Analyzing Pump and jump BKZ algorithm using dynamical systems

Leizhang Wang

State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China
lzwang_2@stu.xidian.edu.cn

Abstract. The analysis of the reduction effort of the lattice reduction algorithm is important in estimating the hardness of lattice-based cryptography schemes. Recently many lattice challenge records have been cracked by using the Pnj-BKZ algorithm which is the default lattice reduction algorithm used in G6K, such as the TU Darmstadt LWE and SVP Challenges. However, the previous estimations of the Pnj-BKZ algorithm are simulator algorithms rather than theoretical upper bound analyses. In this work, we present the first dynamic analysis of Pnj-BKZ algorithm. More precisely, our analysis results show that let L is the lattice spanned by $(\mathbf{a}_i)_{i\le d}$. The shortest vector $\mathbf{b}_1$ output by running $\Omega\left(\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)\right)$ tours reduction of pnj-BKZ(β, J), $\mathbf{b}_1$ satisfied that $\|\mathbf{b}_1\| \le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2} \cdot (\det L)^{\frac{1}{d}}$.

Keywords: Lattice Reduction, Pnj-BKZ, Dynamical Systems

1 Introduction

In recent years, with the development of quantum computers and quantum algorithms like Shor's algorithm [26], the current mainstream public key cryptography schemes (RSA, ECC) are threatened by quantum computing. Therefore, the National Institute of Standards and Technology (NIST) in the United States has called the cryptography schemes which can resist attacks from quantum computers (Post-Quantum Cryptography schemes). As one of the main parts of post-quantum cryptography, lattice-based cryptography recently attracted much interest, since it can construct numerous cryptographic primitives, and the security of lattice-based cryptography schemes is guaranteed by the hardness of lattice problems with worst-case which is considered to be quantum-resistant. In 2022, at the process of NIST's PQC standardization [1], three over four selected schemes as next-generation standard are lattice-based candidates (Kyber [5], Dilithium [9] and Falcon [24]). In the standardization process of lattice-based cryptography schemes, it is necessary to give an accurate estimation of the concrete hardness of lattice problems.

A lattice L is generated by a basis $\mathbf{B}$ which is a set of linearly independent vectors $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^m$. In lattice-based cryptography, the approximated shortest vector problem is a basic and central computational problem. The α-approximate Shortest Vector Problem (α-SVP): given an arbitrary basis $\mathbf{B}$ on lattice $L = L(\mathbf{B})$, find the shortest non-zero vector $\mathbf{v}$ s.t. $\|\mathbf{v}\| \leq \alpha \cdot \lambda_1(L)$.

Over the past few decades, a series works of reduction algorithms were proposed to solve α-SVP. In 1982, Lenstra et al. proposed the first polynomial-time lattice reduction algorithm: LLL algorithm [18] which can solve α-SVP with an exponential approximate factor α. Then Schnorr and Euchner give a stronger lattice reduction algorithm *Block Korkin-Zolotarev reduction* (BKZ) [25] which combined the LLL algorithm and the enumeration algorithm to balance the algorithm's time cost and the quality of output (e.g., the approximation factor α) by adjusting a parameter β called blocksize. In the literature, many variants ([11],[12],[7],[22],[4]) of the original BKZ algorithm [25] are proposed. e.g. By using the extreme pruning technique[13] and early termination operation, BKZ 2.0 [7] speed up enumeration and improve the efficiency of the BKZ algorithm.

In 2019, Albrecht *et al.* [3] designed the *General Sieve Kernel* (G6K) which implemented a new version of BKZ named *Pump and jump BKZ* (Pnj-BKZ) which has two adjustable parameters: size of `Pump` (β) and size of jump (J). Unlike classical BKZ using an enumeration algorithm as its SVP oracle, Pnj-BKZ(β, J) adopts `Pump` to do the reduction in each block. The `Pump` used in G6K combined progressive sieving technology [17] and dimension-for-free (d4f) technique [8] can not only return one short vector but return a lattice basis which is almost HKZ reduced. `Pump` can selectively call the Gauss sieve [21], NV sieve [23], k-list sieve([15],[16]) or BGJ1 sieve [2] to solve α-SVP with very small approximate factor like $\alpha \in [1, 1.05)$. In 2021, Ducas *et al.* [10] improved the efficiency of G6K using GPU and implemented the fastest sieving algorithm BDGL16 [6] in both G6K and G6K-GPU-Tensor.

Another parameter the jump value J controls the jump stage of blocks in BKZ with each `Pump`, which can jump by more than one dimension. For instance, after $L_{[1:\beta]}$ is reduced by the first `Pump`, the next `Pump` will be used to do the reduction on $L_{[1+J:J+\beta]}$. However, unlike the Slide BKZ [11] which can be considered as BKZ with jump value equals β. The jump value J in Pnj-BKZ(β, J) is flexible to adjust witin $[1,\ \beta]$. So Pnj-BKZ(β, J) algorithm is different from Slide BKZ [11].

The Pnj-BKZ algorithm is efficient in solving α-SVP in practice. Recently many lattice challenge records are cracked by using Pnj-BKZ algorithm, such as the TU Darmstadt LWE Challenges: [1] $(n, \alpha) \in \{(40, 0.035), (90, 0.005), (50, 0.025), (55, 0.020), (40, 0.040)\}$, TU Darmstadt SVP Challenges[2] dimensions from 180 up to 186, and TU Darmstadt Ideal Challenges[3] 750-dimension approximate-SVP. Therefore, the study of the reduction effect of the Pnj-BKZ algorithm is crucial to accurately measure the concrete hardness of α-SVP which characterizes the security of the lattice cryptographic schemes.

To simulate the reduction effect of the Pnj-BKZ algorithm, the Pnj-BKZ simulator [28] and its optimized version [27] was proposed which is a polynomial

---

[1] `https://www.latticechallenge.org/lwe_challenge/challenge.php`

[2] `https://www.latticechallenge.org/svp-challenge/halloffame.php`

[3] `https://latticechallenge.org/ideallattice-challenge/index.php`

time the simulator of pnj-BKZ can predict how the length of Gram-Schmidt lattice basis vectors change during the process of running each tour of Pnj-BKZ(β, J) without actually running Pnj-BKZ(β, J). Pnj-BKZ(β, J) is an exponential time algorithm with respect to blocksize β.

However, there is no theoretical analysis like the analysis in [14] and [19] to analyze the upper bound of the approximate factor that Pnj-BKZ(β, J) can achieve in solving α-SVP. More specifically to study lattice reduction algorithms like BKZ-β can solve α-SVP with how small the approximation factor α, many analyses are proposed. In 2011, Hanrot et al. [14] analyzed a certain variant BKZ' of BKZ by dynamic systems. Their results show that after a polynomial number of tours reduction of BKZ'-β, the shortest vector output from BKZ'-β has norm smaller than $2\gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det L)^{\frac{1}{d}}$. In 2020, Li and Nguyen [19] present the first rigorous dynamic analysis of BKZ rather than BKZ'. They proves that after at most $\Theta\left(\frac{d^2}{\beta^2}\log d\right)$ tours reduction of BKZ-β, the Euclidean norm of the first basis vector output from BKZ-β at most $\gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2d(\beta-1)}} \cdot (\det L)^{\frac{1}{d}}$. In 2022, Li and Walter [20] give a rigorous dynamic analysis of Slide BKZ [11]. Slide BKZ is similar to a BKZ with jump, but the jump value J equals the blocksize β in Slide BKZ.

1.1 Contribution

In this paper, we use the dynamical system to analyze the upper bound of the approximate factor in solving α-SVP by using how many tours reduction of Pnj-BKZ(β, J). Here the jump value $J \in [1, \beta]$ rather than $J = \beta$ as that of Slide BKZ [11]. Besides, we focus on a slightly modified ideal variant Pnj-BKZ'(β, J) instead original version of Pnj-BKZ(β, J) algorithm. We construct the dynamical system of Pnj-BKZ' by using the sandpile model and use it to give the first dynamical analysis of an ideal version of Pnj-BKZ'. Our results show that:

Set L be the lattice spanned by $(\mathbf{a}_i)_{i\le d}$. The shortest vector $\mathbf{b}_1$ output by running $C\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)$ tours reduction of Pnj-BKZ'(β, J), which satisfied that $\|\mathbf{b}_1\| \le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2} \cdot (\det L)^{\frac{1}{d}}$. See Table 1 for the details about comparison with other works. From Table 1, we can see that with the same block size β, although the time cost of one tour of Pnj-BKZ(β, J) is only $1/J$ times the time cost of BKZ. However, with the same block size β, when J is greater than 1, the full reduction effect of Pnj-BKZ is not as good as that of BKZ or that of Slide reduction. Therefore, J can be regarded as a new trade-off parameter of the BKZ type lattice reduction algorithm in addition to the block size β, which balances the reduction quality of Pnj-BKZ reduction and the time cost of Pnj-BKZ.

Table 1: Comparison with other works

Technique	GN08[11]	LW23[20]
Algorithm	Slide reduction	Slide reduction
$\|\mathbf{b}_1\|/\lambda_1(L)$	$\leq ((1+\varepsilon)\gamma_\beta)^{(d-\beta)/(\beta-1)}$	$\leq (1+\varepsilon)\gamma_\beta^{\frac{d-1}{2(\beta-1)}}$
Convergence needed Tours	no	$O\left(\frac{d^3 \ln \frac{d}{\varepsilon}}{\beta^2}\right)$
Discrete dynamical systems	no	yes
Technique	HPS11[14]	LN20[19]
Algorithm	BKZ'	BKZ
$\|\mathbf{b}_1\|/\lambda_1(L)$	$\leq 2\gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{3}{2}}$	$\leq \gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2d(\beta-1)}}$
Convergence needed Tours	$\Theta\left(\frac{d^3}{\beta^2}\left(\log d + \log\log \max_i \|\mathbf{b}_i\|\right)\right)$	$\Theta\left(\frac{d^2}{\beta^2}\log d\right)$
Discrete dynamical systems	yes	yes
Technique	Our	
Algorithm	Pnj-BKZ'	
$\|\mathbf{b}_1\|/\lambda_1(L)$	$\leq \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2}$	
Convergence needed Tours	$\Theta\left(\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)\right)$	
Discrete dynamical systems	yes	

2 Preliminaries

2.1 Notations and Basic Definitions

We use $\mathbf{J}_{i,j}$ to represent all-ones matrix where every entry is equal to 1 with i rows and j columns, $\mathbf{0}_{i,j}$ represent $i \times j$ zero matrix, $i,\ j \in \mathbb{N}^*$.

Definition 1 (Lattice). *A lattice L is generated by a basis $\mathbf{B}$ which is a set of linearly independent vectors $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^m$. We will refer to it as $L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^n z_i \mathbf{b}_i, z_i \in \mathbb{Z}\}$. In this paper the length of $\mathbf{v} \in \mathbb{R}^m$ is the Euclidean norm $\|\mathbf{v}\|_2$.*

A non-zero vector in a lattice L that has the minimum norm is called the shortest vector. We use $\lambda_1(L)$ to denote the norm of the shortest vector.

Definition 2. *(α-approximate Shortest Vector Problem(α-SVP)) Given an arbitrary basis $\mathbf{B}$ on lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$, find the shortest non-zero vector $\mathbf{v}$ s.t. $\|\mathbf{v}\| = \alpha \cdot \lambda_1(L)$.*

Definition 3 (Gram-Schmidt Basis and Projective Sublattice). *For a given lattice basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$, we define its Gram-Schmidt orthogonal basis $\mathbf{B}^* := (\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*)$ by $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^*$ for $1 \leq j < i \leq n$, where $\mu_{ij} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$ are the Gram-Schmidt coefficients (abbreviated as GS-coefficients). In this paper we use l_i to represent the value of $\log(\|\mathbf{b}_i^*\|)$. The lattice determinant is defined as $\det(L(\mathbf{B})) := \prod_{i=1}^n \|\mathbf{b}_i^*\|$ and it is equal to the volume $vol(L(\mathbf{B}))$*

of the fundamental parallelepiped. We denote the orthogonal projection by $\pi_i : \mathbb{R}^m \to span(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$ *for* $i \in \{1, 2, \ldots, n\}$*. We denote the local block of the projective sublattice* $L_{[i:j]} := L(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_j))$*, for* $j \in \{i, i+1, \ldots, n\}$*.*

The notion of the norm of the shortest vector is also defined for a projective sublattice as $\lambda_1(L_{[i:j]})$.

Heuristic 1 (Gaussian Heuristic) *Given an* n*-dimensional lattice* L *with determinant* $\det(L)$*, the Gaussian heuristic predicts that there are around* $\mathrm{vol}(C) / \det(L)$ *many lattice points in a measurable subset* C *in* $\mathbb{R}^n$*.*

In addition, the length of the shortest vector can be approximated by the radius of a sphere whose volume is $\det(L)$. This is usually called the Gaussian heuristic of a lattice. Under Gaussian heuristic, it can be denoted as $\lambda_1(L) = \mathrm{GH}(L) = \det(L)^{1/n} / V_n(1)^{1/n}$, where $V_n(1)$ is the volume of unit ball of dimension n. Besides $\mathrm{GH}(L) = \det(L)^{1/n} / V_n(1)^{1/n}$ is usually approximated to $\sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}$ by using Stirling's formula.

Definition 4 (Hermite-Korkine-Zolotarev (HKZ) Reduction). *A lattice basis is HKZ reduced, if it is size reduced and all Gram-Schmidt vectors satisfy* $\|\mathbf{b}_i^*\| = \lambda_1(L_{[i,d]})$*, where* d *is dimension of lattice.*

Heuristic 2 (Sandpile Model Assumption (SMA) [14]) *For any HKZ reduced basis* $(b_i)_{i \le \beta}$*,* $x_i = \frac{1}{2} \ln \gamma_{\beta-i+1} + \frac{1}{\beta-i+1} \sum_{j=i}^{\beta} x_j$ *for all* $i \le \beta$ *with* $(x_i = log\|\mathbf{b}_i^*\|)_{i \le \beta}$*.*

Here γ_i in Heuristic 2 is the i-dimension Hermite's constant which equals to $\frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{dim(L)}}}$. In this paper we use $\frac{dim(L)}{2\pi e}$ to approximate this $\gamma_{dim(L)}$.

Under SMA, once $\sum_i x_i$ (*i.e.*, $|\det(b_i)_i|$) is fixed, the $(x_i = log\|\mathbf{b}_i^*\|)_{i \le \beta}$ of an HKZ-reduced basis is uniquely determined.

Definition 5 (Hermit factor). *A* d*-dimensional lattice with basis* $\mathbf{B}$*, the Hermite factor of* $L(\mathbf{B})$*:* $\mathrm{HF}(\mathbf{B}) = \|\mathbf{b}_1\| / \det(L)^{\frac{1}{d}}$ *is one of quality measurement for a lattice basis* $\mathbf{B}$ *which is reduced by lattice reduction algorithm. And the root Hermite factor (rhf) is defined as* $\mathrm{HF}(\mathbf{B})^{\frac{1}{d}}$*.*

Definition 6 (Characteristic Polynomial). *The characteristic polynomial* $\chi(\mathbf{A})$ *of a matirx* $\mathbf{A}$ *is the polynomial defined as:* $\det(\mathbf{A} - \lambda\mathbf{I})$*, where matirx* $\mathbf{A}$ *is a square matrix and* $\mathbf{I}$ *is the identity matrix of identical dimension.*

2.2 Pump and Jump BKZ Algorithm

Pnj-BKZ is a BKZ-type reduction algorithm that uses `Pump` as its SVP oracle. However, `Pump` can return not only one short vector but many short vectors and insert them at different positions to obtain an almost HKZ-reduced basis.

Specifically, inputting a projected sublattice basis $\mathrm{B}_{\pi[\kappa,r]}$, after the reduction of `Pump`, the output $\mathrm{B}_{\pi[\kappa,r]}$ by `Pump`($\mathrm{B}_{\pi[\kappa,r]}, \kappa, \beta, f$) is an almost HKZ reduced basis. Here f is a dimension for free function related to block size β and the information about the dimension for free technology can be seen in [8]]. More detail about `Pump` can be found in Algorithm 1 or the description of `Pump` in Section 4.1 of G6K[3].

Algorithm 1 `Pump`

Input: $\mathbf{B}, \kappa, \beta, ds = f, \mathrm{stn} = 30$
Output: $\mathbf{B}$

```
r := κ + β; l := max{κ + f + 1, r − stn}; ilb := κ; L := ∅;
B_π[κ,r] := LLL(B_π[κ,r]);
//Phase="init";
L := gauss sieve(B_π[l,r], L);
//Phase="up";
while l > κ + f do
    L := {EL(v, 1) | v ∈ L}, l := l − 1;
    L := sieve(B_π[l,r], L);
end while
//Phase="down";
while d > 1 & ilb < κ + ds do
    BL := best lifts(L); //score all the vectors in best lifts list of L, and
  score each v_i with score(v_i) := θ^{−i} ‖v_i‖ / ‖b_i^*‖;
    if BL ≠ ∅ then
        ii := BL.index(max(BL));//Find the best scoring position;
        Insert v_ii into the basis B_π[κ,r];
        ilb := ii + 1;
    else
        L := {SL(v, 1) | v ∈ L};
    end if
    L := sieve(B_π[l,r], L);
    l := l + 1;
end while
return B
```

Besides unlike classical BKZ, Pnj-BKZ performs `Pump` with an adjustable `jump` which can be bigger than 1. Specifically, PnjBKZ runs each `Pump` with blocksize β and `jump`=J, after a certain block $\mathbf{B}_{[i:i+\beta]}$ is reduced by `Pump`, the next `Pump` will be executed on the $\mathbf{B}_{[i+J:i+\beta+J]}$ block with a `jump` count J rather than $\mathbf{B}_{[i+1:i+\beta+1]}$. More detail can be seen in Algorithm 2. In addition, the jump value J in Pnj-BKZ(β, J) is within the range $[1, \beta]$. When $J = \beta$, it is similar to Slide BKZ[11]. However, when one uses Pnj-BKZ(β, J) to do the reduction of a d-dimension lattice basis in practice, usually there is the following relationship: $J \ll \beta \leq d$. Since the inserting area of each `Pump` is at most the value of dimension for free d4f(β) (Eq.(1)) according to entire block size β. To ensure the output lattice basis of each `Pump` is almost HKZ-reduced lattice basis, one needs $J \leq \mathrm{d4f}(\beta)$. Eq.(1) shows the dimension for free value used in the implementation of G6K([3],[10]). In other words, to ensure the output lattice basis of each `Pump` is almost HKZ-reduced lattice basis, under the dimension for free value setting in G6K, $J \leq 0.076\beta \ll \beta \leq d$ when β is bigger enough.

$$\mathrm{d4f}(\beta) = \begin{cases} 0, & \beta < 40 \\ \lfloor \frac{\beta-40}{2} \rfloor, & 40 \leq \beta \leq 75 \\ \lfloor 11.5 + 0.075\beta \rfloor, & \beta > 75. \end{cases} \tag{1}$$

Algorithm 2 Pump and jump BKZ

Input: $\mathbf{B}$, β, f_{extra}, $jump = J$
Output: $\mathbf{B}^{'}$

$f := min\left\{max\left\{0, \frac{\beta-40}{2}\right\}, \lfloor 11.5 + 0.075\beta \rfloor\right\} + f_{extra}$;
$ds := f + 3$; $\beta := \beta + f_{extra}$;
$\mathbf{B}$=LLL$(\mathbf{B})$;
for $i \in \left\{1, \ldots, \frac{d+2f-\beta}{jump}\right\}$ **do**
  if $1 \leq i \leq \frac{f+1}{jump}$ **then**
    $\kappa, \beta', f' := 1, \beta - f + jump \cdot i - 1, jump \cdot i - 1$
  else if $\frac{f+1}{jump} \leq i \leq \frac{d-\beta+f}{jump}$ **then**
    $j := jump \cdot i - f$
    $\kappa, \beta', f' := j, \beta, f$
  else
    $j := jump \cdot i - (d - \beta + f)$
    $\kappa,\ \beta',\ f' := d - \beta + j,\ \beta - j + 1,\ f - j + 1$
  end if
  $\mathbf{B}_{\pi[k:\beta'+k-1]} \cdot \mathbf{v}_i =$ `Pump` $\left(\mathbf{B}_{\pi[k:\beta'+k-1],\kappa,\beta',f',ds}\right)$
  $\mathbf{B}$=LLL$(\mathbf{B})$
end for
$\mathbf{B}^{'}$=`Pump` $(\mathbf{B}, d - \beta + f + 1, \beta, f)$
return $\mathbf{B}^{'}$

One can obtain an (almost) HKZ reduced basis, by turning on sieving during the Pump-down stage, which has actually already been the default operation in the implementation of G6K-GPU[10]. After turning on sieving during the Pump-down stage the output projected basis of pnj-BKZ(β, J) is very close to an HKZ reduction. More detail about the reduction effect of a `Pump` can be seen in the description of `Pump` in Section 4.1 of G6K[3].

3 Analysis of Pnj-BKZ' in the Sandpile Model

Although the output of a `Pump` is very close to the HKZ reduced basis, it is still not strictly equal to the HKZ reduced basis. In this paper, we will not analyze the original Pnj-BKZ algorithm used in practice, but we will focus on a slightly modified ideal variant instead. That is to say, when each `Pump` called by Pnj-BKZ algorithm, the input projected sublattice basis $\mathrm{B}_{\pi[\kappa,\kappa+\beta]}$, after the reduction of `Pump`$(\mathrm{B}_{\pi[\kappa,\kappa+\beta]}, \kappa, \beta, f)$ is strictly satisfied the property of HKZ reduced basis.

3.1 The sandpile model and dynamical system in Pnj-BKZ'

Heuristic 3 (Ideal `Pump` variant: `Pump'`) *A projected sublattice basis* $\mathrm{B}_{\pi[\kappa,\kappa+\beta]}$ *after the reduction of* `Pump`'$(\mathrm{B}_{\pi[\kappa,\kappa+\beta]}, \kappa, \beta, f)$ *strictly satisfied the property of HKZ reduced basis (Definition 4), for all* $\kappa \in \{1, ..., d-\beta+1\}$*, dimension of entire lattice basis* B *is* d*.*

Then we call a Pnj-BKZ which replaces `Pump` by `Pump`' as Pnj-BKZ'. In this paper, we focus on the analysis of this slightly modified ideal variant of Pnj-BKZ instead.

Under Heuristic 3, the lattice basis $L_{[i:i+\beta-1]}$ reduced by a `Pump`' is a HKZ reduced lattice basis. Let $L^{'}_{[i:i+\beta-(i-1 \bmod J)]}$ or $L^{'}_{[i:d]}$ be the projected sub-lattice after l_j for all $j \in [1, i-1]$ have been replaced during the previous embedding.

Under Sandpile Model Assumption [14] (Heuristic 2), after one tour reduction of Pnj-BKZ'(β, J), new $l^{'}_i$ can be expressed as:

$$l^{'}_i = \begin{cases} \ln \mathrm{GH}\left(L^{'}_{[i:i+\beta-(i-1 \bmod J)]}\right) & , i \in [1, d-\beta] \\ \ln \mathrm{GH}\left(L^{'}_{[i:d]}\right) & , i \in [d-\beta+1, d] \end{cases} \tag{2}$$

We set a_i as:

$$a_i = \begin{cases} \ln\left(\sqrt{\frac{\beta-(i-1 \bmod J)}{2\pi e}}\right) & , i \in [1, d-\beta] \\ \ln\left(\sqrt{\frac{d-i+1}{2\pi e}}\right) & , i \in [d-\beta+1, d] \end{cases} \tag{3}$$

Using Stirling's approximation, Eq.(2) can be written as:

$$l^{'}_i \approx \begin{cases} a_i + \frac{1}{\beta-(i-1 \bmod J)} \ln\left(\mathrm{vol}\left(L^{'}_{[i:i+\beta-(i-1 \bmod J)]}\right)\right), \ i \in [1, d-\beta] \\ a_i + \frac{1}{d-i+1} \ln\left(\mathrm{vol}\left(L^{'}_{[i:d]}\right)\right), \ i \in [d-\beta+1, d] \end{cases} \tag{4}$$

Set $c_i = \ln\left(\sqrt{\frac{i}{2\pi e}}\right)$, $(l'_i)^{(k)}_i$ be the ln value of the length of Gram-Schmidt vectors after k-th `Pump`'$(\kappa = 1+(\alpha-1)J, \beta)$ reduction. $k \in \left[1, \ldots, \left\lceil \frac{d-\beta}{J} \right\rceil\right]$, based on Eq.(4), it gives that:

$$l^{'(1)}_1 = c_\beta + \frac{1}{\beta}\sum_{i=1}^{\beta} l^{(0)}_i \tag{5}$$

Since after $l_1^{(0)}$ changed to $l_1^{'(1)}$, all $l_i^{(0)}$ for $i \in [2, d]$ will change to some $l_i^{\star(0)}$ and such change is hard to predicate. However the value of vol$\left(L_{[1:\beta]}\right)$ will not change after $l_1^{(0)}$ changed to $l_1^{'(1)}$, so we can predict $l_2^{'(1)}$ by calculating $l_2^{'(1)} = c_{\beta-1} + \frac{1}{\beta-1}\sum_{i=2}^{\beta} l_i^{\star(0)}$ by $l_2^{'(1)} = c_{\beta-1} + \frac{1}{\beta-1}\left(\sum_{i=1}^{\beta} l_i^{(0)} - l_1^{'(1)}\right)$. Since $\ln\left(\text{vol}\left(L'_{[2:\beta]}\right)\right) = \ln\left(\text{vol}\left(L_{[1:\beta]}\right)\right) - l_1^{'(1)}$.

Combined with Eq.(5), $l_2^{'(1)}$ can be written as:

$$l_2^{'(1)} = c_{\beta-1} + \frac{1}{\beta-1}\left(\sum_{i=1}^{\beta} l_i^{(0)} - c_\beta - \frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)}\right) = c_{\beta-1} - \frac{1}{\beta-1}c_\beta + \frac{1}{\beta}\left(\sum_{i=1}^{\beta} l_i^{(0)}\right) \tag{6}$$

Lemma 1. *For $j \in [2, ..., \beta-1]$, Eq.(7) holds.*

$$l_j^{'(1)} = \frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} + c_{\beta-j+1} - \sum_{k=1}^{j-1}\frac{1}{\beta-k}c_{\beta-k+1} \tag{7}$$

Proof. $l_2^{'(1)}$ already satisfied Eq.(7). Since $l_{j+1}^{'(1)} = c_{\beta-j} + \frac{1}{\beta-j}\left(\sum_{i=1}^{\beta} l_i^{(0)} - \sum_{k=1}^{j} l_k^{'(1)}\right)$, we obtain that:

$$l_{j+1}^{'(1)} = c_{\beta-j} + \frac{1}{\beta-j}\left[\sum_{i=1}^{\beta} l_i^{(0)} - \sum_{k=1}^{j}\left(\frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} + c_{\beta-k+1} - \sum_{s=1}^{k-1}\frac{1}{\beta-s}c_{\beta-s+1}\right)\right]$$

$$l_{j+1}^{'(1)} = c_{\beta-j} + \frac{1}{\beta-j}\left[\frac{\beta-j}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} - \sum_{k=1}^{j}\left(c_{\beta-k+1} - \sum_{s=1}^{k-1}\frac{1}{\beta-s}c_{\beta-s+1}\right)\right]$$

$$l_{j+1}^{'(1)} = \frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} + c_{\beta-j} + \frac{1}{\beta-j}\left(-\sum_{k=1}^{j} c_{\beta-k+1} + \sum_{k=1}^{j}\sum_{s=1}^{k-1}\frac{1}{\beta-s}c_{\beta-s+1}\right)$$

$$l_{j+1}^{'(1)} = \frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} + c_{\beta-j} + \frac{1}{\beta-j}\left(-\sum_{k=1}^{j} c_{\beta-k+1} + \sum_{k=1}^{j}\frac{j-k}{\beta-k}c_{\beta-k+1}\right)$$

$$l_{j+1}^{'(1)} = \frac{1}{\beta}\sum_{i=1}^{\beta} l_i^{(0)} + c_{\beta-j} - \sum_{k=1}^{j}\frac{1}{\beta-k}c_{\beta-k+1}$$

Therefore, Eq.(7) is held by induction proving. □

Besides, since β-dimensional Pump'($\kappa = 1, \beta$) only affect the GS values in $L_{[1:\beta]}$, for these rest of GS values we have the same conclusion as that in [14]:

$$j \in [1, d] \setminus [1, \beta],\ l_j^{'(1)} = l_j^{(0)} \tag{8}$$

Combining the Eq.(7) and Eq.(8) together shows how these ln values of the length of Gram-Schmidt vectors change after one reduction of a β-dimensional Pump'($\kappa = 1, \beta$) on lattice basis $L_{[1:\beta]}$. Based on Eq.(7) and Eq.(8), $\forall j \in [1:d]$ we can give the estimation of how Gram-Schmidt lengths $l_j^{(original)}$ change to $l_j^{(new)}$ after the reduction of a β-dimensional Pump'(κ, β) on any position $\kappa = i \in [1, d - \beta + 1]$.

$$l_j^{(new)} = \begin{cases} \frac{1}{\beta}\sum_{j=i}^{i+\beta-1} l_i^{(original)} + c_{\beta-j+1} - \sum_{k=1}^{j-1}\frac{1}{\beta-k}c_{\beta-k+1}, & j \in [i, i+\beta-1] \\ l_j^{(original)}, & j \in [1, d] \setminus [i, i+\beta-1] \end{cases} \tag{9}$$

Based on Eq.(9), we can give the discrete-time linear dynamical system of Pnj-BKZ'. During one tour reduction of a Pnj-BKZ'-(β, J), it will call $\left\lceil \frac{d-\beta}{J} \right\rceil$ time Pump' whose first index κ as $\kappa \in \left\{1, 1+J, 1+2J, ..., 1+\left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d-\beta+1\}$.

Let $\mathbf{x} = (l_i)_i$, $(l_i)_i^{(\alpha)}$ be the ln value of the length of Gram-Schmidt vectors after α-th Pump'($\kappa = 1 + (\alpha - 1)J, \beta$) reduction, $\mathbf{x}^{(\alpha)} = (l_i)_i^{(\alpha)}$, $\alpha \in \left[1, 2, \ldots, \left\lceil \frac{d-\beta}{J} \right\rceil\right]$. Then we know that $\forall i \in \left\{1, 1+J, 1+2J, ..., 1+\left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d-\beta+1\}$ and, $\mathbf{x}^{(1+\lfloor \frac{i}{J} \rfloor)} = \mathbf{A}^{(i)} \cdot \mathbf{x}^{(\lfloor \frac{i}{J} \rfloor)} + \mathbf{c}^{(i)}$ with:

$$\mathbf{A}^{(i)} = \begin{pmatrix} \ddots & & & & & \\ & 1 & & & & \\ & & \frac{1}{\beta} & \cdots & \frac{1}{\beta} & & \\ & & \vdots & \ddots & \vdots & & \\ & & \frac{1}{\beta} & \cdots & \frac{1}{\beta} & & \\ & & & & & 1 & \\ & & & & & & \ddots \end{pmatrix} \begin{matrix} \\ \\ (i) \\ \\ (i+\beta-1) \\ \\ \\ \end{matrix}$$

and $\mathbf{c}_j^{(i)} = \begin{cases} 0, & j < i \\ c_{\beta-j} - \sum_{k=1}^{j-1}\frac{c_{\beta-k+1}}{\beta-k}, & j \in [i, i+\beta-1] \\ 0, & i+\beta \le j \end{cases}$. It can be seen that the dynamic system of Pnj-BKZ' actually only has part of the matrix $\mathbf{A}^{(i)}$ that $i \equiv 1 \pmod{J}$ in the dynamic system of BKZ'[14].

The effect of Pnj-BKZ' tour on $\mathbf{x}$ is $\mathbf{Ax} + \mathbf{c}$ with $\mathbf{c} =$

$$\mathbf{c}^{(d-\beta+1)} + \mathbf{A}^{(d-\beta+1)}\left[\mathbf{c}^{\left(1+\lfloor \frac{d-\beta}{J} \rfloor \cdot J\right)} + \mathbf{A}^{\left(1+\lfloor \frac{d-\beta}{J} \rfloor \cdot J\right)}\left(\mathbf{c}^{\left(1+\lfloor \frac{d-\beta}{J} \rfloor \cdot J - J\right)} + \mathbf{A}^{\left(1+\lfloor \frac{d-\beta}{J} \rfloor \cdot J - J\right)} \cdot (\cdots)\right)\right]$$

and $\mathbf{A} = \mathbf{A}^{(d-\beta+1)} \cdot \mathbf{A}^{\left(1+\lfloor \frac{d-\beta}{J} \rfloor \cdot J\right)} \cdot \ldots \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)}$.

We use $\mathbf{J}_{i,j}$ to represent all-ones matrix where every entry is equal to 1 with i rows and j columns, $\mathbf{0}_{i,j}$ represent $i \times j$ zero matrix, and $\mathbf{I}_n$ represent n-dimensional identity matrix. It is easy to get that:

$$\mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} = \begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-J} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,\beta} & \frac{1}{\beta}\mathbf{J}_{\beta,J} & \mathbf{0}_{\beta,d-\beta-J} \\ \mathbf{0}_{d-\beta-J,\beta} & \mathbf{0}_{d-\beta-J,J} & \mathbf{I}_{d-\beta-J,d-\beta-J} \end{pmatrix},$$

$$\mathbf{A}^{(1+2J)} \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} = \begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-2J} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{\beta,d-\beta-2J} \\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{\beta,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,J} & \frac{1}{\beta}\mathbf{J}_{\beta,J} & \mathbf{0}_{\beta,d-\beta-2J} \\ \mathbf{0}_{d-\beta-2J,\beta} & \mathbf{0}_{d-\beta-2J,J} & \mathbf{0}_{d-\beta-2J,J} & \mathbf{I}_{d-\beta-2J,d-\beta-2J} \end{pmatrix},$$

We can set $\mathbf{A}^{(1+(k-1)J)} \cdot \cdots \cdot \mathbf{A}^{(1+2J)} \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} =$

$$\begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-(k-1)J} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-(k-1)J} \\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \frac{1}{\beta}\mathbf{J}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-(k-1)J} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{J,\beta} & \frac{(\beta-J)^{k-3}}{\beta^{k-2}}\mathbf{J}_{J,J} & \frac{(\beta-J)^{k-4}}{\beta^{k-3}}\mathbf{J}_{J,J} & \cdots & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-(k-1)J} \\ \frac{(\beta-J)^{k-1}}{\beta^{k}}\mathbf{J}_{\beta,\beta} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{\beta,J} & \frac{(\beta-J)^{k-3}}{\beta^{k-2}}\mathbf{J}_{\beta,J} & \cdots & \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,J} & \frac{1}{\beta}\mathbf{J}_{\beta,J} & \mathbf{0}_{J,d-\beta-(k-1)J} \\ \mathbf{0}_{d-\beta-(k-1)J,\beta} & \mathbf{0}_{d-\beta-(k-1)J,J} & \mathbf{0}_{d-\beta-(k-1)J,J} & \cdots & \mathbf{0}_{d-\beta-(k-1)J,J} & \mathbf{0}_{d-\beta-(k-1)J,J} & \mathbf{I}_{d-\beta-(k-1)J,d-\beta-(k-1)J} \end{pmatrix}$$

It is hold for $k = 1, 2, 3$. Then $\mathbf{A}^{(1+kJ)} \cdot \mathbf{A}^{(1+(k-1)J)} \cdot \cdots \cdot \mathbf{A}^{(1+2J)} \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} =$
$\begin{pmatrix} \mathbf{I}_{kJ,kJ} & \mathbf{0}_{kJ,\beta} & \mathbf{0}_{kJ,d-\beta-kJ} \\ \mathbf{0}_{\beta,kJ} & \mathbf{J}_{\beta,\beta} & \mathbf{0}_{\beta,d-\beta-kJ} \\ \mathbf{0}_{d-\beta-kJ,kJ} & \mathbf{0}_{d-\beta-kJ,\beta} & \mathbf{I}_{d-\beta-kJ,d-\beta-kJ} \end{pmatrix} \cdot \mathbf{A}^{(1+(k-1)J)} \cdot \cdots \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} =$

Finally, we have: $\mathbf{A}^{(1+kJ)} \cdot \mathbf{A}^{(1+(k-1)J)} \cdot \cdots \cdot \mathbf{A}^{(1+2J)} \cdot \mathbf{A}^{(1+J)} \cdot \mathbf{A}^{(1)} =$

$$\begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-kJ} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-kJ} \\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \frac{1}{\beta}\mathbf{J}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-kJ} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{(\beta-J)^{k-1}}{\beta^{k}}\mathbf{J}_{J,\beta} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{J,J} & \frac{(\beta-J)^{k-3}}{\beta^{k-2}}\mathbf{J}_{J,J} & \cdots & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-\beta-kJ} \\ \frac{(\beta-J)^{k}}{\beta^{k+1}}\mathbf{J}_{\beta,\beta} & \frac{(\beta-J)^{k-1}}{\beta^{k}}\mathbf{J}_{\beta,J} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{\beta,J} & \cdots & \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,J} & \frac{1}{\beta}\mathbf{J}_{\beta,J} & \mathbf{0}_{\beta,d-\beta-kJ} \\ \mathbf{0}_{d-\beta-kJ,\beta} & \mathbf{0}_{d-\beta-kJ,J} & \mathbf{0}_{d-\beta-kJ,J} & \cdots & \mathbf{0}_{d-\beta-kJ,J} & \mathbf{0}_{d-\beta-kJ,J} & \mathbf{I}_{d-\beta-kJ,d-\beta-kJ} \end{pmatrix}$$

When $d - \beta \equiv 0 (mod\ J)$, set $k = \frac{d-\beta}{J}$, we have:

$$\mathbf{A} = \begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} \\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \frac{1}{\beta}\mathbf{J}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{(\beta-J)^{k-1}}{\beta^{k}}\mathbf{J}_{J,\beta} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{J,J} & \frac{(\beta-J)^{k-3}}{\beta^{k-2}}\mathbf{J}_{J,J} & \cdots & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} \\ \frac{(\beta-J)^{k}}{\beta^{k+1}}\mathbf{J}_{\beta,\beta} & \frac{(\beta-J)^{k-1}}{\beta^{k}}\mathbf{J}_{\beta,J} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{\beta,J} & \cdots & \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,J} & \frac{1}{\beta}\mathbf{J}_{\beta,J} \end{pmatrix} \tag{10}$$

When $d-\beta \neq 0(mod\ J)$, set $k = \left\lfloor \frac{d-\beta}{J} \right\rfloor$, we also have $\mathbf{A} :=$

$$\begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{J,\beta} & \mathbf{0}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-kJ-\beta} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-kJ-\beta} \\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \cdots & \mathbf{0}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-kJ-\beta} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{(\beta-J)^{k-1}}{\beta^k}\mathbf{J}_{J,\beta} & \frac{(\beta-J)^{k-2}}{\beta^{k-1}}\mathbf{J}_{J,J} & \cdots & \frac{1}{\beta}\mathbf{J}_{J,J} & \mathbf{0}_{J,J} & \mathbf{0}_{J,d-kJ-\beta} \\ \frac{(\beta-J)^k}{\beta^{k+1}}\mathbf{J}_{d-kJ-\beta,\beta} & \frac{(\beta-J)^{k-1}}{\beta^k}\mathbf{J}_{d-kJ-\beta,J} & \cdots & \frac{\beta-J}{\beta^2}\mathbf{J}_{d-kJ-\beta,J} & \frac{1}{\beta}\mathbf{J}_{d-kJ-\beta,J} & \mathbf{0}_{d-kJ-\beta,d-kJ-\beta} \\ \frac{(\beta-J)^k\cdot(kJ+2\beta-d)}{\beta^{k+2}}\mathbf{J}_{\beta,\beta} & \frac{(\beta-J)^{k-1}\cdot(kJ+2\beta-d)}{\beta^{k+1}}\mathbf{J}_{\beta,J} & \cdots & \frac{(\beta-J)\cdot(kJ+2\beta-d)}{\beta^3}\mathbf{J}_{\beta,J} & \frac{kJ+2\beta-d}{\beta^2}\mathbf{J}_{\beta,J} & \frac{1}{\beta}\mathbf{J}_{\beta,d-kJ\beta} \end{pmatrix} \quad (11)$$

3.2 Solutions of the dynamical system of Pnj-BKZ'

Same proof as that in the Lemma 3 in [14], we know that if $\mathbf{A}\cdot\mathbf{x} = \mathbf{x}$ then $\mathbf{x} \in \text{span}\,(1,1,\ldots,1)^T$.

So it suffices to find one solution of $\mathbf{x} = \mathbf{A}\cdot\mathbf{x} + \mathbf{c}$ to obtain all the solutions. Set $\beta_i^{'} = \beta - (i-1\ mod\ J)$ we define $\bar{\mathbf{x}}$ as follows:

$$\bar{l}_i = \begin{cases} a_i + \frac{1}{\beta_i^{'}}\sum_{j=i}^{i+\beta_i^{'}-1}\bar{l}_j, & i \in [1,\ldots,d-\beta] \\ a_i + \frac{1}{d-i}\sum_{j=i}^{d}\bar{l}_j, & i \in [d-\beta+1,\ldots,d] \end{cases}$$

and we can get $\bar{\mathbf{x}} :=$

$$\bar{l}_i = \begin{cases} \frac{\beta_i^{'}}{\beta_i^{'}-1}a_i + \frac{1}{\beta_i^{'}-1}\sum_{j=i+1}^{i+\beta_i^{'}-1}\bar{l}_j, & i \in [1,\ldots,d-\beta] \\ \frac{\beta_i^{'}}{\beta_i^{'}-1}a_i + \frac{1}{d-i-1}\sum_{j=i+1}^{d}\bar{l}_j, & i \in [d-\beta+1,\ldots,d] \end{cases} \quad (12)$$

Lemma 2. *For $\bar{\mathbf{x}}$ as the form shown in Equ.(12), we have $\bar{\mathbf{x}} = \mathbf{A}\cdot\bar{\mathbf{x}} + \mathbf{c}$.*

Proof. Let $\bar{\mathbf{x}}$ as the length vector of initial input vector. After the reduction of first `Pump`', $\bar{l}_1^{(1)} = a_1 + \frac{1}{\beta}\sum_{j=1}^{\beta}\bar{l}_j^{(0)}$. As the definition of $\bar{\mathbf{x}}$ Equ.(12), we know that $\bar{l}_1^{(1)} = a_1 + \frac{1}{\beta}\sum_{j=1}^{\beta}\bar{l}_j^{(0)} = \bar{l}_1^{(0)}$. Therefore $\bar{l}_1^{(1)} = \bar{l}_1^{(0)}$, there is no change in the value of $\bar{l}_1$ after the reduction of first `Pump`'. Set $\bar{l}_i^{(0)} = \bar{l}_i^{(1)}$, it already hold when $i = 1$. For the case $i+1$, $\bar{l}_{i+1}^{(1)} = a_{i+1} + \frac{1}{\beta_{i+1}^{'}}\sum_{j=i+1}^{i+\beta_{i+1}^{'}}\bar{l}_j^{(0)'} = a_{i+1} + \frac{1}{\beta_{i+1}^{'}}\left(\sum_{j=1}^{i+\beta_{i+1}^{'}}\bar{l}_j^{(0)} - \sum_{j=1}^{i}\bar{l}_j^{(1)}\right) = a_{i+1} + \frac{1}{\beta_{i+1}^{'}}\left(\sum_{j=1}^{i+\beta_{i+1}^{'}}\bar{l}_j^{(0)} - \sum_{j=1}^{i}\bar{l}_j^{(0)}\right) = a_{i+1} + \frac{1}{\beta_{i+1}^{'}}\left(\sum_{j=i+1}^{i+\beta_{i+1}^{'}}\bar{l}_j^{(0)}\right)$. According to the definition of Equ.(12), we know that $\bar{l}_{i+1}^{(0)} = a_{i+1} + \frac{1}{\beta_{i+1}^{'}}\left(\sum_{j=i+1}^{i+\beta_{i+1}^{'}}\bar{l}_j^{(0)}\right)$. Therefore $\bar{l}_{i+1}^{(1)} = \bar{l}_{i+1}^{(0)}$. Then we inductive proved Lemma 2. □

We now give the lower and upper bounds for the coordinates of the solution $\bar{\mathbf{x}}$.

Lemma 3. *For all $i \leq d-\beta+1$, we have $2 \cdot \left(\frac{d-i}{\beta-J} - \frac{3}{2}\right) c_{\beta-J+1} \leq \bar{l}_i - \bar{l}_{d-\beta+1} \leq 2 \cdot \frac{d-i}{\beta-J} c_\beta$.*

Proof. We first consider the upper bound on $\bar{l}_i - \bar{l}_{d-\beta+1}$. Since $\bar{l}_{d-\beta+1} \geq \cdots \geq \bar{l}_d$, it indicates that:

$$\forall i > d-\beta,\ \bar{l}_i - \bar{l}_{d-\beta+1} \leq 0 \leq 2 \cdot \frac{d-i}{\beta-1} c_\beta$$

According to Equ.(12),

$$\bar{l}_i = \frac{\beta_i^{'}}{\beta_i^{'}-1} a_i + \frac{1}{\beta_i^{'}-1} \sum_{j=i+1}^{i+\beta_i^{'}-1} \bar{l}_j,\ i \in [1,\ldots,d-\beta]$$

$\frac{\beta_i^{'}}{\beta_i^{'}-1}$ decreases monotonically with respect to $\beta_i^{'}$. $\beta_i^{'} \in [\beta-J+1,...,\beta]$. So we obtian that:

$$\bar{l}_i \leq \frac{\beta-J+1}{\beta-J} c_\beta + \frac{1}{\beta_i^{'}-1} \sum_{j=i+1}^{i+\beta_i^{'}-1} \bar{l}_j,\ i \in [1,\ldots,d-\beta]$$

The average value $\frac{1}{\beta_i^{'}-1} \sum_{j=i+1}^{i+\beta_i^{'}-1} \bar{l}_j$ is smaller than $\frac{1}{\beta-J} \sum_{j=i+1}^{i+\beta-J} \bar{l}_j$ since $\bar{l}_i$ decreases as the index i increasing and $\beta_i^{'}-1 \geq \beta-J$. It shows that:

$$\bar{l}_i \leq \frac{\beta-J+1}{\beta-J} c_\beta + \frac{1}{\beta-J} \sum_{j=i+1}^{i+\beta-J} \bar{l}_j,\ i \in [1,\ldots,d-\beta]$$

Next, we will prove $\bar{l}_i \leq \bar{l}_{d-\beta+1} + 2 \cdot \frac{d-i}{\beta-J} c_\beta,\ \forall i \in [1,\ldots,d]$ by inductive proof.

$\forall i \in [d-\beta+1,\ldots,d]$, $\bar{l}_i \leq \bar{l}_{d-\beta+1} + 2 \cdot \frac{d-i}{\beta-J} c_\beta$ hold. Since $\bar{l}_i \leq \bar{l}_{d-\beta+1}$ and $\frac{d-i}{\beta-J} c_\beta \geq 0$. Then for the case $i = d-\beta$, from $\bar{l}_i \leq \frac{\beta-J+1}{\beta-J} c_\beta + \frac{1}{\beta-J} \sum_{j=i+1}^{i+\beta-J} \bar{l}_j$, we have:

$$\bar{l}_i \leq \frac{\beta-J+1}{\beta-J} c_\beta + \frac{1}{\beta-J} \sum_{j=i+1}^{i+\beta-J} \left(\bar{l}_{d-\beta+1} + 2 \cdot \frac{d-j}{\beta-J} c_\beta\right)$$

$$\bar{l}_i \leq \frac{\beta-J+1}{\beta-J} c_\beta + \bar{l}_{d-\beta+1} + 2 \cdot \frac{d-i-\frac{\beta-J+1}{2}}{\beta-J} c_\beta$$

$$\bar{l}_i \leq \bar{l}_{d-\beta+1} + 2 \cdot \frac{d-i}{\beta-J} c_\beta \tag{13}$$

By inductive prove, Equ.(13) hold for $\forall i \in [1,\ldots,d]$.

We now give the lower bound on $\bar{l}_i - \bar{l}_{d-\beta+1}$.

According to Equ.(12),

$$\bar{l}_i = \frac{\beta_i^{'}}{\beta_i^{'}-1} a_i + \frac{1}{\beta_i^{'}-1} \sum_{j=i+1}^{i+\beta_i^{'}-1} \bar{l}_j,\ i \in [1,\ldots,d-\beta]$$

As $\bar{l}_j$ is decreased when j is increasing. $\beta_i^{'} \in [\beta - J + 1, ..., \beta]$, for $\forall i \in [d-2(\beta-1),\ldots,d-\beta]$, $i+\beta_i^{'} \leq i+\beta$, it means $\frac{1}{\beta_i^{'}-1}\sum_{j=i+1}^{i+\beta_i^{'}-1} \bar{l}_j \geq \frac{1}{\beta-1}\sum_{j=i+1}^{i+\beta-1} \bar{l}_j$ and we obtain:

$$\bar{l}_i \geq \frac{\beta}{\beta-1} c_{\beta-J+1} + \frac{1}{\beta-1} \left(\sum_{j=i+1}^{d-\beta} \bar{l}_j + \sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \right),\ i \in [1,\ldots,d-\beta] \quad (14)$$

Next, we will prove $\bar{l}_i \geq \bar{l}_{d-\beta+1} + 2 \cdot \left(\frac{d-i}{\beta-J} - \frac{3}{2}\right) c_{\beta-J+1},\ \forall i \in [1,\ldots,d-\beta]$ by inductive proof. As $\bar{l}_j$ is decreased when j is increasing, for $\forall i \in [d-2(\beta-1),\ldots,d-\beta-J]$, we get:

$$\frac{1}{i+2\beta-d-1} \sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \geq \frac{1}{\beta-J+1} \sum_{j=d-\beta+1}^{d-J+2} \bar{l}_j$$

$\forall i \in [d-2(\beta-1),\ldots,d-\beta-J]$, since $\bar{l}_{d-\beta+1} = \mathrm{GH}\left(L_{[d-\beta+1:d]}\right) \leq \frac{1}{\beta-J+1}\sum_{j=d-\beta+1}^{d-J+2} \bar{l}_j + c_{\beta-J+1} = \mathrm{GH}\left(L_{[d-\beta+1:d-J+2]}\right)$. $\forall i \in [d-2(\beta-1),\ldots,d-\beta-J]$, we also have:

$$\frac{1}{i+2\beta-d-1} \sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \geq \frac{1}{\beta-J+1} \sum_{j=d-\beta+1}^{d-J+2} \bar{l}_j \geq \bar{l}_{d-\beta+1} - c_{\beta-J+1},$$

Since $-1 \geq 2 \cdot \frac{1}{i+2\beta-d-1}\sum_{j=d-\beta+1}^{i+\beta-1}\left(\frac{d-j}{\beta-1} - \frac{3}{2}\right)$

$$\frac{1}{i+2\beta-d-1} \sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \geq \bar{l}_{d-\beta+1} + \frac{2 \cdot c_{\beta-J+1}}{i+2\beta-d-1} \sum_{j=d-\beta+1}^{i+\beta-1} \left(\frac{d-j}{\beta-1} - \frac{3}{2}\right) \quad (15)$$

$\forall i \in [d-\beta-J,\ldots,d-\beta]$, since $\frac{1}{i+2\beta-d-1}\sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \geq \frac{1}{\beta}\sum_{j=d-\beta+1}^{d} \bar{l}_j = \bar{l}_{d-\beta+1} - c_\beta$ and $\lim_{\beta\to\infty} c_{\beta-J+1} - c_\beta = 0$ ($\beta >> J$), it gives that:

$$\frac{1}{i+2\beta-d-1} \sum_{j=d-\beta+1}^{i+\beta-1} \bar{l}_j \geq \frac{1}{\beta} \sum_{j=d-\beta+1}^{d} \bar{l}_j \geq \bar{l}_{d-\beta+1} - c_{\beta-J+1},$$

Then Eq.(15) also hold when $\forall i \in [d-\beta-J,\ldots,d-\beta]$. Therefore, $\forall i \in [d-2(\beta-1),\ldots,d-\beta]$ Eq.(15) hold.

Besides, $\forall j \in [d-2(\beta-1),\ldots,d-\beta]$, $\bar{l}_j > \bar{l}_{d-\beta+1}$ and $\sum_{j=i+1}^{d-\beta}\left(\frac{d-j}{\beta-1}-\frac{3}{2}\right) \leq 0$, we have:

$$\frac{1}{d-\beta-i}\sum_{j=i+1}^{d-\beta}\bar{l}_j \geq \bar{l}_{d-\beta+1} + \frac{2\cdot c_{\beta-J+1}}{d-\beta-i}\sum_{j=i+1}^{d-\beta}\left(\frac{d-j}{\beta-1}-\frac{3}{2}\right) \tag{16}$$

Plugging Eq.(15) and Eq.(16) into Eq.(14), it gives that:

$$\bar{l}_i \geq \frac{\beta}{\beta-1}c_{\beta-J+1} + \frac{1}{\beta-1}\left((\beta-1)\cdot\bar{l}_{d-\beta+1} + 2\cdot c_{\beta-J+1}\sum_{j=i+1}^{i+\beta-1}\left(\frac{d-j}{\beta-1}-\frac{3}{2}\right)\right)$$

$$\bar{l}_i \geq \frac{\beta}{\beta-1}c_{\beta-J+1} + 2\cdot\left(\frac{d-i-\frac{\beta}{2}}{\beta-1}-\frac{3}{2}\right)c_{\beta-J+1} + \bar{l}_{d-\beta+1}$$

$$\bar{l}_i \geq \bar{l}_{d-\beta+1} + 2\cdot\left(\frac{d-i}{\beta-1}-\frac{3}{2}\right)c_{\beta-J+1} \tag{17}$$

By inductive proving remain for $\forall i \in [1,\ldots,d-2(\beta-1)]$, we have $\forall i \in [1,\ldots,d-\beta]$, Eq.(17) hold. □

Next in Lemma 4, we give the upper bound of Hermite factor of the Pnj-BKZ' fully reduced lattice basis: $\ln \mathrm{HF}(\mathbf{B}^\infty)$. Here we set $\mathbf{B}^\infty$ as the lattice basis which is fully reduced by Pnj-BKZ'(β, J).

Lemma 4. $\ln \mathrm{HF}(\mathbf{B}^\infty) \leq \left(\frac{d-1}{\beta-J}+4\right)c_\beta \lesssim \left(\frac{d-1}{\beta-J}+4\right)\ln\sqrt{\gamma_\beta}$

Proof.

$$\ln \mathrm{HF}(\mathbf{B}^\infty) = l_1^\infty - \frac{1}{d}\sum_{i=1}^{d} l_i^\infty = l_1^\infty - l_{d-\beta+1}^\infty + l_{d-\beta+1}^\infty - \frac{1}{d}\sum_{i=1}^{d} l_i^\infty$$

Based on Lemma 3 and $\sum_{i=d-\beta+1}^{d} l_i^\infty = \beta\left(l_{d-\beta+1}^\infty - c_\beta\right) \geq \beta l_{d-\beta+1}^\infty + 2\cdot c_\beta\sum_{i=d-\beta+1}^{d}\left(\frac{d-i}{\beta-1}-\frac{3}{2}\right)$. This implies that:

$$\ln \mathrm{HF}(\mathbf{B}^\infty) \leq 2\cdot\frac{d-1}{\beta-J}c_\beta - \frac{1}{d}\left(\sum_{i=1}^{d}\left(l_i^\infty - l_{d-\beta+1}^\infty\right)\right)$$

$$\ln \mathrm{HF}(\mathbf{B}^\infty) \leq 2\cdot\frac{d-1}{\beta-J}c_\beta - \frac{1}{d}\left(\sum_{i=1}^{d}\left(2\cdot\left(\frac{d-i}{\beta-J}-\frac{3}{2}\right)c_{\beta-J+1}\right)\right)$$

$$\ln \mathrm{HF}(\mathbf{B}^\infty) \leq 2\cdot\frac{d-1}{\beta-J}c_\beta - \left(\frac{d-1}{\beta-J}-3\right)c_{\beta-J+1}$$

Meanwhile $\beta >> J$, $c_\beta - c_{\beta-J+1} = \frac{1}{2}\ln\frac{\beta}{\beta-J+1} \leq 1$, and $d = O(\beta)$, we can further obtain:

$$\ln \mathrm{HF}\left(\mathbf{B}^{\infty}\right) \leq \left(\frac{d-1}{\beta-J}+3\right)c_\beta + \frac{d-1}{\beta-J} \leq \left(\frac{d-1}{\beta-J}+4\right)c_\beta$$

Besides, $c_\beta = \ln\left(\sqrt{\frac{\beta}{2\pi e}}\right) \lesssim \ln\sqrt{\gamma_\beta}$. Finally we get

$$\ln \mathrm{HF}\left(\mathbf{B}^{\infty}\right) \leq \left(\frac{d-1}{\beta-J}+4\right)\ln\sqrt{\gamma_\beta} \tag{18}$$

□

We can see that when $J = 1$, Eq.(18) the upper bound of $\ln \mathrm{HF}\left(\mathbf{B}^{\infty}\right)$ degenerates to the form in [14].

4 Convergence speed of the Pnj-BKZ' dynamical system

In this section, we study the speed of convergence of the discrete-time dynamical system $\bar{\mathbf{x}}_{k+1} := \mathbf{A}\bar{\mathbf{x}}_k + \mathbf{c}$ (where $\mathbf{A}_d$ and $\mathbf{c}_d$ are the d-dimensional $\mathbf{A}$ and $\mathbf{c}$ respectively). According to the principle of the power iteration algorithm, the asymptotic speed of convergence of the sequence $(\mathbf{A}_d^{(k)}\bar{\mathbf{x}})_k$ is determined by the eigenvalue of $\mathbf{A}_d$. And we can bound $\left\|\mathbf{A}_d^{(k)}\bar{\mathbf{x}}\right\| \leq \left\|\mathbf{A}_d^{(k)}\right\| \|\bar{\mathbf{x}}\|$, so we mainly study largest eigenvalue of $\mathbf{A}_d^T\mathbf{A}_d$. In fact the largest eigenvalue of $\mathbf{A}_d^T\mathbf{A}_d$ is 1. In the following subsection we want to show that the second largest singular value is smaller than $1 - \frac{\beta(\beta-J)}{2Jd^2}$.

4.1 Upper bound of the second largest eigenvalue of $\mathbf{A}_d^T\mathbf{A}_d$

Set $\mathbf{M}\left[a:b, c:d\right]$ to represent the block matrix composed of elements at the intersection of the area from row a to row b of the matrix $\mathbf{M}$ and the area from columns c to column d. Firstly, based on Eq.(10), we give the form of $\mathbf{M}_d = \mathbf{A}_d^T\mathbf{A}_d$ is Eq.(19).

In fact, according to Eq.(10), we give the form of $\mathbf{M}_{\beta+(k+1)J}$ by Eq.(19) that for $k = 0, 1, \ldots, \left\lfloor\frac{d-\beta}{J}\right\rfloor$:

$$\mathbf{M}_{\beta+(k+1)J} = \mathbf{A}_{\beta+(k+1)J}^T\mathbf{A}_{\beta+(k+1)J} =$$

$$\begin{pmatrix} \frac{J}{\beta^2}\mathbf{J}_{\beta,\beta} + \frac{(\beta-J)^2}{\beta^2}\mathbf{M}_{\beta+kJ}\left[1:\beta,\ 1:\beta\right] & \frac{\beta-J}{\beta}\mathbf{M}_{\beta+kJ}\left[1:\beta,\ (\beta-J):(\beta+kJ)\right] \\ \frac{\beta-J}{\beta}\mathbf{M}_{\beta+kJ}\left[(\beta-J):(\beta+kJ),\ 1:\beta\right] & \mathbf{M}_{\beta+kJ}\left[(\beta-J):(\beta+kJ),\ (\beta-J):(\beta+kJ)\right] \end{pmatrix} \tag{19}$$

Here $\dim(\mathbf{M}_{\beta+kJ}) = \beta + kJ$.

Proof. To prove Eq.(19), one can compare the form of $\mathbf{M}_{\beta+kJ}$ and $\mathbf{M}_{\beta+(k-1)J}$. According to Eq.(10), the coefficient of the first $\beta\times\beta$ dimensional block in $\mathbf{M}_{\beta+kJ}$ is $\sum_{i=0}^{k-1}\frac{J}{\beta^2}\left(\frac{\beta-J}{\beta}\right)^{2i}+\frac{(\beta-J)^{2k}}{\beta^{2k+1}}$, while the coefficient of the first $\beta\times\beta$ dimensional block in $\mathbf{M}_{\beta+(k-1)J}$ is $\sum_{i=0}^{k-2}\frac{J}{\beta^2}\left(\frac{\beta-J}{\beta}\right)^{2i}+\frac{(\beta-J)^{2(k-1)}}{\beta^{2k-1}}$.

$\frac{J}{\beta^2}+\left(\frac{\beta-J}{\beta}\right)^2\left[\sum_{i=0}^{k-2}\frac{J}{\beta^2}\left(\frac{\beta-J}{\beta}\right)^{2i}+\frac{(\beta-J)^{2(k-1)}}{\beta^{2k-1}}\right]=\frac{J}{\beta^2}+\sum_{i=1}^{k-1}\frac{J}{\beta^2}\left(\frac{\beta-J}{\beta}\right)^{2i}+\frac{(\beta-J)^{2k}}{\beta^{2k+1}}=\sum_{i=0}^{k-1}\frac{J}{\beta^2}\left(\frac{\beta-J}{\beta}\right)^{2i}+\frac{(\beta-J)^{2k}}{\beta^{2k+1}}$. Therefore, the relationship shown in Eq.(19) holds for the first $\beta\times\beta$ dimensional block.

Meanwhile, Eq.(10) shows that

$$\mathbf{M}_{\beta+(k+1)J}\left[1:\beta,\ (\beta-J):(\beta+kJ)\right]=\frac{\beta-J}{\beta}\mathbf{M}_{\beta+kJ}\left[1:\beta,\ (\beta-J):(\beta+kJ)\right]$$

$$\mathbf{M}_{\beta+(k+1)J}\left[(\beta-J):(\beta+kJ),\ 1:\beta\right]=\frac{\beta-J}{\beta}\mathbf{M}_{\beta+kJ}\left[(\beta-J):(\beta+kJ),\ 1:\beta\right]$$

$\mathbf{M}_{\beta+(k+1)J}\left[(\beta-J):(\beta+kJ),\ (\beta-J):(\beta+kJ)\right]=\mathbf{M}_{\beta+kJ}[(\beta-J):(\beta+kJ),\ (\beta-J):(\beta+kJ)]$ □

To give a more intuitive representation of $\mathbf{M}_{\beta+kJ}$ in Eq.(19), following we give the cases of $k=1,2,3$ which are easy to calculate by using Eq.(10).

$$\mathbf{M}_{\beta+J}=\mathbf{A}_{\beta+J}^T\mathbf{A}_{\beta+J}=\begin{pmatrix}\left(\frac{J}{\beta^2}+\frac{(\beta-J)^2}{\beta^3}\right)\mathbf{J}_{\beta,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{\beta,J}\\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,\beta} & \frac{1}{\beta}\mathbf{J}_{J,J}\end{pmatrix},$$

$\mathbf{M}_{\beta+2J}=\mathbf{A}_{\beta+2J}^T\mathbf{A}_{\beta+2J}=$

$$\begin{pmatrix}\left(\frac{J}{\beta^2}+\frac{J(\beta-J)^2}{\beta^4}+\frac{(\beta-J)^4}{\beta^5}\right)\mathbf{J}_{\beta,\beta} & \left(\frac{J(\beta-J)}{\beta^3}+\frac{(\beta-J)^3}{\beta^4}\right)\mathbf{J}_{\beta,J} & \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{\beta,J}\\ \left(\frac{J(\beta-J)}{\beta^3}+\frac{(\beta-J)^3}{\beta^4}\right)\mathbf{J}_{J,\beta} & \left(\frac{J}{\beta^2}+\frac{(\beta-J)^2}{\beta^3}\right)\mathbf{J}_{J,J} & \frac{\beta-J}{\beta^2}\mathbf{J}_{.J,J}\\ \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,\beta} & \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \frac{1}{\beta}\mathbf{J}_{J,J}\end{pmatrix}$$

$\mathbf{M}_{\beta+3J}=\mathbf{A}_{\beta+3J}^T\mathbf{A}_{\beta+3J}=(\mathbf{M}_{\beta+3J}[(1:\beta+3J),(1:\beta+J)],\ \mathbf{M}_{\beta+3J}[(1:\beta+3J),(\beta+J+1):(\beta+3J)])$

$\mathbf{M}_{\beta+3J}[(1:\beta+3J),(1:\beta+J)]=$

$$\begin{pmatrix}\left(\frac{J}{\beta^2}+\frac{J(\beta-J)^2}{\beta^4}+\frac{(\beta-J)^4}{\beta^6}+\frac{(\beta-J)^6}{\beta^7}\right)\mathbf{J}_{\beta,\beta} & \left(\frac{J(\beta-J)}{\beta^3}+\frac{J(\beta-J)^3}{\beta^5}+\frac{(\beta-J)^5}{\beta^6}\right)\mathbf{J}_{\beta,J}\\ \left(\frac{J(\beta-J)}{\beta^3}+\frac{J(\beta-J)^3}{\beta^5}+\frac{(\beta-J)^5}{\beta^6}\right)\mathbf{J}_{J,\beta} & \left(\frac{J}{\beta^2}+\frac{J(\beta-J)^2}{\beta^4}+\frac{(\beta-J)^4}{\beta^5}\right)\mathbf{J}_{J,J}\\ \left(\frac{J(\beta-J)^2}{\beta^4}+\frac{(\beta-J)^4}{\beta^5}\right)\mathbf{J}_{J,\beta} & \left(\frac{J(\beta-J)}{\beta^3}+\frac{(\beta-J)^3}{\beta^4}\right)\mathbf{J}_{J,J}\\ \frac{(\beta-J)^3}{\beta^4}\mathbf{J}_{J,\beta} & \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,J}\end{pmatrix}$$

$\mathbf{M}_{\beta+3J}[(1:\beta+3J),(\beta+J+1):(\beta+3J)] =$

$$\begin{pmatrix} \left(\frac{J(\beta-J)^2}{\beta^4}+\frac{(\beta-J)^4}{\beta^5}\right)\mathbf{J}_{\beta,J} & \frac{(\beta-J)^3}{\beta^4}\mathbf{J}_{\beta,J} \\ \left(\frac{J(\beta-J)}{\beta^3}+\frac{(\beta-J)^3}{\beta^4}\right)\mathbf{J}_{J,J} & \frac{(\beta-J)^2}{\beta^3}\mathbf{J}_{J,J} \\ \left(\frac{J}{\beta^2}+\frac{(\beta-J)^2}{\beta^3}\right)\mathbf{J}_{J,J} & \frac{\beta-J}{\beta^2}\mathbf{J}_{.J,J} \\ \frac{\beta-J}{\beta^2}\mathbf{J}_{J,J} & \frac{1}{\beta}\mathbf{J}_{J,J} \end{pmatrix}$$

Let $\chi(\mathbf{M}_{\beta+i})(\lambda) = \chi_{\beta+i}(\lambda)$. Next, we give the characteristic polynomial χ_d of $\mathbf{A}_d^T\mathbf{A}_d$. For $i \geq 0$, $d = \beta + i$.

Lemma 5. *For $i \geq 2$, $d = i + \beta$, $\chi_{\beta+i}(\lambda) =$*

$$\begin{cases} 2\lambda\cdot\chi_{\beta+i-1}(\lambda) - \lambda^2\cdot\chi_{\beta+i-2}(\lambda), & i \bmod J \neq 1 \\ \left[\left(1+\left(\frac{\beta-J}{\beta}\right)^2\right)\lambda - \frac{J}{\beta^2}\right]\cdot\chi_{\beta+i-1}(\lambda) - \left(\frac{\beta-J}{\beta}\right)^2\lambda^2\cdot\chi_{\beta+i-2}(\lambda), & i \bmod J \equiv 1 \end{cases}$$

Proof. When $i \bmod J \neq 1$, according to Eq.(19), the form of $\mathbf{M}_{\beta+i}$ is:

$$\mathbf{M}_{\beta+i} = \begin{pmatrix} a & a & \mathbf{a}^T \\ a & a & \mathbf{a}^T \\ \mathbf{a} & \mathbf{a} & \mathbf{M}_{\beta+i-2} \end{pmatrix}$$

Then

$$\chi_{\beta+i}(\lambda) = \begin{vmatrix} 2\lambda & -\lambda & \mathbf{0} \\ -\lambda & \lambda - a & -\mathbf{a}^T \\ \mathbf{0} & -\mathbf{a} & \mathbf{M}_{\beta+i-2} - \lambda\mathbf{I}_{\beta+i-2} \end{vmatrix}$$

$$\chi_{\beta+i}(\lambda) = 2\lambda\cdot\chi_{\beta+i-1}(\lambda) - \lambda^2\cdot\chi_{\beta+i-2}(\lambda)$$

When $i \bmod J = 1$, the form of $\mathbf{M}_{\beta+i}$ is:

$$\mathbf{M}_{\beta+i} = \begin{pmatrix} a & b & \mathbf{b}^T \\ b & c & \mathbf{b}'^T \\ \mathbf{b} & \mathbf{b}' & \mathbf{M}_{\beta+i-2} \end{pmatrix}$$

Here according to Eq.(19), $\mathbf{b} = \frac{\beta-J}{\beta}\mathbf{b}'$, $b = \frac{\beta-J}{\beta}c$, $a = \frac{J}{\beta^2} + \frac{\beta-J}{\beta}b$, so $a = \frac{J}{\beta^2} + \left(\frac{\beta-J}{\beta}\right)^2 c$. Then $\chi(\mathbf{M}_{\beta+i})(\lambda)$ is:

$$\chi_{\beta+i}(\lambda) = \begin{vmatrix} \left[1+\left(\frac{\beta-J}{\beta}\right)^2\right]\lambda - \frac{J}{\beta^2} & -\frac{\beta-J}{\beta}\lambda & \mathbf{0} \\ -\frac{\beta-J}{\beta}\lambda & \lambda - c & -\mathbf{b}'^T \\ \mathbf{0} & -\mathbf{b}' & \mathbf{M}_{\beta+i-2} - \lambda\mathbf{I}_{\beta+i-2} \end{vmatrix}$$

$$\chi_{\beta+i}(\lambda) = \left[\left(1+\left(\frac{\beta-J}{\beta}\right)^2\right)\lambda - \frac{J}{\beta^2}\right]\cdot\chi_{\beta+i-1}(\lambda) - \left(\frac{\beta-J}{\beta}\right)^2\lambda^2\cdot\chi_{\beta+i-2}(\lambda)$$

□

Lemma 6. *For $J \geq i \geq 0$, $\chi_{\beta+i}(\lambda) = \lambda^{\beta+i-2}(\lambda-1)\left(\lambda - \frac{i^2}{\beta^2}\right)$*

Proof. $\mathbf{A}_\beta^T \mathbf{A}_\beta = \mathbf{A}_\beta$ and $\dim \ker(\mathbf{A}_\beta) = \beta - 1$, so $\lambda^{\beta-1} \mid \chi_\beta(\lambda)$. Besides, $\mathrm{Tr}(\mathbf{A}_\beta) = 1$ thus it implies that $\chi_\beta(\lambda) = \lambda^{\beta-1}(\lambda-1)$. Meanwhile, $\forall i \in \{1, 2, ..., J\}$,

$$\mathbf{A}_{\beta+i} = \begin{pmatrix} \frac{1}{\beta}\mathbf{J}_{i,\beta} & \mathbf{0}_{i,i} \\ \frac{\beta-i}{\beta^2}\mathbf{J}_{\beta,\beta} & \frac{1}{\beta}\mathbf{J}_{\beta,i} \end{pmatrix},$$

$$\mathbf{A}_{\beta+i}^T \mathbf{A}_{\beta+i} = \mathbf{M}_{\beta+i} = \begin{pmatrix} \left(\frac{i}{\beta^2} + \frac{(\beta-i)^2}{\beta^3}\right)\mathbf{J}_{\beta,\beta} & \frac{\beta-i}{\beta^2}\mathbf{J}_{\beta,i} \\ \frac{\beta-i}{\beta^2}\mathbf{J}_{i,\beta} & \frac{1}{\beta}\mathbf{J}_{i,i} \end{pmatrix},$$

We grt that $\mathrm{Tr}(\mathbf{M}_{\beta+i}) = \frac{i}{\beta} + \frac{(\beta-i)^2}{\beta^2} + \frac{i}{\beta} = 1 + \frac{i^2}{\beta^2}$ and $\dim \ker(\mathbf{A}_{\beta+i}) = \beta + i - 2$, so $\lambda^{\beta+i-2} \mid \chi_{\beta+i}(\lambda)$. Meanwhile, it always has that $\mathbf{A}_{\beta+i}^T \mathbf{A}_{\beta+i} \cdot (1, \cdots, 1)^T = (1, \cdots, 1)^T$. Therefore, we obtain that for $i \geq 0$, $\chi_{\beta+i}(\lambda) = \lambda^{\beta+i-2}(\lambda-1)\left(\lambda - \frac{i^2}{\beta^2}\right)$. □

Since $J \ll \beta$, $1 = \lim_{\beta\to\infty}\left(\frac{\beta-J}{\beta}\right)^2$ and $0 = \lim_{\beta\to\infty}\frac{J}{\beta^2}$, we give the following Heuristic 4.

Heuristic 4 *For $i \geq 2$:*

$$\chi_{\beta+i}(\lambda) = \left[\left(1 + \left(\frac{\beta-J}{\beta}\right)^2\right)\lambda - \frac{J}{\beta^2}\right] \cdot \chi_{\beta+i-1}(\lambda) - \left(\frac{\beta-J}{\beta}\right)^2 \lambda^2 \cdot \chi_{\beta+i-2}(\lambda).$$

When Heuristic 4 is hold, we can prove that Heuristic 4 satisfies a second order recurrence formula.

Lemma 7. *For $d \geq \beta$, the largest root of $\chi_d(\lambda)$ is within $\left[\frac{1}{J + \frac{2\beta(\beta-J)\pi^2}{J(d-\beta)^2}}, 1 - \frac{\beta(\beta-J)}{2Jd^2}\right]$*

The proof of the following result relies on several changes of variables to link the polynomials $\chi_d(\lambda)$ to the Chebyshev polynomials of the second kind.

Proof. Let $\bar{\chi}_i(\lambda) = \lambda^i \chi_i\left(\frac{1}{\lambda}\right)$, we have: $\bar{\chi}(\mathbf{M}_{\beta+i})(\lambda) = \lambda^i \cdot \chi(\mathbf{M}_{\beta+i})\left(\frac{1}{\lambda}\right)$,

$\bar{\chi}(\mathbf{M}_{\beta+i})(\lambda) = \lambda^i \cdot \left[\left(1 + \left(\frac{\beta-J}{\beta}\right)^2\right)\frac{1}{\lambda} - \frac{J}{\beta^2}\right] \cdot \chi(\mathbf{M}_{\beta+i-1})\left(\frac{1}{\lambda}\right) - \lambda^i \cdot \left(\frac{\beta-J}{\beta}\right)^2 \frac{1}{\lambda^2} \cdot \chi(\mathbf{M}_{\beta+i-2})\left(\frac{1}{\lambda}\right)$

$\bar{\chi}(\mathbf{M}_{\beta+i})(\lambda) = \lambda^{i-1} \cdot \left[1 + \left(\frac{\beta-J}{\beta}\right)^2 - \frac{J}{\beta^2}\lambda\right] \cdot \chi(\mathbf{M}_{\beta+i-1})\left(\frac{1}{\lambda}\right) - \left(\frac{\beta-J}{\beta}\right)^2 \lambda^{i-2} \cdot \chi(\mathbf{M}_{\beta+i-2})\left(\frac{1}{\lambda}\right)$

$$\bar{\chi}(\mathbf{M}_{\beta+i})(\lambda) = \left[1 + \left(\frac{\beta-J}{\beta}\right)^2 - \frac{J}{\beta^2}\lambda\right] \cdot \bar{\chi}(\mathbf{M}_{\beta+i-1})(\lambda) - \left(\frac{\beta-J}{\beta}\right)^2 \cdot \bar{\chi}(\mathbf{M}_{\beta+i-2})(\lambda)$$

Let $\tau(\lambda') = \left(\frac{J}{\beta^2}\right)^{-1}\left[(2\lambda')\cdot\frac{\beta-J}{\beta} - \left[1+\left(\frac{\beta-J}{\beta}\right)^2\right] + \frac{J}{\beta^2}\right]$, $\psi(\mathbf{M}_{\beta+i})(\lambda') = \left(\frac{\beta}{\beta-J}\right)^i \frac{\bar{\chi}(\mathbf{M}_{\beta+i})\left[1-\tau(\lambda')\right]}{\tau(\lambda')}$, we obtain $\psi(\mathbf{M}_{\beta+i})(\lambda') =$

$$\left(\frac{\beta}{\beta-J}\right)^{i-1}\left(\frac{\beta}{\beta-J}\left\{\left[1+\left(\frac{\beta-J}{\beta}\right)^2 - \frac{J}{\beta^2}\left(1-\tau(\lambda')\right)\right]\right\}\right)\frac{\bar{\chi}(\mathbf{M}_{\beta+i-1})\left[1-\tau(\lambda')\right]}{\tau(\lambda')}$$

$$-\left(\frac{\beta}{\beta-J}\right)^{i-2}\frac{\bar{\chi}(\mathbf{M}_{\beta+i-2})\left[1-\tau(\lambda')\right]}{\tau(\lambda')}$$

$$\psi(\mathbf{M}_{\beta+i})(\lambda') = 2\lambda'\cdot\psi(\mathbf{M}_{\beta+i-1})(\lambda') - \psi(\mathbf{M}_{\beta+i-2})(\lambda') \tag{20}$$

Next we will give the initial two values of $\psi(\mathbf{M}_{\beta+i})$: $\psi(\mathbf{M}_{\beta})$ and $\psi(\mathbf{M}_{\beta+1})$. Then we can use Eq.(20) to represent all characteristic polynomials of different dimensions-d of $\mathbf{M}_d$, $d=\beta+i$, for $i \geq 0$.

Based on Lemma 6, for $J \geq i \geq 0$, $\bar{\chi}_{\beta+i}(\lambda) = \lambda^{\beta+i}\cdot\frac{1}{\lambda^{\beta+i-2}}\left(\frac{1}{\lambda}-1\right)\left(\frac{1}{\lambda}-\frac{i^2}{\beta^2}\right)$.

$$J \geq i \geq 0,\ \bar{\chi}_{\beta+i}(\lambda) = (1-\lambda)\left(1-\frac{i^2}{\beta^2}\lambda\right)$$

Specifically, $\bar{\chi}_{\beta}(\lambda) = 1-\lambda$. Therefore, $\psi(\mathbf{M}_{\beta})(\lambda') = \left(\frac{\beta}{\beta-J}\right)^0 \frac{\bar{\chi}_{\beta}\left[1-\tau(\lambda')\right]}{\tau(\lambda')}$ $= 1\cdot\frac{1-\left[1-\tau(\lambda')\right]}{\tau(\lambda')} = 1$.

Besides, since $\chi_{\beta+1}(\lambda) = \lambda^{\beta-1}(\lambda-1)\left(\lambda-\frac{1}{\beta^2}\right)$, $\frac{1}{\beta^2} \leq \frac{J}{\beta^2} < 1$, both matrix with eigenvalue $\lambda = \frac{1}{\beta^2}$ and matrix with eigenvalue $\lambda = \frac{J}{\beta^2}$ are Lyapunov asymptotically stable according to Lyapunov stability theory (First Method). Therefore, even if we set $\chi_{\beta+1}(\lambda) = \lambda^{\beta-1}(\lambda-1)\left(\lambda-\frac{J}{\beta^2}\right)$, it still asymptotically stable. Then we have $\bar{\chi}_{\beta+1}(\lambda) = 1-\lambda$ and $\bar{\chi}_{\beta}(\lambda) = (1-\lambda)\left(1-\frac{J}{\beta^2}\lambda\right)$.

$$\psi(\mathbf{M}_{\beta+1})(\lambda') = \left(\frac{\beta}{\beta-J}\right)^1 \frac{\bar{\chi}_{\beta+1}\left[1-\tau(\lambda')\right]}{\tau(\lambda')}$$

$$\psi(\mathbf{M}_{\beta+1})(\lambda') = \frac{\beta}{\beta-J}\cdot\frac{1-\left[1-\tau(\lambda')\right]}{\tau(\lambda')}\cdot\left[1-\frac{J}{\beta^2}\left(1-\tau(\lambda')\right)\right]$$

$$\psi(\mathbf{M}_{\beta+1})(\lambda') = \frac{\beta}{\beta-J}\left[1-\frac{J}{\beta^2}+\frac{J}{\beta^2}\tau(\lambda')\right]$$

$$\psi(\mathbf{M}_{\beta+1})(\lambda') = \frac{\beta}{\beta-J}\left\{1-\frac{J}{\beta^2}+(2\lambda')\cdot\frac{\beta-J}{\beta} - \left[1+\left(\frac{\beta-J}{\beta}\right)^2\right]+\frac{J}{\beta^2}\right\}$$

$$\psi(\mathbf{M}_{\beta+1})(\lambda') = 2\lambda' - \frac{\beta-J}{\beta}$$

For $i \geq 0$, let U_i be the the sequence of Chebyshev polynomials of the second kind, $\mathrm{U}_0 = 0$, $\mathrm{U}_1 = 1$, $\mathrm{U}_2 = 2\lambda'$, $i \geq 2$, $\mathrm{U}_i = 2\lambda'\mathrm{U}_{i-1} - \mathrm{U}_{i-2}$. Meanwhile, we know that $\psi(\mathbf{M}_\beta)(\lambda') = 1$, $\psi(\mathbf{M}_{\beta+1})(\lambda') = 2\lambda' - \frac{\beta-J}{\beta}$.

Then for $i \geq 2$, based on Eq.(20), we obtain $\psi(\mathbf{M}_{\beta+i})(\lambda') = \mathrm{U}_{i+1} - \frac{\beta-J}{\beta}\mathrm{U}_i$. Finally, we get $\psi(\mathbf{M}_d)(\lambda') = \mathrm{U}_{d-\beta+1} - \frac{\beta-J}{\beta}\mathrm{U}_{d-\beta}$.

Chebyshev polynomials satisfying that:

$$\forall d \geq 0, \forall x \in \mathbb{R} \setminus \{2k\pi; kx \in \mathbb{Z}\}, \mathrm{U}_d(\cos x) = \frac{\sin(nx)}{\sin x}.$$

Since $\psi(\mathbf{M}_d)\left(\cos\frac{\pi}{d-\beta}\right) = \mathrm{U}_{d-\beta+1}(\cos\frac{\pi}{d-\beta}) - \frac{\beta-J}{\beta}\mathrm{U}_{d-\beta}(\cos\frac{\pi}{d-\beta}) = \frac{\sin(\frac{\pi(d-\beta+1)}{d-\beta})}{\sin\frac{\pi}{d-\beta}} - 0$ and $\frac{\sin(\frac{\pi(d-\beta+1)}{d-\beta})}{\sin\frac{\pi}{d-\beta}} < 0$, we know $\psi(\mathbf{M}_d)\left(\cos\frac{\pi}{d-\beta}\right) < 0$.

$\psi(\mathbf{M}_d)\left(\cos\frac{\pi}{2(d-\beta+1)}\right) = \mathrm{U}_{d-\beta+1}(\cos\frac{\pi}{2(d-\beta+1)}) - \frac{\beta-J}{\beta}\mathrm{U}_{d-\beta}(\cos\frac{\pi}{2(d-\beta+1)}) = \frac{1}{\sin\frac{\pi}{2(d-\beta+1)}} - \frac{\beta-J}{\beta}\cdot\frac{\sin(\frac{\pi(d-\beta)}{2(d-\beta+1)})}{\sin\frac{\pi}{2(d-\beta+1)}}$ and $1 > \sin(\frac{\pi(d-\beta)}{2(d-\beta+1)})$, we get that:

$$\psi(\mathbf{M}_d)\left(\cos\frac{\pi}{2(d-\beta+1)}\right) > 0.$$

Then using intermediate value theorem, there exists $\lambda'_0 \in \left[\cos\frac{\pi}{d-\beta}, \cos\frac{\pi}{2(d-\beta+1)}\right]$ such that $\psi(\mathbf{M}_d)(\lambda'_0) = 0$, and $\psi(\mathbf{M}_d)(\lambda') > 0$ for all $\lambda' \in (\lambda'_0, 1)$. It indicates that

$$\bar{\chi}_d(1 - \tau(\lambda'_0)) = \left(\frac{\beta - J}{\beta}\right)^{d-\beta}\tau(\lambda'_0)\psi(\mathbf{M}_d)(\lambda'_0) = 0,$$

hence $\lambda_0 = (1 - \tau(\lambda'_0))^{-1}$ is a root of $\chi_d(\lambda)$. Since the image of $(\lambda'_0, 1)$ by $\lambda' \mapsto (1 - \tau(\lambda'))^{-1}$ is $(\lambda_0, 1)$, we obtain that λ_0 is the largest root of $\chi_d(\lambda)$ smaller than 1. Next we give the upper bound of λ_0.

$\cos\frac{\pi}{d-\beta} \leq \lambda_0^{'} \leq \cos\frac{\pi}{2(d-\beta+1)} \leq \cos\frac{\pi}{2d}$, $1 - \frac{\pi^2}{(d-\beta)^2} \leq \lambda_0^{'} \leq 1 - \frac{2\pi^2}{17d^2}$, $1 - \tau(\lambda') = (-2\lambda')\frac{\beta(\beta-J)}{J} + \frac{\beta^2}{J}\left[1 + \left(\frac{\beta-J}{\beta}\right)^2\right]$, it implies that:

$$1 - \tau(\lambda') \leq \left(\frac{\beta^2}{J}\right)\left[1 + \left(\frac{\beta - J}{\beta}\right)^2\right] - 2\frac{\beta(\beta - J)}{J}\left(1 - \frac{\pi^2}{(d - \beta)^2}\right)$$

Combining with $\left(\frac{\beta^2}{J}\right)\left[1 + \left(\frac{\beta-J}{\beta}\right)^2\right] - 2\frac{\beta(\beta-J)}{J} = J$, it gives

$$1 - \tau(\lambda') \leq J + \frac{2\beta(\beta - J)\pi^2}{J(d - \beta)^2} \tag{21}$$

$$\left(\frac{\beta^2}{J}\right)\left[1 + \left(\frac{\beta - J}{\beta}\right)^2\right] - 2\frac{\beta(\beta - J)}{J}\left(1 - \frac{2\pi^2}{17d^2}\right) \leq 1 - \tau(\lambda')$$

Since $1 \leq \left(\frac{\beta^2}{J}\right)\left[1+\left(\frac{\beta-J}{\beta}\right)^2\right] - 2\frac{\beta(\beta-J)}{J} = J$, we have:

$$1+\frac{\beta(\beta-J)}{J}\frac{2\pi^2}{17d^2} \leq 1+2\frac{\beta(\beta-J)}{J}\frac{2\pi^2}{17d^2} \leq 1-\tau(\lambda')$$

Combining this with Eq.(21), we can obtain that

$$\frac{1}{J+\frac{2\beta(\beta-J)\pi^2}{J(d-\beta)^2}} \leq \frac{1}{1-\tau(\lambda')} \leq \frac{1}{1+\frac{\beta(\beta-J)}{J}\frac{2\pi^2}{17d^2}} \leq 1-\frac{\beta(\beta-J)}{J}\frac{1}{2d^2}.$$

In addition, set $\varphi_d(\lambda) = \frac{\chi_d(\lambda)}{\lambda-1}$, based on Heuristic 4, we have $\varphi_d(1) \neq 0$, for $d \geq \beta$, which means that 1 is never a multiple root of $\chi_d(\lambda)$. □

5 Upper bound of the length of the Pnj-BKZ' reduction vector and convergence speed

In this section, we combined the conclusion in Lemma 4 and Lemma 7 to prove the following theorem which describes the upper bound of the length of fully Pnj-BKZ' reduced vector and the convergence speed of Pnj-BKZ' reduction.

Theorem 1. *Under SMA, there exists $C>0$ such that the following holds for all d, β and J. Let $(\mathbf{a}_i)_{i\leq d}$ be the input of Pnj-BKZ'(β,J). Set L be the lattice spanned by $(\mathbf{a}_i)_{i\leq d}$. After $C\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)$ tours reduction of Pnj-BKZ'(β,J), the output lattice basis $(\mathbf{b}_i)_{i\leq d}$ satisfies $\|\mathbf{x}-\mathbf{x}^\infty\|_2 \leq 1$, here $\mathbf{x}=(x_1,\ldots,x_d)^T$ and $x_i = \ln\frac{\|\mathbf{b}_i^*\|}{(\det L)^{1/d}}$ for all i and $\mathbf{x}^\infty$ is the unique solution of the equation $\mathbf{x}^\infty = \mathbf{A}\mathbf{x}^\infty + \mathbf{c}$. Specifically $\|\mathbf{b}_1\| \leq 2\gamma_\beta^{\frac{d-1}{2(\beta-J)}+2}\cdot(\det L)^{\frac{1}{d}}$.*

Proof. Let $\left(\mathbf{b}_i^{(k)}\right)_{i\leq d}$ be the basis after k tours reduction of Pnj-BKZ'(β,J) and set $\mathbf{x}_i^{(k)} = \ln\frac{\left\|\mathbf{b}_i^{(k)*}\right\|}{(\det L)^{1/d}}$, we have $\mathbf{x}^{(k)}-\mathbf{x}^{(\infty)} = \mathbf{A}^k\left(\mathbf{x}^{(k)}-\mathbf{x}^{(\infty)}\right)$. Both $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(\infty)} \in \mathrm{Span}\,(1,\ldots,1)^\perp$. Using $\mathbf{A}_\varepsilon$ be the restriction of $\mathbf{A}$ to $\mathrm{Span}\,(1,\ldots,1)^\perp$,

$$\left\|\mathbf{x}^{(k)}-\mathbf{x}^{(\infty)}\right\|_2 \leq \|\mathbf{A}_\varepsilon\|_2^k\left\|\mathbf{x}^{(0)}-\mathbf{x}^{(\infty)}\right\|_2 = \rho\left(\mathbf{A}_\varepsilon^T\mathbf{A}_\varepsilon\right)^{k/2}\left\|\mathbf{x}^{(0)}-\mathbf{x}^{(\infty)}\right\|_2$$

By Lemma 7 we know the largest eigenvalue $\mathbf{A}_\varepsilon$ is bounded in Lemma 7 by $1-\frac{\beta(\beta-J)}{2Jd^2}$. Then we obtain that

$$\left\|\mathbf{x}^{(k)}-\mathbf{x}^{(\infty)}\right\|_2 \leq \left(1-\frac{\beta(\beta-J)}{2Jd^2}\right)^{k/2}\left\|\mathbf{x}^{(0)}-\mathbf{x}^{(\infty)}\right\|_2$$

Meanwhile the tern $\left\|\mathbf{x}^{(0)}-\mathbf{x}^{(\infty)}\right\|_2$ can be bounded by $\left\|\mathbf{x}^{(0)}\right\|_2+\left\|\mathbf{x}^{(\infty)}\right\|_2 \leq \left(\ln\max_i\frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}d\right)+d^{O(1)}$, then $\ln\left\|\mathbf{x}^{(0)}-\mathbf{x}^{(\infty)}\right\|_2 = O\left(\ln d+\ln\ln\max_i\frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)$.

There exists constant number C to make $\left\|\mathbf{x}^{(k)}-\mathbf{x}^{(\infty)}\right\|_2 \le 1$ when $k \ge C\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\|\mathbf{a}_i^*\|}{(\det L)^{1/d}}\right)$.

Next we give the uppper bound of $\left\|\mathbf{b}_1^{(k)}\right\|$. By Lemma 4, $\ln \mathrm{HF}\left(\mathbf{B}^{\infty}\right) \lesssim \left(\frac{d-1}{\beta-J}+4\right)\ln\sqrt{\gamma_\beta}$, i.e $\mathbf{x}_1^{(\infty)} \lesssim \left(\frac{d-1}{\beta-J}+4\right)\ln\sqrt{\gamma_\beta}$. Using the inequality $\mathbf{x}_1^{(k)} \le \mathbf{x}_1^{(\infty)}+1$, we directly get the upper bound of $\left\|\mathbf{b}_1^{(k)}\right\| \le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2}\cdot(\det L)^{\frac{1}{d}}$. □

6 Verification experiments

From Section 5, after running sufficient tours of Pnj-BKZ(β, J), the first vector $\mathbf{b}_1$ in lattice basis output from Pnj-BKZ(β, J): $\frac{\|\mathbf{b}_1\|}{(\det L)^{\frac{1}{d}}} \le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2}$. In this part, we show that the actual the root Hermit factor of the Pnj-BKZ reduced lattice basis $\left(\frac{\|\mathbf{b}_1\|}{(\det L)^{\frac{1}{d}}}\right)^{\frac{1}{d}}$ is indeed smaller than the theoretical upper bound $\gamma_\beta^{\frac{d-1}{2(\beta-J)d}+\frac{2}{d}}$, which we give in Section 5. See Fig. 1 and Fig. 2 for more details.

The x-axis in Fig. 1 and Fig. 2 is the number of Pnj-BKZ(β, J) that have been run. The y-axis in Fig. 1 and Fig. 2 is the root of the Hermit factor. The red line in Fig. 1 and Fig. 2 is the theoretical upper bound $\gamma_\beta^{\frac{d-1}{2(\beta-J)d}+\frac{2}{d}}$ of the root of Hermit factor for a Pnj-BKZ(β, J) reduced lattice basis. The blue points in Fig. 1 and Fig. 2 are the root of the Hermit factor of lattice basis reduced by each tour of Pnj-BKZ(β, J).

From Fig. 1 and Fig. 2, we can see that the actual reduction effort of Pnj-BKZ is consistent with our theoretical estimation. Specifically, the root Hermite factor of the lattice basis reduced by each tour of Pnj-BKZ(β, J) will gradually decrease and finally is smaller than our theoretical upper bound of root Hermite factor $\gamma_\beta^{\frac{d-1}{2(\beta-J)d}+\frac{2}{d}}$. In addition, the theoretical upper bound is very close to the actual value for the small block size reduction testing. The test results of larger blocks show that the actual reduction effect is better than the theoretical upper bound. It may be caused by the contraction of our theoretical derivation, and we will give tighter theoretical upper bounds in the future.

References

1. PQC Standardization Process: Fourth Round Candidate Announcement, 2022. `https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4`.
2. B. A., G. N., and J. A. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. In *IACR Cryptology ePrint*, page 2015/522. IACR Cryptology ePrint Archive, 2015.
3. 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 Y. Ishai and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 717–746, Cham, 2019. Springer International Publishing.

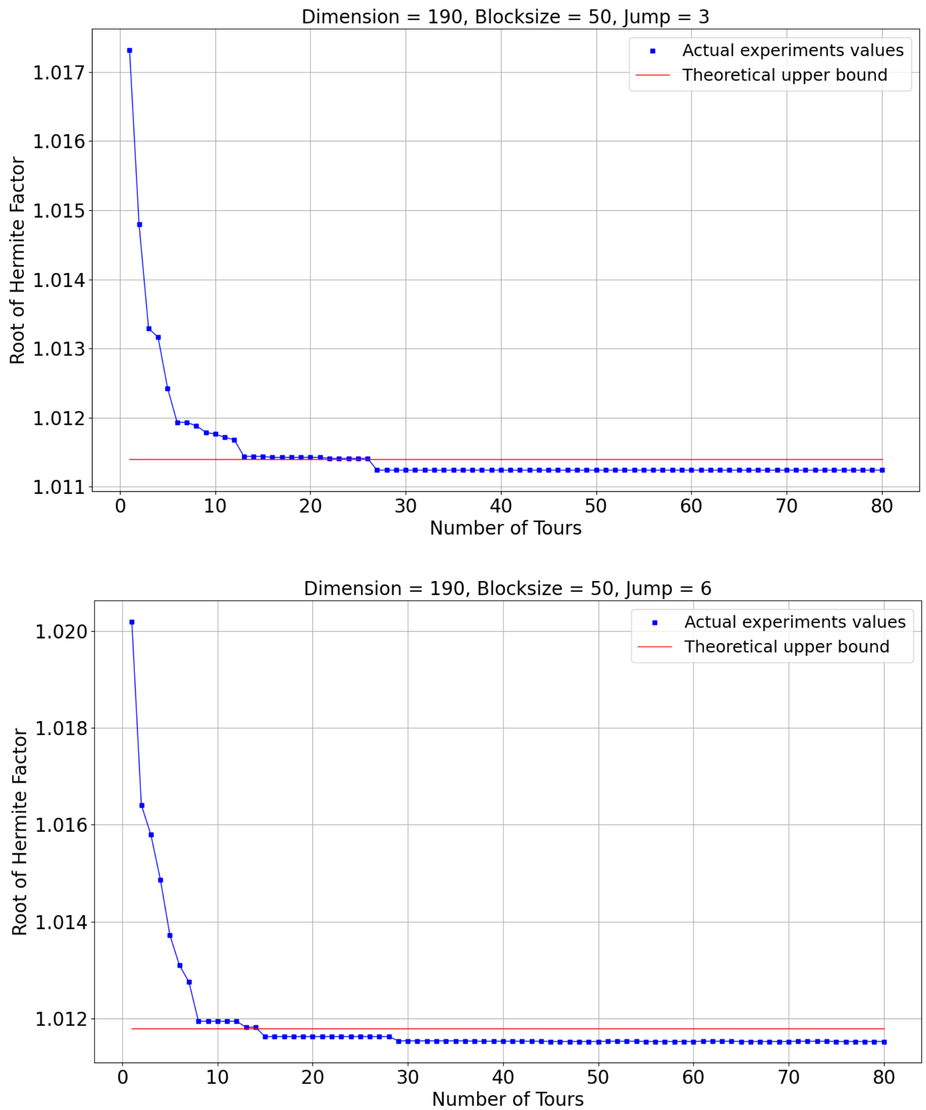
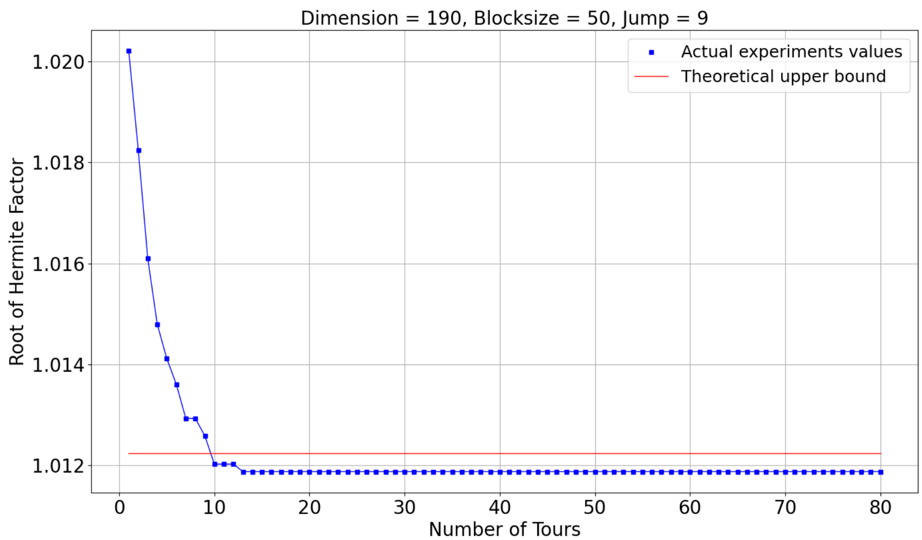


Fig. 1: Actual experiments value and theoretical upper bound of the root Hermit factor during Pnj-BKZ reduction for TU Darmstadt's SVP challenges (Dimensions 190). We test also 5 times for each reduction parameters.

4. Y. Aono, Y. Wang, T. Hayashi, and T. Takagi. Improved progressive bkz algorithms and their precise cost estimation by sharp simulator. In M. Fischlin and J.-S. Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 789–819, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.



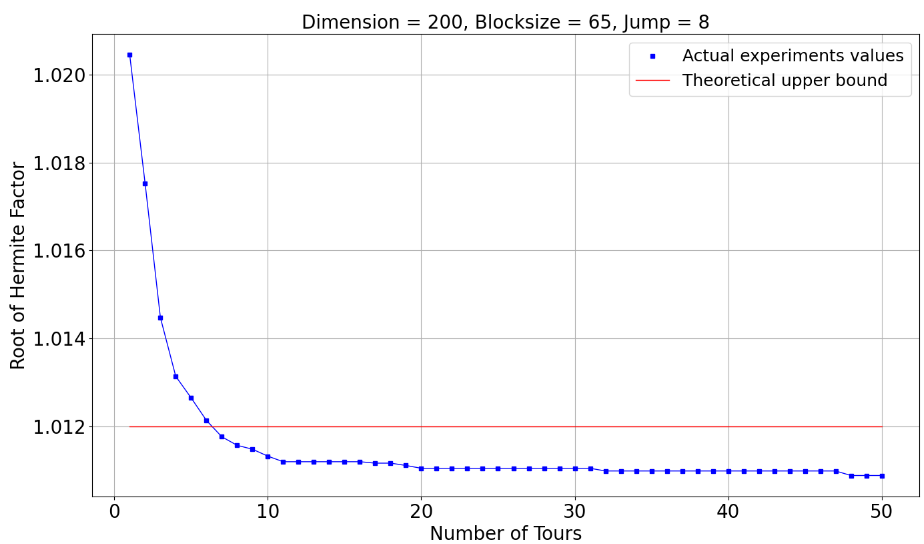


Fig. 2: Actual experiments value and theoretical upper bound of the root Hermit factor during Pnj-BKZ reduction for TU Darmstadt's SVP challenges (Dimensions 190-200). We test also 5 times for each reduction parameters.

5. R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. Kyber(Round 3). page 42, 2020.
6. A. Becker, L. Ducas, N. Gama, and T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '16, page 10–24,

USA, 2016. Society for Industrial and Applied Mathematics.
7. Y. Chen and P. Q. Nguyen. Bkz 2.0: Better lattice security estimates. In D. H. Lee and X. Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 1–20, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.
8. L. Ducas. Shortest vector from lattice sieving: A few dimensions for free. In J. B. Nielsen and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 125–145, Cham, 2018. Springer International Publishing.
9. L. Ducas, T. L. Eike Kiltz, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. *Dilithium(Round 3)*. NIST PQC probject, 2020.
10. L. Ducas, M. Stevens, and W. van Woerden. Advanced lattice sieving on gpus, with tensor cores. In A. Canteaut and F.-X. Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 249–279, Cham, 2021. Springer International Publishing.
11. N. Gama and P. Q. Nguyen. Finding short lattice vectors within mordell's inequality. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 207–216, New York, NY, USA, 2008. Association for Computing Machinery.
12. N. Gama, P. Q. Nguyen, and O. Regev. Lattice enumeration using extreme pruning. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 257–278, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
13. N. Gama, P. Q. Nguyen, and O. Regev. Lattice Enumeration Using Extreme Pruning. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and H. Gilbert, editors, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110, pages 257–278. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. Series Title: Lecture Notes in Computer Science.
14. G. Hanrot, X. Pujol, and D. Stehlé. Terminating bkz. *IACR Cryptol. ePrint Arch.*, 2011:198, 2011.
15. G. Herold and E. Kirshanova. Improved algorithms for the approximate k-list problem in euclidean norm. In S. Fehr, editor, *Public-Key Cryptography – PKC 2017*, pages 16–40, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.
16. G. Herold, E. Kirshanova, and T. Laarhoven. Speed-ups and time–memory trade-offs for tuple lattice sieving. In M. Abdalla and R. Dahab, editors, *Public-Key Cryptography – PKC 2018*, pages 407–436, Cham, 2018. Springer International Publishing.
17. T. Laarhoven and A. Mariano. Progressive lattice sieving. In T. Lange and R. Steinwandt, editors, *Post-Quantum Cryptography*, pages 292–311, Cham, 2018. Springer International Publishing.
18. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, Dec. 1982.
19. J. Li and P. Q. Nguyen. A complete analysis of the bkz lattice reduction algorithm. *IACR Cryptol. ePrint Arch.*, 2020:1237, 2020.
20. J. Li and M. Walter. Improving convergence and practicality of slide-type reductions. *Inf. Comput.*, 291(C), mar 2023.
21. D. Micciancio and P. Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '10, page 1468–1480, USA, 2010. Society for Industrial and Applied Mathematics.
22. D. Micciancio and M. Walter. Practical, predictable lattice basis reduction. In M. Fischlin and J.-S. Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 820–849, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

23. P. Q. Nguyen and T. Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008.
24. T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. page 67, 2020. Publisher: falcon-sifn.info.
25. C. P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In L. Budach, editor, *Fundamentals of Computation Theory*, Lecture Notes in Computer Science, pages 68–85, Berlin, Heidelberg, 1991. Springer.
26. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
27. L. Wang, Y. Wang, and B. Wang. A trade-off svp-solving strategy based on a sharper pnj-bkz simulator. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '23, page 664–677, New York, NY, USA, 2023. Association for Computing Machinery.
28. W. Xia, L. Wang, GengWang, D. Gu, and B. Wang. Improved progressive bkz with lattice sieving and a two-step mode for solving usvp. Cryptology ePrint Archive, Paper 2022/1343, 2022. `https://eprint.iacr.org/2022/1343`.