ: this is

* Information Security Group, Royal Holloway, University of London. Email: lijianweithu@sina.com
** Inria and DIENS, CNRS, PSL. Email: pnguyen@inria.fr

similar to [HPS11]. The execution of BKZ consists of a sequence of tours: each tour modifies the basis using LLL and a subroutine which finds shortest nonzero vectors in a lattice of rank $\leq \beta$. After each tour, all the basis vectors have been examined, and may have been modified. Informally, our analysis proves that after a number of tours at most

$$\Theta\left(\frac{n^2}{\beta^2}\log n\right), \tag{1}$$

the first basis vector of BKZ is short, with Euclidean norm at most:

$$\gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2n(\beta-1)}}\mathrm{vol}(L)^{1/n}, \tag{2}$$

where γ_β and $\mathrm{vol}(L)$ denote as usual Hermite's constant and the volume of L. More generally, our analysis shows that not only the first vector is short, also the whole basis is already reduced: namely, it gives upper bounds (which we omit in this introduction) on the volume of the paralellepiped formed by the first i vectors of the basis for any $i \in \{1,\dots,n-1\}$, which is related to Rankin's constant (see [GHGKN06]). Such volume bounds are useful to upper bound the heuristic running time of enumeration algorithms using partially BKZ-reduced bases. In particular, it validates the recursive preprocessing strategy used in BKZ 2.0 [CN11] and FP(y)LLL [FPL19,FPy19].

Prior to our work, the only comparable result was that of [HPS11], who showed that if a certain variant BKZ' of BKZ was given an input basis B_0, then after a number of tours at most

$$\Theta\left(\frac{n^2}{\beta^2}\left(\log n + \log\log\frac{\|B_0\|}{\mathrm{vol}(L)^{1/n}}\right)\right), \tag{3}$$

the first basis vector of BKZ' has norm essentially at most:

$$\nu_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}}\mathrm{vol}(L)^{1/n}, \tag{4}$$

where $\nu_\beta = \max_{1\leq i\leq\beta}\gamma_i$.

In fact, our analysis not only applies to BKZ itself, it extends to a general family of BKZ algorithms, including among others BKZ' and BKZ with weaker subroutines. Yet, our bounds (1) and (2) still improve upon (3) and (4). First, our bound (1) on a sufficient number of tours is the first for BKZ to be independent of the input basis B_0. Next, our bound (2) is much closer to Mordell's inequality reached by [GN08a,MW16,ALNS20] using different algorithms. More precisely, the main multiplicative term $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$ in (2) corresponds to Mordell's inequality $\gamma_n \leq \gamma_\beta^{\frac{n-1}{\beta-1}}$ for any $2 \leq \beta \leq n$ [Mor44]. However, (4) involves a potentially worse function $\nu_\beta \geq \gamma_\beta$, and the additional exponent $\frac{\beta(\beta-2)}{2n(\beta-1)}$ in (2) is smaller than both $\frac{3}{2}$ in (4) and the improved constant given in the appendix of [HPS11]: for any $\beta = \Theta(n) < (1-\ln 2)n$, (2) implies the best provable polynomial Hermite factor of $\gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2n(\beta-1)}}$; for any $\beta = o(n)$, $\frac{\beta(\beta-2)}{2n(\beta-1)}$ converges to zero; and for any $\beta = O(n^{1-\varepsilon})$ where $\varepsilon > 0$, the multiplicative term $\gamma_\beta^{\frac{\beta(\beta-2)}{2n(\beta-1)}}$ converges to one, which is better than all previously known bounds for (full) BKZ-reduced bases.

Furthermore, our work provides a better understanding of BKZ, by justifying several design choices:

- The fact that each BKZ tour consists of consecutive iterations with nearly-maximal overlap is crucial for our analysis. At each iteration, the block examined by BKZ is shifted by only one position:[1] our analysis would break down if it was even two positions.
- The initial LLL reduction in BKZ is crucial to make our bound (1) independent of the input basis.
- Our analysis clarifies why LLL is used many times by BKZ, and by which algorithms it could be replaced, which might be useful for certain applications.

[1] This fact was also used in the analysis of [HPS11] for a certain variant BKZ' rather than BKZ itself.

As a secondary result, we deduce that in certain approximation regimes, BKZ with approximate-SVP oracles (be it sieving or enumeration) is more efficient than BKZ with exact-SVP oracles. This justifies the common practice of implementing BKZ with a subroutine which does not always output a shortest nonzero lattice vector [CN11,BSW18]: we show that the speed-up is larger when the SVP subroutine is enumeration with cylinder pruning [SH95,GNR10], by adapting the asymptotic analysis of Gama *et al.* [GNR10]. Intuitively, this can be explained as follows. When the SVP-oracle is replaced by an approximate-SVP-oracle, each oracle call is faster by a factor exponential in the blocksize (if the oracle is enumeration or sieving), but our general analysis of BKZ guarantees that the loss in the global approximation factor is limited: overall, we obtain better time/quality trade-offs for certain approximation regimes.

Technical Overview. Given as input a lattice basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, a lattice reduction algorithm keeps modifying the current basis B until it is "reduced". For BKZ-type algorithms [SE94,HPS11,MW16,BSW18,ABF$^+$20], these modifications can be structured as a sequence of tours, where each tour makes a limited number of elementary modifications.

To analyze the behaviour of BKZ', Hanrot *et al.* [HPS11] introduced the use of dynamical systems to study the quality of the current basis B at the end of each tour, rather than just at the end of the algorithm. To do so, they defined a profile function $\mathcal{P}$, mapping any lattice basis onto a vector of $\mathbb{R}^n$. This function $\mathcal{P}$ is chosen to satisfy two properties. First, if one knows $\mathbf{u} \in \mathbb{R}^n$ with "small" entries such that $\mathcal{P}(B) \leq \mathbf{u}$ component-wise, then the quality of B is guaranteed. Second, one can upper bound $\mathcal{P}(B)$ during the execution of the algorithm. More precisely, [HPS11] built a matrix $M \in \mathbb{R}^{n \times n}$ and a vector $\mathbf{v} \in \mathbb{R}^n$ such that component-wise:

$$\mathcal{P}(B_k) \leq \mathcal{P}(B_{k-1})M + \mathbf{v} \tag{5}$$

where B_k denotes the basis at the end of the k-th tour, and B_0 is the input basis. If the map $\mathbf{x} \leftarrow \mathbf{x}M + \mathbf{v}$ has a fixed point $\mathbf{w} \in \mathbb{R}^n$, then (5) can be rewritten as

$$\mathcal{P}(B_k) - \mathbf{w} \leq (\mathcal{P}(B_{k-1}) - \mathbf{w})M.$$

If all the entries of M are ≥ 0, this implies that $\mathcal{P}(B_k) - \mathbf{w} \leq (\mathcal{P}(B_0) - \mathbf{w})M^k$, hence

$$\mathcal{P}(B_k) \leq \mathbf{w} + (\mathcal{P}(B_0) - \mathbf{w})M^k. \tag{6}$$

Thanks to properties of both M and $\mathcal{P}(B_0) - \mathbf{w}$, [HPS11] showed that $(\mathcal{P}(B_0) - \mathbf{w})M^k$ converges to zero with an explicit vectorial upper bound. And the latter bound can be reinjected into (6) to guarantee the quality of B_k for all sufficiently large k, provided that the fixed point $\mathbf{w}$ can also be bounded.

Our proof follows the same strategy as [HPS11]. The most difficult part is to show that an inequality like (5) actually holds for BKZ, and not just for BKZ'. To explain the difficulty, it is helpful to outline the differences between BKZ and BKZ'. Each tour of either BKZ or BKZ' consists of $n-1$ consecutive iterations, but a BKZ' iteration may only modify at most β consecutive basis vectors, whereas any BKZ iteration can potentially also modify all the front basis vectors before the latter ones, due to the use of a wide LLL reduction inside each BKZ iteration. [HPS11] proved (5) for BKZ' by establishing an analogue inequality for each BKZ' iteration. Unfortunately, such inequalities are unlikely to hold for a BKZ iteration, because of LLL. Intuitively, BKZ' is easier to analyze because it relies on a local HKZ-reduction which restricts the range of modifications at each iteration.

To solve this problem, we exploit two ideas. The first one shows that the impact of the LLL reduction is limited, thanks to the recent work [LN19], which revisited the fundamental problem of computing a basis given only a lattice generating set: [LN19] identified desirable properties of basis algorithms, which are shared by BKZ's LLL subroutine and are essential to preserve (5) during the execution of BKZ. The second idea is loosely related to the BKZ simulator of Chen and Nguyen [CN11]: there, it was noted that the basis profile at the end of a tour could be heuristically guessed, even though not all entries of the profile were known at the end of each iteration during the execution of a tour. Similarly, we observe that each BKZ iteration nearly implies (5): a vectorial inequality holds except for at most β consecutive coordinates. Yet, that is surprisingly enough to achieve a full (5) at the end of each tour.

Our dynamical system is a variant of [HPS11]'s dynamical system, but it has slightly better properties: it uses a slightly different profile function, has a unique fixed point, has better constants and is a bit simpler to analyze.

Related Work. Recently, Neumaier introduced in [Neu17] a simplification of the method of Hanrot *et al.* [HPS11] to analyze dynamically blockwise reduction algorithms. Roughly speaking, this simplification replaces the dynamical system by a one-dimensional one: instead of using a vectorial inequality on consecutive profiles, [Neu17] looks for a single inequality on the max-norm of consecutive profiles. This method simplifies the analysis by removing the need to study matrices, and was shown to be especially useful in the case of the DBKZ algorithm [MW16] and LLL-type algorithms [NS16,Neu17]. We stress that in these latter applications, the oracles all use the same rank. However, BKZ uses oracles of varying rank (because the tail blocks have smaller ranks): our analysis can be rewritten using Neumaeir's strategy, but it turns out that the bounds obtained are noticeably worse. Intuitively, this is because the max-norm forgets that we have better bounds for certain coordinates (due to the tail blocks). Thus, Neumaier's method is simpler, but does not seem adapted to the situation of varying ranks, leading to much worse bounds, namely replacing (2) with the following bound:

$$\left(\prod_{\kappa=2}^{\beta} \gamma_\kappa^{\frac{1}{\kappa-1}}\right)^{\frac{n-1}{2(\beta-1)}} \mathrm{vol}(L)^{1/n}.$$

Note that $\prod_{\kappa=2}^{\beta} \gamma_\kappa^{\frac{1}{\kappa-1}} = \Theta(\beta^{\frac{1}{2}\ln\beta})$ is asymptotically much larger than $\gamma_\beta = \Theta(\beta)$. We address this issue [Neu20] in details in Appendix A.

We stress that our work is a provable worst-case analysis of BKZ, so (2) does not intend to reflect the average-case behaviour of BKZ on typical lattices. For that setting, other works [CN11,BSW18] propose heuristic analyses of BKZ by essentially replacing Hermite's constant in (2) by some estimate based on the Gaussian heuristic: such analyses require to assume that projected lattices behave roughly like independent random lattices. Yet, our analysis can also provide theoretical guarantees under the same heuristic model: (2) can then be modified using the Gaussian heuristic, thanks to elementary inequalities shared by both Hermite's constant and some versions of the Gaussian heuristic. In particular, if we plug the heuristic estimates used by the BKZ simulator [CN11] into our dynamical system, the bounds we obtain are not very far from the output of the BKZ simulator, which illustrates the interest of dynamical systems.

Roadmap. Sect. 2 recalls background and usual notation. Sect. 3 presents our main result: the analysis of BKZ using the dynamical systems framework of [HPS11]. In Sect. 4, we show how to adapt the analysis to study the practical behaviour of BKZ, when the worst-case inequalities based on Hermite's constant are replaced by inequalities based on the Gaussian heuristic and supported by experiments. These stronger inequalities are directly inspired by results from random lattices theory, and give rise to better bounds. Sect. 5 deals with our secondary result: we show that enumeration with cylinder pruning [SH95,GNR10] is exponentially faster for approximate-SVP than for exact-SVP, and exploit this speed-up in the context of BKZ. In Appendix A, we explain how Neumaier's method can be adapted to BKZ, but leads to worse bounds.

2 Background

Notation. We use row-representation of both vectors and matrices throughout this paper: bold lower case letters and upper case letters denote row vectors and matrices, respectively. Furthermore, the i-th row and j-th column of a matrix M are denoted by $\mathbf{m}_i$ and $M|_j$ respectively, when no confusion can arise. The i-th entry of an n-dimensional vector $\mathbf{v}$ is denoted by v_i. The n-dimensional row vector with each entry 1 is denoted by $\mathbf{1}_n$. The $n \times n$ identity matrix is denoted by $1_{n\times n}$. The set of $n \times m$ matrices with coefficients in the ring $\mathbb{A}$ is denoted by $\mathbb{A}^{n\times m}$, and we identify $\mathbb{A}^m$ with $\mathbb{A}^{1\times m}$.

For a matrix $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of n rows, we let $\|B\| = \max\{\|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\|\}$, where $\|\cdot\|$ is the Euclidean norm. If the rows of B generate a lattice, we denote it by $L(B)$ or $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

For an $n \times n$ matrix M, we denote its spectral norm by $\|M\|_2$. We write $M \geq 0$ if all the entries of M are ≥ 0. For two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, we write $\mathbf{u} \leq \mathbf{v}$ if the inequalities hold componentwise. We will use the key elementary property: if $\mathbf{u} \leq \mathbf{v}$ and $M \geq 0$, then $\mathbf{u}M \leq \mathbf{v}M$.

The size of an object is the length of its binary representation. The notations $\log(\cdot)$ and $\ln(\cdot)$ respectively stand for the base 2 and natural logarithms.

2.1 Gram-Schmidt Orthogonalization

Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times m}$ be a basis of a lattice L. Lattice algorithms rely on the orthogonal projections $\pi_i : \mathbb{R}^m \mapsto \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$ for $i = 1, \ldots, n$. The *Gram-Schmidt orthogonalization* (GSO) of B is $B^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ where the Gram-Schmidt vector $\mathbf{b}_i^*$ is $\pi_i(\mathbf{b}_i)$. Then $\mathbf{b}_1^* = \mathbf{b}_1$ and $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$ for $i = 2, \ldots, n$, where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$. The GSO can also be extended to linearly dependent vectors, in which case some $\mathbf{b}_i^*$'s can be zero [LN19].

Profiles. We will use the notation $B_{[i,j]}$ for the projected block $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_j))$. In particular, $B_{[1,j]} = (\mathbf{b}_1, \ldots, \mathbf{b}_j)$. In order to assess the quality of bases, [HPS11] used two profiles $(\log\|\mathbf{b}_1^*\|, \log\|\mathbf{b}_2^*\|, \ldots, \log\|\mathbf{b}_n^*\|)$ and $(\log \mathrm{vol}(B_{[1,1]}), \log \mathrm{vol}(B_{[1,2]})^{1/2}, \ldots, \log \mathrm{vol}(B_{[1,n]})^{1/n})$. We use two slightly different but closely related profiles, which we call the *Gram-Schmidt* and *Rankin profiles*:

$$\mathcal{G}(B) = (\mathcal{G}_1(B), \mathcal{G}_2(B), \ldots, \mathcal{G}_n(B)) \in \mathbb{R}^n \quad \text{with each} \quad \mathcal{G}_i(B) = \log \frac{\|\mathbf{b}_i^*\|}{\mathrm{vol}(L)^{1/n}},$$

$$\mathcal{R}(B) = (\mathcal{R}_1(B), \mathcal{R}_2(B), \ldots, \mathcal{R}_n(B)) \in \mathbb{R}^n \quad \text{with each} \quad \mathcal{R}_i(B) = \log \frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(L)^{i/n}}.$$

These profiles only depend on the $\|\mathbf{b}_i^*\|$'s: their first coordinate measures the norm of the first basis vector. The Gram-Schmidt profile $\mathcal{G}(B)$ measures these norms in logarithmic scale, whereas the Rankin profile $\mathcal{R}(B)$ upper bounds the Rankin invariants [GHGKN06] of the lattice. We have: $\sum_{i=1}^n \mathcal{G}_i(B) = \mathcal{R}_n(B) = 0$ and the scale invariance $\mathcal{G}(B) = \mathcal{G}(\rho \cdot B)$ and $\mathcal{R}(B) = \mathcal{R}(\rho \cdot B)$ for any real $\rho \neq 0$. Notice that $\mathcal{G}(B)$ can be linearly transformed into $\mathcal{R}(B)$, and reciprocally, namely $\mathcal{R}(B) = \mathcal{G}(B)E$ and $\mathcal{G}(B) = \mathcal{R}(B)E^{-1}$ via the upper triangular matrix E and its inverse:

$$E = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ & 1 & 1 & \cdots & 1 \\ & & 1 & \cdots & 1 \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix} \in \mathbb{Z}^{n\times n} \quad \text{and} \quad E^{-1} = \begin{pmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ & & & & 1 \end{pmatrix} \in \mathbb{Z}^{n\times n}. \tag{7}$$

2.2 Lattices

Hermite's constant. The *Hermite invariant* of an n-rank lattice L is $\gamma_n(L) = \lambda_1(L)^2/\mathrm{vol}(L)^{2/n}$, where $\lambda_1(L) = \min_{\mathbf{v}\in L\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$ is the *first minimum* of L. *Hermite's constant* of dimension n is the maximum $\gamma_n = \max \gamma_n(L)$ over all n-rank lattices L. The exact value of γ_n is known for $1 \leq n \leq 8$ and $n = 24$. The best asymptotical bounds known are [CS87,MH73]: $\frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} \leq \gamma_n \leq \frac{1.744n}{2\pi e} + o(n)$.

Primitive set. Linearly independent vectors $\mathbf{p}_1, \ldots, \mathbf{p}_r$ in a lattice L form a *primitive set* for L iff they can be extended to a basis of L. In particular, single $\mathbf{p} \in \mathbb{Z}^n$ is a *primitive vector* for $\mathbb{Z}^n$ iff it can be extended to a unimodular matrix.

Size-reduction and LLL-reduction. Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis. B is *size-reduced* if $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$. The single vector $\mathbf{b}_i$ is *size-reduced* (w.r.t. B) if $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i$.

For $\xi \in (\frac{1}{4}, 1]$, B is *ξ-LLL-reduced* if it is size-reduced and every 2-rank projected block $B_{[i-1,i]}$ satisfies Lovász's condition: $\xi\|\mathbf{b}_{i-1}^*\|^2 \leq \|\mu_{i,i-1}\mathbf{b}_{i-1}^* + \mathbf{b}_i^*\|^2$ for $2 \leq i \leq n$. In such a case, it is well-known that $\mathcal{R}(B)$ can be upper bounded independently of B, namely $\mathcal{R}(B) \leq \left(\frac{i(n-i)}{4} \log \frac{4}{4\xi - 1}\right)_{1\leq i\leq n}$ [PT10]. The LLL

algorithm [LLL82] provides efficient procedures for size-reducing a single vector and computing an LLL-reduced basis.
SVP-reduction and its extensions. Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of a lattice L and $\delta \geq 1$ be a relaxation factor.

B is *SVP-reduced* if $\|\mathbf{b}_1\| = \lambda_1(L)$. There is a natural relaxation: B is *δ-SVP-reduced* if $\|\mathbf{b}_1\|^2 \leq \delta \times \lambda_1(L)^2$.

B is *HKZ-reduced* [Her50,KZ73] if it is size-reduced and $B_{[i,n]}$ is SVP-reduced for $i = 1, \ldots, n$.

B is *β-BKZ-reduced* [Sch87] if it is size-reduced and $B_{[i,\min\{i+\beta-1,n\}]}$ is SVP-reduced for $i = 1, \ldots, n$. There is a relaxed variant: B is *(δ, β)-BKZ-reduced* [SE94] if it is size-reduced and $B_{[i,\min\{i+\beta-1,n\}]}$ is δ-SVP-reduced for $i = 1, \ldots, n$.

SVP-oracle. A δ-SVP-oracle with relaxation factor $\delta \geq 1$ is any algorithm which, given as input a β-rank lattice Λ with basis B, outputs a primitive vector α for $\mathbb{Z}^\beta$ such that $\|\alpha B\|^2 \leq \delta \times \lambda_1(\Lambda)^2$. Then $\|\alpha B\| \leq \sqrt{\delta\gamma_\beta} \times \mathrm{vol}(\Lambda)^{1/\beta}$. The LLL algorithm [LLL82] can efficiently achieve $\|\alpha B\| \leq 2^{(\beta-1)/4} \times \mathrm{vol}(\Lambda)^{1/\beta}$ [LLL82, Eq. (1.9)]. So, one could restrict $1 \leq \delta \leq \frac{2^{(\beta-1)/2}}{\gamma_\beta}$ (*e.g.* in Theorem 2).

2.3 The BKZ Algorithm

We recall the (original) BKZ algorithm introduced by Schnorr and Euchner [SE94] in Algorithm 1. It computes (δ, β)-BKZ-reduced bases in high rank, using an exact SVP-oracle in rank $\leq \beta$ as a subroutine and running the LLL algorithm to remove the linear dependency right after inserting a lattice vector (found by the oracle) in the current basis. Here,

- the variable z counts the number of indices j such that $B_{[j,n_j]}$ is δ-SVP-reduced. Then "z=n-1" on termination means that the current basis is already (δ, β)-BKZ-reduced.
- "stage j" at Step 6 means to run LLL already from index j. This is the same as running LLL because $(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1})$ is already LLL-reduced right before Step 6.

Algorithm 1 BKZ: Schnorr-Euchner's Blockwise Korkine-Zolotarev algorithm [SE94]

Input: A blocksize $\beta \in (2, n)$, a relaxation factor $\delta \in (1, 2)$, and a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L in $\mathbb{Z}^m$.
Output: A (δ, β)-BKZ-reduced basis of L.
1: $z \leftarrow 0$; $j \leftarrow 0$; $\frac{1}{\delta}$-LLL-reduce B
2: **while** z < n-1 **do**
3: $\quad j \leftarrow (j \bmod (n-1)) + 1$; $n_j \leftarrow \min\{j+\beta-1, n\}$; $h \leftarrow \min\{j+\beta, n\}$
4: $\quad$ Run an enumeration for $L(B_{[j,n_j]})$ to find $(\alpha_j, \ldots, \alpha_{n_j}) \in \mathbb{Z}^{n_j-j+1}$ and compute $\mathbf{b} = \sum_{i=j}^{n_j} \alpha_i \mathbf{b}_i$ such that $\|\pi_j(\mathbf{b})\| = \lambda_1(L(B_{[j,n_j]}))$
5: $\quad$ **if** $\|\mathbf{b}_j^*\|^2 > \delta \times \|\pi_j(\mathbf{b})\|^2$ **then**
6: $\quad\quad z \leftarrow 0$; $\frac{1}{\delta}$-LLL-reduce $(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}, \mathbf{b}_j, \ldots, \mathbf{b}_h)$ at stage j
7: $\quad$ **else**
8: $\quad\quad z \leftarrow z + 1$; 0.99-LLL-reduce $(\mathbf{b}_1, \ldots, \mathbf{b}_h)$ at stage $h - 1$
9: $\quad$ **end if** //Due to LLL calls, $B_{[j,n_j]}$ may no longer be δ-SVP-reduced right after this step.
10: **end while**
11: **return** B. //It is folklore in practice to allow $\delta = 1$ and run (say,) 0.99-LLL-reductions at Steps 1 and 6.

Originally, the SVP subroutine implemented in [SE94] was the simplest form of lattice enumeration, but it is now replaced by better subroutines, such as pruned enumeration [GNR10] in BKZ 2.0 [CN11]/FP(y)LLL [FPL19,FPy19], enumeration in rank κ with extended preprocessing in "blocksize" $\lceil (1+c) \cdot \kappa \rceil$ in [ABF+20]'s BKZ variant for some small constant $c \geq 0$, and (asymptotically) faster sieving in the General Sieve Kernel [ADH+19]. In practice, BKZ is typically implemented with an approximate (rather than exact) SVP-oracle. There are essentially two classes of SVP-oracles:

- Exponential-space algorithms, like sieve algorithms. The fastest provably exact SVP algorithm is the Aggarwal-Dadush-Regev-Stephens-Davidowitz (ADRS) algorithm with $2^{\beta+o(\beta)}$-time and space [ADRS15].

The Ajtai-Kumar-Sivakumar (AKS) sieve algorithm [AKS01] can be modified into a δ-SVP-oracle with $2^{0.802\beta+o(\beta)}$-time and $2^{0.401\beta+o(\beta)}$-space for some large constant factor δ [ADRS15,WLW15].

– Polynomial-space algorithms, like enumeration algorithms. Most implementations [CN11,AWHT16,Sho20,ABF$^+$20] of BKZ use enumeration with cylinder pruning [SH95,GNR10]. Compared to sieving, pruned enumeration can heuristically achieve bigger exponential speed-ups when relaxing the approximation factor, which we will clarify in Section 5.

Our analysis in Section 3 shows that if equipped with an approximate SVP-oracle rather than exact oracle, BKZ can achieve substantial speedups for approximating SVP with a minor loss in the approximation factor. For instance, if BKZ is equipped with AKS's variant instead of the ADRS algorithm, we obtain:

– Polynomial speedups (approximately $n^{0.198p}$ w.r.t. blocksize $\beta = p \log n$ with constant p) for approximating SVP to within sub-exponential factors, provided that the SVP-oracle dominates the global cost of the algorithm.
– Exponential speedups (essentially $2^{0.198n/q}$ w.r.t. blocksize $\beta = n/q$ with constant $q \in \mathbb{Q}_{>1}$) for approximating SVP to within polynomial factors.

2.4 Hanrot-Pujol-Stehlé's Analysis

The original BKZ algorithm [SE94] (see Alg. 1) has a bad worst-case complexity upper bound, and its experimental running time degrades significantly when the blocksize β is ≥ 30 [GN08b]. As a result, the execution of BKZ is usually aborted early [CN11,BSW18]. By introducing dynamical systems, Hanrot *et al.* [HPS11] showed that if one terminates a certain variant BKZ' (Alg. 2) of BKZ early, using only polynomially many calls to an exact SVP-oracle, one obtains a basis almost as reduced as the full BKZ algorithm.

Algorithm 2 BKZ': the BKZ variant analyzed in [HPS11, Algorithm 2]

Input: A blocksize $\beta \geq 2$ and a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L.
Output: A new basis of L.
1: **repeat**
2:   **for** $j = 1$ to $n - \beta + 1$ **do**
3:     Modify $(\mathbf{b}_j, \ldots, \mathbf{b}_{j+\beta-1})$ so that $B_{[j,j+\beta-1]}$ is HKZ-reduced
4:     Size-reduce $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ //Different from Steps 5-9 of Alg. 1, $B_{[j,j+\beta-1]}$ is HKZ-reduced during this step.
5:   **end for** //A BKZ' tour refers to a single execution of Steps 2-5.
6: **until** no change occurs or termination is requested, and **return** B.

Theorem 1 ([HPS11, Th. 1 and Lem. 11]). *There exists a constant $C > 0$ such that the following holds. Let $n > \beta \geq 2$ be integers and let $0 < \varepsilon \leq 1$. Given as input a blocksize β and a basis B_0 of an n-rank lattice L in $\mathbb{R}^m$, BKZ' aborted after $C\frac{n^2}{\beta^2}(\log\frac{n}{\varepsilon} + \log\log\frac{\|B_0^*\|}{\mathrm{vol}(L)^{1/n}})$ tours outputs a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that*

$$\|\mathbf{b}_1\| \leq (1+\varepsilon)\nu_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}}\mathrm{vol}(L)^{1/n}.$$

Moreover, if L is a rational lattice, then the overall cost is $\leq$ Poly$(m, \log\|B_0\|) \cdot HKZ(\beta)$, where $HKZ(\beta)$ denotes the cost of HKZ-reduction in rank β.

Here, ν_β is the ad-hoc constant used in [HPS11] (instead of Hermite's constant γ_β, because it is unknown if γ_i increases with i): $\nu_i = \max\{\gamma_j : 1 \leq j \leq i\}$, which increases over $i = 1, 2, \ldots$.

Th. 1 relies on a discrete-time affine dynamical system, as explained in the introduction overview. First, [HPS11] uses the following profile function $\mathcal{F}$: if B is a basis of an n-rank lattice L, let

$$\mathcal{F}(B) = \left(\log\frac{\mathrm{vol}(B_{[1,1]})^{1/1}}{\mathrm{vol}(L)^{1/n}}, \log\frac{\mathrm{vol}(B_{[1,2]})^{1/2}}{\mathrm{vol}(L)^{1/n}}, \ldots, \log\frac{\mathrm{vol}(B_{[1,n]})^{1/n}}{\mathrm{vol}(L)^{1/n}}\right) \in \mathbb{R}^n.$$

Notice that $\mathcal{F}(B)$ is a linear function of the Gram-Schmidt profile $\mathcal{G}(B)$: $\mathcal{F}(B) = \mathcal{G}(B)P$ where $P = (p_{i,j}) \in \mathbb{Q}^{n\times n}$ is the upper triangular matrix with entries $p_{i,j} = \frac{1}{j}$ for $1 \le i \le j \le n$.

The proof of Th. 1 is based on the following key technical result, which shows that BKZ' satisfies an inequality of the type (5):

Proposition 1 ([HPS11, Lemma 9]). *There exist a matrix $A \in \mathbb{Q}^{n\times n}$ and a vector $\mathbf{g} \in \mathbb{R}^n$ such that $P^{-1}AP \ge 0$ and for any tour of BKZ', the basis B at the beginning of the tour and the basis C at the end of the tour satisfy:*

$$\mathcal{F}(C) \le \mathcal{F}(B)P^{-1}AP + \mathbf{g}P.$$

The matrix A and vector $\mathbf{g}$ are explicitly constructed in [HPS11]. More precisely, letting $\omega = \frac{\beta-1}{\beta}$:

$$A = \frac{1}{\beta} \times \begin{array}{c} \left(\begin{array}{cccc|cccc}
1 & \omega & \cdots & \omega^{n-\beta-1} & \omega^{n-\beta} & \cdots & \omega^{n-\beta} \\
\vdots & \vdots & & \vdots & \vdots & & \vdots \\
1 & \omega & \cdots & \omega^{n-\beta-1} & \omega^{n-\beta} & \cdots & \omega^{n-\beta} \\
\hline
 & 1 & \cdots & \omega^{n-\beta-2} & \omega^{n-\beta-1} & \cdots & \omega^{n-\beta-1} \\
 & & \ddots & \vdots & \vdots & & \vdots \\
 & & & 1 & \omega & \cdots & \omega \\
 & & & & 1 & \cdots & 1
\end{array}\right) \\
\underbrace{\hphantom{1\ \omega\ \cdots\ \omega^{n-\beta-1}}}_{n-\beta \text{ columns}}\ \underbrace{\hphantom{\omega^{n-\beta}\ \cdots\ \omega^{n-\beta}}}_{\beta \text{ columns}}
\end{array}
\begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} \beta \text{ rows} \\ \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\\ 1\end{array}}\right\} n-\beta \text{ rows} \end{array}
\in \mathbb{Q}^{n\times n}. \tag{8}$$

This A was actually built as a matrix product $A = A^{(1)} \cdot \ldots \cdot A^{(n-\beta+1)}$, where for $j = 1, \ldots, n-\beta+1$, each term is a doubly stochastic matrix

$$A^{(j)} = \begin{array}{c} \left(\begin{array}{ccc|ccc|ccc}
1 & & & & & & & & \\
 & \ddots & & & & & & & \\
 & & 1 & & & & & & \\
\hline
 & & & \frac{1}{\beta} & \cdots & \frac{1}{\beta} & & & \\
 & & & \vdots & \ddots & \vdots & & & \\
 & & & \frac{1}{\beta} & \cdots & \frac{1}{\beta} & & & \\
\hline
 & & & & & & 1 & & \\
 & & & & & & & \ddots & \\
 & & & & & & & & 1
\end{array}\right) \\
\hphantom{1\ \ddots\ 1\ }\underbrace{\hphantom{\frac{1}{\beta}\ \cdots\ \frac{1}{\beta}}}_{\beta \text{ columns}}\hphantom{1\ \ddots\ 1}
\end{array}
\begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \ddots\\ 1\end{array}}\right\} j-1 \text{ rows} \\ \left.\vphantom{\begin{array}{c}1\\ \ddots\\ 1\end{array}}\right\} \beta \text{ rows} \\ \left.\vphantom{\begin{array}{c}1\\ \ddots\\ 1\end{array}}\right\} n+1-j-\beta \text{ rows} \end{array}
\in \mathbb{Q}^{n\times n}.$$

Then:

$$\mathbf{g} = \sum_{j=1}^{n-\beta+1} \mathbf{g}^{(j)} \cdot A^{(j+1)} \cdot \ldots \cdot A^{(n-\beta+1)} \in \mathbb{R}^n \tag{9}$$

where $\mathbf{g}^{(j)} = (g_1^{(j)}, \ldots, g_n^{(j)}) \in \mathbb{R}^n$ is defined by

$$g_i^{(j)} = \begin{cases} 0 & \text{for } i = 1, \ldots, j-1, \\ \frac{1}{2}\log \nu_\beta & \text{for } i = j, \\ \frac{1}{2}\log \nu_{\beta-i+j} - \sum_{\kappa=\beta-i+j+1}^{\beta} \frac{\log \nu_\kappa}{2(\kappa-1)} & \text{for } i = j+1, \ldots, j+\beta-1, \\ 0 & \text{for } i = j+\beta, \ldots, n. \end{cases}$$

From the introduction overview, the inequality of Prop. 1 can be transformed into an inequality of the type (6) if we find a fixed point $\mathbf{w}$ of the dynamical system $\mathbf{x} \leftarrow \mathbf{x}P^{-1}AP + \mathbf{g}P$. Since P is an invertible matrix, this is equivalent to $\mathbf{w}P^{-1}$ being a fixed point of $\mathbf{x} \leftarrow \mathbf{x}A + \mathbf{g}$. [HPS11] constructed a fixed point $\overline{\mathbf{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$ of the latter as:

$$\overline{x}_j = \begin{cases} g_j^{(n-\beta+1)} & \text{for } j = n, \ldots, n-\beta+1, \\ \frac{\beta}{2(\beta-1)} \log \nu_\beta + \frac{1}{\beta-1} \sum_{i=j+1}^{j+\beta-1} \overline{x}_i & \text{for } j = n-\beta, \ldots, 1. \end{cases} \tag{10}$$

Then the inequality of type (6) allowed to prove Th. 1. Unfortunately, [HPS11] could not extend their analysis to the original BKZ: they could not prove an analogue of Prop. 1 for BKZ, because their proof of Prop. 1 worked by iterating a similar result for each iteration of BKZ', but an individual iteration of BKZ does not satisfy Prop. 1. This is why [HPS11, §3] claimed: "*it does not seem easy to use our techniques to analyze*" the original BKZ.

Spoiler Alert. The following observations are proved in Appendix B and will be useful in the next section: Item 1 will be used to prove Item 2, Lemma 2 in Section 3.3 and Proposition 3 in Section 3.5; Item 2 inspires us to explicitly define analogues of the vectors $\mathbf{g}$ and $\overline{\mathbf{x}}$ for a dynamical system of the original BKZ:

Fact 1. *Let $A \in \mathbb{Q}^{n\times n}$, $E \in \mathbb{Z}^{n\times n}$, $\mathbf{g} \in \mathbb{R}^n$ and $\overline{\mathbf{x}} \in \mathbb{R}^n$ be the matrices and vectors defined in Eq. (8), Eq. (7), Eq. (9) and Eq. (10), respectively. Let $\beta_j = \min\{\beta, n-j+1\}$ and $n_j = \min\{j+\beta-1, n\}$ for $j = 1, \ldots, n$. Then*

1. *For $j = 1, \ldots, n$, $E|_{n_j} = \sum_{i=1}^{j-1} A|_i + \beta_j A|_j$, or equivalently, $AE|_j = AE|_{j-1} + \frac{1}{\beta_j}(E|_{n_j} - AE|_{j-1})$.*
2. *$\mathbf{g}$ and $\overline{\mathbf{x}}$ have respectively internal recurrence relations:*

$$g_j = \begin{cases} \frac{1}{2}\log \nu_\beta & \textit{for } j = 1, \\ \frac{1}{2}\log \nu_{\beta_j} - \frac{1}{\beta_j}\sum_{i=1}^{j-1} g_i & \textit{for } j = 2, \ldots, n-1, \\ -\sum_{i=1}^{n-1} g_i & \textit{for } j = n, \end{cases}$$

$$\overline{x}_j = \begin{cases} -\sum_{\kappa=2}^{\beta} \frac{\log \nu_\kappa}{2(\kappa-1)} & \textit{for } j = n, \\ \frac{\beta_j}{2(\beta_j-1)} \log \nu_{\beta_j} + \frac{1}{\beta_j-1}\sum_{i=j+1}^{n_j} \overline{x}_i & \textit{for } j = n-1, \ldots, 1. \end{cases}$$

3 Worst-Case Analysis of BKZ Using Dynamical Systems

In this section, we show that it is actually possible to adapt the analysis of [HPS11] to the original BKZ, and more generally, to a generic BKZ algorithm which includes BKZ, BKZ' and other variants. Besides, we will see that our analysis offers both quantitative and qualitative improvements over [HPS11].

3.1 A Generic BKZ Algorithm

In order to analyze the worst-case behaviour of BKZ (Alg. 1), we introduce a generic BKZ algorithm, which we call GBKZ (Alg. 3), of which Alg. 1 is only a particular instantiation: this allows to better understand which properties of BKZ are essential, and to modify BKZ while preserving its most important properties.

Algorithm 3 GBKZ: a generic BKZ algorithm

Input: A blocksize $\beta \geq 2$, two relaxation factors $\delta \geq \eta \geq 1$, a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L in $\mathbb{R}^m$, and two GBKZ-compatible subroutines $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$.
Output: A new basis of L.
1: **repeat**
2:   **for** $j = 1$ to $n-1$ **do**
3:     $\beta_j \leftarrow \min\{\beta, n-j+1\}$; $n_j \leftarrow \min\{j+\beta-1, n\}$ //We have $\beta_j = \beta$ and $n_j = j+\beta-1$ if $j \leq n-\beta+1$.
4:     Find a primitive vector $\mathbf{b}$ for $L(\mathbf{b}_j, \ldots, \mathbf{b}_{n_j})$ such that $\|\pi_j(\mathbf{b})\| \leq \sqrt{\eta\gamma_{\beta_j}} \times \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$
5:     **if** $\eta \times \|\mathbf{b}_j^*\|^2 > \delta \times \|\pi_j(\mathbf{b})\|^2$ **then**
6:       Extract a new basis B by calling $\mathcal{A}_{\text{extract}}$ on $G = (\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}, \mathbf{b}_j, \ldots, \mathbf{b}_n)$
7:     **else**
8:       Reduce B by calling $\mathcal{A}_{\text{reduce}}$ //Right before this step, B satisfies: $\|\mathbf{b}_j^*\| \leq \sqrt{\delta\gamma_{\beta_j}} \times \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$.
9:     **end if**
10:   **end for**
11: **until** no change occurs or termination is requested, and **return** B.

A GBKZ iteration refers to a single execution of Steps 4-9: we call j the iteration index. The j-th GBKZ iteration retrieves the sublattice $L(\mathbf{b}_j, \ldots, \mathbf{b}_{n_j})$ whose rank β_j varies over index j: $\beta_j = \beta$ if $j \leq n - \beta + 1$ and $\beta_j \in \{2, \ldots, \beta-1\}$ otherwise. For convenience, we use the notation β_j and n_j throughout Section 3.

A GBKZ tour refers to a single execution of Steps 2-10, which corresponds to $n-1$ consecutive iterations from index 1 to $n-1$.

GBKZ requires two *GBKZ-compatible* subroutines $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$:
– $\mathcal{A}_{\text{reduce}}$ denotes any algorithm which, given as input a basis B of L, outputs a basis C of L such that $\mathcal{R}(C) \leq \mathcal{R}(B)$.
– $\mathcal{A}_{\text{extract}}$ denotes any algorithm with the property below, which is "almost" the same as the previous $\mathcal{R}(C) \leq \mathcal{R}(B)$.

We present and explain the requirement of $\mathcal{A}_{\text{extract}}$. Let L be the input lattice of BKZ. Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be the current basis. The crucial step of Alg. 1 is Step 4, where BKZ calls an oracle on the projected lattice $L(B_{[j,n_j]})$: this provides a primitive vector $\mathbf{b}$ in the sublattice $L(\mathbf{b}_j, \ldots, \mathbf{b}_{n_j})$, whose projection reaches the first minimum of $L(B_{[j,n_j]})$. If this vector is better than $\mathbf{b}_j$, BKZ executes Step 5, which means that it builds the generator matrix $G = (\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}, \mathbf{b}_j, \ldots, \mathbf{b}_n) \in \mathbb{R}^{(n+1)\times m}$ by inserting $\mathbf{b}$ at index j.

Step 6 of BKZ then runs the modified LLL algorithm [Poh87] for linearly dependent vectors on the first $\min\{j+\beta+1, n+1\}$ vectors of G: it concatenates the output with the last $\max\{n-j-\beta, 0\}$ vectors of G to form a new lattice basis. In GBKZ, we replace this step by $\mathcal{A}_{\text{extract}}$ which, given as input G, outputs a basis C of L such that $C \preccurlyeq_j G$. Here, the notation $C \preccurlyeq_j G$ for a basis C of L means that

$$\mathrm{vol}(C_{[1,i]}) \leq \begin{cases} \mathrm{vol}(G_{[1,i]}) = \mathrm{vol}(B_{[1,i]}) & \text{if } \ i = 1, \ldots, j-1, \\ \mathrm{vol}(G_{[1,i]}) & \text{if } \ i = j, \\ \mathrm{vol}(L(G_{[1,i+1]})) = \mathrm{vol}(B_{[1,i]}) & \text{if } \ i = n_j, \ldots, n. \end{cases}$$

This is equivalent to $\mathcal{R}_\ell(C) \leq \mathcal{R}_\ell(B)$ for all $\ell \in \{1, \ldots, n\} \setminus \{j, \ldots, n_j - 1\}$ and $\mathcal{R}_j(C) \leq \log \frac{d}{\mathrm{vol}(L)^{1/n}} + \mathcal{R}_{j-1}(B)$ where d is the distance of $\mathbf{b}$ to the subspace spanned by $B_{[1,j-1]}$.

Notice that BKZ is a particular instantiation of GBKZ where $\mathcal{A}_{\text{reduce}}$ is a partial LLL reduction (on $B_{[1,\min\{j+\beta,n\}]}$ rather than the whole B) and $\mathcal{A}_{\text{extract}}$ is a partial LLL for linearly dependent vectors, restricted to the first $\min\{j+\beta+1, n+1\}$ vectors of G. It follows from classical properties of LLL that in the case of BKZ, $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$ satisfy our two constraints: $\mathcal{R}(\text{output}(\mathcal{A}_{\text{reduce}})) \leq \mathcal{R}(\text{input}(\mathcal{A}_{\text{reduce}}))$ and $\mathcal{R}(\text{output}(\mathcal{A}_{\text{extract}})) \preccurlyeq_j \mathcal{R}(\text{input}(\mathcal{A}_{\text{extract}}))$. When these two constraints are satisfied, we say that $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$ are GBKZ-compatible.

Alternatively, we could select a full LLL reduction for $\mathcal{A}_{\text{extract}}$ and a trivial algorithm for $\mathcal{A}_{\text{reduce}}$: this choice is also GBKZ-compatible.

Finally, it can be checked that [HPS11]'s BKZ' is also an instantiation of GBKZ where the choice of $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$ is GBKZ-compatible.

Thus, GBKZ captures both BKZ and BKZ', as well as a simple modification of BKZ. We note that it is also possible to define different GBKZ-compatible algorithms $\mathcal{A}_{\text{reduce}}$ and $\mathcal{A}_{\text{extract}}$ without using LLL at all: for instance, one can rely on Li-Nguyen's XGCD-based basis algorithm [LN19].

3.2 Overview

The main result of this paper is as follows:

Theorem 2. *Let $n > \beta \geq 2$ be integers and let $0 < \varepsilon \leq 1 \leq \delta \leq \frac{2^{(\beta-1)/2}}{\gamma_\beta}$. Given as input a blocksize β, two relaxation factors $\delta \geq \eta \geq 1$, and a $\frac{3}{4}$-LLL-reduced basis B_0 of an n-rank lattice L in $\mathbb{R}^m$, if terminated after $\left\lceil 4(\ln 2)\frac{n^2}{\beta^2}\log\frac{n^2}{\varepsilon}\right\rceil$ tours, then Alg. 3 (GBKZ) outputs a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that*

$$\frac{\operatorname{vol}(B_{[1,i]})}{\operatorname{vol}(L)^{i/n}} \leq \begin{cases} (1+\varepsilon)^{\sqrt{i}}(\delta\gamma_\beta)^{\frac{i(n-i)}{2(\beta-1)}+\frac{i\beta(\beta-2)}{2n(\beta-1)}} & \text{if } i = 1, \ldots, n-\beta, \\ (1+\varepsilon)^{\sqrt{n-\beta}}(\delta\gamma_\beta)^{\frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)}\left(\prod_{\kappa=n-i+1}^{\beta}(\delta\gamma_\kappa)^{\frac{n-i}{2(\kappa-1)}}\right) & \text{if } i = n-\beta+1, \ldots, n-1. \end{cases}$$

As a by-product, our analysis gives the bound $\|\mathbf{b}_1\| \leq \gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2n(\beta-1)}}\operatorname{vol}(L)^{1/n}$ for β-BKZ reduced bases, which improves the previous bound $\|\mathbf{b}_1\| \leq \gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{1}{2}}\operatorname{vol}(L)^{1/n}$ [GN08b].

Analysis Overview. We summarize the structure of our analysis. We use the Rankin profile $\mathcal{R}(\cdot)$ to assess the quality of bases. Our proof of Th. 2 has the same structure as our introduction overview.

Let B_0 be the input basis of GBKZ, and denote by B_k the current basis of GBKZ at the end of the k-th tour, where $k \geq 1$. We construct an $n \times n$ matrix $M \geq 0$ and a vector $\mathbf{v} \in \mathbb{R}^n$ such that for any $k \geq 1$:

$$\mathcal{R}(B_k) \leq \mathcal{R}(B_{k-1})M + \mathbf{v}.$$

Then, we select a fixed point $\mathbf{w} \in \mathbb{R}^n$ of the map $\mathbf{x} \leftarrow \mathbf{x}M + \mathbf{v}$, which implies that:

$$\mathcal{R}(B_k) \leq (\mathcal{R}(B_0) - \mathbf{w})M^k + \mathbf{w}.$$

Finally, we build a vector $\mathbf{c} \in \mathbb{R}^n$ such that $\mathcal{R}(B_0) - \mathbf{w} \leq \mathbf{c}$, then

$$\mathcal{R}(B_k) \leq \|\mathbf{c}\| \cdot \|M\|_2^k \cdot \mathbf{1}_n + \mathbf{w}. \tag{11}$$

It follows that if B_0 is LLL-reduced, then we can take $\mathbf{c} = n^{O(1)} \cdot \mathbf{1}_n$ (because $\mathcal{R}(B_0) \leq n^{O(1)} \cdot \mathbf{1}_n$ and $\|\mathbf{w}\| \leq n^{O(1)}$) such that

$$\mathcal{R}(B_k) \leq n^{O(1)} \cdot \|M\|_2^k \cdot \mathbf{1}_n + \mathbf{w}.$$

By upper bounding $\mathbf{w}$ and the spectral norm $\|M\|_2$ (< 1), we deduce a good upper bound on $\mathcal{R}(B_k)$ for any sufficiently large k, independent of the input LLL-reduced basis B_0.

3.3 Analysis of GBKZ Iterations

The Case of One Iteration. Consider the j-th iteration of an arbitrary GBKZ tour (Step 2 of Alg. 3): let B and C be the current basis at respectively the beginning and the end of the iteration, that is, at the beginning of Step 4 and at the end of Step 9. [HPS11] could only analyze a variant of BKZ, because it is not possible to upper bound $\mathcal{R}(C)$ using only $\mathcal{R}(B)$. Yet, we can upper bound most of the entries of $\mathcal{R}(C)$ by some affine linear transform of $\mathcal{R}(B)$, thanks to the following key elementary lemma:

Lemma 1 (Propagation-lemma). *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and C be two bases of an n-rank lattice L in $\mathbb{R}^m$. Let $G = (\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}, \mathbf{b}_j, \ldots, \mathbf{b}_n) \in \mathbb{R}^{(n+1)\times m}$ be a generator matrix of L obtained by inserting at index j in B a primitive vector $\mathbf{b}$ of the sublattice $L(\mathbf{b}_j, \ldots, \mathbf{b}_{n_j})$. If either of the following two conditions hold for some $q > 0$:*

- *Condition 1: $C \preccurlyeq_j G$ and $\|\pi_j(\mathbf{b})\| \leq q \cdot \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$ where π_j is the orthogonal projection onto span$(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1})^\perp$;*
- *Condition 2: $\mathcal{R}(C) \leq \mathcal{R}(B)$ and $\|\mathbf{b}_j^*\| \leq q \cdot \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$,*

then

$$\mathcal{R}_j(C) \leq \frac{\beta_j - 1}{\beta_j}\mathcal{R}_{j-1}(B) + \frac{1}{\beta_j}\mathcal{R}_{n_j}(B) + \log q, \tag{12}$$

$$\mathcal{R}_i(C) \leq \mathcal{R}_i(B) \quad \text{if} \quad 1 \leq i < j \quad \text{or} \quad n_j \leq i \leq n. \tag{13}$$

Proof. If Condition 1 holds, then the definition of $C \preccurlyeq_j G$ in Section 3.1 implies:

$$\begin{aligned}
\mathrm{vol}(C_{[1,j]}) &\leq \mathrm{vol}(G_{[1,j]}) \\
&= \mathrm{vol}(B_{[1,j-1]}) \cdot \|\pi_j(\mathbf{b})\| \\
&\leq \mathrm{vol}(B_{[1,j-1]}) \cdot q \cdot \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j} \\
&= q \cdot \mathrm{vol}(B_{[1,j-1]}) \cdot \left(\frac{\mathrm{vol}(B_{[1,n_j]})}{\mathrm{vol}(B_{[1,j-1]})}\right)^{1/\beta_j} \\
&= q \cdot \mathrm{vol}(B_{[1,j-1]})^{(\beta_j-1)/\beta_j} \cdot \mathrm{vol}(B_{[1,n_j]})^{1/\beta_j}.
\end{aligned}$$

Since $\frac{j}{n} = \frac{j-1}{n} \times \frac{\beta_j - 1}{\beta_j} + \frac{n_j}{n} \times \frac{1}{\beta_j}$, we divide both sides by $\mathrm{vol}(L)^{j/n}$ to deduce (12). Furthermore, $\mathcal{R}_i(C) \leq \mathcal{R}_i(B)$ if $1 \leq i < j$ or $n_j \leq i \leq n$ because $C \preccurlyeq_j G$. Similarly, one can prove the same statements if Condition 2 holds. □

Our requirements that $\mathcal{A}_{\text{extract}}$ and $\mathcal{A}_{\text{reduce}}$ are GBKZ-compatible imply that either one of the two conditions of Lemma 1 holds at the end of each iteration. Thus, Lemma 1 allows to upper bound most coordinates of $\mathcal{R}(C)$, thanks to some affine transform of $\mathcal{R}(B)$.

The Case of Consecutive Iterations. Since GBKZ encompasses BKZ' studied by [HPS11], it should have a similar dynamical system as BKZ': in particular, one expects the matrix A used in [HPS11]'s analysis (see Section 2.4) to be useful to analyze GBKZ.

At any GBKZ tour, we are able to upper bound $\mathcal{R}(C)$ partially at the end of the iteration of any index j using $\mathcal{R}(B)$ at the beginning of the tour, thanks to the key observation that Lemma 1 can be composed into a matrix expression in terms of the known matrix A.

To see this, consider two consecutive GBKZ iterations of index j and $j+1$: denote by B (resp. C) the current basis at the start of the iteration of index j (resp. $j+1$), and denote by D the basis at the end of the iteration of index $j+1$. By Lemma 1, we can upper bound $\mathcal{R}(D)$ partially using $\mathcal{R}(C)$:

$$\begin{gathered}
\mathcal{R}_{j+1}(D) \leq \frac{\beta_{j+1} - 1}{\beta_{j+1}}\mathcal{R}_j(C) + \frac{1}{\beta_{j+1}}\mathcal{R}_{n_{j+1}}(C) + \frac{1}{2}\log(\delta\gamma_{\beta_{j+1}}), \\
\mathcal{R}_i(D) \leq \mathcal{R}_i(C) \text{ if } 1 \leq i < j+1 \text{ or } n_{j+1} \leq i \leq n.
\end{gathered}$$

Sin $n_{j+1} \geq n_j$, any coordinate $\mathcal{R}_\ell(C)$ appearing on the right-hand side can be upper-bounded using $\mathcal{R}(B)$ by Lemma 1:

$$\begin{gathered}
\mathcal{R}_j(C) \leq \frac{\beta_j - 1}{\beta_j}\mathcal{R}_{j-1}(B) + \frac{1}{\beta_j}\mathcal{R}_{n_j}(B) + \frac{1}{2}\log(\delta\gamma_{\beta_j}), \\
\mathcal{R}_i(C) \leq \mathcal{R}_i(B) \text{ if } 1 \leq i < j \text{ or } n_j \leq i \leq n.
\end{gathered}$$

By combining these inequalities together, we can upper bound $\mathcal{R}(D)$ partially using $\mathcal{R}(B)$:

$$
\begin{aligned}
\mathcal{R}_{j+1}(D) &\leq \frac{\beta_{j+1}-1}{\beta_{j+1}}\left(\frac{\beta_j-1}{\beta_j}\mathcal{R}_{j-1}(B)+\frac{1}{\beta_j}\mathcal{R}_{n_j}(B)+\frac{1}{2}\log(\delta\gamma_{\beta_j})\right)+\frac{1}{\beta_{j+1}}\mathcal{R}_{n_{j+1}}(B)+\frac{1}{2}\log(\delta\gamma_{\beta_{j+1}}),\\
\mathcal{R}_j(D) &\leq \mathcal{R}_j(C) \leq \frac{\beta_j-1}{\beta_j}\mathcal{R}_{j-1}(B)+\frac{1}{\beta_j}\mathcal{R}_{n_j}(B)+\frac{1}{2}\log(\delta\gamma_{\beta_j}),\\
\mathcal{R}_i(D) &\leq \mathcal{R}_i(C) \leq \mathcal{R}_i(B) \text{ if } 1 \leq i < j \text{ or } n_{j+1} \leq i \leq n.
\end{aligned}
$$

Another important thing is that the number of coordinates of $\mathcal{R}(D)$ (upper-bounded using $\mathcal{R}(B)$) is exactly equal to that of $\mathcal{R}(D)$ (upper-bounded using $\mathcal{R}(C)$), and is equal to or greater than that of $\mathcal{R}(C)$ (upper-bounded using $\mathcal{R}(B)$).

By composing multiple iterations instead of just two, we obtain the second key elementary lemma:

Lemma 2 (Aggregation-lemma). *Let $A \in \mathbb{Q}^{n\times n}$ and $E \in \mathbb{Z}^{n\times n}$ be the matrices defined in Eq. (8) and Eq. (7), respectively. Let $\mathbf{g} = (g_1, \dots, g_n)$ be a vector in $\mathbb{R}^n$ depending on the relaxation factor $\delta \geq 1$ and defined by*

$$
g_j = \begin{cases} \frac{1}{2}\log(\delta\gamma_\beta) & \text{for } j = 1,\\ \frac{1}{2}\log(\delta\gamma_{\beta_j}) - \frac{1}{\beta_j}\sum_{i=1}^{j-1} g_i & \text{for } j = 2,\dots,n-1,\\ -\sum_{i=1}^{n-1} g_i & \text{for } j = n. \end{cases} \tag{14}
$$

If a GBKZ tour transforms a basis $B^{(j-1)}$ of an n-rank lattice L into another basis $B^{(j)}$ of L in turn over the iteration index $j = 1,\dots,n-1$ where $B^{(0)} = B$, then for all $j = 1,\dots,n-1$,

$$
\mathcal{R}_i(B^{(j)}) \leq \mathcal{R}(B)E^{-1}AE|_i + \mathbf{g}E|_i \quad \text{if} \quad i = 1,\dots,j, \tag{15}
$$

$$
\mathcal{R}_i(B^{(j)}) \leq \mathcal{R}_i(B) \quad \text{if} \quad i = n_j,\dots,n. \tag{16}
$$

Our construction of the above vector $\mathbf{g}$ is inspired by the observation illustrated in Fact 1.2. We stress that both $\mathbf{g}$ defined in Eq. (14) and Eq. (9) are different: Besides depending on the relaxation factor δ, the vector $\mathbf{g}$ in Eq. (14) is expressed in terms of Hermite's constant γ_i (rather than [HPS11]'s ad-hoc constant ν_i; See Section 2.4).

One key point here is that the number $\mathcal{N}(j)$ of coordinates of $\mathcal{R}(B^{(j)})$ (upper-bounded using $\mathcal{R}(B)$) increases over index j and reaches n as $j = n-1$:

$$
\mathcal{N}(j) = j + (n - n_j + 1) = \max\{j+1, n-\beta+2\} \in \{n-\beta+2,\dots,n\} \quad \text{for} \quad j = 1,\dots,n-1.
$$

Proof of Lemma 2. Eq. (16) follows from Eq. (13) in Lemma 1, because for all $j = 1,\dots,n-1$,

$$
\mathcal{R}_i(B^{(j)}) \leq \mathcal{R}_i(B^{(j-1)}) \leq \cdots \leq \mathcal{R}_i(B^{(0)}) = \mathcal{R}_i(B) \quad \text{if} \quad i = n_j,\dots,n.
$$

The main difficulty is to show Eq. (15), which is done by induction on j.

The inequality $\mathcal{R}_1(B^{(1)}) \leq \mathcal{R}(B)E^{-1}AE|_1 + \mathbf{g}E|_1$ holds. Indeed, Eq. (12) in Lemma 1 implies $\mathcal{R}_1(B^{(1)}) \leq \frac{1}{\beta}\mathcal{R}_\beta(B) + \frac{1}{2}\log(\delta\gamma_\beta)$. It can be checked that $\frac{1}{\beta}\mathcal{R}_\beta(B) = \mathcal{G}(B)A|_1 = (\mathcal{R}(B)E^{-1})(AE|_1)$ and $\frac{1}{2}\log(\delta\gamma_\beta) = g_1 = \mathbf{g}E|_1$. This implies the desired inequality.

Assume that $\mathcal{R}_i(B^{(j-1)}) \leq \mathcal{R}(B)E^{-1}AE|_i + \mathbf{g}E|_i$ holds over $i = 1,\dots,j-1$ for some index $j \in [2, n-1]$.

We need to upper bound $\mathcal{R}_i(B^{(j)})$ over $i = 1,\dots,j$. Eq. (13) implies that $\mathcal{R}_i(B^{(j)}) \leq \mathcal{R}_i(B^{(j-1)})$ over $i = 1,\dots,j-1$. By the induction hypothesis, we have $\mathcal{R}_i(B^{(j)}) \leq \mathcal{R}(B)E^{-1}AE|_i + \mathbf{g}E|_i$ over $i = 1,\dots,j-1$.

By applying Eq. (12) to $\mathcal{R}_j(B^{(j)})$, we obtain:

$$
\mathcal{R}_j(B^{(j)}) \leq \frac{\beta_j-1}{\beta_j}\mathcal{R}_{j-1}(B^{(j-1)}) + \frac{1}{\beta_j}\mathcal{R}_{n_j}(B^{(j-1)}) + \frac{1}{2}\log(\delta\gamma_{\beta_j}).
$$

Note that Eq. (16) guarantees that $\mathcal{R}_{n_j}(B^{(j-1)}) \leq \mathcal{R}_{n_j}(B)$. The definition of $\mathcal{R}(\cdot)$ implies that $\mathcal{R}_{n_j}(B) = \mathcal{R}(B)E^{-1}E|_{n_j}$. It follows from the induction hypothesis $\mathcal{R}_{j-1}(B^{(j-1)}) \leq \mathcal{R}(B)E^{-1}AE|_{j-1} + \mathbf{g}E|_{j-1}$ that

$$
\begin{aligned}
\mathcal{R}_j(B^{(j)}) &\leq \left(1 - \frac{1}{\beta_j}\right)\mathcal{R}_{j-1}(B^{(j-1)}) + \frac{1}{\beta_j}\mathcal{R}(B)E^{-1}E|_{n_j} + \frac{1}{2}\log(\delta\gamma_{\beta_j}) \\
&\leq \mathcal{R}(B)E^{-1}AE|_{j-1} + \mathbf{g}E|_{j-1} + \frac{\mathcal{R}(B)E^{-1}}{\beta_j}(E|_{n_j} - AE|_{j-1}) + \frac{1}{2}\log(\delta\gamma_{\beta_j}) - \frac{1}{\beta_j}\mathbf{g}E|_{j-1} \\
&= \mathcal{R}(B)E^{-1}AE|_j + \mathbf{g}E|_j + \left(\frac{1}{2}\log(\delta\gamma_{\beta_j}) - \frac{1}{\beta_j}\sum_{i=1}^{j-1} g_i - g_j\right) && \text{(By Fact 1.1)} \\
&= \mathcal{R}(B)E^{-1}AE|_j + \mathbf{g}E|_j, && \text{(By Eq. (14))}
\end{aligned}
$$

as desired. This completes the proof. $\square$

3.4 A Dynamical System for GBKZ Tours

At any GBKZ tour, we are able to upper bound $\mathcal{R}(C)$ partially at the end of any iteration using $\mathcal{R}(B)$ at the beginning of the tour, thanks to Lemma 2. Right after the last iteration of the tour, the partial profile has become a full profile. This shows that GBKZ satisfies an inequality like (5), where the iterative matrix is "positive", and the corresponding dynamical system has a unique fixed point (which we will show in Section 3.5). From the introduction overview, this means that GBKZ also satisfies an inequality of type (6).

Proposition 2. *Let $A \in \mathbb{Q}^{n\times n}$, $E \in \mathbb{Z}^{n\times n}$ and $\mathbf{g} \in \mathbb{R}^n$ be the matrices and vector defined in Eq. (8), Eq. (7) and Eq. (14), respectively. Let $Q \in \mathbb{Q}^{n\times n}$ be the orthogonal projection onto span($\mathbf{1}_n$). Let L be an n-rank lattice. If a GBKZ tour transforms a basis B of L into another basis C of L, then*

$$\mathcal{R}(C) \leq \mathcal{R}(B)E^{-1}(A-Q)E + \mathbf{g}E \quad \textit{with} \quad E^{-1}AE \geq 0. \tag{17}$$

Moreover, let $\mathbf{w} \in \mathbb{R}^n$ be a fixed point of the dynamical system $\mathbf{x} \leftarrow \mathbf{x}E^{-1}(A-Q)E + \mathbf{g}E$. If B_0 is the input basis of L to GBKZ and B_k is the current basis at the end of the k-th tour, then

$$\mathcal{R}(B_k) \leq (\mathcal{R}(B_0) - \mathbf{w})\, E^{-1}(A-Q)^k E + \mathbf{w} \quad \textit{for} \quad \forall k \in \mathbb{Z}^+. \tag{18}$$

Before proceeding to the proof, we first explain the meaning of the matrix Q. It follows from [YTT11, Example 2.3] that $1_{n\times n} - Q$ is the orthogonal projection onto span$(\mathbf{1}_n)^\perp$ and

$$Q = \mathbf{1}_n^T(\mathbf{1}_n\mathbf{1}_n^T)^{-1}\mathbf{1}_n = \frac{1}{n}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{Q}^{n\times n}. \tag{19}$$

Since Q is the orthogonal projection onto span($\mathbf{1}_n$), one could replace the matrix $A-Q$ in both Eq. (17) and Eq. (18) by any matrix $A - \rho\cdot Q$ where $\rho \in \mathbb{R}$. However, we choose $A-Q$ because $A-Q$ has the smallest spectral norm $\|A-Q\|_2 \leq \|A-\rho\cdot Q\|_2$. Indeed, it follows from the basic knowledge that $\|M\|_2^2$ is the largest eigenvalue of MM^T for any matrix M and the claim below (see Appendix B for the proof):

Claim 1. *Let $A \in \mathbb{Q}^{n\times n}$ and $Q \in \mathbb{Q}^{n\times n}$ be the matrices defined in Eq. (8) and Eq. (19), respectively. Let $\Phi(M)$ denote the set of eigenvalues of matrix M. Then*

$$\Phi((A-Q)(A-Q)^T) \subseteq \Phi((A-\rho\cdot Q)(A-\rho\cdot Q)^T) \quad \textit{for any} \quad \rho \in \mathbb{R}.$$

In particular, $\Phi((A-Q)(A-Q)^T) = \Phi(AA^T)\backslash\{1\}$.

The proof of Proposition 2 will use the following basic facts:

– For any n-rank basis B, $\mathcal{R}_n(B) = 0$ and $(\mathcal{R}(B)E^{-1})Q = \mathbf{0}$.
– It can be checked that A is a doubly stochastic matrix and hence

$$A^i Q = QA^i = QA^T = Q^i = Q^T = Q \quad \text{for any} \quad i \in \mathbb{Z}^+. \tag{20}$$

In particular, $(\mathcal{R}(B)E^{-1})(AE|_n) = 0$ and $(A-Q)E|_n = \mathbf{0}^T$.
– $\mathbf{g}E|_n = \sum_{i=1}^n g_i = 0$ (by Eq. (14)).

Proposition 2 follows from Lemma 2.

Proof of Proposition 2. First, since we know the explicit expressions of matrices E^{-1}, A and E (*e.g.*, both E^{-1} and E are simple upper triangular matrices), a direct calculation by hand allows to validate $E^{-1}AE \geq 0$.

To show Eq. (17), it is equivalent to prove that

$$\mathcal{R}(C) \leq \mathcal{R}(B)E^{-1}AE + \mathbf{g}E. \tag{21}$$

Note that $\mathcal{R}_n(C) \leq \mathcal{R}(B)E^{-1}AE|_n + \mathbf{g}E|_n$ holds, because both sides are zero. With the notations of Lemma 2, $C = B^{(n-1)}$: hence, Eq. (15) in Lemma 2 for index $j = n-1$ implies Eq. (21). This proved Eq. (17).

It remains to show Eq. (18). Note that the last entry of $\mathbf{w}$ is zero, because $w_n = \mathbf{w}E^{-1}(A-Q)E|_n + \mathbf{g}E|_n$. It is easy to check that the first $n-1$ rows of $E^{-1}Q$ are zero. This implies that $\mathcal{R}(B)E^{-1}Q = \mathbf{w}E^{-1}Q = \mathbf{0}$. Applying Fact (20), it follows that

$$(\mathcal{R}(B) - \mathbf{w})E^{-1}(A-Q)^k = (\mathcal{R}(B) - \mathbf{w})E^{-1}A^k \quad \text{for} \quad \forall k \in \mathbb{Z}^+. \tag{22}$$

Thus, to show Eq. (18), it is equivalent to prove the following inequality:

$$\mathcal{R}(B_k) \leq (\mathcal{R}(B_0) - \mathbf{w})\, E^{-1}A^kE + \mathbf{w} \quad \text{for} \quad \forall k \in \mathbb{Z}^+. \tag{23}$$

This is done by induction on k.

First, since $\mathbf{w} = \mathbf{w}E^{-1}AE + \mathbf{g}E$, it follows from Eq. (21) that Eq. (23) holds for $k = 1$.

Assume that Eq. (23) holds for some $k \in \mathbb{Z}^+$.

The crucial fact $E^{-1}AE \geq 0$ allows us to iterate the following inequalities:

$$\begin{aligned}
\mathcal{R}(B_{k+1}) &\leq \mathcal{R}(B_k)E^{-1}AE + \mathbf{g}E && \text{(By Eq. (21))}\\
&\leq (\mathcal{R}(B_0) - \mathbf{w})\, E^{-1}A^{k+1}E + \mathbf{w}E^{-1}AE + \mathbf{g}E && \text{(By the induction hypothesis)}\\
&= (\mathcal{R}(B_0) - \mathbf{w})\, E^{-1}A^{k+1}E + \mathbf{w}.
\end{aligned}$$

Thus, we proved Eq. (23) and hence Eq. (18). This completes the proof of Proposition 2. □

Remark 1. A direct calculation by hand implies:

$$E^{-1}QE = \frac{1}{n}\begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 2 & \cdots & n \end{pmatrix} \in \mathbb{Q}^{n\times n},$$

so that $(E^{-1}(A-Q)E)_{[1,n-1]} \geq 0$, but the last row of $E^{-1}(A-Q)E$ has negative entries. Yet, since the last entry of both $\mathbf{w}$ and $\mathcal{R}(B)$ for any basis B is zero, $E^{-1}QE$ amounts to a zero matrix when multiplying $\mathcal{R}(B) - \mathbf{w}$ with $E^{-1}(A-Q)E$. As a result, Eq. (22) ensures that it is still possible to iterate and deduce Eq. (18), with condition $E^{-1}AE \geq 0$.

It is known that any HKZ-reduced basis C of rank β has Rankin profile: $\mathcal{R}_j(C) \leq (\beta - j)\sum_{\kappa=\beta-j+1}^{\beta} \frac{\log \gamma_\kappa}{2(\kappa-1)}$ for $j = 1, \ldots, \beta - 1$ [HS07, Lemma 3]. We note that the tail projected block $B_{[n-\beta+1,n]}$ of the current basis B at the end of any GBKZ tour satisfies a similar inequality:

Corollary 1. *Let $A \in \mathbb{Q}^{n\times n}$, $E \in \mathbb{Z}^{n\times n}$ and $Q \in \mathbb{Q}^{n\times n}$ be the matrices defined in Eq. (8), Eq. (7) and (19), respectively. Let $\mathbf{w} \in \mathbb{R}^n$ be a fixed point of the dynamical system $\mathbf{x} \leftarrow \mathbf{x}E^{-1}(A-Q)E + \mathbf{g}E$. Let B_0 be the input basis of an n-rank lattice L to GBKZ and B_k be the current basis at the end of the k-th tour. For any $k \in \mathbb{Z}^+$ and all $j = n-\beta+1,\dots,n-1$, we have:*

$$\mathcal{R}_j(B_k) \le \frac{n-j}{\beta}\left(w_{n-\beta} + \left(\mathcal{R}(B_0)-\mathbf{w}\right)E^{-1}(A-Q)^k E|_{n-\beta}\right) + (n-j)\sum_{\kappa=n-j+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)}.$$

Proof. Corollary 1 is a consequence of Lemmas 1, 2 and Proposition 2.

Let $k \in \mathbb{Z}^+$ be fixed. Let $B_k^{(j)}$ denote the current basis at the end of the iteration of index $j = 1,\dots,n-1$ during the k-th GBKZ tour. We first prove by induction that for $j = n-\beta,\dots,n-1$,

$$\mathcal{R}_j(B_k^{(j)}) \le \frac{n-j}{\beta}\left(w_{n-\beta} + \left(\mathcal{R}(B_0)-\mathbf{w}\right)E^{-1}(A-Q)^k E|_{n-\beta}\right) + (n-j)\sum_{\kappa=n-j+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)}. \tag{24}$$

Eq. (24) holds initially when $j = n-\beta$. This is because

$$\begin{aligned}
\mathcal{R}_{n-\beta}(B_k^{(n-\beta)}) &\le \left(\mathcal{R}(B_{k-1})E^{-1}(A-Q) + \mathbf{g}\right)E|_{n-\beta} && \text{(By Lemma 2)}\\
&\le \left(\left(\mathcal{R}(B_0)-\mathbf{w}\right)E^{-1}(A-Q)^k + \mathbf{w}E^{-1}(A-Q) + \mathbf{g}\right)E|_{n-\beta} && \text{(Applying Eq. (18) to } \mathcal{R}(B_{k-1}))\\
&= w_{n-\beta} + \left(\mathcal{R}(B_0)-\mathbf{w}\right)E^{-1}(A-Q)^k E|_{n-\beta}.
\end{aligned}$$

Here, the last equality used the fact: $\mathbf{w} = (\mathbf{w}E^{-1}(A-Q)+\mathbf{g})E$ implies $(\mathbf{w}E^{-1}(A-Q)+\mathbf{g})E|_{n-\beta} = w_{n-\beta}$.

Assume that Eq. (24) holds over $j = n-\beta,\dots,\ell-1$ for some index $\ell \in [n-\beta+1, n-1]$.

Applying Eq. (12) in Lemma 1 and the induction hypothesis for $\mathcal{R}_{\ell-1}(B_k^{(\ell-1)})$ in turn, we have

$$\begin{aligned}
\mathcal{R}_\ell(B_k^{(\ell)}) &\le \frac{n-\ell}{n-\ell+1}\mathcal{R}_{\ell-1}(B_k^{(\ell-1)}) + \log\sqrt{\delta\gamma_{n-\ell+1}} && \text{(Since } \mathcal{R}_n(B_k^{(\ell-1)}) = 0)\\
&\le \frac{n-\ell}{\beta}\left(w_{n-\beta} + \left(\mathcal{R}(B_0)-\mathbf{w}\right)E^{-1}(A-Q)^k E|_{n-\beta}\right) + (n-\ell)\sum_{\kappa=n-\ell+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)}.
\end{aligned}$$

Thus, we proved Eq. (24) for all $j = n-\beta,\dots,n-1$.

Eq. (13) in Lemma 1 ensures $\mathcal{R}_j(B_k) \le \mathcal{R}_j(B_k^{(n-1)}) \le \cdots \le \mathcal{R}_j(B_k^{(j)})$ for all $j = n-\beta,\dots,n-1$. By Eq. (24), Corollary 1 follows. ☐

3.5 Properties of the Dynamical System

The effect of a GBKZ tour on $\mathcal{R}(B)$ can be interpreted as the dynamical system $\mathbf{x} \leftarrow \mathbf{x}E^{-1}(A-Q)E + \mathbf{g}E$, thanks to Eq. (17). Its fixed point(s) and speed of convergence encode information on the output quality and runtime of GBKZ, respectively, as illustrates by Eq. (18). Since E is an invertible matrix, it is equivalent to study another simpler dynamical system

$$\mathbf{x} \leftarrow \mathbf{x}(A-Q) + \mathbf{g}. \tag{25}$$

[HPS11]'s system $\mathbf{x} \leftarrow \mathbf{x}A + \mathbf{g}$ (with different $\mathbf{g}$ in Eq. (9)) has spectral norm $\|A\|_2 = 1$ and fixed point set $\overline{\mathbf{x}} + \mathrm{span}(\mathbf{1}_n)$ (see [HPS11, §4]). However, our system (25) converges and has a unique fixed point:

Proposition 3. *Let $A \in \mathbb{Q}^{n\times n}$, $Q \in \mathbb{Q}^{n\times n}$ and $\mathbf{g} \in \mathbb{R}^n$ be respectively the matrices and vectors defined in Eq. (8), Eq. (19) and Eq. (14), where $\mathbf{g}$ depends on the relaxation factor $\delta \ge 1$.*

1. *$A-Q$ has spectral norm: $\|A-Q\|_2 \le \sqrt{1-\frac{\beta^2}{2n^2}}$.*

2. The system $\mathbf{x} \leftarrow \mathbf{x}(A - Q) + \mathbf{g}$ *has a unique fixed point*

$$\widehat{\mathbf{w}} = (\widehat{w}_1, \dots, \widehat{w}_n) := \widehat{\mathbf{x}}(1_{n\times n} - Q) \in \mathbb{R}^n, \tag{26}$$

which is the orthogonal projection onto span$(\mathbf{1}_n)^\perp$ *of* $\widehat{\mathbf{x}} = (\widehat{x}_1, \dots, \widehat{x}_n) \in \mathbb{R}^n$ *defined by*

$$\widehat{x}_j = \begin{cases} -\sum_{\kappa=2}^{\beta} \frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)} & \text{for } j = n, \\ \frac{\beta_j}{2(\beta_j-1)} \log(\delta\gamma_{\beta_j}) + \frac{1}{\beta_j - 1}\sum_{i=j+1}^{n_j} \widehat{x}_i & \text{for } j = n-1, \dots, 1. \end{cases} \tag{27}$$

Proof. We first argue Item 1. It was shown in [HPS11, §4.3] that the largest and second largest eigenvalues of AA^T is 1 and belongs to $[1 - \frac{\pi^2\beta^2}{(n-\beta)^2}, 1 - \frac{\beta^2}{2n^2}]$, respectively. Since $\|A - Q\|_2^2$ is the largest eigenvalue of $(A - Q)(A - Q)^T$, Claim 1 immediately implies $\|A - Q\|_2^2 \le 1 - \frac{\beta^2}{2n^2}$. This proves Item 1.

We now show Item 2. The hard part is to argue the following equality:

Claim 2. $\widehat{\mathbf{x}} = \widehat{\mathbf{x}}A + \mathbf{g}$.

Proof of Claim 2. It suffices to prove by induction on i that the following equalities hold:

$$\widehat{x}_i = \widehat{\mathbf{x}}A|_i + g_i \quad \text{for} \quad i = 1, \dots, n. \tag{28}$$

The concrete approach is to just simply exploit the definitions of both $\mathbf{g}$ and $\widehat{\mathbf{x}}$.

Eq. (28) holds initially when $i = 1$. Indeed, applying Eq. (27) and Eq. (14) in turn, we have

$$\widehat{x}_1 = \frac{1}{2}\log(\delta\gamma_\beta) + \frac{1}{\beta}\sum_{i=1}^{\beta} \widehat{x}_i = \widehat{\mathbf{x}}A|_1 + g_1.$$

Assume that Eq. (28) holds over $i = 1, \dots, j-1$ for some index $j \in [2, n-1]$.

The summation of Eq. (28) over $i = 1, \dots, j-1$ implies:

$$\begin{aligned} \sum_{i=1}^{j-1} \widehat{x}_i &= \widehat{\mathbf{x}}\left(\sum_{i=1}^{j-1} A|_i\right) + \sum_{i=1}^{j-1} g_i = \widehat{\mathbf{x}}\left(E|_{n_j} - \beta_j A|_j\right) + \sum_{i=1}^{j-1} g_i && \text{(By Fact 1.1)} \\ &= \widehat{\mathbf{x}}\left(E|_{n_j} - \beta_j A|_j\right) + \beta_j\left(\frac{1}{2}\log(\delta\gamma_{\beta_j}) - g_j\right) && \text{(By Eq. (14))} \\ &= \sum_{i=1}^{n_j} \widehat{x}_i + \beta_j\left(\frac{1}{2}\log(\delta\gamma_{\beta_j}) - \widehat{\mathbf{x}}A|_j - g_j\right). \end{aligned}$$

This means that $\frac{1}{2}\log(\delta\gamma_{\beta_j}) + \frac{1}{\beta_j}\sum_{i=j}^{n_j} \widehat{x}_i = \widehat{\mathbf{x}}A|_j + g_j$. Since $\widehat{x}_j = \frac{1}{2}\log(\delta\gamma_{\beta_j}) + \frac{1}{\beta_j}\sum_{i=j}^{n_j} \widehat{x}_i$ (by Eq. (27)), this implies $\widehat{x}_j = \widehat{\mathbf{x}}A|_j + g_j$, that is, Eq. (28) holds for $i = j$.

Thus, we proved Eq. (28) for all $i = 1, \dots, n-1$. In particular, we have $\sum_{i=1}^{n-1} \widehat{x}_i = \sum_{i=1}^{n-1} (\widehat{\mathbf{x}}A|_i + g_i)$.

Since A is a doubly stochastic matrix, we have $\sum_{i=1}^{n} A|_i = \mathbf{1}_n^T$. Note that $\sum_{i=1}^{n} g_i = 0$ (by Eq. (14)), then

$$\sum_{i=1}^{n} \widehat{x}_i = \widehat{\mathbf{x}}\left(\sum_{i=1}^{n} A|_i\right) + \sum_{i=1}^{n} g_i = \sum_{i=1}^{n} (\widehat{\mathbf{x}}A|_i + g_i).$$

It follows that $\widehat{x}_n = \widehat{\mathbf{x}}A|_n + g_n$. This proves Claim 2. ☐

Returning to the proof of Item 2, it follows from $Q^2 = Q$ (see Eq. (20)) that $\widehat{\mathbf{w}}Q = \mathbf{0}$, or equivalently, $\sum_{i=1}^{n} \widehat{w}_i = 0$. Then $\widehat{\mathbf{w}}$ is the orthogonal projection of $\widehat{\mathbf{x}}$ onto span$(\mathbf{1}_n)^\perp$. Since $QA = Q$ (see Eq. (20)), applying the fact $\widehat{\mathbf{x}} = \widehat{\mathbf{w}} + \widehat{\mathbf{x}}Q$ to Claim 2, we have $\widehat{\mathbf{w}} = \widehat{\mathbf{w}}A + \mathbf{g}$. This implies $\widehat{\mathbf{w}} = \widehat{\mathbf{w}}(A - Q) + \mathbf{g}$.

It remains to show the unicity. Let $\lambda_1, \lambda_2, \dots, \lambda_n$ denote the n eigenvalues of $A - Q$. It is classical that $\max_{1\le i\le n} |\lambda_i| \le \|A - Q\|_2$. By Item 1, 1 is not an eigenvalue of $A - Q$. Then the linear system $\mathbf{x}(A - Q) = \mathbf{x}$ only has zero solution. Therefore, $\widehat{\mathbf{w}}$ is the unique solution to $\mathbf{x} = \mathbf{x}(A - Q) + \mathbf{g}$. This completes the proof. ☐

By Proposition 3.2, $\widehat{\mathbf{w}}E$ is the unique fixed point of the system $\mathbf{x} \leftarrow \mathbf{x}E^{-1}(A-Q)E + \mathbf{g}E$. Then Eq. (18) in Proposition 2 implies that the tail term $(\mathcal{P}(B_0) - \mathbf{w})M^k$ of Eq. (6) in the context of GBKZ is exactly $(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k E$. It has an explicit vectorial upper bound as exhibited in Eq. (11), which converges to zero by Proposition 3.1:

Proposition 4. *Let $n > \beta \geq 2$ be integers and $\delta \geq 1$. Let $A \in \mathbb{Q}^{n\times n}$, $E \in \mathbb{Z}^{n\times n}$, $Q \in \mathbb{Q}^{n\times n}$ and $\widehat{\mathbf{w}} \in \mathbb{R}^n$ be the matrices and vector defined in Eq. (8), Eq. (7), Eq. (19) and Eq. (26), respectively. If B is a basis of an n-rank lattice, then*

$$(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k E \leq \left(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\right) \cdot \|A-Q\|_2^k \cdot \left(1, \sqrt{2}, \ldots, \sqrt{n}\right) \quad \textit{for } \forall k \in \mathbb{Z}^+.$$

Here, $\overline{\mathcal{R}}(B)$ denotes any vector in $\mathbb{R}^n$ satisfying $\mathcal{R}(B) \leq \overline{\mathcal{R}}(B)$ and $\mathcal{R}_n(B) = \overline{\mathcal{R}}_n(B) = 0$.

Moreover, for $0 < \varepsilon \leq 1$, if

$$k \geq 4(\ln 2)\frac{n^2}{\beta^2} \log \frac{\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|}{\varepsilon}, \tag{29}$$

then

$$(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k E \leq \left(1, \sqrt{2}, \ldots, \sqrt{n}\right) \times \log(1+\varepsilon) \in \mathbb{R}^n_{>0}.$$

Proof. We show the first assertion. Let $\mathbf{w}^{(k)} = (\overline{\mathcal{R}}(B)E^{-1} - \widehat{\mathbf{w}})(A-Q)^k$ for $k \in \mathbb{Z}^+$.

As argued for Eq. (22) in the proof of Proposition 2, we similarly have

$$\begin{aligned}(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k &= (\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}A^k,\\ \left(\overline{\mathcal{R}}(B) - \widehat{\mathbf{w}}E\right) E^{-1}(A-Q)^k &= \left(\overline{\mathcal{R}}(B) - \widehat{\mathbf{w}}E\right) E^{-1}A^k.\end{aligned}$$

Since $E^{-1}AE \geq 0$ (see Eq. (17)), $(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}A^kE \leq \left(\overline{\mathcal{R}}(B) - \widehat{\mathbf{w}}E\right) E^{-1}A^kE$. It follows that

$$(\mathcal{R}(B) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k E \leq \mathbf{w}^{(k)}E.$$

It follows from $\frac{1}{i}\sum_{j=1}^{i} |w_j^{(k)}| \leq \sqrt{\frac{1}{i}\sum_{j=1}^{i}(w_j^{(k)})^2} \leq \frac{1}{\sqrt{i}} \times \|\mathbf{w}^{(k)}\|$ that

$$\mathbf{w}^{(k)}E|_i \leq \left|\mathbf{w}^{(k)}E|_i\right| = \left|\sum_{j=1}^{i} w_j^{(k)}\right| \leq \sqrt{i} \times \|\mathbf{w}^{(k)}\| \quad \text{for} \quad i = 1, \ldots, n.$$

Since the spectral norm $\|\cdot\|_2$ on $\mathbb{R}^{n\times n}$ is consistent with the Euclidean norm $\|\cdot\|$ on $\mathbb{R}^n$, we have

$$\|\mathbf{w}^{(k)}\| \leq \|\overline{\mathcal{R}}(B)E^{-1} - \widehat{\mathbf{w}}\| \cdot \|A-Q\|_2^k \leq \left(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\right) \cdot \|A-Q\|_2^k.$$

Combining the above, this implies the first assertion.

It remains to show the second assertion under the assumption that k satisfies Eq. (29). Thanks to the first assertion, it suffices to prove $\left(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\right) \cdot \|A-Q\|_2^k \leq \log(1+\varepsilon)$. Since $\|A-Q\|_2 \leq \sqrt{1 - \frac{\beta^2}{2n^2}}$, consider the positive real number N such that $\left(1 - \frac{\beta^2}{2n^2}\right)^{N/2} \left(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\right) = \log(1+\varepsilon)$. Then

$$N = \frac{2(\log\left(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\right) - \log\log(1+\varepsilon))}{\log(1 - \frac{\beta^2}{2n^2})^{-1}}.$$

Since $\log(1-x)^{-1} \geq \frac{x}{\ln 2}$ and $\log(1+x) \geq x$ for $0 < x < 1$, we have

$$\log\left(1 - \frac{\beta^2}{2n^2}\right)^{-1} \geq \frac{1}{2\ln 2} \cdot \frac{\beta^2}{n^2} \quad \text{and} \quad \log\log(1+\varepsilon) \geq \log\varepsilon.$$

It follows that

$$N \leq 4(\ln 2)\frac{n^2}{\beta^2}\log\frac{\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|}{\varepsilon}.$$

Since k satisfies Eq. (29), then $k \geq N$ implies $\big(\|\overline{\mathcal{R}}(B)E^{-1}\| + \|\widehat{\mathbf{w}}\|\big) \cdot \|A - Q\|_2^k \leq \log(1+\varepsilon)$. This proves the second assertion and completes the proof of Proposition 4. $\square$

Eq. (18) in Proposition 2 and Eq. (29) in Proposition 4 suggest to upper bound the fixed point $\widehat{\mathbf{w}}E$ and the norm $\|\widehat{\mathbf{w}}\|$:

Proposition 5. *Let $n > \beta \geq 2$ be integers and $\delta \geq 1$. Let $\widehat{\mathbf{w}} \in \mathbb{R}^n$ be the vector defined in Eq. (26).*

1. *Its first entries satisfy: $\sum_{j=1}^{i} \widehat{w}_j = \widehat{\mathbf{w}}E|_i \leq \left(\frac{i(n-i)}{2(\beta-1)} + \frac{i\beta(\beta-2)}{2n(\beta-1)}\right)\log(\delta\gamma_\beta)$ for $i = 1, \ldots, n-\beta$.*
2. *Its norm satisfies: $\|\widehat{\mathbf{w}}\| \leq n \cdot \widehat{w}_1$.*

Sketched Proof of Proposition 5. A full proof can be found in Appendix C. Here, we only describe the main ideas behind the proof of Item 1, which is the most technical part of the proposition.

For convenience, we define two vectors related to Hermite's constants:

$$\mathbf{h} = (h_2, h_3, \ldots, h_\beta) \in \mathbb{R}^{\beta-1} \quad \text{with each} \quad h_\kappa = \frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)},$$
$$\overline{\mathbf{h}} = \left(\overline{h}_2, \overline{h}_3, \ldots, \overline{h}_\beta\right) \in \mathbb{R}^{\beta-1} \quad \text{with each} \quad \overline{h}_\kappa = \frac{\beta\log(\delta\gamma_\beta)}{2\kappa(\kappa-1)}.$$

Firstly, with direct calculations by hand, the definition of $\widehat{\mathbf{x}} = (\widehat{x}_1, \ldots, \widehat{x}_n)$ in Eq. (27) can be rewritten into the following more explicit form:

$$\widehat{x}_j = \begin{cases} -\sum_{\kappa=2}^{\beta} h_\kappa & \text{if } j = n, \\ (n-j)h_{n-j+1} - \sum_{\kappa=n-j+2}^{\beta} h_\kappa & \text{if } j = n-1, \ldots, n-\beta+2, \\ (\beta-1)h_\beta & \text{if } j = n-\beta+1, \\ \beta \cdot h_\beta + \frac{1}{\beta-1}\sum_{\kappa=2}^{\beta} h_\kappa & \text{if } j = n-\beta, \\ \beta \cdot h_\beta + \frac{1}{\beta-1}\sum_{i=j+1}^{n-\beta} \widehat{x}_i + \frac{n-\beta+1-j}{\beta-1}\sum_{\kappa=n-\beta-j+2}^{\beta} h_\kappa & \text{if } n-2\beta+2 \leq j \leq n-\beta-1, \\ \beta \cdot h_\beta + \frac{1}{\beta-1}\sum_{i=j+1}^{j+\beta-1} \widehat{x}_i & \text{if } 1 \leq j \leq n-2\beta+1. \end{cases} \tag{30}$$

It can be checked that the summation of the tail $\widehat{x}_j$'s is zero, namely

$$\sum_{j=n-\beta+1}^{n} \widehat{x}_j = 0.$$

Eq. (26) implies $\widehat{\mathbf{w}} = \widehat{\mathbf{x}} - \frac{1}{n}\left(\sum_{j=1}^{n} \widehat{x}_j\right) \cdot \mathbf{1}_n$. Then $\sum_{j=1}^{i} \widehat{w}_j$ can be expressed as a linear combination of the head $\widehat{x}_j$'s:

$$\sum_{j=1}^{i} \widehat{w}_j = \sum_{j=1}^{i} \widehat{x}_j - \frac{i}{n}\sum_{j=1}^{n} \widehat{x}_j = \left(1 - \frac{i}{n}\right)\sum_{j=1}^{i} \widehat{x}_j - \frac{i}{n}\sum_{j=i+1}^{n-\beta} \widehat{x}_j \quad \text{for} \quad i = 1, \ldots, n-\beta. \tag{31}$$

Secondly, one observes that each $\sum_{j=1}^{i} \widehat{w}_j$ can be written as a linear combination of h_κ for $\kappa = 2, \ldots, \beta$, because this is true for each $\widehat{x}_j$ (by Eq. (30)). The main issue is to upper bound and lower bound each $h_\kappa \triangleq \frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)}$ in terms of $h_\beta \triangleq \frac{\log(\delta\gamma_\beta)}{2(\beta-1)}$. To do so, we can use two classical inequalities on Hermite's constants: for $\kappa = 2, \ldots, \beta$,

$$\text{(Mordell's inequality [Mor44])} \qquad \gamma_\beta^{1/(\beta-1)} \leq \gamma_\kappa^{1/(\kappa-1)}, \tag{32}$$
$$\text{(Newman's inequality [New63])} \qquad \gamma_\kappa^{\kappa} \leq \gamma_\beta^{\beta}. \tag{33}$$

Thus, we can simultaneously upper bound and lower bound each h_κ in terms of h_β:

$$h_\beta \leq h_\kappa \leq \overline{h}_\kappa = \frac{\beta(\beta-1)}{\kappa(\kappa-1)} h_\beta \quad \text{for} \quad \kappa = 2, \ldots, \beta.$$

Applying it to Eq. (30) and distinguishing two cases $n - 2\beta + 2 \leq j \leq n - \beta$ and $j \leq n - 2\beta + 1$, it can be checked by backward induction on j that the following explicit bounds for the head $\widehat{x}_j$'s hold:

$$(2(n-j) - (\beta - 1))\, h_\beta \leq \widehat{x}_j \leq (2(n-j) - 1)\, h_\beta \quad \text{for} \quad j = 1, \ldots, n - \beta, \tag{34}$$

where the first inequality used Mordell's inequality and the second one used Newman's inequality.

By applying Eq. (34) to Eq. (31), we obtain the following bounds, which are slightly worse than Item 1:

$$\begin{aligned}\sum_{j=1}^{i} \widehat{w}_j &\leq \left(1 - \frac{i}{n}\right) \sum_{j=1}^{i} (2(n-j) - 1)\, h_\beta - \frac{i}{n} \sum_{j=i+1}^{n-\beta} (2(n-j) - (\beta - 1))\, h_\beta \\ &= i(n-i) \left(1 + \frac{\beta - 2}{n}\right) h_\beta = \left(\frac{i(n-i)}{2(\beta-1)} + \frac{i(n-i)(\beta-2)}{2n(\beta-1)}\right) \log(\delta\gamma_\beta) \quad \text{for} \quad i = 1, \ldots, n - \beta.\end{aligned}$$

To obtain the claimed upper bounds on the $\sum_{j=1}^{i} \widehat{w}_j$'s, we only use Newman's inequality and the following key observations.

First, we observe by Eq. (30) that each $\widehat{x}_j$ is a rational linear combination of the h_κ's. More precisely, we have the linear transform:

$$\widehat{x}_j = \mathbf{c}_j \cdot \mathbf{h}^{\mathrm{T}} = \sum_{\kappa=2}^{\beta} c_{j,\kappa} \cdot h_\kappa \quad \text{for} \quad j = 1, \ldots, n.$$

where $\mathbf{c}_j = (c_{j,2}, \ldots, c_{j,\beta}) \in \mathbb{Q}^{\beta-1}$ is defined by

$$(\mathbf{c}_n, \mathbf{c}_{n-1}, \ldots, \mathbf{c}_{n-\beta+1}, \mathbf{c}_{n-\beta}) = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ 1 & -1 & \cdots & -1 & -1 \\ 0 & 2 & \ddots & \ddots & -1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & (\beta-2) & -1 \\ 0 & 0 & \cdots & 0 & (\beta-1) \\ \frac{1}{\beta-1} & \frac{1}{\beta-1} & \cdots & \frac{1}{\beta-1} & (\frac{1}{\beta-1} + \beta) \end{pmatrix} \in \mathbb{Q}^{(\beta+1)\times(\beta-1)}, \tag{35}$$

$$\mathbf{c}_j = \begin{cases} (\underbrace{0, \ldots, 0}_{n-\beta-j \text{ zeros}}, \frac{n-\beta+1-j}{\beta-1}, \ldots, \frac{n-\beta+1-j}{\beta-1}, \frac{n-\beta+1-j}{\beta-1} + \beta) + \frac{1}{\beta-1} \sum_{i=j+1}^{n-\beta} \mathbf{c}_i & \text{if } n - 2\beta + 2 \leq j \leq n - \beta - 1, \\ (0, \ldots, 0, \beta) + \frac{1}{\beta-1} \sum_{i=j+1}^{j+\beta-1} \mathbf{c}_i & \text{if } 1 \leq j \leq n - 2\beta + 1. \end{cases} \tag{36}$$

It can be checked that $\mathbf{c}_j \geq \mathbf{0}$ for $j = n - \beta + 1, n - \beta, \ldots, 1$. Our first key observation is that the linear expression of $\sum_{j=1}^{i} \widehat{w}_j = \sum_{j=1}^{i} \widehat{x}_j - \frac{i}{n} \sum_{j=1}^{n} \widehat{x}_j$ in terms of the "variable" h_κ's also has nonnegative rational coefficients (see Lemma 3 in Appendix C.1): for $i = 1, \ldots, n - \beta$,

$$\sum_{j=1}^{i} \widehat{w}_j = \left(\sum_{j=1}^{i} \mathbf{c}_j - \frac{i}{n} \sum_{j=1}^{n} \mathbf{c}_j\right) \cdot \mathbf{h}^{\mathrm{T}} \quad \text{with} \quad \sum_{j=1}^{i} \mathbf{c}_j - \frac{i}{n} \sum_{j=1}^{n} \mathbf{c}_j \geq \mathbf{0}. \tag{37}$$

Then Newman's inequality (33) implies

$$\sum_{j=1}^{i} \widehat{w}_j \leq \left(\sum_{j=1}^{i} \mathbf{c}_j - \frac{i}{n} \sum_{j=1}^{n} \mathbf{c}_j\right) \cdot \overline{\mathbf{h}}^{\mathrm{T}} \quad \text{for} \quad i = 1, \ldots, n - \beta. \tag{38}$$

This inspires us to introduce the following related sequence of the $\widehat{x}_j$'s, by simply replacing each "variable" h_κ of $\widehat{x}_j = \sum_{\kappa=2}^{\beta} c_{j,\kappa} \cdot h_\kappa$ with new "variable" $\overline{h}_\kappa$:

$$\widehat{y}_j := \mathbf{c}_j \cdot \overline{\mathbf{h}}^{\mathrm{T}} = \sum_{\kappa=2}^{\beta} c_{j,\kappa} \cdot \overline{h}_\kappa = \begin{cases} -\frac{\beta-1}{2} \log(\delta\gamma_\beta) & \text{for } j = n, \\ \frac{1}{2} \log(\delta\gamma_\beta) & \text{for } j = n-1, \dots, n-\beta+1, \\ \frac{\beta}{2(\beta-1)} \log(\delta\gamma_\beta) + \frac{1}{\beta-1} \sum_{i=j+1}^{j+\beta-1} \widehat{y}_i & \text{for } j = n-\beta, \dots, 1. \end{cases} \tag{39}$$

Then Eq. (38) becomes the following inequalities (*i.e.*, Corollary 3 in Appendix C.1):

$$\sum_{j=1}^{i} \widehat{w}_j \le \sum_{j=1}^{i} \widehat{y}_j - \frac{i}{n} \sum_{j=1}^{n} \widehat{y}_j \quad \text{for} \quad i = 1, \dots, n-\beta. \tag{40}$$

A direct calculation by hand implies:

$$\widehat{y}_j = \left(1 + \left(\frac{\beta}{\beta-1} \right)^{n-\beta+1-j} \right) \frac{\log(\delta\gamma_\beta)}{2} \quad \text{if} \quad \max\{1, n-2\beta+1\} \le j \le n-\beta. \tag{41}$$

Our second key observation is that with the method of backward induction, one is able to use such **exact values** of $\widehat{y}_j$ for tail indices $n-2\beta < j \le n$ and the internal recurrence relation of the sequence $\widehat{y}_j$'s to upper bound $\sum_{j=1}^{i} \widehat{y}_j - \frac{i}{n} \sum_{j=1}^{n} \widehat{y}_j$ well (*i.e.*, Lemma 4 in Appendix C.1) and hence $\sum_{j=1}^{i} \widehat{w}_j$ as desired in Item 1.

We now intuitively explain why the second method (40) is better than the first method (34). Consider a toy example: if one wants to upper bound $(\overline{c} - \underline{c})h_\kappa$ (for any positive coefficients $\overline{c} > \underline{c} > 0$ and for any index $\kappa \in \{2, \dots, \beta-1\}$) with h_β, then the estimate solely with Newman's inequality

$$(\overline{c} - \underline{c})h_\kappa \le (\overline{c} - \underline{c}) \frac{\beta(\beta-1)}{\kappa(\kappa-1)} h_\beta$$

is obviously tighter than the estimate with both Mordell's inequality and Newman's inequality

$$(\overline{c} - \underline{c})h_\kappa \le \overline{c} \cdot \frac{\beta(\beta-1)}{\kappa(\kappa-1)} h_\beta - \underline{c} \cdot h_\beta.$$

The (tedious) proof of Item 1 is relegated to Appendix C.1, while we prove Item 2 in Appendix C.2. ☐

3.6 Quantitative Analysis of GBKZ

Proof of the Main Result. We now prove Theorem 2 by combining previous analyses.

Proof of Theorem 2. In order to assess the basis quality of GBKZ tours, we denote the current basis at the end of the k-th tour by B_k. Let $A \in \mathbb{Q}^{n\times n}$, $E \in \mathbb{Z}^{n\times n}$, $Q \in \mathbb{Q}^{n\times n}$ and $\widehat{\mathbf{w}} \in \mathbb{R}^n$ be the matrices and vector defined by Eq. (8), Eq. (7), Eq. (19) and Eq. (26), respectively.

Let $k \ge 4(\ln 2)\frac{n^2}{\beta^2} \log \frac{\|\overline{\mathcal{R}}(B_0)E^{-1}\| + \|\widehat{\mathbf{w}}\|}{\varepsilon}$, where $\overline{\mathcal{R}}(\cdot)$ is defined as in Proposition 4. We have:

$$\begin{aligned} \mathcal{R}(B_k) &\le \widehat{\mathbf{w}}E + (\mathcal{R}(B_0) - \widehat{\mathbf{w}}E)\, E^{-1}(A-Q)^k E & & \text{(Applying Prop. 3.2 to Eq. (18))} \\ &\le \widehat{\mathbf{w}}E + \left(1, \sqrt{2}, \dots, \sqrt{n}\right) \times \log(1+\varepsilon). & & \text{(By Prop. 4)} \end{aligned} \tag{42}$$

That is, $\mathcal{R}_i(B_k) \le \sum_{j=1}^{i} \widehat{w}_j + \sqrt{i} \times \log(1+\varepsilon)$ for $i = 1, \dots, n$. By Prop. 5.1, this implies:

$$\mathcal{R}_i(B_k) \le \left(\frac{i(n-i)}{2(\beta-1)} + \frac{i\beta(\beta-2)}{2n(\beta-1)} \right) \log(\delta\gamma_\beta) + \sqrt{i} \times \log(1+\varepsilon) \quad \text{for} \quad i = 1, \dots, n-\beta.$$

We now upper bound $\mathcal{R}_i(B_k)$ for $i = n-\beta+1, \ldots, n-1$:

$$\begin{aligned}
\mathcal{R}_i(B_k) &\le \frac{n-i}{\beta}\left(\sum_{j=1}^{n-\beta}\widehat{w}_j + \left(\mathcal{R}(B_0) - \widehat{\mathbf{w}}E\right)E^{-1}(A-Q)^k E\big|_{n-\beta}\right) + (n-i)\sum_{\kappa=n-i+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)} && \text{(By Cor. 1)}\\
&\le \frac{n-i}{\beta}\left(\sum_{j=1}^{n-\beta}\widehat{w}_j + \sqrt{n-\beta}\times\log(1+\varepsilon)\right) + (n-i)\sum_{\kappa=n-i+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)} && \text{(By Prop. 4)}\\
&\le \frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)\log(\delta\gamma_\beta) + \sqrt{n-\beta}\times\log(1+\varepsilon) + (n-i)\sum_{\kappa=n-i+1}^{\beta}\frac{\log(\delta\gamma_\kappa)}{2(\kappa-1)}. && \text{(By Prop. 5.1)}
\end{aligned}$$

Since $\mathcal{R}_i(B_k) = \log\frac{\mathrm{vol}((B_k)_{[1,i]})}{\mathrm{vol}(L)^{i/n}}$, we have proved:

$$\frac{\mathrm{vol}((B_k)_{[1,i]})}{\mathrm{vol}(L)^{i/n}} \le \begin{cases} (1+\varepsilon)^{\sqrt{i}}(\delta\gamma_\beta)^{\frac{i(n-i)}{2(\beta-1)}+\frac{i\beta(\beta-2)}{2n(\beta-1)}} & \text{if } i = 1,\ldots,n-\beta,\\ (1+\varepsilon)^{\sqrt{n-\beta}}(\delta\gamma_\beta)^{\frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)}\left(\prod_{\kappa=n-i+1}^{\beta}(\delta\gamma_\kappa)^{\frac{n-i}{2(\kappa-1)}}\right) & \text{if } i = n-\beta+1,\ldots,n-1.\end{cases}$$

Since the input basis B_0 is $\frac{3}{4}$-LLL-reduced, we have $\mathcal{R}(B_0) \le \left(\frac{i(n-i)}{4}\right)_{1\le i\le n}$ [PT10]. We take $\overline{\mathcal{R}}(B_0) = \left(\frac{i(n-i)}{4}\right)_{1\le i\le n}$ and hence $\overline{\mathcal{R}}(B_0)E^{-1} = \left(\frac{n-2i+1}{4}\right)_{1\le i\le n}$. Proposition 5 implies $\|\overline{\mathcal{R}}(B_0)E^{-1}\| + \|\widehat{\mathbf{w}}\| \le n^2$. Thus,

$$4(\ln 2)\frac{n^2}{\beta^2}\log\frac{n^2}{\varepsilon} \ge 4(\ln 2)\frac{n^2}{\beta^2}\log\frac{\|\overline{\mathcal{R}}(B_0)E^{-1}\| + \|\widehat{\mathbf{w}}\|}{\varepsilon}.$$

This completes the proof of Theorem 2. □

Worst Case Behaviour of GBKZ. Hanrot and Stehlé [HS08, Cor. 4] showed that for $n > \beta > 8e\pi$, there is a β-BKZ reduced basis $B = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$ with $\|\mathbf{b}_i^*\| = \left(\frac{8e\pi}{\beta-1}\right)^{i/\beta}$ for $i = 1, \ldots, n$. Then

$$\frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(B)^{i/n}} = \left(\frac{\beta-1}{8e\pi}\right)^{\frac{i(n-i)}{2\beta}} \quad \text{for} \quad i = 1,\ldots,n.$$

Since $\gamma_\beta \le \frac{\beta+6}{7}$ [Neu17], this means that the upper bound on $\mathrm{vol}(B_{[1,i]})/\mathrm{vol}(L)^{i/n}$ for $i = 1, \ldots, n-\beta$ in Theorem 2 is essentially tight as $\delta = 1$.

Experiments suggest that Eq. (42) is sharp. For simplicity, consider the upper bound on the logarithmic Hermite factor in Eq. (42):

$$\mathcal{G}_1(B_k) \le \widehat{w}_1 + \left(\mathcal{G}(B_0) - \widehat{\mathbf{w}}\right)(A-Q)^k E\big|_1 \quad \text{for} \quad k = 1, 2, \ldots. \tag{43}$$

It can be checked that Eq. (42) and the above inequality still hold, even if replacing Hermite's constants γ_i inside $\widehat{\mathbf{w}}$ with their upper bounds (which would increase $\widehat{w}_1$ by Eq. (37)). With the exact value of γ_i if $i \in \{1, 2, \ldots, 8, 24\}$ and Blichfeldt's inequality $\gamma_i \le \frac{2}{\pi}\cdot\Gamma(1+\frac{i}{2})^{2/i}$ [Bli14] otherwise, we are able to experimentally verify the tightness of Eq. (43) (and hence Eq. (42)): more specifically, the upper bound on the *root Hermite factor* (RHF) $(\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n})^{1/(n-1)}$ from Eq. (43) is sharp at least for $\delta = 1$, when given as input the Gram-Schmidt profile of the above worst-case β-BKZ reduced basis.[2]

[2] For readers' convenience, we provide our pseudo-code in Appendix D.

Complexity Analysis of GBKZ. So far, we have only looked at the number of required iterations. To show that GBKZ runs in polynomial time (apart from SVP-oracle calls), we need additional requirements on $\mathcal{A}_{\text{extract}}$ or $\mathcal{A}_{\text{reduce}}$. Following what happens with LLL and blockwise reduction algorithms, we ask that $\mathcal{A}_{\text{extract}}$ and $\mathcal{A}_{\text{reduce}}$ are polynomial-time algorithms which, given as input a generator matrix or a basis G of an n-rank lattice Λ, they output a basis C of Λ such that $\|C^*\| \leq \|G^*\|$ and C is *size-controlled*, that is, $\|C\|/\|C^*\|$ can be upper bounded by a polynomial function of n. This is achieved by the partial LLL subroutines used by BKZ, but other choices are possible.

Then the current basis B at the end of any GBKZ tour always has size polynomial in the size of the input basis $B_0 \in \mathbb{Z}^{n\times m}$:

$$\|B^*\| \leq \|B_0^*\| \quad \Rightarrow \quad \|B\| \leq \text{poly}(n) \cdot \|B^*\| \leq \text{poly}(n) \cdot \|B_0^*\| \leq \text{poly}(n) \cdot \|B_0\|.$$

For instance, we always have $\|B^*\| \leq \|B_0^*\|$ and $\|B\| \leq \sqrt{n} \cdot \|B_0\|$ during the execution of BKZ. As a result, all intermediate entries and the total cost during the execution of any GBKZ tour (excluding oracle queries) remain polynomially bounded if the input lattice is integral.

4 Heuristic Analysis of BKZ Using Dynamical Systems

It is well-known [NS06,GN08b,MW16] that there is a gap between theoretical worst-case analyses and practical performances of lattice reduction algorithms. In the context of cryptanalysis, we are more interested in the practical behaviour of algorithms. Interestingly and as a side result, our previous worst-case analysis of GBKZ using dynamical systems can to some extent also be applied to the practical behaviour of BKZ.

Our heuristic assertions in this section are especially applicable to the case of significantly larger blocksize which is tricky for both experiments and simulations due to (accumulative) precision errors.[3]

4.1 The First Minimum of Random Lattices

We recall facts on random lattices and establish weak bounds on their first minimum. The set of full-rank lattices in $\mathbb{R}^n$ of unit volume is classically identified with the moduli space $\mathcal{L}_n = SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. Siegel [Sie45] introduced a Haar-based measure μ_n over $\mathcal{L}_n$ such that $\mu_n(\mathcal{L}_n) = 1$. In the mathematical literature, a random lattice is a lattice in $\mathbb{R}^n$ of unit volume chosen with distribution μ_n. For this distribution, Rogers [Rog56] studied the moments of the number of lattice points in a set C:

Theorem 3 ([Rog56, Theorem 3])**.** *Let $\rho(\cdot)$ be the characteristic function of a measurable set C in $\mathbb{R}^n$ whose volume is V, and symmetric with respect to $\mathbf{0}$. Then, provided that $n \geq \frac{k^2}{4} + 3$:*

$$\begin{aligned} 0 &\leq \int_{L\in\mathcal{L}_n} \rho(L \setminus \{0\})^k d\mu_n - 2^k e^{-\frac{V}{2}} \sum_{r=0}^{\infty} \frac{r^k}{r!}\left(\frac{V}{2}\right)^r \\ &\leq \left(2 \times 3^{\frac{k^2}{4}} \left(\sqrt{\frac{3}{4}}\right)^n + 21 \times 5^{\frac{k^2}{4}} \left(\frac{1}{2}\right)^n\right) \times (V+1)^k. \end{aligned}$$

Rogers deduced the following corollary:

Corollary 2. *Let C be a measurable set in $\mathbb{R}^n$ of fixed volume V, symmetric with respect to $\mathbf{0}$. Then the number N_n of pairs of nonzero points $\pm\mathbf{x}$ of a lattice $L \in \mathcal{L}_n$ in C has a limit distribution, as n becomes large, which is the Poisson distribution with mean $V/2$.*

Th. 3 is also useful for varying V:

[3] For instance, the simulation code in [ABF+20, §4] for computing parameters of pruning enumeration simply crashed with a floating-point error in dimension 324.

Corollary 3. *There exist constants $c_1 > 0$ and $c_2 > 0$ such that for all sufficiently large n, the number N_n of pairs of nonzero points $\pm\mathbf{x}$ of a random lattice $L \in \mathcal{L}_n$ in a measurable set C of volume V, symmetric with respect to $\mathbf{0}$, satisfies:*

$$\mathrm{Exp}(N_n) = \frac{V}{2}(1 + O(2^{-c_1 n})),$$
$$\mathrm{Var}(N_n) = \frac{V}{2} + (V+1)^2 O(2^{-c_2 n}).$$

Proof. First, let us clarify the expression in Th. 3. It is classical that $f(x) := xe^x = \sum_{r=0}^{\infty} \frac{r}{r!}x^r$. Then $f'(x) = e^x + xe^x = \sum_{r=0}^{\infty} \frac{r^2}{r!}x^{r-1}$. This implies:

$$e^{-\frac{V}{2}} \sum_{r=0}^{\infty} \frac{r}{r!} \left(\frac{V}{2}\right)^r = e^{-\frac{V}{2}} f(\frac{V}{2}) = \frac{V}{2},$$
$$e^{-\frac{V}{2}} \sum_{r=0}^{\infty} \frac{r^2}{r!} \left(\frac{V}{2}\right)^r = \frac{V}{2} e^{-\frac{V}{2}} f'(\frac{V}{2}) = V/2 + (V/2)^2.$$

Second, with the characteristic function $\rho(\cdot)$ of C, $\rho(L \setminus \{0\})$ is the number of nonzero points in $L \bigcap C$. It follows from the expectation and variance formulae that

$$\mathrm{Exp}(N_n) = \int_{L \in \mathcal{L}_n} \frac{\rho(L \setminus \{0\})}{2} d\mu_n,$$
$$\mathrm{Var}(N_n) = \int_{L \in \mathcal{L}_n} \left(\frac{\rho(L \setminus \{0\})}{2}\right)^2 d\mu_n - \mathrm{Exp}(N_n)^2.$$

By combining the above equalities with Th. 3, then the corollary follows. □

Let $h(n)$ denote the radius of the unit-volume n-dimensional ball, *i.e.* $h(n) = 1/\mathrm{V}_n(1)^{1/n}$ where $\mathrm{V}_n(R)$ denotes the volume of the n-dimensional Euclidean ball of radius $R > 0$. It is well-known that

$$h(n) = \frac{\Gamma(n/2+1)^{1/n}}{\sqrt{\pi}} \simeq \sqrt{\frac{n}{2\pi e}} \cdot (\pi n)^{\frac{1}{2n}}.$$

For an arbitrary n-rank lattice L, the quantity $\mathrm{GH}(L) = h(n)\mathrm{vol}(L)^{1/n}$ is a classical heuristic estimate of $\lambda_1(L)$, known as the Gaussian heuristic, because the ball of radius $\mathrm{GH}(L)$ has volume $\mathrm{vol}(L)$.

It is possible to show that $h(n)$ is a rigorous estimate for a random lattice, by combining Markov's inequality with Cor. 3:

Theorem 4. *Let L be a random unit-volume full-rank lattice in $\mathbb{R}^n$. Then, with probability at least $1 - o(1)$ as n grows to infinity:*

$$1 - (\log\log n)/n \le \frac{\lambda_1(L)}{h(n)} \le 1 + (\log\log n)/n,$$

Thus, $\mathrm{Exp}(\lambda_1(L)/h(n))$ converges to 1, and therefore $\mathrm{Exp}(\lambda_1(L))$ is asymptotically equivalent to $h(n)$.

Proof. Markov's inequality ensures that for any $t > 0$:

$$\Pr(|N_n - \mathrm{Exp}(N_n)| > t) \le \mathrm{Var}(N_n)/t^2,$$

or equivalently, $\Pr(\mathrm{Exp}(N_n) - t \le N_n \le \mathrm{Exp}(N_n) + t) \ge 1 - \mathrm{Var}(N_n)/t^2$.

Let $t = (\log n)/8$ and C be the centered ball of volume $V = (\log n)/2$. By Cor. 3, for sufficiently large n,

$$\mathrm{Exp}(N_n) - t = ((\log n)/4)(1 + O(2^{-c_1 n})) - (\log n)/8 = ((\log n)/8)(1 + O(2^{-c_1 n})) > 1,$$
$$\mathrm{Var}(N_n)/t^2 = 64((\log n)/4 + ((\log n)/2 + 1)^2 O(2^{-c_2 n}))/\log^2 n = 16/\log n + O(2^{-c_2 n}).$$

Therefore, with probability at least $1 - o(1)$, $N_n \geq \mathrm{Exp}(N_n) - t > 1$: i.e. $L \bigcap C$ includes nonzero points and hence $\lambda_1(L)$ is less than or equal to the radius of the ball C, which is $((\log n)/2)^{1/n} h(n) \leq (1 + (\log\log n)/n)h(n)$ for all sufficiently large n.

To obtain the lower bound, let $t = 1/\log\log n$ and C be the centered ball of volume $V = 2/\log n$. Its radius is $(2/\log n)^{1/n} h(n) \geq (1 - (\log\log n)/n)h(n)$ for all sufficiently large n. Furthermore, Cor. 3 implies: $\mathrm{Exp}(N_n) + t = (1/\log n)(1 + O(2^{-c_1 n})) + 1/\log\log n = o(1)$ and $\mathrm{Var}(N_n)/t^2 = o(1)$. Therefore, with probability at least $1 - o(1)$, $N_n \leq \mathrm{Exp}(N_n) + t = o(1)$: i.e. $L \bigcap C = \{\mathbf{0}\}$ and hence $\lambda_1(L)$ is greater than or equal to the radius of the ball C, which proves the lower bound.

We conclude that the bounds on $\lambda_1(L)/h(n)$ hold with probability at least $1 - o(1)$. And by Minkowski's bound, we always have $0 < \lambda_1(L)/h(n) \leq 2$. It follows that $\mathrm{Exp}(\lambda_1(L)/h(n))$ converges to 1. $\square$

For $n > 24$, Blichfeldt's inequality $\gamma_n \leq \frac{2}{\pi} \cdot \Gamma(1 + \frac{n}{2})^{2/n}$ [Bli14] implies that any lattice L of rank n satisfies $\lambda_1(L) \leq \sqrt{2}\mathrm{GH}(L)$. Theorem 4 suggests the following weak version of the Gaussian heuristic: for any $\epsilon \in (0, \sqrt{2} - 1]$, there exists $N > 0$ such that for "most" random lattices L of rank $n \geq N$,

$$\lambda_1(L) \leq (1 + \epsilon)\mathrm{GH}(L).$$

We note that Bai *et al.* [BSW18] also considered an expectation $\mathrm{Exp}(\lambda_1(L))$ (and even variance), but their expectation is not the actual expectation corresponding to random lattices: their notation is debatable because it is actually the expectation of a specific distribution which is only conjectured to be close to that of the $\lambda_1(L)$ of a random lattice.

4.2 Heuristically Modeling the Practical Behavior of BKZ

We adapt our previous worst-case analysis of GBKZ to heuristically model the practical behaviour of BKZ.

It was experimentally verified [CN11] that the first minimum of most local blocks during the execution of BKZ roughly looks like that of a random lattice of rank the blocksize: this phenomenon does not hold in small blocksize ≤ 30, but it becomes more and more true as the blocksize increases. The BKZ simulator of [CN11] assumed that for every projected lattice L of rank ≥ 50, $\lambda_1(L) \approx \mathrm{GH}(L)$. This assumption was also used to heuristically analyze DBKZ [MW16].

Here, we are going to assume that for some $\epsilon \in (0, \sqrt{2} - 1]$ and $N = 50$, our weak version of the Gaussian heuristic holds for high-rank projected lattices L arising during the execution of BKZ, that is $\lambda_1(L) \leq (1 + \epsilon)\mathrm{GH}(L)$. Thus, we let $\widetilde{\gamma}_i$ denote the heuristic analog of Hermite's constant γ_i in the context of BKZ: $\widetilde{\gamma}_i$ is $(1 + \epsilon)^2$ times the average Hermite invariant (computed experimentally) of random HKZ-reduced bases in rank i if $i \leq 50$ and is the Gaussian heuristic upper bound $(1 + \epsilon)^2 h(i)^2$ otherwise. Let $\widetilde{\mathbf{w}}$ denote the heuristic analog of the fixed point $\widehat{\mathbf{w}}$ (defined in Eq. (26)), by replacing each γ_i inside $\widehat{\mathbf{w}}$ with $\widetilde{\gamma}_i$.

Suppose that every projected lattice $L(B_{[j,n_j]})$ appearing at Step 4 of Alg. 1 satisfies $\lambda_1(L(B_{[j,n_j]})) \leq \sqrt{\widetilde{\gamma}_{\beta_j}} \times \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$ where $\beta_j = n_j - j + 1$. Let B_0 be the input basis of L to Alg. 1 and B_k be the current basis at the end of the k-th tour. By checking our analyses in Sections 3.3-3.6 step by step, we can deduce the following heuristic analog of Eq. (42):

$$\mathcal{R}(B_k) \leq \widetilde{\mathbf{w}}E + (\mathcal{R}(B_0) - \widetilde{\mathbf{w}}E)\, E^{-1}(A - Q)^k E \quad \text{for} \quad k = 1, 2, \ldots.$$

We stress that with our experimental data, $\widetilde{\gamma}_i$ satisfies a Newman-type inequality just like Eq. (33) for Hermite's constant γ_i (see the bottom of this subsection for the proof):

$$\widetilde{\gamma}_i^{\,i} \leq \widetilde{\gamma}_{i+1}^{\,i+1} \quad \text{for} \quad i = 2, 3, \ldots. \tag{44}$$

This key fact allows to similarly deduce the heuristic analog of Prop. 5:

$$\sum_{j=1}^{i} \widetilde{w}_j \leq \left(\frac{i(n-i)}{2(\beta-1)} + \frac{i\beta(\beta-2)}{2n(\beta-1)}\right)\log(\delta\widetilde{\gamma}_\beta) \quad \text{for} \quad i = 1, \ldots, n - \beta \quad \text{and} \quad \|\widetilde{\mathbf{w}}\| \leq n \cdot \widetilde{w}_1.$$

As a result, with almost the same argument of Th. 2, we have the following heuristic version of Th. 2:

Theorem 5. *Let $n > \beta \geq 2$ be integers and let $0 < \varepsilon \leq 1 \leq \delta \leq 2$. Given as input a blocksize β, a relaxation factor δ, and a $\frac{3}{4}$-LLL-reduced basis B_0 of an n-rank lattice L in $\mathbb{R}^m$, if every projected lattice $L(B_{[j,n_j]})$ of rank β_j appearing at Step 4 satisfies $\lambda_1(L(B_{[j,n_j]})) \leq \sqrt{\widetilde{\gamma}_{\beta_j}} \times \mathrm{vol}(B_{[j,n_j]})^{1/\beta_j}$, then Alg. 1 (BKZ) aborted after $\left\lceil 4(\ln 2)\frac{n^2}{\beta^2}\log\frac{n^2}{\varepsilon}\right\rceil$ tours outputs a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that*

$$\frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(L)^{i/n}} \leq \begin{cases} (1+\varepsilon)^{\sqrt{i}}(\delta\widetilde{\gamma}_\beta)^{\frac{i(n-i)}{2(\beta-1)}+\frac{i\beta(\beta-2)}{2n(\beta-1)}} & \text{if } i = 1, \ldots, n-\beta, \\ (1+\varepsilon)^{\sqrt{n-\beta}}(\delta\widetilde{\gamma}_\beta)^{\frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)}\left(\prod_{\kappa=n-i+1}^{\beta}(\delta\widetilde{\gamma}_\kappa)^{\frac{n-i}{2(\kappa-1)}}\right) & \text{if } i = n-\beta+1, \ldots, n. \end{cases}$$

The resulting RHF $\left(\frac{\|\mathbf{b}_1\|}{\mathrm{vol}(L)^{1/n}}\right)^{\frac{1}{n-1}} \leq 2^{\frac{1}{n-1}}(\delta\widetilde{\gamma}_\beta)^{\frac{1}{2(\beta-1)}+\frac{\beta}{2n^2}} \approx \left(\frac{\delta\beta}{2\pi e}\cdot(\pi\beta)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}+\frac{\beta}{2n^2}}$ as $n > \beta \geq 51$.

Proof of Eq. (44). Using the average Hermite invariant of 2000 random HKZ-reduced bases, we obtain the following experimental data:
$\left(\log\frac{\sqrt{\widetilde{\gamma}_2}}{1+\epsilon}, \ldots, \log\frac{\sqrt{\widetilde{\gamma}_{50}}}{1+\epsilon}\right)$ =(-0.00510196377567085, -0.00107666327046254, 0.00721493331037026, 0.0172922379408905, 0.0276993093781221, 0.0382859795952343, 0.0482936766761646, 0.0578479066018888, 0.0670563192422883, 0.0759546553618141, 0.0846666235685110, 0.0931642619685445, 0.101751890904296, 0.110211280460018, 0.118625981719138, 0.127004786199126, 0.135383008495571, 0.143757200453911, 0.152206424810413, 0.160800754179335, 0.169534179980289, 0.178425728374139, 0.187470594890389, 0.196699422286623, 0.206070776730679, 0.215623123978602, 0.225445595769477, 0.235460006114398, 0.245673786121561, 0.256089307622679, 0.266677881224944, 0.277432795118217, 0.288458936247855, 0.299662098010410, 0.311028574491920, 0.322580433523455, 0.334333870090499, 0.346211635100222, 0.358221887890187, 0.370347436279772, 0.382589642859170, 0.394977800976732, 0.407413847184503, 0.419916229563308, 0.432378898312800, 0.444727344751010, 0.456892456678605, 0.468535755828720, 0.478808739222082).
Since $\log\frac{\sqrt{\widetilde{\gamma}_{51}}}{1+\epsilon} = \log\frac{\Gamma(26.5)^{1/51}}{\sqrt{\pi}}$, it can be numerically checked that $i\log\frac{\sqrt{\widetilde{\gamma}_i}}{1+\epsilon} \leq (i+1)\log\frac{\sqrt{\widetilde{\gamma}_{i+1}}}{1+\epsilon}$ and hence $\widetilde{\gamma}_i^i \leq \widetilde{\gamma}_{i+1}^{i+1}$ for $i = 2, \ldots, 50$.

Now, assume $i \geq 51$. It remains to show $\widetilde{\gamma}_i^i \leq \widetilde{\gamma}_{i+1}^{i+1}$. Since $\widetilde{\gamma}_i = (1+\epsilon)^2 h(i)^2$, it suffices to prove $h(i)^i \leq h(i+1)^{i+1}$, or equivalently,

$$\pi \cdot \Gamma\left(\frac{i}{2}+1\right)^2 \leq \Gamma\left(\frac{i+1}{2}+1\right)^2. \tag{45}$$

Indeed, applying Stirling's formula

$$\sqrt{2\pi x}\left(\frac{x}{e}\right)^x < \Gamma(x+1) < \sqrt{2\pi x}\left(\frac{x}{e}\right)^x e^{\frac{1}{12x}} \quad \text{for} \quad x > 0,$$

we set respectively $x = \frac{i}{2}$ and $x = \frac{i+1}{2}$ to obtain:

$$\pi \cdot \Gamma\left(\frac{i}{2}+1\right)^2 < \pi^2 i\left(\frac{i}{2e}\right)^i e^{1/(3i)} \quad \text{and} \quad \pi(i+1)\left(\frac{i+1}{2e}\right)^{i+1} < \Gamma\left(\frac{i+1}{2}+1\right)^2.$$

Using two basic facts $2\pi e^{1/(3i)} < i+1$ and $e \leq \left(1+\frac{1}{i}\right)^{i+1}$, our manual calculation implies:

$$\pi^2 i\left(\frac{i}{2e}\right)^i e^{1/(3i)} < \pi(i+1)\left(\frac{i+1}{2e}\right)^{i+1}.$$

Combining the above three inequalities, then Eq. (45) follows. This completes the proof of Eq. (44). □

4.3 Validating Recursive BKZ Preprocessing

Our upper bounds on $\frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(L)^{i/n}}$'s stated in Theorem 2 somehow validate the recursive BKZ preprocessing strategy implemented in Chen-Nguyen's BKZ 2.0 [CN11] and FP(y)LLL [FPL19,FPy19].

Consider the cost of enumeration with an n-rank reduced basis B obtained by terminating BKZ early: assuming the Gaussian heuristic, if the blocksize is $\beta = n - O(\frac{n}{\log n})$, then the heuristic cost of enumeration is bounded by $n^{\frac{n}{2e}} 2^{O(n)}$ like for the quasi-HKZ bases used in Kannan's algorithm [Kan83,HS07]. This is because:

$$\begin{aligned}
\max_{0 \le i < n} \frac{\mathrm{V}_{n-i}(\sqrt{\gamma_n}\mathrm{vol}(B)^{1/n})}{\mathrm{vol}(B_{[i+1,n]})} &= \max_{0 \le i < n} \frac{\mathrm{V}_{n-i}(1)\sqrt{\gamma_n}^{n-i}\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(B)^{i/n}} \\
&\le \left(\max_{1 \le i \le n} \frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(B)^{i/n}} \right) \cdot \max_{1 \le j \le n} \left(\mathrm{V}_j(1)\sqrt{\gamma_n}^{j} \right) \\
&\le 2^{O(n)} \cdot \max_{1 \le i \le n} \frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(B)^{i/n}} \\
&\le 2^{O(n)} \cdot \max_{n-\beta \le i \le n} \left(\gamma_\beta^{\frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)} \left(\prod_{\kappa=n-i+1}^{\beta} \gamma_\kappa^{\frac{n-i}{2(\kappa-1)}} \right) \right) \quad \text{(By Theorem 2)} \\
&\le 2^{O(n)} \cdot \max_{n-\beta \le i \le n} \left(\gamma_\beta^{\frac{(n-\beta)(n-i)}{2(\beta-1)}\left(1+\frac{\beta-2}{n}\right)} \cdot n^{\frac{n-i}{2} \ln \frac{n}{n-i}} \right) \quad \text{(By [HS07, Lemma 2])} \\
&\le n^{\frac{n}{2e}} 2^{O(n)}.
\end{aligned}$$

We mention that [Wal15, Cor. 1] proved a worst-case time bound $n^{2n}2^{O(n)}$ for the same β.

However, as opposed to Kannan-type algorithms, the preprocessing is much lighter, because the required number of tours is relatively small, namely $O(\log n)$, and independent of the input basis. By recursively using a blocksize $\beta' = n' - O(\frac{n'}{\log n'})$, the total number of enumeration calls is only $O\left((n \log n)^{\log n}\right) = 2^{O(\log^2 n)}$, each with a rank $\le n - O(\frac{n}{\log n})$.

By contrast, the fastest variants of Kannan's algorithm known [MW15] require either $2^{n/\log n}$ calls and $n^{0.75n}$-time, or $2^{O(n(\log\log n)/k)}$ calls and $n^{\frac{n}{2e}}2^{O(kn)}$-time with index $1 \le k \in O(1)$. It is therefore a different trade-off, but [MW15]'s complexity analysis is completely rigorous: it does not require the Gaussian heuristic.

5 Enumeration with Cylinder Pruning: The Case of Approximation

5.1 Background

Enumeration [Mic81,Kan83,FP85,SE94,MW15] is the simplest algorithm to solve SVP: given a full-rank lattice L in $\mathbb{R}^n$ and a radius $R > 0$, it outputs $L \bigcap \mathrm{Ball}_n(R)$ by a depth-first tree search.

Cylinder pruning (introduced by Schnorr and Hörner [SH95], and analyzed by Gama, Nguyen and Regev [GNR10]) speeds up enumeration by replacing the search region $\mathrm{Ball}_n(R)$ with a (much smaller) subset $\mathrm{P}_f(B, R)$ defined by a bounding function $f : \{1, \ldots, n\} \to [0, 1]$, a basis B of L and R:

$$\mathrm{P}_f(B, R) = \{\mathbf{x} \in \mathbb{R}^n : \|\pi_{n+1-k}(\mathbf{x})\| \le f(k)R \text{ for all } 1 \le k \le n\} \subseteq \mathrm{Ball}_n(R),$$

where π_i is the orthogonal projection over $\mathrm{span}(B_{[1,i-1]})^\perp$. The set $\mathrm{P}_f(B, R)$ is an intersection of cylinders, since each equation $\|\pi_{n+1-k}(\mathbf{x}/R)\| \le f(k)$ defines a k-dimensional cylinder

$$C_{f,k} = \left\{ (x_1, \ldots, x_k) \in \mathbb{R}^k : \forall\, j \le k, \sum_{i=1}^{j} x_i^2 \le f(j)^2 \right\} \subseteq \mathrm{Ball}_k(1) \quad \text{for} \quad k = 1, \ldots, n.$$

Algorithm 4 recalls enumeration with extreme cylinder pruning, where one repeats enumeration with cylinder pruning many times over different subsets $\mathrm{P}_f(B, R)$ by randomizing B.

Algorithm 4 Enumeration with extreme cylinder pruning [GNR10, Algorithm 1]

Input: (L, R, f), where L is a full-rank lattice in $\mathbb{R}^n$ specified by a basis, $R > 0$ is a radius and f is a bounding function.

Output: A nonzero vector in $L \bigcap \mathrm{Ball}_n(R)$.

WHILE no nonzero vector in $L \bigcap \mathrm{Ball}_n(R)$ has been found:

1: Compute a (randomized) reduced basis B by applying basis reduction to a "random" basis of L

2: Compute $L \bigcap \mathrm{P}_f(B, R)$ by enumeration with cylinder pruning //This is a single cylinder pruning

Enumeration is often used in public-key cryptanalysis either as standalone algorithms, or as subroutines in blockwise lattice reduction algorithms. These roughly correspond to two settings respectively:

- **Unique setting**: $L \bigcap \mathrm{Ball}_n(R) = \{\mathbf{0}, \pm\mathbf{u}\}$. The goal here is to find the unique shortest nonzero vector $\mathbf{u}$ of L (up to sign).
- **Approximation setting** (formalized in [AN17,ANSS18]): One is interested in finding just one non-zero point in $L \bigcap \mathrm{P}_f(B, R)$ for some basis B produced at Step 1. This actually corresponds to the use of cylinder pruning in blockwise lattice reduction: it allows to suitably relax radius R, as shown in Section 3.

In [GNR10], Gama *et al.* provided the first sound analysis of cylinder pruning and showed that in the unique setting, extreme cylinder pruning provided heuristically an exponential speedup over full enumeration. More precisely, they gave a simple bounding function such that Alg. 4 was heuristically expected to find $\mathbf{u}$ in $2^{n/2}$ times less operations than full enumeration over $L \bigcap \mathrm{Ball}_n(R)$. However, this asympotical analysis only covered the unique setting: the approximation setting was studied by [AN17], but for a different form of pruning, known as discrete pruning.

In this section, we fill this gap by adapting the asymptotical analysis of [GNR10] for cylinder pruning to the approximation setting. Naturally, we obtain further exponential speedups over full enumeration: we note that similar speedups were already exploited in solving SVP challenges [LR20] with enumeration.

5.2 Asymptotic Analysis

All complexity analyses of pruned enumeration in [GNR10,AN17,ANSS18] rely on the Gaussian heuristic (revisited in Section 4.1). We will also use the notation $\mathrm{GH}(L)$ and $\mathrm{V}_n(1)$ defined as in Section 4.1.

Step 2 of Alg. 4 will stop the loop if and only if $L \cap P_f(B, R) \not\subseteq \{\mathbf{0}\}$. As observed in [AN17,ANSS18], the probability of this event is heuristically:

$$p_{\mathrm{succ}}(f, R) = \min\left\{1, \frac{\mathrm{vol}(C_{f,n})R^n}{\mathrm{vol}(L)}\right\}. \tag{46}$$

Furthermore, [GNR10] showed that a single execution of Step 2 takes $\sum_{k=1}^{n} N_k$ polynomial-time operations, where N_k denotes the cardinality of the set $\pi_{n+1-k}(L \bigcap \mathrm{P}_f(B, R))$. Under the Gaussian heuristic, we have:

$$N_k \approx \frac{\mathrm{vol}(\pi_{n+1-k}(\mathrm{P}_f(B, R)))}{\mathrm{vol}(\pi_{n+1-k}(L))} = \frac{\mathrm{vol}(C_{f,k})R^k}{\mathrm{vol}(B_{[n-k+1,n]})}.$$

The standard heuristic estimate for the cost of one enumeration with cylinder pruning (Step 2) is therefore:

$$N(f, R, B) = \sum_{k=1}^{n} \frac{\mathrm{vol}(C_{f,k})R^k}{\mathrm{vol}(B_{[n-k+1,n]})}. \qquad \text{(See [ANSS18, Eq. (5)])}$$

Thus, Alg. 4 will find a non-zero vector in $L \bigcap \mathrm{Ball}_n(R)$ within a number of poly-time operations which is heuristically:

$$\begin{aligned} T_{\mathrm{extreme}}(f, R) &= \frac{N(f, R, B)}{p_{\mathrm{succ}}(f, R)} \qquad \text{(See [GNR10, Eq. (7)])} \\ &= \max\left\{\frac{1}{\mathrm{vol}(C_{f,n})}, \frac{R^n}{\mathrm{vol}(L)}\right\} \cdot \sum_{k=1}^{n} \frac{\mathrm{vol}(C_{f,k})\mathrm{vol}(B_{[1,n-k]})}{R^{n-k}}. \end{aligned} \tag{47}$$

Here, as in [GNR10], we assume that:
- The cost of Algorithm 4 is dominated by enumeration with cylinder pruning at Step 2, rather than the repeated reductions of Step 1.
- The term $\mathrm{vol}(B_{[1,n-k]})$ assumes that all the bases B of Step 1 have approximately the same $\mathrm{vol}(B_{[1,n-k]})$, that is, $\mathcal{R}(B)$ is independent of B.

The following result clarifies the heuristic asymptotic speed-up achieved by cylinder pruning in the approximation setting:

Theorem 6. *Let L be a full-rank lattice in $\mathbb{R}^n$. Let $\alpha \geq 1$ and $\rho \in (0, \frac{1}{2})$ be constants such that $4\alpha^4\rho(1-\rho) < 1$. Let $R = \alpha \times GH(L)$ and $f(i) = \begin{cases} \sqrt{\rho} \text{ if } 1 \leq i \leq n/2, \\ 1 \quad \text{otherwise.} \end{cases}$ Assume that all the reduced bases B of Alg. 4 follow the Geometric Series Assumption: there exists $r > 0$ (depending on the basis reduction procedure at Step 1) such that $\|\mathbf{b}_i^*\|/\|\mathbf{b}_{i+1}^*\| = r$ for all i, i.e. $\mathcal{G}(B)$ is an arithmetic sequence. Then the heuristic estimate $T_{extreme}(f, R)$ of the running time of Alg. 4 is less than that of full enumeration on $L \bigcap Ball_n(GH(L))$ by a multiplicative factor of $(4\alpha^2(1-\rho))^{n/4}$ (up to some polynomial factor).*

In order to achieve bigger exponential speedups in the approximation setting, one can simultaneously relax R and decrease ρ. In particular, when ρ goes to zero, the global speedup is asymptotically roughly $(2\alpha)^{n/2}$. For instance, the extreme pruning regime with $\alpha = 2$ and $\rho \leq \frac{1}{64}$ leads to an exponential speedup of about 2^n over full enumeration on $L \bigcap \mathrm{Ball}_n(\mathrm{GH}(L))$, which is better than the $2^{n/2}$ speed-up of [GNR10] for the unique setting.

As an application, Th. 6 allows to further deduce that if using relaxed (rather than exact) enumeration with extreme cylinder pruning as an SVP-oracle, BKZ can achieve better time/quality trade-offs for certain approximation regimes including implementable regimes. The concrete approach is to compare heuristic time estimates between relaxed and exact oracles, but for reaching the same RHFs. We will detail it in another full paper, as well as verifications from both simulations and experiments.

5.3 Proof of Theorem 6

The analysis of [GNR10] shows that if the basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ at Step 2 is a typical reduced basis, namely that $\|\mathbf{b}_i^*\|/\|\mathbf{b}_{i+1}^*\| = r$ where r depends on the basis reduction algorithm at Step 1, the number of enumeration nodes is maximized in the middle depth $k \approx n/2$. In the pruning regime, the success probability of every Step 2 is less than 1, namely $\frac{\mathrm{vol}(C_{f,n})R^n}{\mathrm{vol}(L)} < 1$, then Eq. (47) implies:

$$T_{\mathrm{extreme}}(f, R) = g(n)\frac{\mathrm{vol}(C_{f,n/2})\mathrm{vol}(B_{[1,n/2]})}{\mathrm{vol}(C_{f,n})R^{n/2}}. \tag{48}$$

where $g(n) = n^{O(1)} \geq 1$. By our choice of f:
- $C_{f,n/2}$ is an $\frac{n}{2}$-dimensional ball of radius $\sqrt{\rho}$ and has volume $\mathrm{vol}(C_{f,n/2}) = \rho^{n/4}\mathrm{V}_{\frac{n}{2}}(1)$.
- $C_{f,n} = \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n/2} x_i^2 \leq \rho \text{ and } \sum_{i=1}^{n} x_i^2 \leq 1\right\} \subseteq \mathrm{Ball}_n(1)$ is the so-called *ball-cylinder* defined in [ANSS18]. By [ANSS18, Lemma 2], $\mathrm{vol}(C_{f,n}) = I_\rho(\frac{n}{4}, \frac{n}{4}+1)\mathrm{V}_n(1)$, where $I_\rho(\frac{n}{4}, \frac{n}{4}+1) = \frac{1}{B(\frac{n}{4}, \frac{n}{4}+1)} \int_0^\rho x^{\frac{n}{4}-1}(1-x)^{\frac{n}{4}} dx$ is the *regularized incomplete beta function* with beta function $B(\frac{n}{4}, \frac{n}{4}+1) \approx 2e\sqrt{\frac{\pi}{n}} \cdot 2^{-n/2}$.

Now, the issue is to estimate the integral term of $I_\rho(\frac{n}{4}, \frac{n}{4}+1)$. It follows from [Dut81, §2] that

$$\int_0^\rho x^{\frac{n}{4}-1}(1-x)^{\frac{n}{4}} dx = \frac{4}{n} \times \rho^{\frac{n}{4}}(1-\rho)^{\frac{n}{4}+1} \times F(\frac{n}{2}+1, 1, \frac{n}{4}+1, \rho)$$

where $F(\frac{n}{2}+1, 1, \frac{n}{4}+1, \rho) = 1 + \frac{\frac{n}{2}+1}{\frac{n}{4}+1}\rho + \frac{(\frac{n}{2}+1)(\frac{n}{2}+2)}{(\frac{n}{4}+1)(\frac{n}{4}+2)}\rho^2 + \frac{(\frac{n}{2}+1(\frac{n}{2}+2)(\frac{n}{2}+3)}{(\frac{n}{4}+1)(\frac{n}{4}+2)(\frac{n}{4}+3)}\rho^3 + \cdots$. We have $1 < F(\frac{n}{2}+1, 1, \frac{n}{4}+1, \rho) < \frac{1}{1-2\rho}$.

Recall that the success probability of every Step 2 in the extreme pruning regime is required to be exponentially small, so one presets $4\alpha^4\rho(1-\rho) < 1$. Then Eq. (46) implies

$$p_{\text{succ}}(f,R) = \min\left\{1, \alpha^n \times I_\rho(\frac{n}{4}, \frac{n}{4}+1)\right\} \approx \frac{2(1-\rho)F(\frac{n}{2}+1, 1, \frac{n}{4}+1, \rho)}{e\sqrt{\pi n}}(4\alpha^4\rho(1-\rho))^{n/4}.$$

Finally, using the definition $\mathrm{GH}(L) = \mathrm{V}_n(1)^{-1/n} \times \mathrm{vol}(L)^{1/n}$, Eq. (48) implies:

$$T_{\text{extreme}}(f,R) = g(n) \cdot \frac{\rho^{n/4}\mathrm{V}_{\frac{n}{2}}(1)\mathrm{vol}(B_{[1,n/2]})}{I_\rho(\frac{n}{4}, \frac{n}{4}+1)\mathrm{V}_n(1)(\alpha \times \mathrm{GH}(L))^{n/2}} = g(n) \cdot (4\alpha^2(1-\rho))^{-n/4} \cdot \frac{\mathrm{V}_{\frac{n}{2}}(1)\mathrm{vol}(B_{[1,n/2]})}{\sqrt{\mathrm{V}_n(1)\mathrm{vol}(L)}}.$$

Recall that the number of poly-time operations of a full enumeration on $L \bigcap \mathrm{Ball}_n(\mathrm{GH}(L))$ is heuristically

$$T_{\text{full}} = h(n)\frac{\mathrm{V}_{\frac{n}{2}}(\mathrm{GH}(L))}{\mathrm{vol}(B_{[\frac{n}{2}+1,n]})} = h(n)\frac{\mathrm{V}_{\frac{n}{2}}(1)\mathrm{vol}(B_{[1,n/2]})}{\sqrt{\mathrm{V}_n(1)\mathrm{vol}(L)}},$$

for some $h(n) = n^{O(1)} \geq 1$. We conclude that, up to some polynomial factors, the speed-up of Alg. 4 in the given extreme pruning regime over full enumeration on $L \bigcap \mathrm{Ball}_n(\mathrm{GH}(L))$ is

$$\frac{T_{\text{full}}}{T_{\text{extreme}}(f,R)} \approx (4\alpha^2(1-\rho))^{n/4}.$$

This completes the proof of Theorem 6.

References

[ABF+20] M. Albrecht, S. Bai, P.-A. Fouque, P. Kirchner, D. Stehlé, and W. Wen. Faster enumeration-based lattice reduction: Root Hermite factor $k^{1/(2k)}$ in time $k^{k/8+o(k)}$. In *Proceedings of CRYPTO '20*, volume 12171 of *LNCS*, pages 186–212. Springer, 2020. 1, 3, 6, 7, 23

[ADH+19] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens. The general sieve kernel and new records in lattice reduction. In *Proceedings of EUROCRYPT '19*, volume 11477 of *LNCS*, pages 717–746. Springer, 2019. 1, 6

[ADRS15] D. Aggarwal, D. Dadush, O. Regev, and N. Stephens-Davidowitz. Solving the shortest vector problem in 2^{n} time using discrete Gaussian sampling. In *Proceedings of STOC '15*, pages 733–742. ACM, 2015. 6, 7

[AKS01] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of STOC '01*, pages 601–610. ACM, 2001. 7

[ALNS20] D. Aggarwal, J. Li, P. Q. Nguyen, and N. Stephens-Davidowitz. Slide reduction, revisited — filling the gaps in SVP approximation. In *Proceedings of CRYPTO '20*, volume 12171 of *LNCS*, pages 274–295. Springer, 2020. 1, 2

[AN17] Y. Aono and P. Q. Nguyen. Random sampling revisited: Lattice enumeration with discrete pruning. In *Proceedings of EUROCRYPT '17*, volume 10211 of *LNCS*, pages 65–102. Springer, 2017. 28

[ANSS18] Y. Aono, P. Q. Nguyen, T. Seito, and J. Shikata. Lower bounds on lattice enumeration with extreme pruning. In *Proceedings of CRYPTO '18*, volume 10992 of *LNCS*, pages 608–637. Springer, 2018. 28, 29

[AWHT16] Y. Aono, Y. Wang, T. Hayashi, and T. Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In *Proceedings of EUROCRYPT '16*, volume 9665 of *LNCS*, pages 789–819. Springer, 2016. 1, 7

[Bli14] H. F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 16:227–235, 1914. 22, 25, 42

[BSW18] S. Bai, D. Stehlé, and W. Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. In *Proceedings of ASIACRYPT '18*, volume 11272 of *LNCS*, pages 369–404. Springer, 2018. 1, 3, 4, 7, 25

[CN11] Y. Chen and P. Q. Nguyen. BKZ 2.0: better lattice security estimates. In *Proceedings of ASIACRYPT '11*, volume 7073 of *LNCS*, pages 1–20. Springer, 2011. Full version at http://www.di.ens.fr/-ychen/research/Full_BKZ.pdf. 1, 2, 3, 4, 6, 7, 25, 26

[CS87] J. H. Conway and N. J. A. Sloane. *Sphere-packings, Lattices, and Groups.* Springer, 1987. 5

[Dut81] J. Dutka. The incomplete beta function: a historical profile. *Archive for History of Exact Sciences*, 24:11–29, 1981. 29

[FP85] U. Fincke and M. Phost. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, 1985. 27

[FPL19] FPLLL development team. FPLLL, a lattice reduction library. Available at https://github.com/fplll/fplll, 2019. 1, 2, 6, 26

[FPy19] FPyLLL development team. FPyLLL, a Python interface to FPLLL. Available at https://github.com/fplll/fpylll, 2019. 1, 2, 6, 26

[GHGKN06] N. Gama, N. Howgrave-Graham, H. Koy, and P. Nguyen. Rankin's constant and blockwise lattice reduction. In *Proceedings of CRYPTO '06*, volume 4117 of *LNCS*, pages 112–130. Springer, 2006. 1, 2, 5

[GN08a] N. Gama and P. Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In *Proceedings of STOC '08*, pages 207–216. ACM, 2008. 1, 2

[GN08b] N. Gama and P. Q. Nguyen. Predicting lattice reduction. In *Proceedings of EUROCRYPT '08*, volume 4965 of *LNCS*, pages 31–51. Springer, 2008. 7, 11, 23

[GNR10] N. Gama, P. Q. Nguyen, and O. Regev. Lattice enumeration using extreme pruning. In *Proceedings of EUROCRYPT '10*, volume 6110 of *LNCS*, pages 257–278. Springer, 2010. 3, 4, 6, 7, 27, 28, 29

[Her50] C. Hermite. Second letter to M. Jacobi (in French). *J. Reine Angew. Math.*, 40:279–290, 1850. 6

[HPS11] G. Hanrot, X. Pujol, and D. Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *Proceedings of CRYPTO '11*, volume 6841 of *LNCS*, pages 447–464. Springer, 2011. Full version at https://eprint.iacr.org/2011/198.pdf. 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 16, 17, 32, 33, 36

[HS07] G. Hanrot and D. Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm. In *Proceedings of CRYPTO '07*, volume 4622 of *LNCS*, pages 170–186. Springer, 2007. 15, 27, 35

[HS08] G. Hanrot and D. Stehlé. Worst-case Hermite-Korkine-Zolotarev reduced lattice bases. Available at https://arxiv.org/pdf/0801.3331.pdf, 2008. 22

[Kan83] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of STOC '83*, pages 193–206. ACM, 1983. 27

[KZ73] A. Korkine and G. Zolotareff. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873. 6

[LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:366–389, 1982. 1, 6

[LN19] J. Li and P. Q. Nguyen. Computing a lattice basis revisited. In *Proceedings of ISSAC '19*, pages 275–282. ACM, 2019. 3, 5, 11

[LR20] R. Lindner and M. Ruckert. TU Darmstadt lattice challenge. Available at http://www.latticechallenge.org/, 2020. 1, 28

[MH73] J. Milnor and D. Husemoller. *Symmetric bilinear forms.* Springer, 1973. 5

[Mic81] P. Michael. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *SIGSAM Bulletin*, 15:37–44, 1981. 27

[Mor44] L. J. Mordell. Observation on the minimum of a positive quadratic form in eight variables. *Journal of the London Mathematical Society*, 19:3–6, 1944. 2, 19

[MW15] D. Micciancio and M. Walter. Fast lattice point enumeration with minimal overhead. In *Proceedings of SODA '15*, pages 276–294. ACM/SIAM, 2015. 27

[MW16] D. Micciancio and M. Walter. Practical, predictable lattice basis reduction. In *Proceedings of EUROCRYPT '16*, volume 9665 of *LNCS*, pages 820–849. Springer, 2016. 1, 2, 3, 4, 23, 25, 32, 33

[Neu17] A. Neumaier. Bounding basis reduction properties. *Designs, Codes and Cryptography*, 84(1-2):237–259, 2017. 4, 22, 32, 33, 34

[Neu20] A. Neumaier. Private communication. Jan, 2020. 4

[New63] M. Newman. Bounds for cofactors and arithmetic minima of quadratic forms. *Journal of the London Mathematical Society*, 38:215–217, 1963. 19

[NS06] P. Q. Nguyen and D. Stehlé. LLL on the average. In *Proceedings of ANTS-VII*, volume 4076 of *LNCS*, pages 238–256. Springer, 2006. 23

[NS16] A. Neumaier and D. Stehlé. Faster LLL-type reduction of lattice bases. In *Proceedings of ISSAC '16*, pages 373–380. ACM, 2016. 4, 33

[Poh87] M. Pohst. A modification of the LLL reduction algorithm. *Journal of Symbolic Computation*, 4(1):123–127, 1987. 10

[PT10] G. Pataki and M. Tural. Unifying LLL inequalities. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.8131&rep=rep1&type=pdf, 2010. 5, 22

[Rog56] C. A. Rogers. The number of lattice points in a set. *Proceedings of the London Mathematical Society*, 3-6, 1956. 23

[Sch87] C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987. 1, 6

[SE94] C. P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–199, 1994. Preliminary version in *Proceedings of FCT '91*. 1, 3, 6, 7, 27

[SH95] C. P. Schnorr and H. H. Hörner. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In *Proceedings of EUROCRYPT '95*, volume 921 of *LNCS*, pages 1–12. Springer, 1995. 1, 3, 4, 7, 27

[Sho20] V. Shoup. NTL 11.4.3: Number theory c++ library. http://www.shoup.net/ntl/, 2020. 1, 7

[Sie45] C. L. Siegel. A mean value theorem in Geometry of Numbers. *Annals of Mathematics*, 46:340–347, 1945. 23

[Wal15] M. Walter. Lattice point enumeration on block reduced bases. In *Proceedings of ICITS '15*, volume 9063 of *LNCS*, pages 269–282. Springer, 2015. 27

[WLW15] W. Wei, M. Liu, and X. Wang. Finding shortest lattice vectors in the presence of gaps. In *Proceedings of CT-RSA '15*, volume 9048 of *LNCS*, pages 239–257. Springer, 2015. 7

[YTT11] H. Yanai, K. Takeuchi, and Y. Takane. *Projection Matrices, Generalized Inverse Matrices, and Singular Value*. Springer, 2011. 14

A Neumaier's Analysis for BKZ Variants

Neumaier [Neu17, §3.3] analyzed (S)DBKZ (introduced by Micciancio and Walter [MW16]) and mentioned analyses of other BKZ variants with one paragraph in [Neu17, p. 256]:

"The cyclic variant of the BKZ algorithm analyzed in Hanrot et al. [HPS11] proceeds by using primal tours only, but these are extended to shorter blocks towards the end of the basis. In this case, a similar analysis works, with the same N but using the symmetric bit defect defined by [Neu17, Eq. (57)]. The resulting new proof (whose details are left to the reader) is far simpler than that of [HPS11] and results in the same convergence rate as given above for DBKZ, which is a factor of approximately 16 better the bound on the rate derived in [HPS11]. The final bound on μ and hence the Hermite factor resulting for BKZ is slightly weaker than that for DBKZ."

Section A.1 concisely recalls Neumaier's analysis for DBKZ. We reconstruct Neumaier's analysis for BKZ' [HPS11] in Section A.2: it gives noticeably worse output bounds than our Theorem 2; with our Lemma 1, the similar analysis and same conclusion hold for the original BKZ.

We think that Neumaier's technique seems not to be suitable for analyses of BKZ variants which call an SVP-oracle over varying ranks. This can intuitively be explained as follows:

- The most important difference between DBKZ and BKZ/BKZ' is that the first calls an SVP-oracle in fixed rank β, whereas the latter makes oracle queries over varying ranks $2, 3, \ldots, \beta$. Such a difference is also highlight in [MW16, §1]. This means that any analysis for DBKZ only involves the single Hermite's constant γ_β, while all of different Hermite's constants γ_κ over $\kappa = 2, 3, \ldots, \beta$ would appear in the

Algorithm 5 One DBKZ tour analyzed in [Neu17]

Input: A block size $\beta \geq 2$ and a basis B of an n-rank lattice L.
Output: A new basis of L.
1: **for** $i = n - \beta + 1$ **to** 1 **do**
2: DSVP-reduce $B_{[i,i+\beta-1]}$
3: **end for**
4: **for** $j = 1$ **to** $n - \beta + 1$ **do**
5: SVP-reduce $B_{[j,j+\beta-1]}$.
6: **end for**

analysis of BKZ/BKZ' whatever technique we use, except the simplest case $\beta = 2$ like that for LLL-type algorithms analyzed in [NS16,Neu17] .

It should also be noted that we know very little about Hermite's constants.

– Our analysis uses the Rankin profile $\mathcal{R}(B)$ (defined in Section 2.1), which maps any basis B to a real row vector. We show that when a BKZ tour updates the current basis, there is a vectorial inequality (17). Neumaier suggests to use a real-valued potential $\mu(B)$ (see Eq. (49)) for DBKZ and another real-valued potential $\widetilde{\mu}(B)$ (see Eq. (53)) for BKZ', which result in a real-valued inequality for characterising any DBKZ/BKZ' tour (see Eq. (50) and Eq. (54), respectively). This simplifies a bit the proof by avoiding matrix calculations, but it also provides less information. Moreover, the single real-valued inequality (54) needs to "melt" all of different Hermite's constants γ_κ over $\kappa = 2, 3, \ldots, \beta$, so that it would be naturally "rough" to analyze BKZ/BKZ'. Yet, this is not the case for DBKZ [MW16] or LLL [NS16,Neu17].

This shows that the original vectorial technique of Hanrot et al. [HPS11] still has some benefits, at least when analyzing BKZ variants which call an SVP-oracle over varying ranks.

A.1 Neumaier's Analysis for DBKZ

Neumaier [Neu17, Eq. (2)] defines the bit profile of an n-rank basis B as $g_i(B) = \log \mathrm{vol}(B_{[1,i]})^2$ for $i = 1, \ldots, n$. Neumaier uses the following real-valued potential [Neu17, Eq. (58)]

$$\mu(B) = \max_{1 \leq i \leq n-\beta} \frac{1}{n-i}\left(\frac{g_i(B)}{i} - \frac{g_n(B)}{n}\right) = \max_{1 \leq i \leq n-\beta} \log\left(\frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(L)^{i/n}}\right)^{\frac{2}{i(n-i)}} = \max_{1 \leq i \leq n-\beta} \frac{2\mathcal{R}_i(B)}{i(n-i)} \tag{49}$$

to measure the effect of one DBKZ tour (see Alg. 5).

More precisely, [Neu17, §3.3] proved that if $\mu(B) > \mu_\beta := \frac{\log \gamma_\beta}{\beta - 1}$, then a DBKZ tour transforms a basis B of an n-rank lattice into another basis C s.t.

$$\mu(C) \leq \mu_\beta + \left(1 - \frac{1}{N}\right)^2 (\mu(B) - \mu_\beta), \tag{50}$$

where

$$N = \begin{cases} \frac{n-1}{\beta-1} & \text{if } n \leq 2\beta + 1, \\ \frac{n^2}{4\beta(\beta-1)} + 1 & \text{if } n \geq 2\beta + 2. \end{cases} \tag{51}$$

Since DBKZ calls an SVP-oracle in fixed rank β, Eq. (50) only contains the single Hermite's constant γ_β.

As a result, if k consecutive DBKZ tours transform a $\frac{3}{4}$-LLL-reduced basis B_0 of an n-rank lattice L into another basis B_k s.t. $\mu(B_j) > \mu_\beta$ for $j = 0, \ldots, k-1$, it follows from $\mu(B_0) \leq \frac{1}{2}$ and $1 - \frac{1}{N} \leq e^{-1/N}$ that

$$\mu(B_k) \leq \mu_\beta + \left(1 - \frac{1}{N}\right)^{2k} (\mu(B_0) - \mu_\beta) \leq \mu_\beta + e^{-2k/N}\left(\frac{1}{2} - \mu_\beta\right).$$

As $k = \left\lceil \frac{N}{2} \ln \frac{\frac{1}{2} - \mu_\beta}{\log(1+\varepsilon)} \right\rceil \in O(\frac{n^2}{\beta^2} \log \frac{1}{2\varepsilon})$ (independent of $\|B_0\|$) with $0 < \varepsilon < 0.1$, then $\mu(B_k) \leq \mu_\beta + \log(1+\varepsilon)$, that is,

$$\frac{\mathrm{vol}((B_k)_{[1,i]})}{\mathrm{vol}(L)^{i/n}} \leq (1+\varepsilon)^{\frac{i(n-i)}{2}} \gamma_\beta^{\frac{i(n-i)}{2(\beta-1)}} \quad \text{for} \quad i = 1, \ldots, n - \beta. \tag{52}$$

A.2 Reconstructing Neumaier's Analysis for BKZ'

The real-valued potential of an n-rank basis B defined in [Neu17, Eq. (57)] is:

$$\widetilde{\mu}(B) = \max_{1 \le i \le n-1} \frac{1}{n-i}\left(\frac{g_i(B)}{i} - \frac{g_n(B)}{n}\right) = \max_{1 \le i \le n-1} \log\left(\frac{\mathrm{vol}(B_{[1,i]})}{\mathrm{vol}(L)^{i/n}}\right)^{\frac{2}{i(n-i)}} = \max_{1 \le i \le n-1} \frac{2\mathcal{R}_i(B)}{i(n-i)}. \tag{53}$$

Following Neumaier's hint [Neu17, p. 256], the claim below holds:

Claim 3. *Let $\beta \ge 2$ be the blocksize of BKZ' (see Alg. 2) and let $\widetilde{\mu}_\beta = \frac{1}{\beta-1}\sum_{\kappa=2}^{\beta} \frac{\log \gamma_\kappa}{\kappa-1}$. If $\widetilde{\mu}(B) > \widetilde{\mu}_\beta$, then a BKZ' tour transforms a basis B of an n-rank lattice L into another basis C s.t.*

$$\widetilde{\mu}(C) \le \widetilde{\mu}_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \widetilde{\mu}_\beta), \tag{54}$$

where N is defined in Eq. (51).

Since BKZ' makes SVP calls over varying ranks (mainly for HKZ-reducing the tail block $B_{[n-\beta+1,n]}$), Eq. (54) naturally contains all of different Hermite's constants γ_κ over $\kappa = 2, 3, \ldots, \beta$.

From the proof of Claim 3 (for "Case 2: $j \ge n-\beta+1$", which corresponds to SVP-reductions on the tail block $B_{[n-\beta+1,n]}$), we are not able to set a smaller $\widetilde{\mu}_\beta$ in the above claim.

Similarly to $\mu_\beta = \frac{\log \gamma_\beta}{\beta-1}$ for DBKZ (see Eq. (52)), $\widetilde{\mu}_\beta$ implies the Hermite factor for BKZ':

Corollary 2. *Using the notation $\beta, \widetilde{\mu}_\beta$ and N defined in Claim 3, let $k = \left\lceil N \times \ln \frac{\frac{1}{2} - \widetilde{\mu}_\beta}{\log(1+\varepsilon)} \right\rceil \in O(\frac{n^2}{\beta^2} \log \frac{1}{2\varepsilon})$ with $0 < \varepsilon < 0.1$. If k consecutive BKZ' tours transform a $\frac{3}{4}$-LLL-reduced basis B_0 of an n-rank lattice L into another basis B_k s.t. $\widetilde{\mu}(B_j) > \widetilde{\mu}_\beta$ for $j = 0, \ldots, k-1$, then*

$$\frac{\mathrm{vol}((B_k)_{[1,i]})}{\mathrm{vol}(L)^{i/n}} \le (1+\varepsilon)^{\frac{i(n-i)}{2}} \left(\prod_{\kappa=2}^{\beta} \gamma_\kappa^{\frac{1}{\kappa-1}}\right)^{\frac{i(n-i)}{2(\beta-1)}} \quad \textit{for} \quad i = 1, \ldots, n-1. \tag{55}$$

In particular, the first basis vector $\mathbf{b}_1$ of B_k satisfies

$$\frac{\|\mathbf{b}_1\|}{\mathrm{vol}(L)^{1/n}} \le (1+\varepsilon)^{\frac{n-1}{2}} \left(\prod_{\kappa=2}^{\beta} \gamma_\kappa^{\frac{1}{\kappa-1}}\right)^{\frac{n-1}{2(\beta-1)}}.$$

Note that

$$\prod_{\kappa=2}^{\beta} \gamma_\kappa^{\frac{1}{\kappa-1}} = \prod_{j=1}^{\beta-1} \Theta(j)^{\frac{1}{j}} = \Theta(\beta^{\frac{1}{2}\ln\beta})$$

is asymptotically much larger than $\gamma_\beta = \Theta(\beta)$, this means that the quality bounds in Eq. (55) for BKZ' (with Neumaier's technique) is significantly worse than those in Eq. (52) for DBKZ.

We now prove Claim 3 and Corollary 2:

Proof of Claim 3. For simplicity, assume that $\mathrm{vol}(L) = 1$. Then $g_n(B) = g_n(C) = 0$. In order to prove Eq. (54), it suffices to show

$$g_i(C) \le \begin{cases} i(n-i)\left(\mu_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \mu_\beta)\right) & \text{if } i = 1, \ldots, n-\beta, \\ i(n-i)\left(\widetilde{\mu}_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \widetilde{\mu}_\beta)\right) & \text{if } i = n-\beta+1, \ldots, n-1. \end{cases} \tag{56}$$

As did in [Neu17], we do this by induction on i.

Let B_j be the current basis at the end of Step 4 of BKZ' w.r.t. index j. Note that $C_{[1,j]} = (B_j)_{[1,j]}$ for $j = 1, \ldots, n-\beta+1$ and $C = B_{n-\beta+1}$, we have

$$g_j(C) = \begin{cases} g_j(B_j) & \text{if } \ j = 1, \ldots, n-\beta+1, \\ g_j(B_{n-\beta+1}) & \text{if } \ j = n-\beta+1, \ldots, n. \end{cases}$$

We first show Eq. (56) for $i = 1$. Since $(B_1)_{[1,\beta]}$ is SVP-reduced, Eq. (12) in Lemma 1 implies

$$\begin{aligned} g_1(B_1) &\le \frac{1}{\beta} g_\beta(B) + \log \gamma_\beta \\ &\le (n-\beta)\widetilde{\mu}(B) + \log \gamma_\beta && \text{(By the definition of } \widetilde{\mu}(B)) \\ &= (n-\beta)\widetilde{\mu}(B) + (\beta-1)\mu_\beta \\ &\le (n-1)\left(\mu_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \mu_\beta)\right), \end{aligned}$$

where the last inequality used the conditions $N \ge \frac{n-1}{\beta-1}$ and $\widetilde{\mu}(B) > \widetilde{\mu}_\beta \ge \mu_\beta$.

Assume that Eq. (56) holds over $i = 1, \ldots, j-1$ for some index $2 \le j \le n-1$.

We now show Eq. (56) for $i = j$. There are two cases:

Case 1: $j \le n - \beta$. Since $(B_j)_{[j,j+\beta-1]}$ is SVP-reduced, Eq. (12) in Lemma 1 implies

$$\begin{aligned} g_j(B_j) &\le \frac{\beta-1}{\beta} g_{j-1}(B_{j-1}) + \frac{1}{\beta} g_{j+\beta-1}(B) + \log \gamma_\beta \\ &\le \frac{\beta-1}{\beta} g_{j-1}(B_{j-1}) + \frac{(j+\beta-1)(n+1-j-\beta)}{\beta}\widetilde{\mu}(B) + \log \gamma_\beta && \text{(By the definition of } \widetilde{\mu}(B)) \\ &\le \frac{\beta-1}{\beta}(j-1)(n+1-j)\left(\mu_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \mu_\beta)\right) \\ &\quad + \frac{(j+\beta-1)(n+1-j-\beta)}{\beta}\widetilde{\mu}(B) + (\beta-1)\mu_\beta && \text{(By the induction hypothesis)} \\ &\le j(n-j)\left(\mu_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \mu_\beta)\right), \end{aligned}$$

where the last inequality used the definition of N and the condition $\widetilde{\mu}(B) > \mu_\beta$.

Case 2: $j \ge n - \beta + 1$. Since $C_{[n-\beta+1,n]}$ is HKZ-reduced and $\mathrm{vol}(C) = 1$, we have

$$\begin{aligned} \mathrm{vol}(C_{[1,j]}) &= \mathrm{vol}(C_{[1,n-\beta]}) \cdot \mathrm{vol}(C_{[n-\beta+1,j]}) \\ &\le \mathrm{vol}(C_{[1,n-\beta]}) \cdot \left(\prod_{\kappa=n-j+1}^{\beta} \gamma_\kappa^{\frac{n-j}{2(\kappa-1)}} \right) \mathrm{vol}(C_{[n-\beta+1,n]})^{(j+\beta-n)/\beta} && \text{(By [HS07, Lemma 3])} \\ &= \left(\prod_{\kappa=n-j+1}^{\beta} \gamma_\kappa^{\frac{n-j}{2(\kappa-1)}} \right) \cdot \mathrm{vol}(C_{[1,n-\beta]})^{(n-j)/\beta}. \end{aligned}$$

Equivalently, $g_j(C) \le \frac{n-j}{\beta} g_{n-\beta}(C) + (n-j)\sum_{\kappa=n-j+1}^{\beta} \frac{\log \gamma_\kappa}{\kappa-1}$. Applying the induction hypothesis to $g_{n-\beta}(C)$, we have

$$\begin{aligned} g_j(C) &\le (n-j)(n-\beta)\left(\mu_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \mu_\beta)\right) + (n-j)\sum_{\kappa=n-j+1}^{\beta} \frac{\log \gamma_\kappa}{\kappa-1} \\ &\le j(n-j)\left(\widetilde{\mu}_\beta + \left(1 - \frac{1}{N}\right)(\widetilde{\mu}(B) - \widetilde{\mu}_\beta)\right), \end{aligned}$$

where the last inequality used the condition $\widetilde{\mu}(B) > \widetilde{\mu}_\beta \ge \frac{1}{j+\beta-n}\sum_{\kappa=n-j+1}^{\beta} \frac{\log \gamma_\kappa}{\kappa-1}$. Here, Mordell's inequality (32) implies $\widetilde{\mu}_\beta \ge \frac{1}{j+\beta-n}\sum_{\kappa=n-j+1}^{\beta} \frac{\log \gamma_\kappa}{\kappa-1}$.

This proved Eq. (56) for $i = j$ and completes the proof of Claim 3. $\square$

Proof of Corollary 2. Applying Claim 3, it follows from $\widetilde{\mu}(B_0) \leq \frac{1}{2}$ and $1 - \frac{1}{N} \leq e^{-1/N}$ that

$$\widetilde{\mu}(B_k) \leq \widetilde{\mu}_\beta + \left(1 - \frac{1}{N}\right)^k (\widetilde{\mu}(B_0) - \widetilde{\mu}_\beta) \leq \widetilde{\mu}_\beta + e^{-k/N}\left(\frac{1}{2} - \widetilde{\mu}_\beta\right).$$

Since $k \geq N \times \ln \frac{\frac{1}{2} - \widetilde{\mu}_\beta}{\log(1+\varepsilon)}$, we have $\widetilde{\mu}(B_k) \leq \widetilde{\mu}_\beta + \log(1+\varepsilon)$. This implies Eq. (55). □

B Proofs of Fact 1 and Claim 1

Proof of Fact 1. We use the notation of Section 2.4.

Since we know the explicit expressions of both A and E (*e.g.*, A is a doubly stochastic matrix and E is a simple upper triangular matrix), a direct calculation by hand allows to validate Item 1.

It remains to show Item 2. We first justify the recurrence relation for $\overline{\mathbf{x}}$. To do so, recall the definition of $\mathbf{g}^{(n-\beta+1)} = (g_1^{(n-\beta+1)}, \ldots, g_n^{(n-\beta+1)})$ (right after Eq. (9)):

$$g_i^{(n-\beta+1)} = \begin{cases} 0 & \text{for } i = 1, \ldots, n-\beta, \\ \frac{1}{2}\log \nu_\beta & \text{for } i = n-\beta+1, \\ \frac{1}{2}\log \nu_{n+1-i} - \sum_{\kappa=n+2-i}^{\beta} \frac{\log \nu_\kappa}{2(\kappa-1)} & \text{for } i = n-\beta+2, \ldots, n. \end{cases}$$

It follows that $g_j^{(n-\beta+1)} = \frac{n-j+1}{2(n-j)} \log \nu_{n-j+1} + \frac{1}{n-j}\sum_{i=j+1}^{n} g_i^{(n-\beta+1)}$ for $j = n-\beta+1, \ldots, n-1$ and $g_n^{(n-\beta+1)} = -\sum_{\kappa=2}^{\beta} \frac{\log \nu_\kappa}{2(\kappa-1)}$. Then the definition of $\overline{\mathbf{x}}$ in Eq. (10) implies:

$$\overline{x}_j = \begin{cases} -\sum_{\kappa=2}^{\beta} \frac{\log \nu_\kappa}{2(\kappa-1)} & \text{for } j = n, \\ \frac{n-j+1}{2(n-j)} \log \nu_{n-j+1} + \frac{1}{n-j}\sum_{i=j+1}^{n} \overline{x}_i & \text{for } j = n-1, \ldots, n-\beta+1, \\ \frac{\beta}{2(\beta-1)} \log \nu_\beta + \frac{1}{\beta-1}\sum_{i=j+1}^{j+\beta-1} \overline{x}_i & \text{for } j = n-\beta, \ldots, 1. \end{cases}$$

With the notation β_j and n_j, this proves the recurrence relation for $\overline{\mathbf{x}}$.

We now justify the recurrence relation for $\mathbf{g}$. To do so, we use the following equivalent form of the recurrence equation on the $\overline{x}_j$'s:

$$\overline{x}_j = \frac{1}{2}\log \nu_{\beta_j} + \frac{1}{\beta_j}\sum_{i=j}^{n_j} \overline{x}_i \quad \text{for } j = 1, \ldots, n-1. \tag{57}$$

[HPS11, Lemma 4] proves $\overline{\mathbf{x}} = \overline{\mathbf{x}}A + \mathbf{g}$. That is,

$$\overline{x}_i = \overline{\mathbf{x}}A|_i + g_i \quad \text{for} \quad i = 1, \ldots, n. \tag{58}$$

The identity $\overline{\mathbf{x}}A|_1 = \frac{1}{\beta}\sum_{i=1}^{\beta} \overline{x}_i$ implies $\overline{x}_1 = \frac{1}{\beta}\sum_{i=1}^{\beta} \overline{x}_i + g_1$. Then Eq. (57) for $j = 1$ implies $g_1 = \frac{1}{2}\log \nu_\beta$.

Eq. (57) also implies:

$$\overline{x}_j + \frac{1}{\beta_j}\sum_{i=1}^{j-1} \overline{x}_i = \frac{1}{2}\log \nu_{\beta_j} + \frac{1}{\beta_j}\overline{\mathbf{x}}E|_{n_j} \quad \text{for} \quad j = 2, \ldots, n-1.$$

Substituting Eq. (58) with $i = 1, \ldots, j$ into the left side of the above equation, we have

$$\frac{1}{\beta_j}\overline{\mathbf{x}}\left(\sum_{i=1}^{j-1} A|_i + \beta_j A|_j\right) + g_j + \frac{1}{\beta_j}\sum_{i=1}^{j-1} g_i = \frac{1}{2}\log \nu_{\beta_j} + \frac{1}{\beta_j}\overline{\mathbf{x}}E|_{n_j} \quad \text{for} \quad j = 2, \ldots, n-1.$$

By Item 1, this implies $g_j + \frac{1}{\beta_j}\sum_{i=1}^{j-1} g_i = \frac{1}{2}\log \nu_{\beta_j}$ for $j = 2, \ldots, n-1$.

Since A is a doubly stochastic matrix, we have $\sum_{i=1}^{n} A|_i = \mathbf{1}_n^T$. It follows from Eq. (58) that

$$\sum_{i=1}^{n} g_i = \sum_{i=1}^{n} \overline{x}_i - \overline{\mathbf{x}}\left(\sum_{i=1}^{n} A|_i\right) = \sum_{i=1}^{n} \overline{x}_i - \overline{\mathbf{x}} \cdot \mathbf{1}_n^T = 0.$$

Thus, we proved the recurrence relation for $\mathbf{g}$. This completes the proof of Fact 1. □

Proof of Claim 1. By Eq. (20), we have $(A-\rho\cdot Q)(A-\rho\cdot Q)^T = AA^T + (\rho^2 - 2\rho)Q$ for any $\rho \in \mathbb{R}$. In particular, $(A-Q)(A-Q)^T = AA^T - Q$. Hence, it suffices to verify

$$\Phi(AA^T - Q) \subseteq \Phi(AA^T)\backslash\{1\} \subseteq \Phi(AA^T + (\rho^2 - 2\rho)Q) \;\text{ for any }\; \rho \in \mathbb{R}. \tag{59}$$

First, we show $\Phi(AA^T - Q) \subseteq \Phi(AA^T)\backslash\{1\}$. Let $\lambda \in \Phi(AA^T - Q)$ and let $\mathbf{v} \in \mathbb{R}^n\backslash\{\mathbf{0}\}$ be an eigenvector for $AA^T - Q$ associated with λ. Then $\mathbf{v}(AA^T - Q) = \lambda\mathbf{v}$. Note that $\mathbf{v}(AA^T - Q)(1_{n\times n} - Q) = \lambda\mathbf{v}(1_{n\times n} - Q)$ is equivalent to $\mathbf{v}(AA^T - Q) = \lambda\mathbf{v} - \lambda\mathbf{v}Q$, this implies $\lambda\mathbf{v}Q = \mathbf{0}$. There are two cases:

- If $\lambda = 0$, then $\lambda \in \Phi(AA^T)\backslash\{1\}$. Indeed, $(1,-1,0,\ldots,0) \in \mathbb{R}^n$ is an eigenvector for AA^T associated with 0, since $(1,-1,0,\ldots,0)AA^T = \mathbf{0}$.
- Otherwise $\lambda \neq 0$ and $\mathbf{v}Q = \mathbf{0}$. Then $\mathbf{v}AA^T = \lambda\mathbf{v}$. We claim that $\lambda < 1$: indeed, it follows from $\mathbf{v}Q = \mathbf{0}$ that $\sum_{i=1}^n v_i = 0$; without loss of generality, assume that $v_1 = \max_{1\le i\le n} v_i > 0 > \min_{1\le i\le n} v_i$; we have $\lambda v_1 = \mathbf{v}A\mathbf{a}_1^T < v_1(\mathbf{1}_n A\mathbf{a}_1^T) = v_1$, which proves $\lambda < 1$. This implies $\lambda \in \Phi(AA^T)\backslash\{1\}$.

Then we proved $\Phi(AA^T - Q) \subseteq \Phi(AA^T)\backslash\{1\}$.

Next, we show $\Phi(AA^T)\backslash\{1\} \subseteq \Phi(AA^T + (\rho^2 - 2\rho)Q)$. Let $\lambda \in \Phi(AA^T)\backslash\{1\}$ and let $\mathbf{v} \in \mathbb{R}^n\backslash\{\mathbf{0}\}$ be an eigenvector for AA^T associated with λ. Then $\mathbf{v}AA^T = \lambda\mathbf{v}$. Note that $\mathbf{v}AA^T(1_{n\times n} - Q) = \lambda\mathbf{v}(1_{n\times n} - Q)$ is equivalent to $\mathbf{v}AA^T = \lambda\mathbf{v} + (1-\lambda)\mathbf{v}Q$, this implies $\mathbf{v}Q = \mathbf{0}$ and hence $\mathbf{v}(AA^T + (\rho^2 - 2\rho)Q) = \lambda\mathbf{v}$. Then $\lambda \in \Phi(AA^T + (\rho^2 - 2\rho)Q)$, which proves $\Phi(AA^T)\backslash\{1\} \subseteq \Phi(AA^T + (\rho^2 - 2\rho)Q)$.

Thus, we proved Eq. (59), which implies Claim 1. This competes the proof. □

C Proof of Proposition 5

In this section, we prove Prop. 5, by following the notation in Section 3.5.

C.1 Proof of Proposition 5.1

We follow the technical ideas illustrated right after Prop. 5 to prove its Item 1, with Newman's inequality (33) and without Mordell's inequality (32). More specifically, among Lemma 3, Cor. 3 and Lemma 4 below, only Cor. 3 uses Newman's inequality.

Our first key observation (37) is formalized as follows:

Lemma 3. *Let $n > \beta \geq 2$ be integers and let $\mathbf{c}_j \in \mathbb{Q}^{\beta-1}$ be the vector defined in Eq. (35)/Eq. (36) for $j = 1,\ldots,n$. Then*

$$\sum_{j=1}^{i} \mathbf{c}_j - \frac{i}{n}\sum_{j=1}^{n} \mathbf{c}_j \geq \mathbf{0} \;\; \textit{for} \;\; i = 1,\ldots,n-\beta. \tag{60}$$

Proof. To show the lemma, the hard part is to argue the following special case of Eq. (60):

$$\mathbf{c}_i - \frac{1}{n-i+1}\sum_{j=i}^{n} \mathbf{c}_j \geq \mathbf{0} \;\text{ or equivalently }\; (n-i)\mathbf{c}_i - \sum_{j=i+1}^{n} \mathbf{c}_j \geq \mathbf{0} \;\text{ for }\; i = 1,\ldots,n-\beta. \tag{61}$$

Proof of Eq. (61). We prove this assertion by backward induction over i.

First, it follows from the definition of the $\mathbf{c}_j$'s in Eq. (35)/Eq. (36) that $\sum_{j=n-\beta+1}^{n} \mathbf{c}_j = \mathbf{0}$ and

$$\mathbf{c}_j \geq \mathbf{0} \;\text{ for }\; j = n-\beta+1, n-\beta, \ldots, n-2\beta+2. \tag{62}$$

This implies Eq. (61) for $i = n-\beta$: $\beta\mathbf{c}_{n-\beta} - \sum_{j=n-\beta+1}^{n} \mathbf{c}_j = \beta\mathbf{c}_{n-\beta} \geq \mathbf{0}$.

Assume that Eq. (61) holds over $i = k+1,\ldots,n-\beta$ for some index $k \in [1, n-\beta-1]$.

We prove Eq. (61) for $i = k$ by distinguishing two cases:

Case 1: $n-2\beta+2 \le k \le n-\beta-1$. By Eq. (36), $\mathbf{c}_k$ is the sum of a non-negative vector and $\frac{1}{\beta-1}\sum_{j=k+1}^{n-\beta}\mathbf{c}_j$. This implies:

$$
\begin{aligned}
&(n-k)\mathbf{c}_k - \sum_{j=k+1}^{n}\mathbf{c}_j = (n-k)\mathbf{c}_k - \sum_{j=k+1}^{n-\beta}\mathbf{c}_j \\
&= (n-k)(\underbrace{0,\dots,0}_{n-\beta-k \text{ zeros}}, \frac{n-\beta+1-k}{\beta-1},\dots,\frac{n-\beta+1-k}{\beta-1},\frac{n-\beta+1-k}{\beta-1}+\beta) + \frac{n-\beta+1-k}{\beta-1}\sum_{j=k+1}^{n-\beta}\mathbf{c}_j \\
&\ge \mathbf{0}. \qquad\qquad \text{(By Eq. (62))}
\end{aligned}
$$

Case 2: $1 \le k \le n-2\beta+1$. By Eq. (36), $\mathbf{c}_k$ is the sum of a non-negative vector and $\frac{1}{\beta-1}\sum_{j=k+1}^{k+\beta-1}\mathbf{c}_j$. Then

$$
\begin{aligned}
&(n-k)\mathbf{c}_k - \sum_{j=k+1}^{n}\mathbf{c}_j \\
&= (n-k)(0,\dots,0,\beta) + \frac{n-k}{\beta-1}\sum_{j=k+1}^{k+\beta-1}\mathbf{c}_j - \sum_{j=k+1}^{n}\mathbf{c}_j \\
&= (n-k)(0,\dots,0,\beta) + \frac{n-\beta+1-k}{\beta-1}\left(\sum_{j=k+1}^{k+\beta-1}\mathbf{c}_j - \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\mathbf{c}_j\right).
\end{aligned}
$$

We claim that $\sum_{j=k+1}^{k+\beta-1}\mathbf{c}_j \ge \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\mathbf{c}_j$. Indeed, the induction hypothesis implies $\mathbf{c}_i \ge \frac{1}{n-i}\sum_{j=i+1}^{n}\mathbf{c}_j$ for $i=k+1,\dots,n-\beta$. Using it to eliminate each term $\mathbf{c}_j$ in turn over $j=k+1,\dots,k+\beta-1$, we have:

$$
\begin{aligned}
\sum_{j=k+1}^{k+\beta-1}\mathbf{c}_j &\ge \frac{n-k}{n-k-1}\sum_{j=k+2}^{k+\beta-1}\mathbf{c}_j + \frac{1}{n-k-1}\sum_{j=k+\beta}^{n}\mathbf{c}_j \\
&\ge \frac{n-k}{n-k-2}\sum_{j=k+3}^{k+\beta-1}\mathbf{c}_j + \frac{2}{n-k-2}\sum_{j=k+\beta}^{n}\mathbf{c}_j \\
&\cdots \quad \cdots \\
&\ge \frac{n-k}{n-k-\beta+2}\mathbf{c}_{k+\beta-1} + \frac{\beta-2}{n-k-\beta+2}\sum_{j=k+\beta}^{n}\mathbf{c}_j \\
&\ge \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\mathbf{c}_j.
\end{aligned}
$$

It follows that $(n-k)\mathbf{c}_k - \sum_{j=k+1}^{n}\mathbf{c}_j \ge \mathbf{0}$.

Then Eq. (61) for $i=k$ follows. Thus, we proved Eq. (61) for all $i=1,\dots,n-\beta$. □

Returning to the proof of Eq. (60), we show it using Eq. (61) and by induction over i.

First, Eq. (60) for $i=1$ holds, because which is exactly Eq. (61) for $i=1$.

Assume that Eq. (60) holds over $i=\ell-1$ for some index $\ell \in [2, n-\beta]$. This induction hypothesis $\sum_{j=1}^{\ell-1}\mathbf{c}_j - \frac{\ell-1}{n}\sum_{j=1}^{n}\mathbf{c}_j \ge \mathbf{0}$ implies:

$$
\sum_{j=1}^{\ell-1}\mathbf{c}_j \ge \frac{\ell-1}{n-\ell+1}\sum_{j=\ell}^{n}\mathbf{c}_j.
$$

Using this inequality and the fact $\left(1-\frac{\ell}{n}\right)\frac{\ell-1}{n-\ell+1}-\frac{\ell}{n}=-\frac{1}{n-\ell+1}$, we verify Eq. (60) for $i=\ell$:

$$\begin{aligned}\sum_{j=1}^{\ell}\mathbf{c}_j-\frac{\ell}{n}\sum_{j=1}^{n}\mathbf{c}_j &= \mathbf{c}_\ell-\frac{\ell}{n}\sum_{j=\ell}^{n}\mathbf{c}_j+\left(1-\frac{\ell}{n}\right)\sum_{j=1}^{\ell-1}\mathbf{c}_j\\ &\geq \mathbf{c}_\ell-\frac{\ell}{n}\sum_{j=\ell}^{n}\mathbf{c}_j+\left(1-\frac{\ell}{n}\right)\frac{\ell-1}{n-\ell+1}\sum_{j=\ell}^{n}\mathbf{c}_j\\ &= \mathbf{c}_\ell-\frac{1}{n-\ell+1}\sum_{j=\ell}^{n}\mathbf{c}_j\geq\mathbf{0}. \qquad \text{(By Eq. (61) for } i=\ell)\end{aligned}$$

Thus, we proved Eq. (60) for all $i=1,\dots,n-\beta$. This completes the proof of Lemma 3. □

By Lemma 3, Eq. (40) can be rigorously argued below, where Newman's inequality (33) plays a key role.

Corollary 3. *Let $n>\beta\geq 2$ be integers and $\delta\geq 1$. Let $\widehat{x}_j$'s and $\widehat{y}_j$'s be the sequences defined in Eq. (30) and Eq. (39), respectively. Then*

$$\sum_{j=1}^{i}\widehat{x}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{x}_j\leq\sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j \quad \text{for} \quad i=1,\dots,n-\beta.$$

Proof. Let $\mathbf{c}_j\in\mathbb{Q}^{\beta-1}$ be the vectors defined in Eq. (35)/Eq. (36). With the two vectors $\mathbf{h}$ and $\overline{\mathbf{h}}$ (defined right after Prop. 5), we have $\widehat{x}_j=\mathbf{c}_j\cdot\mathbf{h}^{\mathrm{T}}$ and $\widehat{y}_j=\mathbf{c}_j\cdot\overline{\mathbf{h}}^{\mathrm{T}}$ for $j=1,\dots,n$, as mentioned in the sketched proof of Prop. 5. This implies that for $i=1,\dots,n$,

$$\begin{aligned}\sum_{j=1}^{i}\widehat{x}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{x}_j &= \left(\sum_{j=1}^{i}\mathbf{c}_j-\frac{i}{n}\sum_{j=1}^{n}\mathbf{c}_j\right)\cdot\mathbf{h}^{\mathrm{T}},\\ \sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j &= \left(\sum_{j=1}^{i}\mathbf{c}_j-\frac{i}{n}\sum_{j=1}^{n}\mathbf{c}_j\right)\cdot\overline{\mathbf{h}}^{\mathrm{T}}.\end{aligned}$$

By Newman's inequality (33), we have $\mathbf{h}\leq\overline{\mathbf{h}}$. It follows from Lemma 3 that for $i=1,\dots,n-\beta$,

$$\left(\sum_{j=1}^{i}\mathbf{c}_j-\frac{i}{n}\sum_{j=1}^{n}\mathbf{c}_j\right)\cdot\mathbf{h}^{\mathrm{T}}\leq\left(\sum_{j=1}^{i}\mathbf{c}_j-\frac{i}{n}\sum_{j=1}^{n}\mathbf{c}_j\right)\cdot\overline{\mathbf{h}}^{\mathrm{T}}.$$

This implies the desired and completes the proof. □

Eq. (40) suggests to upper bound $\sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j$ for $i=1,\dots,n-\beta$. To do so, our second key observation gives rise to the lemma below. For conciseness, we use the notation g_1 for $\frac{1}{2}\log(\delta\gamma_\beta)$ by Eq. (14).

Lemma 4. *Let $n>\beta\geq 2$ be integers and $\widehat{y}_j$'s be the sequence defined in Eq. (39) with $\delta\geq 1$. Then*

$$\sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j\leq\left(\frac{i(n-i)}{\beta-1}+\frac{i\beta(\beta-2)}{n(\beta-1)}\right)g_1 \quad \text{for } i=1,\dots,n-\beta. \tag{63}$$

Proof. Without loss of generality, we may assume that $n\geq 2\beta+1$. Note that $\sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j=\left(\sum_{j=1}^{i}\mathbf{c}_j-\frac{i}{n}\sum_{j=1}^{n}\mathbf{c}_j\right)\cdot\overline{\mathbf{h}}^{\mathrm{T}}$ for each i, we show this lemma by following the similar strategy in the proof of Lemma 3. The hard part is to argue the following special case of Eq. (63):

$$\widehat{y}_i-\frac{1}{n-i+1}\sum_{j=i}^{n}\widehat{y}_j\leq\left(\frac{n-i}{\beta-1}+\frac{\beta(\beta-2)}{(n-i+1)(\beta-1)}\right)g_1 \quad \text{for } i=1,\dots,n-\beta. \tag{64}$$

Proof of Eq. (64). First, since $\sum_{j=n-\beta+1}^{n}\widehat{y}_j = 0$ (see Eq. (39)), the exact expression of $\widehat{y}_j$ for tail indices j in Eq. (41) implies that for $i = n-2\beta+1,\ldots,n-\beta$,

$$\widehat{y}_i - \frac{1}{n-i+1}\sum_{j=i}^{n}\widehat{y}_j = \left(\frac{2\beta}{n-i+1} + \frac{n-i+1-\beta}{n-i+1}\left(\frac{\beta}{\beta-1}\right)^{n-i+1-\beta}\right) g_1.$$

It can be checked that $\frac{2\beta}{z} + \frac{z-\beta}{z}\left(\frac{\beta}{\beta-1}\right)^{z-\beta} \leq \frac{z-1}{\beta-1} + \frac{\beta(\beta-2)}{z(\beta-1)}$ for any integers $2 \leq \beta < z \leq 2\beta$. By setting $z = n-i+1$, this implies Eq. (64) for $i = n-2\beta+1,\ldots,n-\beta$.

Assume that Eq. (64) holds over $i = k+1,\ldots,n-\beta$ for some index $k \in [1, n-2\beta]$.

We show Eq. (64) for $i = k$. To do so, the definition of $\widehat{y}_k$ in Eq. (39) implies

$$\begin{aligned}
&\widehat{y}_k - \frac{1}{n-k+1}\sum_{j=k}^{n}\widehat{y}_j \\
&= \frac{n-k}{n-k+1}\left(\frac{\beta}{\beta-1}g_1 + \frac{1}{\beta-1}\sum_{j=k+1}^{k+\beta-1}\widehat{y}_j\right) - \frac{1}{n-k+1}\sum_{j=k+1}^{n}\widehat{y}_j \\
&= \frac{(n-k)\beta}{(n-k+1)(\beta-1)}g_1 + \frac{n-k-\beta+1}{(n-k+1)(\beta-1)}\left(\sum_{j=k+1}^{k+\beta-1}\widehat{y}_j - \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\widehat{y}_j\right).
\end{aligned}$$

Now, the only issue is to prove $\sum_{j=k+1}^{k+\beta-1}\widehat{y}_j - \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\widehat{y}_j \leq \left(n-k+\frac{\beta(\beta-2)}{n-k-\beta+1}\right)g_1$. Indeed, the induction hypothesis implies $\widehat{y}_i \leq \frac{1}{n-i}\sum_{j=i+1}^{n}\widehat{y}_j + \frac{1}{\beta-1}\left(n-i+1+\frac{\beta(\beta-2)}{n-i}\right)g_1$ for $i = k+1,\ldots,n-\beta$. Using it to eliminate each term $\widehat{y}_j$ in turn over $j = k+1,\ldots,k+\beta-1$, we have

$$\begin{aligned}
\sum_{j=k+1}^{k+\beta-1}\widehat{y}_j &\leq \frac{n-k}{n-k-1}\sum_{j=k+2}^{k+\beta-1}\widehat{y}_j + \frac{1}{n-k-1}\sum_{j=k+\beta}^{n}\widehat{y}_j + \frac{1}{\beta-1}\left(n-k+\frac{\beta(\beta-2)}{n-k-1}\right)g_1 \\
&\leq \frac{n-k}{n-k-2}\sum_{j=k+3}^{k+\beta-1}\widehat{y}_j + \frac{2}{n-k-2}\sum_{j=k+\beta}^{n}\widehat{y}_j + \frac{2}{\beta-1}\left(n-k+\frac{\beta(\beta-2)}{n-k-2}\right)g_1 \\
&\cdots \quad \cdots \\
&\leq \frac{n-k}{n-k-\beta+2}\widehat{y}_{k+\beta-1} + \frac{\beta-2}{n-k-\beta+2}\sum_{j=k+\beta}^{n}\widehat{y}_j + \frac{\beta-2}{\beta-1}\left(n-k+\frac{\beta(\beta-2)}{n-k-\beta+2}\right)g_1 \\
&\leq \frac{\beta-1}{n-k-\beta+1}\sum_{j=k+\beta}^{n}\widehat{y}_j + \left(n-k+\frac{\beta(\beta-2)}{n-k-\beta+1}\right)g_1.
\end{aligned}$$

Then Eq. (64) for $i = k$ follows. Thus, we proved Eq. (64) for all $i = 1,\ldots,n-\beta$. □

Returning to the proof of Eq. (63), we show it using Eq. (64) and by induction over i.

First, Eq. (63) for $i = 1$ holds, because which is exactly Eq. (64) for $i = 1$.

Assume that Eq. (63) holds over $i = \ell-1$ for some index $\ell \in [2, n-\beta]$. This induction hypothesis $\sum_{j=1}^{\ell-1}\widehat{y}_j - \frac{\ell-1}{n}\sum_{j=1}^{n}\widehat{y}_j \leq \frac{\ell-1}{\beta-1}\left(n-\ell+1+\frac{\beta(\beta-2)}{n}\right)g_1$ implies:

$$\sum_{j=1}^{\ell-1}\widehat{y}_j \leq \frac{\ell-1}{n-\ell+1}\sum_{j=\ell}^{n}\widehat{y}_j + \frac{\ell-1}{\beta-1}\left(n+\frac{\beta(\beta-2)}{n-\ell+1}\right)g_1.$$

Using this inequality and the fact $\left(1-\frac{\ell}{n}\right)\frac{\ell-1}{n-\ell+1}-\frac{\ell}{n}=-\frac{1}{n-\ell+1}$, we verify Eq. (63) for $i=\ell$:

$$\begin{aligned}
&\sum_{j=1}^{\ell}\widehat{y}_j-\frac{\ell}{n}\sum_{j=1}^{n}\widehat{y}_j=\widehat{y}_\ell-\frac{\ell}{n}\sum_{j=\ell}^{n}\widehat{y}_j+\left(1-\frac{\ell}{n}\right)\sum_{j=1}^{\ell-1}\widehat{y}_j\\
\leq&\widehat{y}_\ell-\frac{\ell}{n}\sum_{j=\ell}^{n}\widehat{y}_j+\left(1-\frac{\ell}{n}\right)\frac{\ell-1}{n-\ell+1}\sum_{j=\ell}^{n}\widehat{y}_j+\frac{(\ell-1)(n-\ell)}{\beta-1}\left(1+\frac{\beta(\beta-2)}{n(n-\ell+1)}\right)g_1\\
=&\widehat{y}_\ell-\frac{1}{n-\ell+1}\sum_{j=\ell}^{n}\widehat{y}_j+\frac{(\ell-1)(n-\ell)}{\beta-1}\left(1+\frac{\beta(\beta-2)}{n(n-\ell+1)}\right)g_1\\
\leq&\left(\frac{\ell(n-\ell)}{\beta-1}+\frac{\ell\beta(\beta-2)}{n(\beta-1)}\right)g_1. \qquad \text{(By Eq. (64) for } i=\ell)
\end{aligned}$$

Thus, we proved Eq. (63) for all $i=1,\ldots,n-\beta$. This completes the proof of Lemma 4. □

Proof of Proposition 5.1. Combining Eq. (31), Cor. 3 and Lemma 4, we conclude that

$$\sum_{j=1}^{i}\widehat{w}_j=\sum_{j=1}^{i}\widehat{x}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{x}_j\leq\sum_{j=1}^{i}\widehat{y}_j-\frac{i}{n}\sum_{j=1}^{n}\widehat{y}_j\leq\left(\frac{i(n-i)}{\beta-1}+\frac{i\beta(\beta-2)}{n(\beta-1)}\right)g_1$$

for $i=1,\ldots,n-\beta$. Since $g_1=\frac{1}{2}\log(\delta\gamma_\beta)$ defined by Eq. (14), this completes the proof of Prop. 5.1. □

C.2 Proof of Proposition 5.2

Proposition 5.2 is a consequence of the following two claims:

Claim 4. *Let $\mathbf{v}=(v_1,\ldots,v_n)$ be a vector in $\mathbb{R}^n$ such that $\sum_{i=1}^n v_i=0$. Then $\|\mathbf{v}\|\leq n\cdot\max_{1\leq i\leq n}v_i$.*

Proof. Since $\sum_{i=1}^n v_i=0$, without loss of generality, assume that $v_1,\ldots,v_k\leq 0$ and $v_{k+1},\ldots v_n>0$ for some index $k\in[1,n]$. Note that $\left(\sum_{i=1}^k v_i\right)^2=\left(\sum_{i=k+1}^n v_i\right)^2\leq(n-k)\sum_{i=k+1}^n v_i^2$, we have

$$\sum_{i=1}^n v_i^2\leq\left(\sum_{i=1}^k v_i\right)^2+\sum_{i=k+1}^n v_i^2\leq(n-k+1)\sum_{i=k+1}^n v_i^2\leq(n-k)(n-k+1)\cdot\max_{k+1\leq i\leq n}v_i^2.$$

This implies $\|\mathbf{v}\|\leq n\cdot\max_{1\leq i\leq n}v_i$. □

Claim 5. *With the notation of Proposition 5, we have: $\widehat{w}_1\geq\widehat{w}_2\geq\cdots\geq\widehat{w}_n$.*

Proof. Since $\widehat{\mathbf{w}}=\widehat{\mathbf{x}}-\frac{1}{n}\left(\sum_{j=1}^n\widehat{x}_j\right)\cdot\mathbf{1}_n$, it suffices to show $\widehat{x}_1\geq\widehat{x}_2\geq\cdots\geq\widehat{x}_n$.

By Eq. (30), Newman's inequality (33) implies $\widehat{x}_{n-\beta}\geq\widehat{x}_{n-\beta+1}\geq\cdots\geq\widehat{x}_n$.

Assume that $\widehat{x}_{k+1}\geq\widehat{x}_{k+2}\geq\cdots\geq\widehat{x}_n$ for some index $k\in[1,n-\beta-1]$.

We claim that $\widehat{x}_k\geq\widehat{x}_{k+1}$. Indeed, the definitions of $\widehat{x}_k$ and $\widehat{x}_{k+1}$ in Eq. (27) imply:

$$\begin{aligned}
\widehat{x}_k-\widehat{x}_{k+1}&=\frac{1}{\beta-1}\left(\sum_{j=k+1}^{k+\beta-1}\widehat{x}_j-\sum_{j=k+2}^{k+\beta}\widehat{x}_j\right)\\
&=\frac{1}{\beta-1}\sum_{j=k+1}^{k+\beta-1}(\widehat{x}_j-\widehat{x}_{j+1})\geq 0. \qquad \text{(By the induction hypothesis)}
\end{aligned}$$

Thus, we proved $\widehat{x}_1\geq\widehat{x}_2\geq\cdots\geq\widehat{x}_n$. Then the claim follows. □

Proof of Prop. 5.2. By Claim 5, $\max_{1\le i\le n} \widehat{w}_i = \widehat{w}_1$. Since $\sum_{i=1}^{n} \widehat{w}_i = 0$, Claim 4 implies Prop. 5.2. $\square$

D Pseudo-code for Testing Eq. (43)

The following simple pseudo-code can be used to experimentally test the tightness of Eq. (43), as well as its evolution w.r.t. the number of tours.

Algorithm 6 Pseudo-code for testing Eq. (43)

Input: A blocksize $\beta \ge 2$, a number $k \ge 1$ of tours, and the Gram-Schmidt profile $\mathcal{G}(B_0)$ of an n-rank basis B_0.
Output: An upper bound for the logarithmic Hermite factor $\log \frac{\|\mathbf{b}_1\|}{\mathrm{vol}(B)^{1/n}}$ right after k BKZ tours.

1: **for** $i = 1$ to β **do**
2:     **if** $i \in \{1, 2, \ldots, 8, 24\}$ **then**
3:         $r_i \leftarrow \log \sqrt{\gamma_i}$
4:     **else**
5:         $r_i \leftarrow \log \left(\sqrt{\frac{2}{\pi}} \cdot \Gamma(1 + \frac{i}{2})^{1/i} \right)$ //For i here, $\gamma_i \le \frac{2}{\pi} \cdot \Gamma(1 + \frac{i}{2})^{2/i}$ [Bli14] implies $\log \sqrt{\gamma_i} \le r_i$.
6:     **end if**
7: **end for**
8: Compute an analog $\overline{\mathbf{y}}$ of $\widehat{\mathbf{x}}$ (defined in Eq. (27) with $\delta = 1$) via Steps 9-10, by replacing each $\log \sqrt{\gamma_i}$ with r_i:
9: **for** $j = n$ downto $n - \beta + 1$ **do** $\overline{y}_j \leftarrow r_{n-j+1} - \sum_{\kappa=n-j+2}^{\beta} \frac{r_\kappa}{\kappa - 1}$
10: **for** $s = n - \beta$ downto 1 **do** $\overline{y}_s \leftarrow \frac{\beta}{\beta-1} r_\beta + \frac{1}{\beta-1} \sum_{t=s+1}^{s+\beta-1} \overline{y}_t$
11: Compute an analog $\mathbf{y}$ of $\widehat{\mathbf{w}}$ (defined in Eq. (26) with $\delta = 1$), by replacing each $\log \sqrt{\gamma_i}$ with r_i: $\mathbf{y} \leftarrow \overline{\mathbf{y}}(1_{n\times n} - Q)$
12: $\mathcal{G}_1(B_k)' \leftarrow y_1 + (\mathcal{G}(B_0) - \mathbf{y})(A - Q)^k E|_1$ //$\mathcal{G}_1(B_0)' = \mathcal{G}_1(B_0)$ and $\mathcal{G}_1(B_k)'$ converges to y_1 as k increases.
13: **return** $\mathcal{G}_1(B_k)'$.   //Eq. (37) implies $\widehat{w}_1 \le y_1$, then $\lim_{k\to+\infty} \mathcal{G}_1(B_k)' = y_1 \ge \widehat{w}_1$.