Analyzing Pump and jump BKZ algorithm using dynamical systems

Leizhang Wang[1]

State Key Laboratory of Integrated Service Networks, Xidian University[1]

June 12, 2024

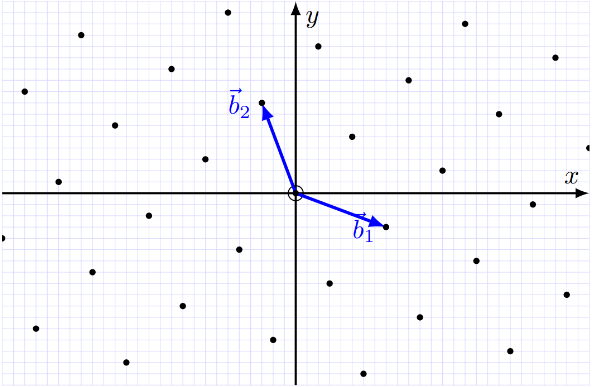
Contents

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ’ in the Sandpile Model
4. Convergence speed of the Pnj-BKZ’ dynamical system
5. Our results

Current Section

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ’ in the Sandpile Model
4. Convergence speed of the Pnj-BKZ’ dynamical system
5. Our results

Lattices!



Definition 1 (Lattice)

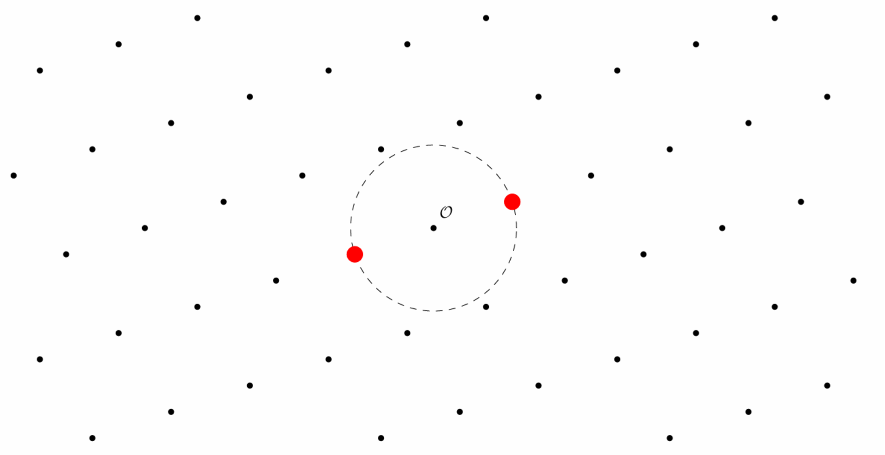
A lattice L is a discrete subgroup of a finite-dimensional Euclidean vector space.

Lattices

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

$$L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i, z_i \in \mathbb{Z} \right\}.$$

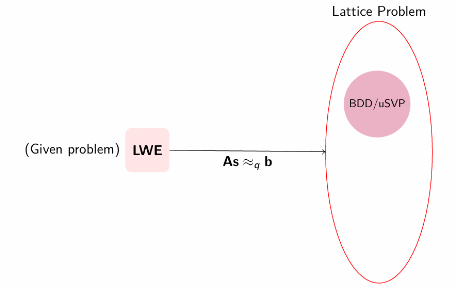
Lattice Problem



Lattice problems are about finding short and close vectors.

Lattice Problem

For most lattice-based encryption schemes (Kyber) their security are based on the hardness of LWE which can be reduced to the unique-SVP (u-SVP) on the special lattice basis.



Kannan's embedding: reduced LWE $(\mathbf{A}, \mathbf{b}, q)$ to uSVP on $L_q(\mathbf{M})$.

$$\mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{b} \\ 0 & 1 \end{pmatrix}$$

Lattice Problem

For most lattice-based signature schemes (Dilithium) their security are based on the hardness of SIS which can be reduced to the approximate-SVP (α-SVP) on an random orthogonal lattice basis.
A random $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m) \in \mathbb{Z}^{n \times m}$, given some bound M, goal find nonzero short vector $\mathbf{z} \in \mathbb{Z}^m$, $\|\mathbf{z}\| \leq M$ such that:

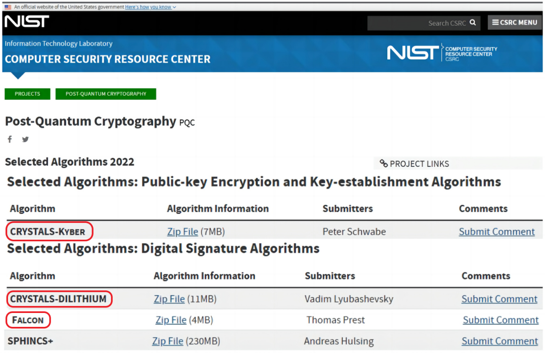
$$\underbrace{\begin{pmatrix} \cdots\cdots & \mathbf{A} & \cdots\cdots \\ & & \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

$L_q^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0}\ mod\ q\}$. SIS is an α-SVP on $L_q^{\perp}(\mathbf{A})$.
$(\mathbf{A}_1 | \mathbf{A}_2) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{n \times (m-n)}$, $\mathbf{A}_1$ is invertible matrix.

$$L_q^{\perp}(\mathbf{A}) = \begin{pmatrix} q\mathbf{I}_n & 0 \\ -(\mathbf{A}_1^{-1}\mathbf{A}_2)^T & \mathbf{I}_{m-n} \end{pmatrix}$$

Significance

- So it is necessary to obtain a good understanding of these lattice problems, such as the SVP and their approximate versions (u-SVP, α-SVP) to design more secure and efficient lattice-based cryptographic schemes in the post-quantum age.
- NIST in 2022 announced the PQC standardization whose three over four algorithms are lattice-based candidates.


An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PROJECTS
POST-QUANTUM CRYPTOGRAPHY
PROJECT LINKS

Post-Quantum Cryptography PQC

Selected Algorithms 2022

Selected Algorithms: Public-key Encryption and Key-establishment Algorithms

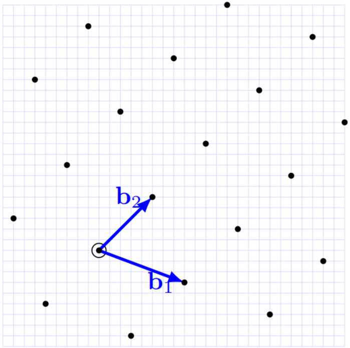
Algorithm	Algorithm Information	Submitters	Comments
CRYSTALS-KYBER	Zip File (7MB)	Peter Schwabe	Submit Comment

Selected Algorithms: Digital Signature Algorithms

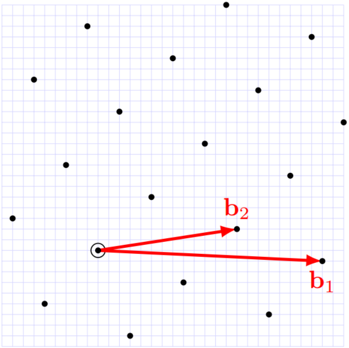
Algorithm	Algorithm Information	Submitters	Comments
CRYSTALS-DILITHIUM	Zip File (11MB)	Vadim Lyubashevsky	Submit Comment
FALCON	Zip File (4MB)	Thomas Prest	Submit Comment
SPHINCS+	Zip File (230MB)	Andreas Hulsing	Submit Comment

Bases of a Lattice

The security of lattice scheme based on the hardness of lattice problem while the difficulty of lattice problem heavily depends on the "shape" of the input basis **B**. In cryptography, a "bad" **B** is given.



Good Basis $\mathbf{G}$ of L



Bad Basis $\mathbf{B}$ of L

G → **B** : easy (randomization);
B → **G** : hard (LLL, BKZ, Lattice Sieve...).

An important invariant: the Volume

For any two bases $\mathbf{G}, \mathbf{B}$ of the same lattice Λ:

$$\det(\mathbf{G}\mathbf{G}^t) = \det(\mathbf{B}\mathbf{B}^t).$$

We can therefore define:

$$\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G}\mathbf{G}^t)}.$$

Geometrically: the volume of any **fundamental domain of** Λ.

Let $\mathbf{G}^*$ be the Gram-Schmidt Orthogonalization of $\mathbf{G}$

G* is **not** a basis of Λ, nevertheless:

$$\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G}^*\mathbf{G}^{*t})} = \prod \|\mathbf{g}_i^*\|$$

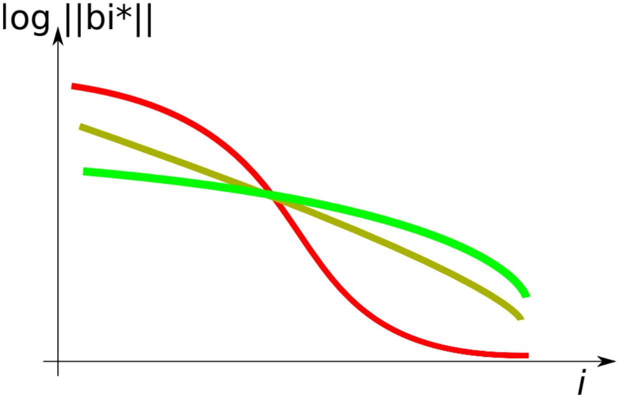
Profile of a Basis

Good basis

$$\max \|\mathbf{b}_i^*\| \approx \min \|\mathbf{b}_i^*\|$$

Bad basis

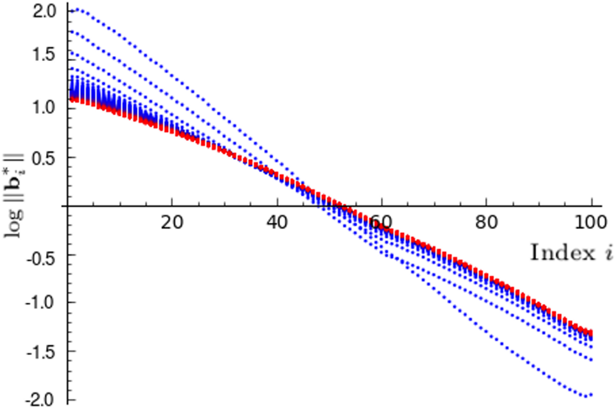
$$\max \|\mathbf{b}_i^*\| \gg \min \|\mathbf{b}_i^*\|$$



They have the same area, the only difference is slope.

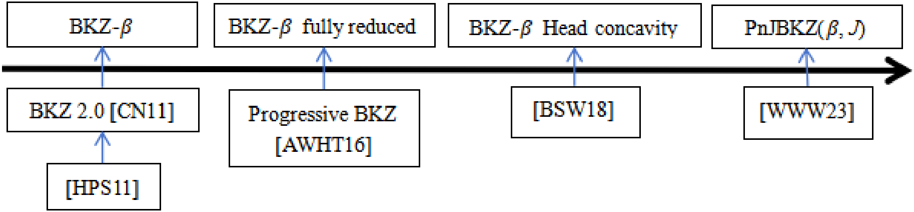
Lattice reduction algorithm

To solve an α-SVP or u-SVP, the main tool is lattice reduction algorithm like BKZ which can improve the quality of lattice basis.



We want to study the reduction effort of BKZ.

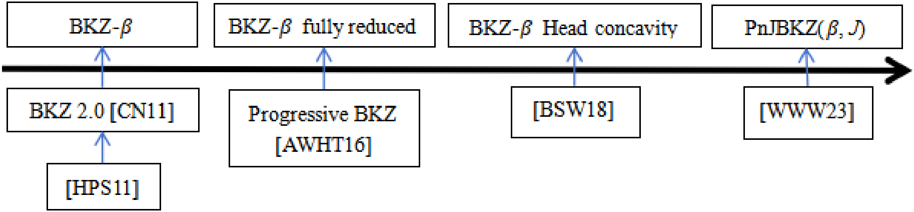
BKZ simulator



Based on the Gaussian heuristic, a BKZ simulator is a polynomial time algorithm to predict the reduction effort of the exponential time BKZ algorithm.

BKZ simulator

Based on the Gaussian heuristic, a BKZ simulator is a polynomial time algorithm to predict the reduction effort of the exponential time BKZ algorithm.



BKZ-β

BKZ 2.0 [CN11]

[HPS11]

BKZ-β fully reduced

Progressive BKZ [AWHT16]

BKZ-β Head concavity

[BSW18]

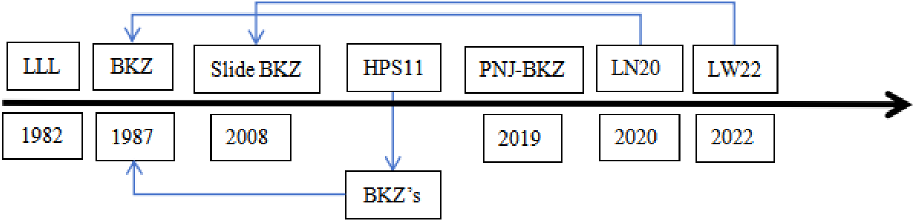
PnJBKZ(β, J)

[WWW23]

However, they are only the simulators, can not provide the accurate theoretical bound estimation.

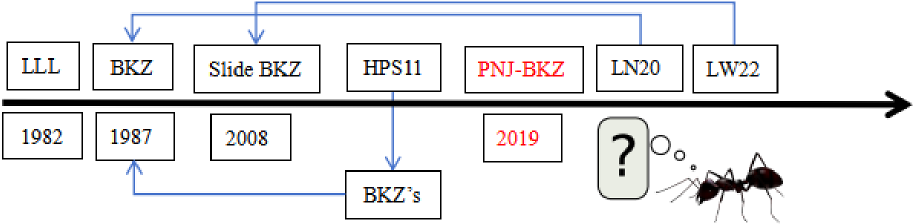
Theoretical Analysis of Lattice reduction algorithm

Based on dynamical systems, many works has been done to give the rigorous theoretical analysis of reduction effect of classical lattice reduction algorithm and tours needed for convergence .



Theoretical Analysis of Lattice reduction algorithm

There is no rigorous theoretical analysis of new lattice reduction algorithm: PnJ-BKZ, which is very efficient in practice.



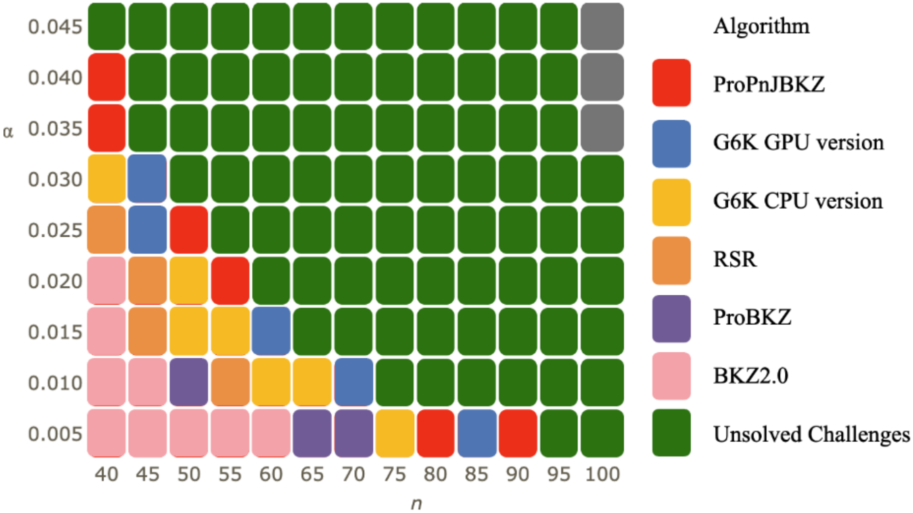
PnJ-BKZ was first proposed in G6K (CPU version, Albrecht et al. Eurocrypt 2019).

Current Section

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ' in the Sandpile Model
4. Convergence speed of the Pnj-BKZ' dynamical system
5. Our results

Main idea

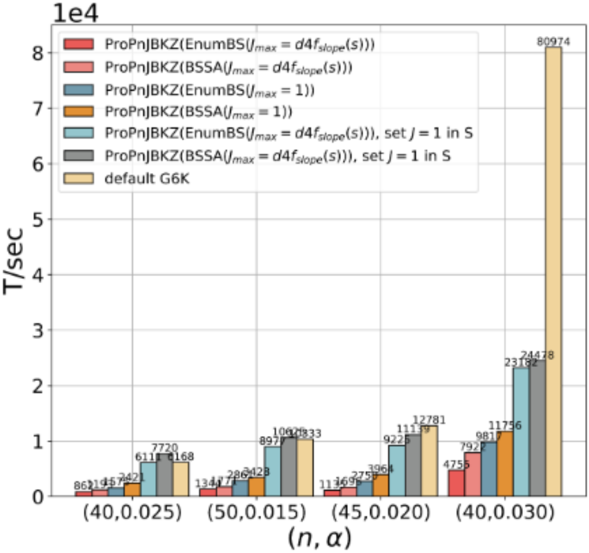
The efficiency of PnJBKZ in solving TU Darmstadt LWE Challenge.



https://www.latticechallenge.org/lwe_challenge/challenge.php

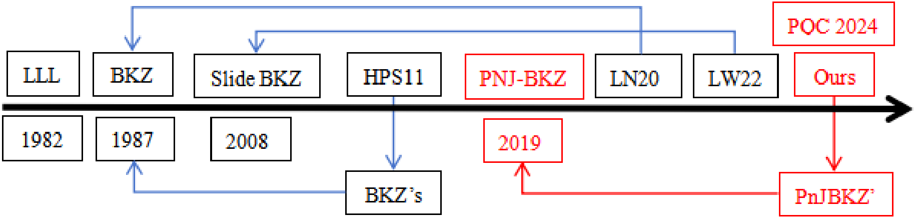
Main idea

The efficiency of PnJBKZ in solving TU Darmstadt LWE Challenge.



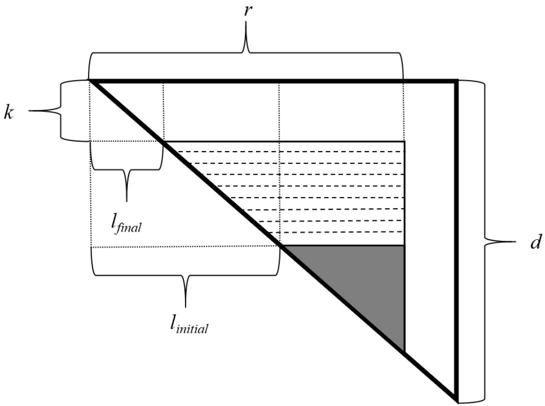
Main idea

We study the reduction effort of the new efficient Lattice reduction algorithm PnJBKZ and give the rigorous theoretical analysis to give a more accurate security estimation of lattice-based schemes.

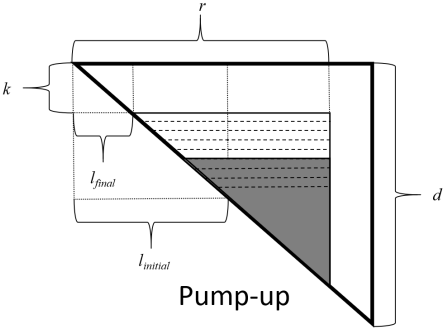


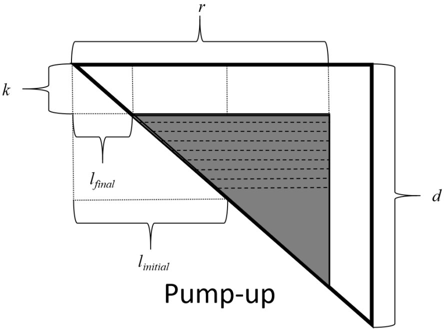
PnJBKZ algorithm

Pump and Jump BKZ is a BKZ-type reduction algorithm that uses Pump as its SVP oracle. It is worth mentioning that Pump can insert more than one vector into the inputting basis of sublattice and Pump will output a nearly HKZ-reduced lattice basis.

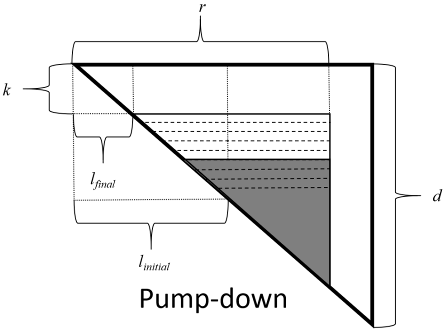


Pump

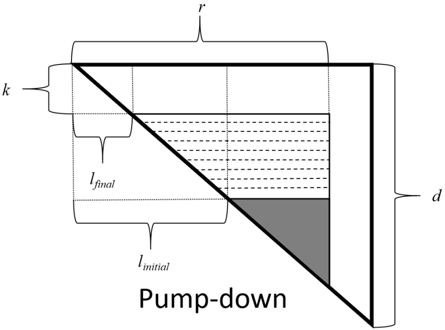




Pump



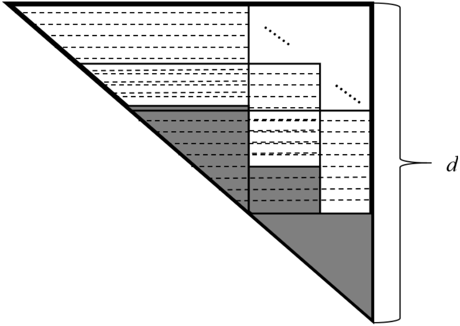
r
k
l_{final}
$l_{initial}$
d
Pump-down



r
k
l_{final}
$l_{initial}$
d
Pump-down

PnJBKZ algorithm

PnJBKZ can perform Pump with an adjustable parameter jump no less than 1. Specifically, running a PnJBKZ with blocksize β and jump=J means that after executing Pump on a certain block $\mathbf{B}_{[i:i+\beta]}$, the next Pump will be executed on the $\mathbf{B}_{[i+J:i+\beta+J]}$ block with a jump$=J$ rather than $\mathbf{B}_{[i+1:i+\beta+1]}$.



Main goal

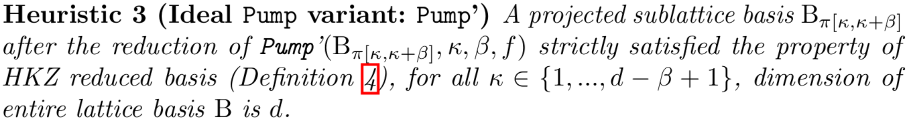
Goal: Constructing the dynamical system of PnJBKZ(β, J) which can help us to analyze the theoretical upper bound of the approximate factor in solving α-SVP by using PnJBKZ and analyze how many tours it needed for convergence.

Current Section

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ’ in the Sandpile Model
4. Convergence speed of the Pnj-BKZ’ dynamical system
5. Our results

The sandpile model and dynamical system in Pnj-BKZ'

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 PnJBKZ algorithm used in practice, but we will focus on a slightly modified ideal variant instead.



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*.*

Dynamical system of PnJBKZ

Under Sandpile Model Assumption [HPS11] and Stirling's approximation, after one tour reduction of Pnj-BKZ'(β, J), new $l_i^{'}$ can be expressed as:

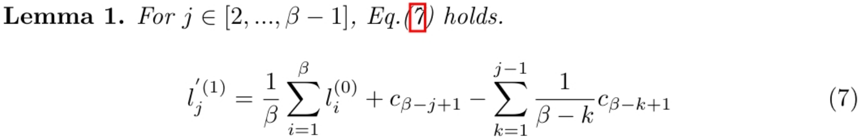
$$l_i^{'} \approx \begin{cases} a_i + \frac{1}{\beta-(i-1 \mod J)} \ln\left(\mathrm{vol}\left(L^{'}_{[i:i+\beta-(i-1 \mod J)]}\right)\right), & i \in [1, d-\beta] \\ a_i + \frac{1}{d-i+1} \ln\left(\mathrm{vol}\left(L^{'}_{[i:d]}\right)\right), & i \in [d-\beta+1, d] \end{cases} \tag{4}$$

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

$$c_i = \ln\left(\sqrt{\frac{i}{2\pi e}}\right),$$

Then we can prove Lemma 1 which estimates $l_i^{'}$ for $i \in [2, \cdots, \beta-1]$.

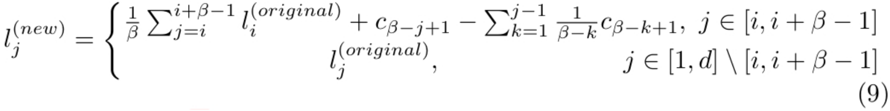
Dynamical system of PnJBKZ



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

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

Based on Lemma 1, we can give the estimation that how the lengths of Gram-Schmidt vectors $l_j^{(original)}$ change to $l_j^{(new)}$ after the reduction of a β-dimensional Pump'(κ, β) on any position $\kappa \in [1, d-\beta+1]$.



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

Dynamical system of PnJBKZ

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

Then we expressed the above complex relation equations by linear transformation. Let $\mathbf{x} = (l_i)_i$, $(l_i)_i^{(\alpha)}$ be the ln value of the length of GS vectors after α-th Pump'$(\kappa = 1 + (\alpha - 1)J, \beta)$ reduction, $\mathbf{x}^{(\alpha)} = (l_i)_i^{(\alpha)}$, $\alpha \in \left[1, 2, \ldots, \left\lceil \frac{d-\beta}{J} \right\rceil\right]$. $\forall i \in \left\{1, 1+J, ..., 1 + \left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d - \beta + 1\}$:

$$\mathbf{x}^{(1+\lfloor \frac{i}{J} \rfloor)} = \mathbf{A}^{(i)} \cdot \mathbf{x}^{(\lfloor \frac{i}{J} \rfloor)} + \mathbf{c}^{(i)}$$

Dynamical system of PnJBKZ

Reduction effort of 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 $\forall i \in \left\{1, 1+J, ..., 1 + \left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d - \beta + 1\}$,

$$\mathbf{x}^{(1+\lfloor \frac{i}{J} \rfloor)} = \mathbf{A}^{(i)} \cdot \mathbf{x}^{(\lfloor \frac{i}{J} \rfloor)} + \mathbf{c}^{(i)}$$

with:

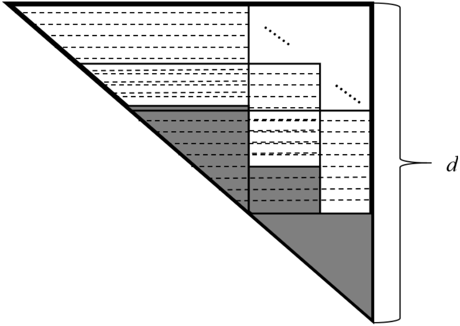
$$\mathbf{A}^{(i)} = \left(\begin{array}{ccccccc} \ddots &&&&&& \\ & 1 &&&&& \\ && \frac{1}{\beta} & \cdots & \frac{1}{\beta} && \\ && \vdots & \ddots & \vdots && \\ && \frac{1}{\beta} & \cdots & \frac{1}{\beta} && \\ &&&&& 1 & \\ &&&&&& \ddots \end{array}\right) \begin{array}{c} \\ \\ (i) \\ \\ (i+\beta-1) \\ \\ \\ \end{array}$$

$$\mathbf{c}_j^{(i)} = \begin{cases} 0, & j < i \\ c_{\beta-j} - \sum_{k=1}^{j-1} \frac{c_{\beta-k+1}}{\beta-k}, & j \in [i, i+\beta-1] \\ 0, & i + \beta \leq j \end{cases}$$

Thus we express the complex reduction process of any Pump by using a simple linear transformation.

Dynamical system of PnJBKZ

Consider Pump is used in different position $\kappa \in \left\{1, 1+J, ..., 1+\left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d-\beta+1\}$ during one tour reduction of a Pnj-BKZ'-(β, J), we can give the dynamical system of Pnj-BKZ'-(β, J) by considering all these Pumps.



Dynamical system of PnJBKZ

$$\forall i \in \left\{1, 1+J, ..., 1+\left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d-\beta+1\},$$

$$\mathbf{x}^{(1+\lfloor \frac{i}{J} \rfloor)} = \mathbf{A}^{(i)} \cdot \mathbf{x}^{(\lfloor \frac{i}{J} \rfloor)} + \mathbf{c}^{(i)}$$

Meanwhile, consider Pump is used in different position $\kappa \in \left\{1, 1+J, ..., 1+\left\lfloor \frac{d-\beta}{J} \right\rfloor J\right\} \cup \{d-\beta+1\}$, we show the reduction effort of one tour reducrion of PnJ-BKZ(β,J) on the norm vector **x**:

$$\mathbf{A}\mathbf{x} + \mathbf{c}$$

Dynamical system of PnJBKZ

The reduction effort of one tour reducrion of PnJ-BKZ(β,J) on the norm vector **x**:

$$\mathbf{Ax}+\mathbf{c}$$

with **c** =

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

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

$$\mathbf{A}^{(i)}=\left(\begin{array}{ccccccc}\ddots &&&&&& \\ & 1 &&&&& \\ && \frac{1}{\beta} & \cdots & \frac{1}{\beta} && \\ && \vdots & \ddots & \vdots && \\ && \frac{1}{\beta} & \cdots & \frac{1}{\beta} && \\ &&&&& 1 & \\ &&&&&& \ddots\end{array}\right)\begin{array}{c} \\ \\ (i) \\ \\ (i+\beta-1) \\ \\ \\ \end{array}$$

$$\mathbf{c}_j^{(i)}=\begin{cases}0, & j<i\\ c_{\beta-j}-\sum_{k=1}^{j-1}\frac{c_{\beta-k+1}}{\beta-k}, & j\in[i,i+\beta-1]\\ 0, & i+\beta\leq j\end{cases}$$

Dynamical system of PnJBKZ

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:

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

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

Dynamical system of PnJBKZ

We can inductive prove the case of *k*.

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

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

Dynamical system of PnJBKZ

$$\mathbf{Ax}+\mathbf{c}$$

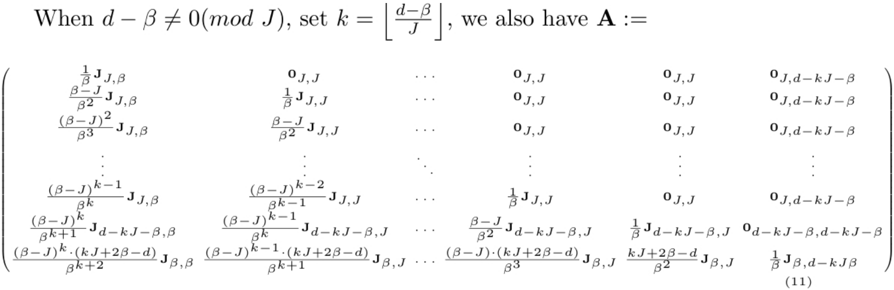
Then there are two cases:

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

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

Dynamical system of PnJBKZ

$$\mathbf{Ax}+\mathbf{c}$$



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

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

Solutions of the dynamical system of Pnj-BKZ’

We prove that $\mathbf{A} \cdot \mathbf{x} = \mathbf{x}$ then $\mathbf{x} \in \mathrm{span}(1, 1, \ldots, 1)^T$. So it suffices to find one solution of $\mathbf{x} = \mathbf{A} \cdot \mathbf{x} + \mathbf{c}$ to obtain all the solutions. Combined with Lemma 2 we give the solution for the dynamical system of PnJBKZ.

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 $\bar{\mathbf{x}} :=$

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

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

$\|\mathbf{b}_1\| / \lambda_1(L)$ after the PnJBKZ' fully reduced

After get solutions of the PnJBKZ' dynamical system, We prove Lemma 3 and Lemma 4 to give the upper bound of $\|\mathbf{b}_1\| / \lambda_1(L)$.

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

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

Next we give the uppper bound of $\left\|\mathbf{b}_1^{(k)}\right\|$. By Lemma 3 and Lemma 4, $\ln \mathrm{HF}(\mathbf{B}^\infty) \lesssim \left(\frac{d-1}{\beta-J} + 4\right) \ln \sqrt{\gamma_\beta}$, 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 $\left\|\mathbf{b}_1^{(k)}\right\| \le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2} \cdot (\det(L))^{\frac{1}{d}}$.

Current Section

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ’ in the Sandpile Model
4. Convergence speed of the Pnj-BKZ’ dynamical system
5. Our results

Convergence speed of the Pnj-BKZ' dynamical system

After we know the solution of Pnj-BKZ' dynamical system, we should study the speed of convergence of the discrete-time dynamical system:

$$\mathbf{x}_{k+1} := \mathbf{A}\mathbf{x}_k + \mathbf{c}$$

According to the principle of the power iteration algorithm, the asymptotic speed of convergence of the sequence $(\mathbf{A}_d^{(k)}\mathbf{x})_k$ is determined by the eigenvalue of $\mathbf{A}_d$. If this value smaller than 1 then this dynamical system will convergence to the solution.

Upper bound of the second 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 and we will show that the second largest eigenvalue value is smaller than $1-\frac{\beta(\beta-J)}{2Jd^2}$. So the sequence $(\mathbf{A}_d^{(k)}\mathbf{x})_k$ does converge.

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

Based the dynamical system of PnJBKZ we build before, we first proved Eq. (19) which is a recursion formula of $\mathbf{A}_d^T\mathbf{A}_d$.

for $k = 0, 1, \ldots, \left\lfloor \frac{d-\beta}{J} \right\rfloor$:

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

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

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

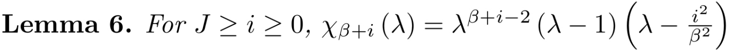
Then we prove Lemma 5, which gives the recursion formula of characteristic polynomial χ_d of $\mathbf{A}_d^T\mathbf{A}_d$.

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

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

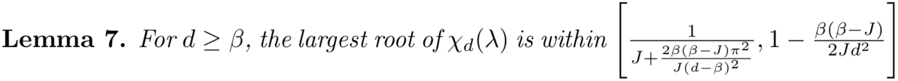
Upper bound of the second largest eigenvalue of $\mathbf{A}_d^T\mathbf{A}_d$

Then Lemma 6 calculates the first J terms of $\chi_{\beta+i}(\lambda)$



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

Finally based on Lemma 5 and Lemma 6, we use Chebyshev polynomials of the second kind to prove Lemma 7 which shows the bound of the second largest eigenvalue of $\mathbf{A}_d^T\mathbf{A}_d$.



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

Current Section

1. Preliminaries
2. Main Idea
3. Analysis of Pnj-BKZ’ in the Sandpile Model
4. Convergence speed of the Pnj-BKZ’ dynamical system
5. Our results

Our results

Based on Lemma 4 and 7, we prove Theorem 1 which describes the norm upper bound of shortest vector output from fully Pnj-BKZ' reduced basis 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 $\|\mathbf{b}_1\| \leq \gamma_\beta^{\frac{d-1}{2(\beta - J)} + 2} \cdot (\det L)^{\frac{1}{d}}$.*

Comparison with other works

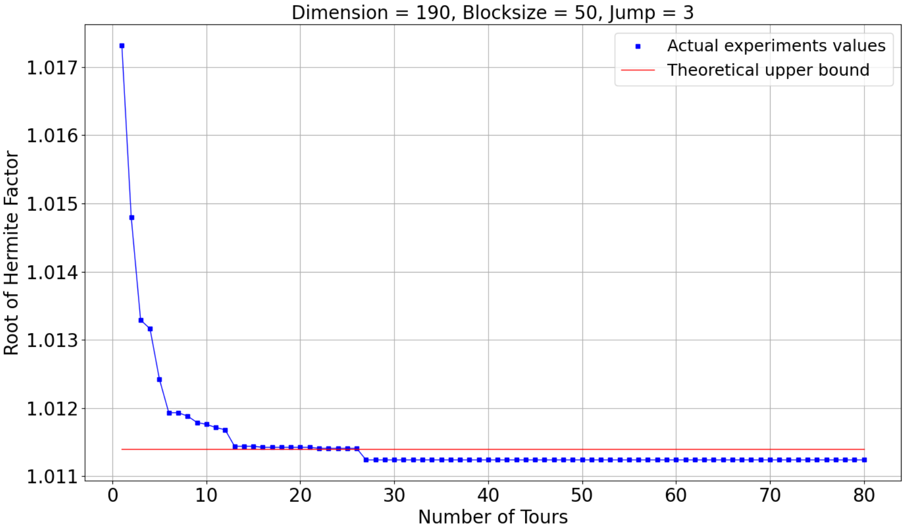
Table 1: Comparison with other works

Technique	GN08[11]	LW23[20]
Algorithm	Slide reduction	Slide reduction
$\lVert \mathbf{b}_1 \rVert / \lambda_1(L)$	$\le ((1+\varepsilon)\gamma_\beta)^{(d-\beta)/(\beta-1)}$	$\le (1+\varepsilon)\gamma_\beta^{\frac{d-1}{2(\beta-1)}}$
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
$\lVert \mathbf{b}_1 \rVert / \lambda_1(L)$	$\le 2\gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{3}{2}}$	$\le \gamma_\beta^{\frac{d-1}{2(\beta-1)}+\frac{\beta(\beta-2)}{2d(\beta-1)}}$
Convergence needed Tours	$\Theta\left(\frac{d^3}{\beta^2}\left(\log d + \log\log \max_i \lVert \mathbf{b}_i \rVert\right)\right)$	$\Theta\left(\frac{d^2}{\beta^2}\log d\right)$
Discrete dynamical systems	yes	yes
Technique	Our	
Algorithm	Pnj-BKZ'	
$\lVert \mathbf{b}_1 \rVert / \lambda_1(L)$	$\le \gamma_\beta^{\frac{d-1}{2(\beta-J)}+2}$	
Convergence needed Tours	$\Theta\left(\frac{2Jd^2}{\beta(\beta-J)}\left(\ln d + \ln\ln \max_i \frac{\lVert \mathbf{a}_i^* \rVert}{(\det L)^{1/d}}\right)\right)$	
Discrete dynamical systems	yes	

PnJBKZ algorithm has an extra parameter Jump value J to trade-off the time cost and reduction effect.

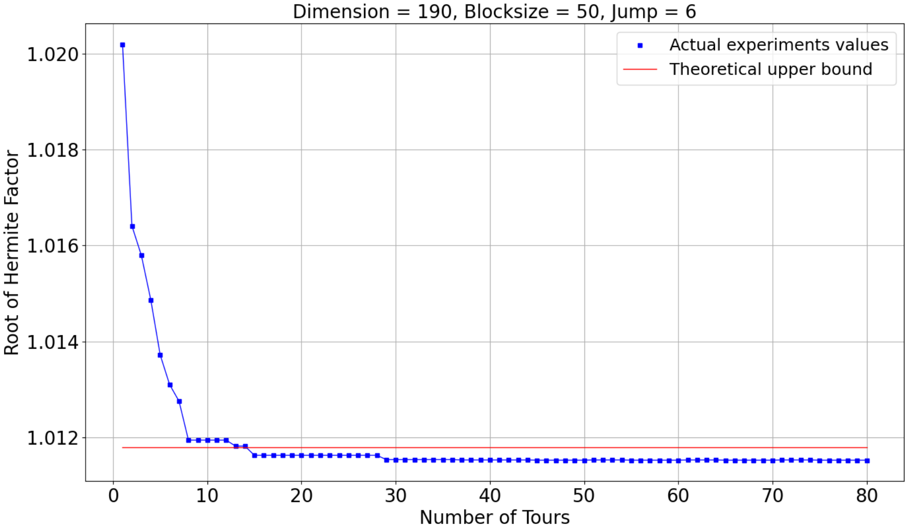
Verification experiments

190-dimensional random lattice basis from TU Darmstadt SVP Challenge.



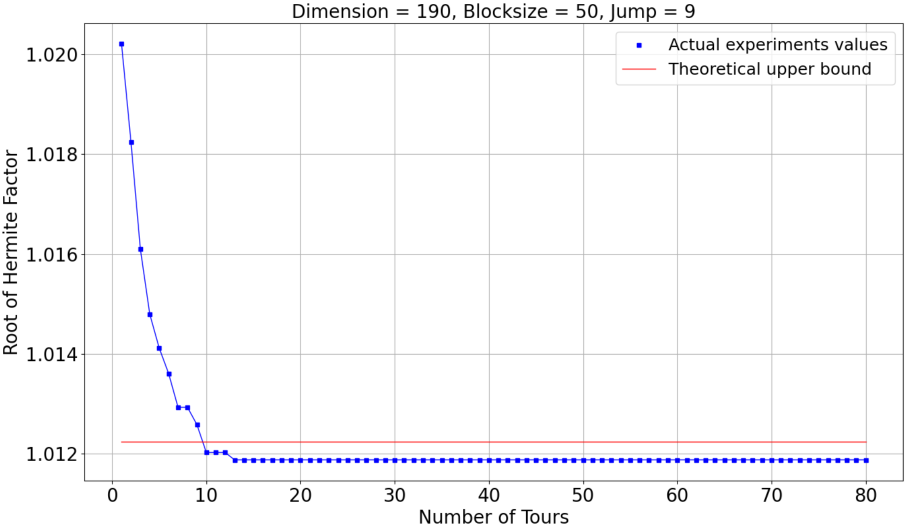
Verification experiments

190-dimensional random lattice basis from TU Darmstadt SVP Challenge.



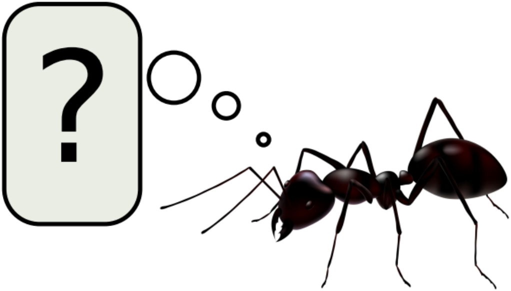
Verification experiments

190-dimensional random lattice basis from TU Darmstadt SVP Challenge.

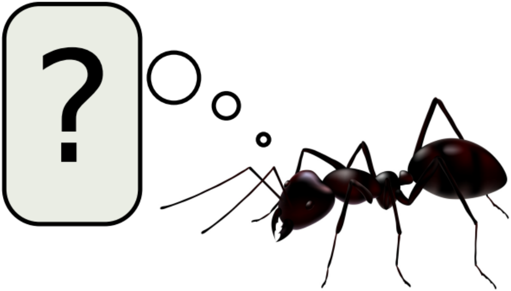


Open questiones

Can one remove the ideal heuristic that Pump outputs HKZ-reduced lattice basis?
Given more tight upper bound estimation and number of tours needed for convergence of Pnj-BKZ.



Thank You



Thank You