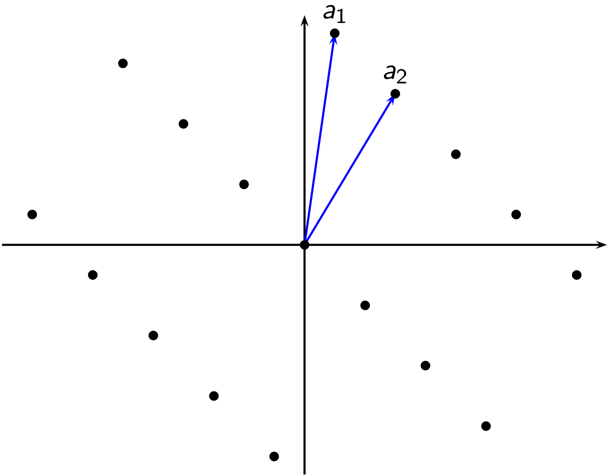
Analysis of BKZ

Guillaume Hanrot, Xavier Pujol, Damien Stehlé

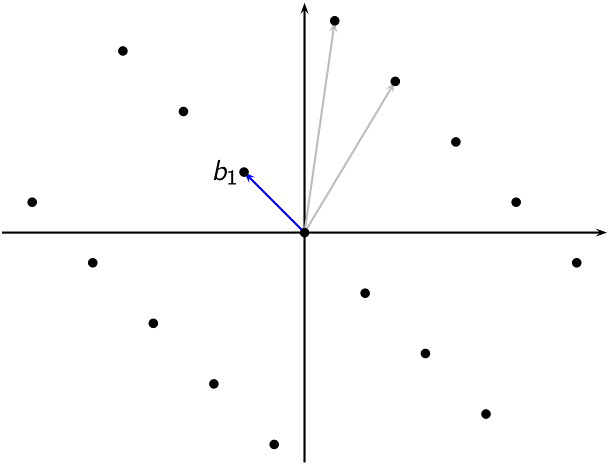
ENSL, LIP, CNRS, INRIA, Université de Lyon, UCBL

May 5, 2011

Lattices

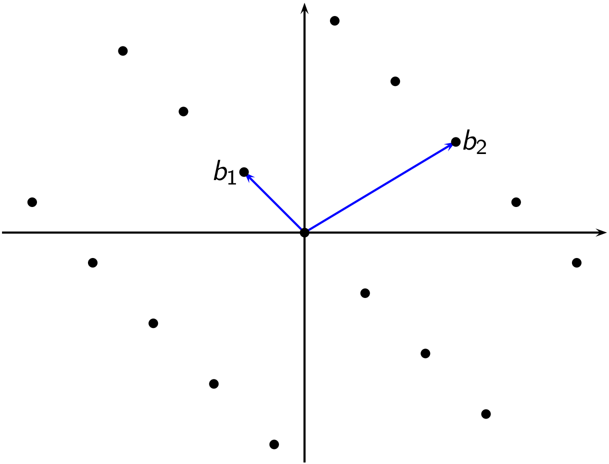


Lattices



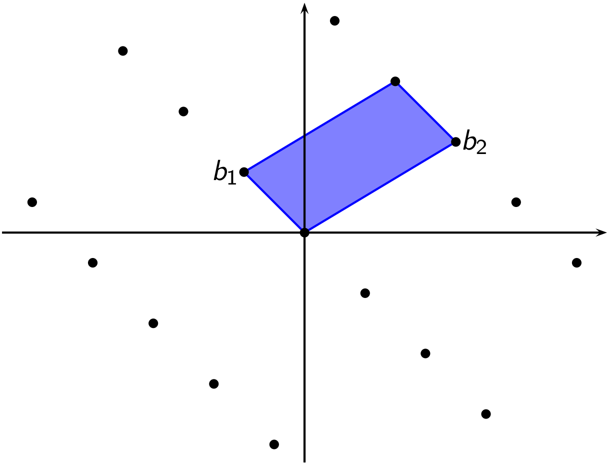
Shortest vector problem (SVP)

Lattices



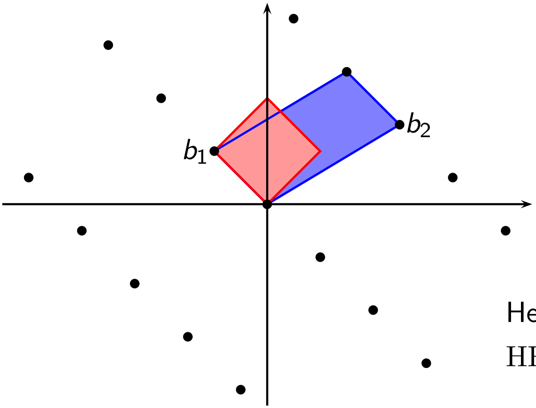
Lattice reduction

Lattices



Determinant

Lattices

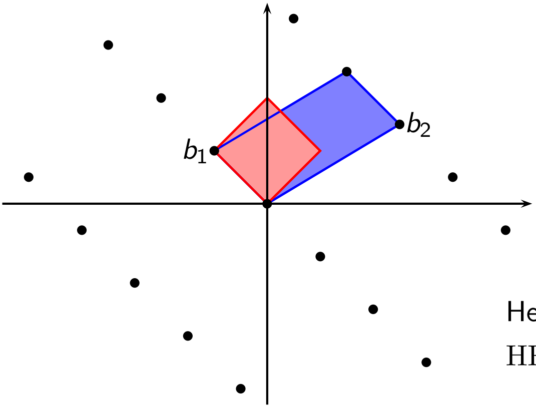


Hermite factor:

$$\mathrm{HF}(b_1, \ldots, b_n) = \frac{\|b_1\|}{(\det L)^{1/n}}$$

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with γ_n = Hermite constant $\leq n$.

Lattices

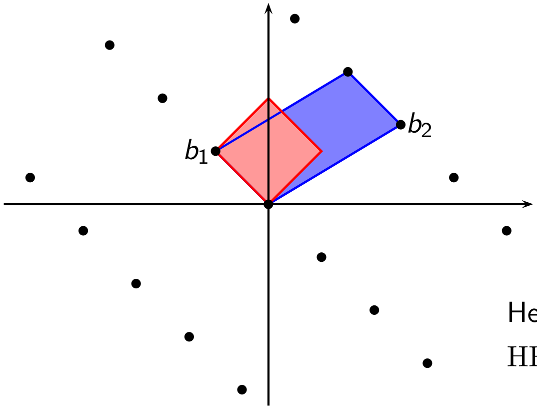


Hermite factor:

$$\mathrm{HF}(b_1, \ldots, b_n) = \frac{\|b_1\|}{(\det L)^{1/n}}$$

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with γ_n = Hermite constant $\leq n$.

Lattices



Hermite factor:

$$\mathrm{HF}(b_1, \ldots, b_n) = \frac{\|b_1\|}{(\det L)^{1/n}}$$

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with γ_n = Hermite constant $\leq n$.

Lattice reduction

Lattice reduction and shortest vector problem:

- The security of lattice-based cryptosystems relies on the hardness of (variants of) SVP.
- SVP and lattice reduction are interdependent problems.

Hierarchy of lattice reductions in dimension n:

	HKZ	BKZ$_\beta$	LLL
Hermite factor	$\sqrt{\gamma_n}$	$\simeq (\gamma_\beta(1+\epsilon))^{\frac{n-1}{2(\beta-1)}}$	$(\gamma_2(1+\epsilon))^{\frac{n-1}{2}}$
Time	$2^{O(n)}$	$2^{O(\beta)} \times ?$	Poly(n)

HKZ = Hermite-Korkine-Zolotareff

BKZ = Block Korkine-Zolotareff

Lattice reduction

Lattice reduction and shortest vector problem:

- The security of lattice-based cryptosystems relies on the hardness of (variants of) SVP.
- SVP and lattice reduction are interdependent problems.

Hierarchy of lattice reductions in dimension n:

	HKZ	BKZ_β	LLL
Hermite factor	$\sqrt{\gamma_n}$	$\simeq (\gamma_\beta(1+\epsilon))^{\frac{n-1}{2(\beta-1)}}$	$(\gamma_2(1+\epsilon))^{\frac{n-1}{2}}$
Time	$2^{O(n)}$	$2^{O(\beta)} \times ?$	$\mathrm{Poly}(n)$

HKZ = Hermite-Korkine-Zolotareff

BKZ = Block Korkine-Zolotareff

Lattice reduction

Lattice reduction and shortest vector problem:

- The security of lattice-based cryptosystems relies on the hardness of (variants of) SVP.
- SVP and lattice reduction are interdependent problems.

Hierarchy of lattice reductions in dimension n:

	HKZ	BKZ$_\beta$	LLL
Hermite factor	$\sqrt{\gamma_n}$	$\simeq (\gamma_\beta(1+\epsilon))^{\frac{n-1}{2(\beta-1)}}$	$(\gamma_2(1+\epsilon))^{\frac{n-1}{2}}$
Time	$2^{O(n)}$	$2^{O(\beta)} \times ?$	$\mathrm{Poly}(n)$

HKZ = Hermite-Korkine-Zolotareff

BKZ = Block Korkine-Zolotareff

Lattice reduction

Lattice reduction and shortest vector problem:

- The security of lattice-based cryptosystems relies on the hardness of (variants of) SVP.
- SVP and lattice reduction are interdependent problems.

Hierarchy of lattice reductions in dimension n:

	HKZ	BKZ_β	LLL
Hermite factor	$\sqrt{\gamma_n}$	$\simeq (\gamma_\beta(1+\epsilon))^{\frac{n-1}{2(\beta-1)}}$	$(\gamma_2(1+\epsilon))^{\frac{n-1}{2}}$
Time	$2^{O(n)}$	$2^{O(\beta)} \times ?$	$\text{Poly}(n)$

HKZ = Hermite-Korkine-Zolotareff

BKZ = Block Korkine-Zolotareff

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

History of BKZ

Practice

- Schnorr and Euchner (1994): algorithm for BKZ-reduction, without complexity analysis.
- Shoup: first public implementation of BKZ in NTL.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

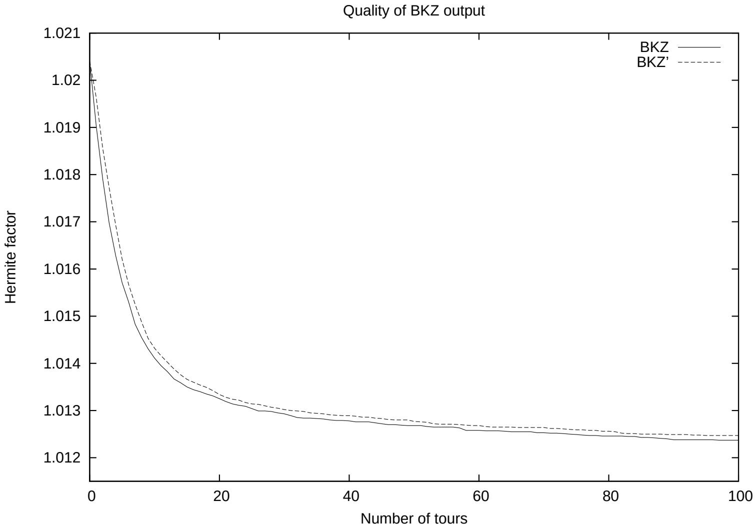
Theory

- Schnorr (1987): first hierarchies of algorithms between LLL and HKZ.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

Slide-reduction:

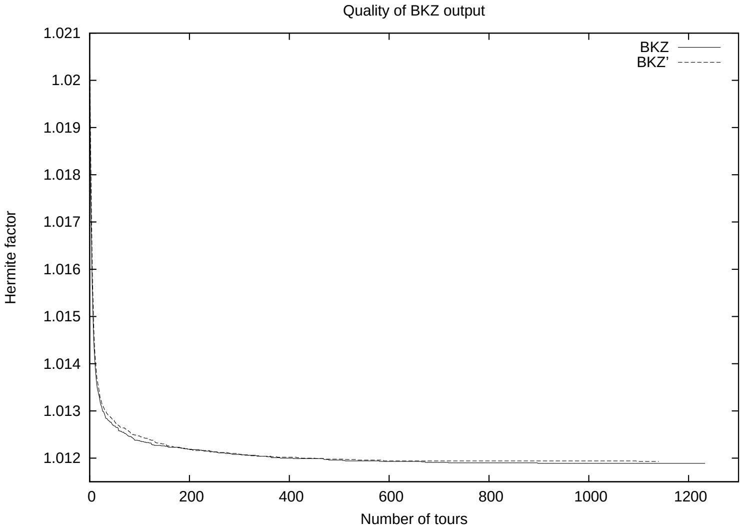
- Outputs a basis whose theoretical quality is equivalent to BKZ.
- Polynomial number of calls to a SVP oracle.
- Not as efficient as BKZ in practice.

Progress made during the execution of BKZ



Experience on 64 LLL-reduced knapsack-like matrices ($n = 108, \beta = 24$).

Progress made during the execution of BKZ



Experience on 64 LLL-reduced knapsack-like matrices ($n = 108, \beta = 24$).

Our result

γ_β = Hermite constant $\leq \beta$.
L a lattice with basis $(b_1, \ldots, b_n)$.

Theorem

After $\mathcal{O}\left(\frac{n^3}{\beta^2}\left(\log\frac{n}{\epsilon} + \log\log\max\frac{\|b_i\|}{(\det L)^{1/n}}\right)\right)$ *calls to* HKZ_β*, BKZ_β returns a basis C of L such that:*

$$\mathrm{HF}(C) \leq (1+\epsilon)\gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}}$$

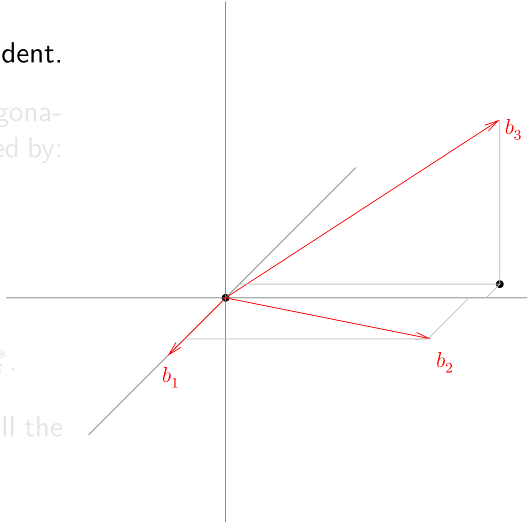
Gram-Schmidt orthogonalization

$b_1, \ldots, b_n$ linearly independent.

The Gram-Schmidt orthogonalization $b_1^*, \ldots, b_n^*$ is defined by:

- For all $i > j$, $\mu_{i,j} = \frac{(b_i, b_j^*)}{\|b_j^*\|^2}$.
- For all i, $b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*$.

A basis is size-reduced if all the $|\mu_{i,j}|$ are $\leq \frac{1}{2}$.



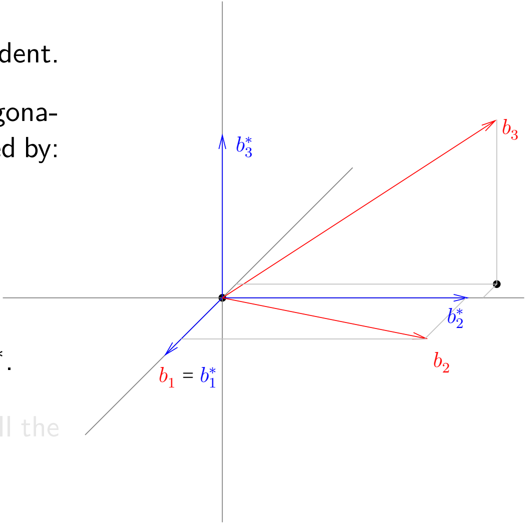
Gram-Schmidt orthogonalization

$b_1, \ldots, b_n$ linearly independent.

The Gram-Schmidt orthogonalization $b_1^*, \ldots, b_n^*$ is defined by:

- For all $i > j$, $\mu_{i,j} = \frac{(b_i, b_j^*)}{\|b_j^*\|^2}$.
- For all i, $b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*$.

A basis is size-reduced if all the $|\mu_{i,j}|$ are $\leq \frac{1}{2}$.



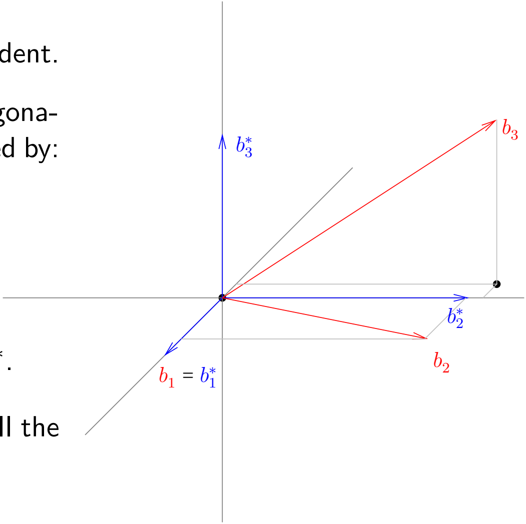
Gram-Schmidt orthogonalization

$b_1, \ldots, b_n$ linearly independent.

The Gram-Schmidt orthogonalization $b_1^*, \ldots, b_n^*$ is defined by:

- For all $i > j$, $\mu_{i,j} = \frac{(b_i, b_j^*)}{\|b_j^*\|^2}$.
- For all i, $b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*$.

A basis is size-reduced if all the $|\mu_{i,j}|$ are $\leq \frac{1}{2}$.



LLL

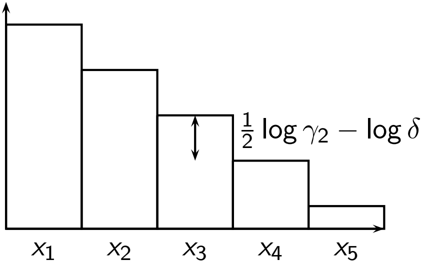
B is δ-LLL-reduced if:

- It is size-reduced;
- $\delta\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2 + \mu_{i+1,i}^2\|b_i^*\|^2$ for all $i < n$.
  $\rightarrow x_i \leq \frac{1}{2}\log\gamma_2 + x_{i+1} - \log\delta \quad (x_i = \log\|b_i^*\|)$

LLL

B is δ-LLL-reduced if:

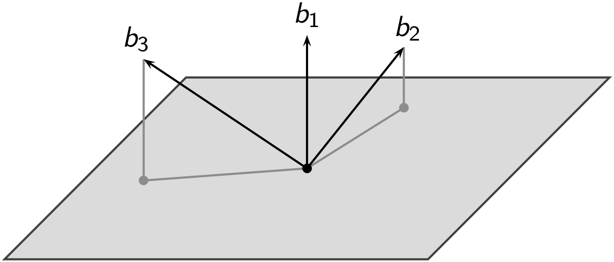
- It is size-reduced;
- $\delta\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2 + \mu_{i+1,i}^2\|b_i^*\|^2$ for all $i < n$.
  $\rightarrow x_i \leq \frac{1}{2}\log\gamma_2 + x_{i+1} - \log\delta \quad (x_i = \log\|b_i^*\|)$



HKZ

B is HKZ-reduced if:

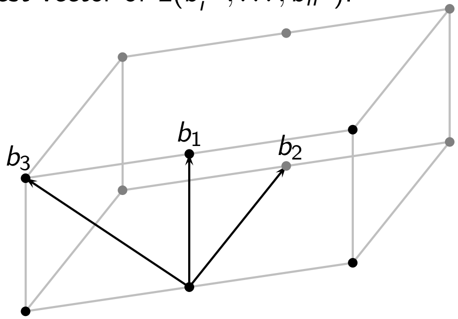
- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

B is HKZ-reduced if:

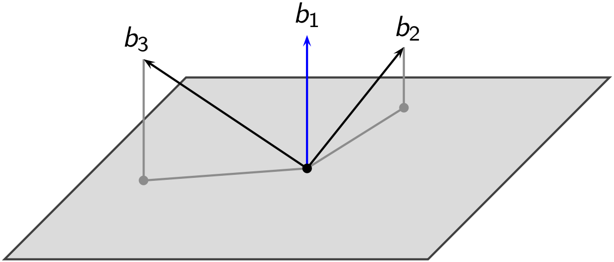
- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

B is HKZ-reduced if:

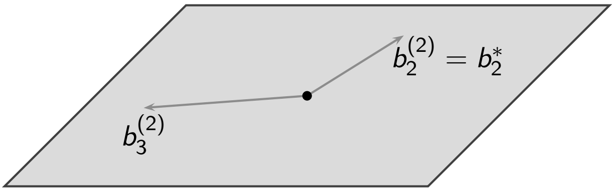
- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

B is HKZ-reduced if:

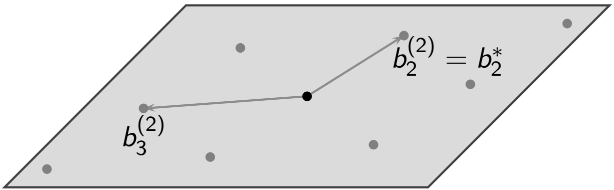
- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

B is HKZ-reduced if:

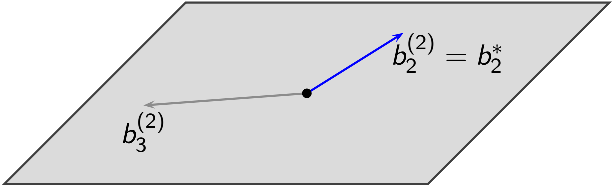
- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

B is HKZ-reduced if:

- It is size-reduced.
- $\|b_i^*\|$ = shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.



HKZ

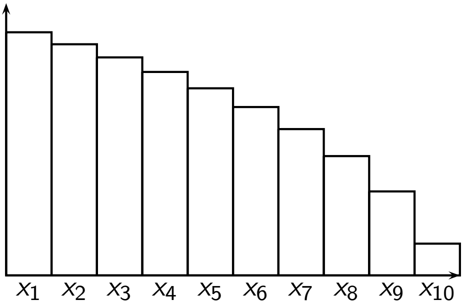
B is HKZ-reduced if:

- It is size-reduced.
- $\|b_i^*\| =$ shortest vector of $L(b_i^{(i)}, \ldots, b_n^{(i)})$.

For $i < n$,
$\mathrm{HF}(b_i^{(i)}, \ldots, b_n^{(i)}) \leq \sqrt{\gamma_{n-i+1}}$

Worst-case HKZ profile:

$$\begin{aligned} x_i &= \log \|b_i^*\| \\ &= \mathcal{O}(\log^2(n-i)) \end{aligned}$$



BKZ

Algorithm (BKZ$_\beta$, modified version)

Input: B of dimension n.
Repeat ... times
    For i from 1 to $n - \beta + 1$ do
        Size-reduce B.
        HKZ-reduce the projected sublattice $(b_i^{(i)}, \ldots, b_{i+\beta-1}^{(i)})$.
        Report the transformation on B.

Termination?

BKZ

Algorithm (BKZ$_\beta$, modified version)

Input: B of dimension n.

Repeat ... times

  For i from 1 to $n - \beta + 1$ do

    Size-reduce B.

    HKZ-reduce the projected sublattice $(b_i^{(i)}, \ldots, b_{i+\beta-1}^{(i)})$.

    Report the transformation on B.

Termination?

Sandpile model

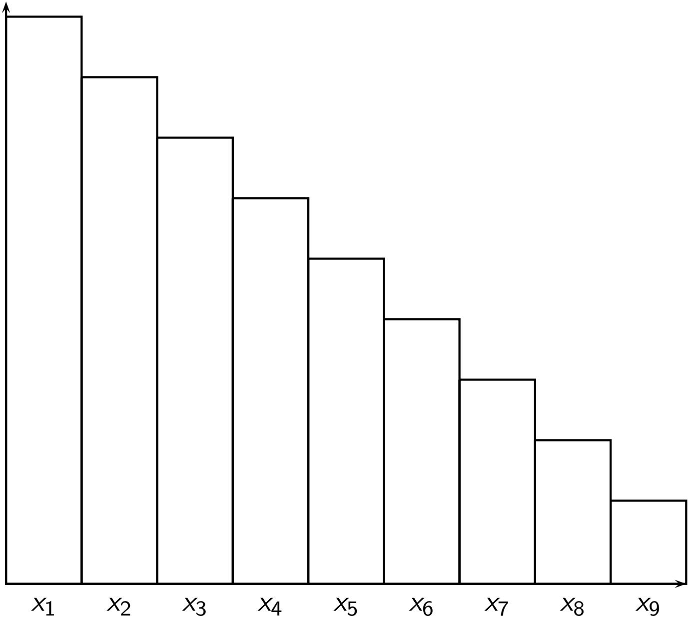
- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- Each HKZ-reduction gives a worst-case profile.
  $\rightarrow$ The initial x_i's fully determine the x_i's after a call to HKZ.
- The sandpile execution of BKZ is deterministic.

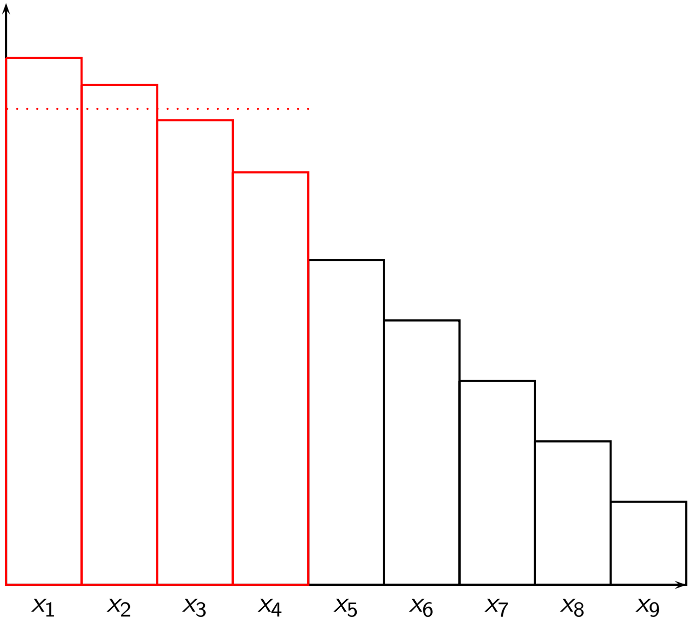
Sandpile model

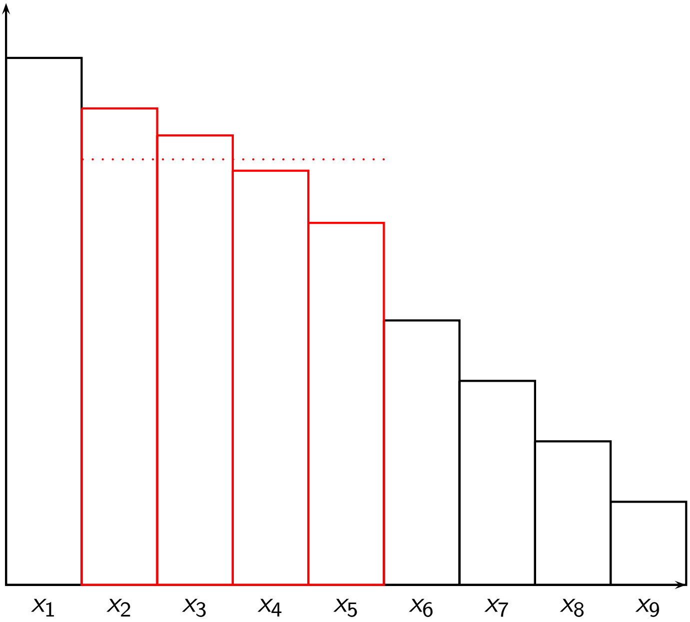
- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- Each HKZ-reduction gives a worst-case profile.
  $\rightarrow$ The initial x_i's fully determine the x_i's after a call to HKZ.
- The sandpile execution of BKZ is deterministic.

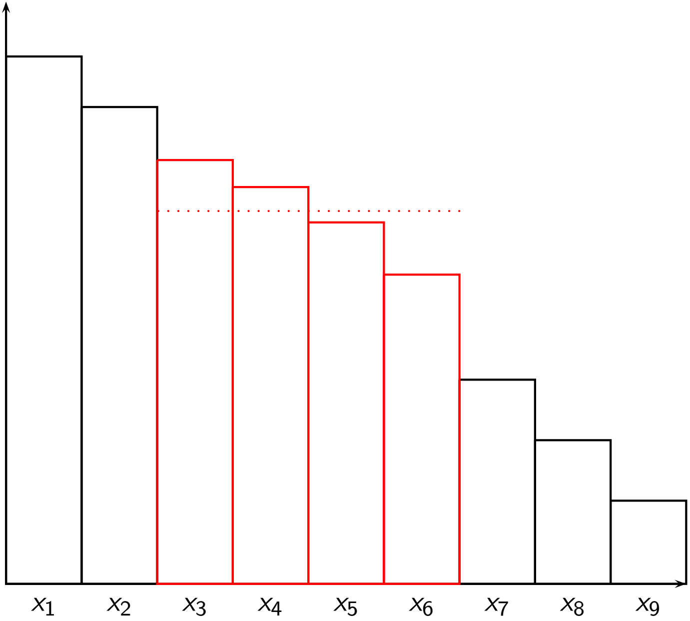
Sandpile model

- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- Each HKZ-reduction gives a worst-case profile.
  $\rightarrow$ The initial x_i's fully determine the x_i's after a call to HKZ.
- The sandpile execution of BKZ is deterministic.

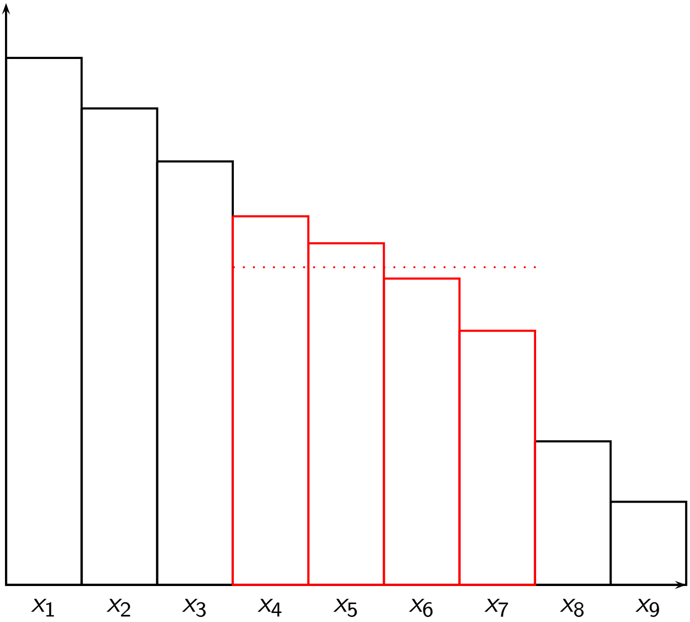

x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9


x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9

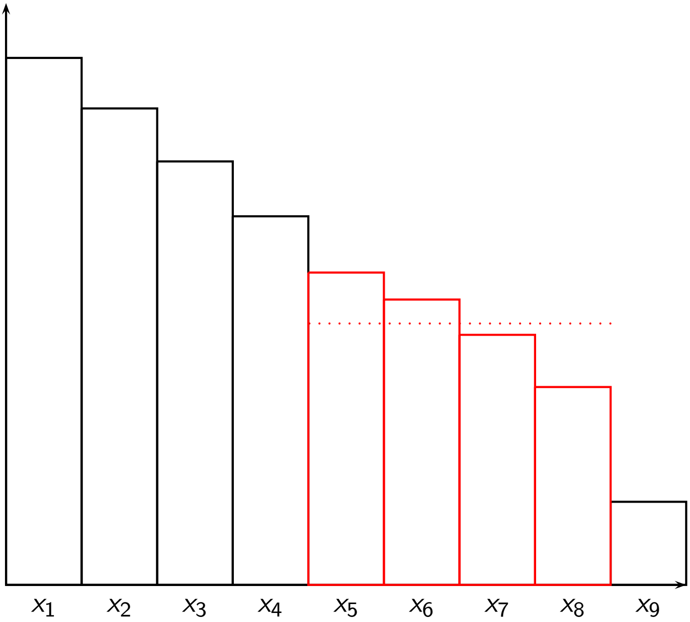

x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9

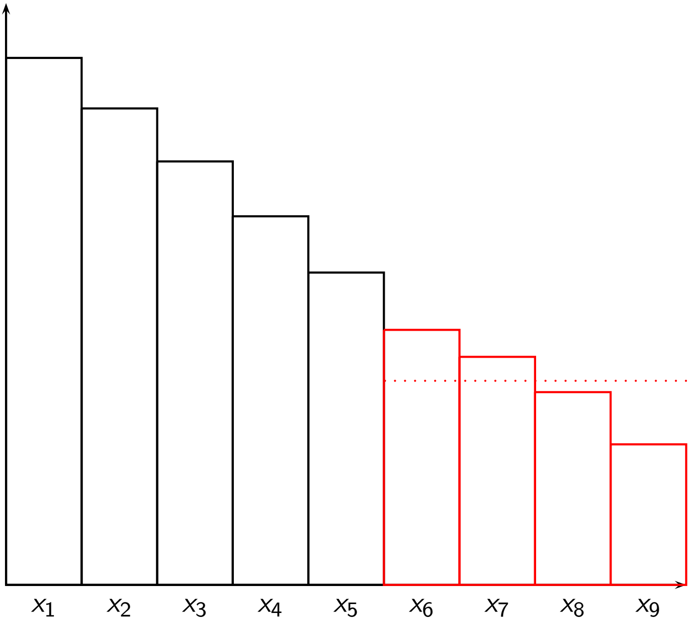


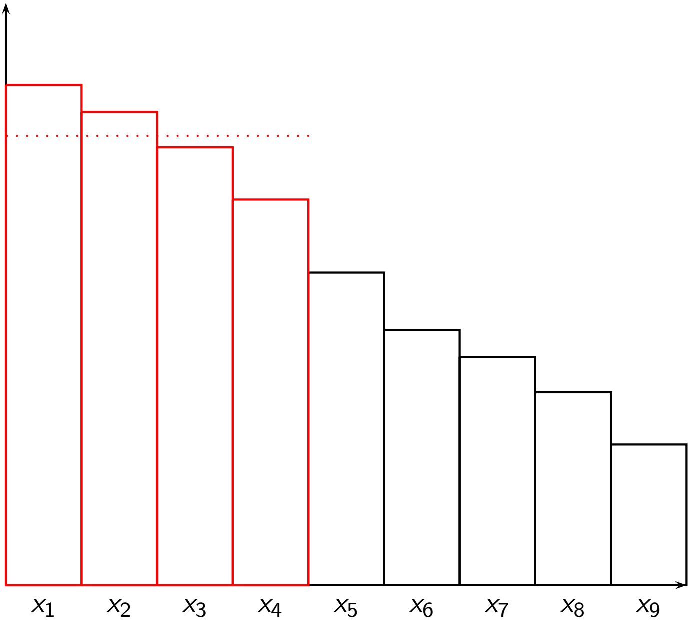
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9



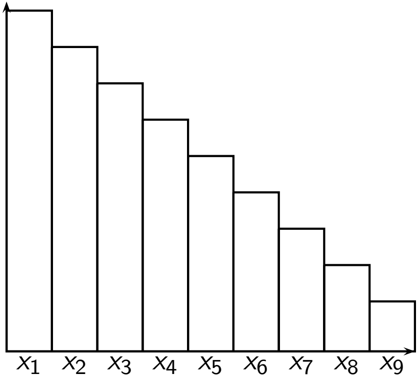
x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9


x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9


x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9


x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9

Matricial interpretation



$X = (x_1, \dots, x_n)^T$

$X_{0.5} \leftarrow A_1 X$

$X_1 \leftarrow A_1 X + \Gamma_1$

$X_2 \leftarrow A_2 X_1 + \Gamma_2$

...

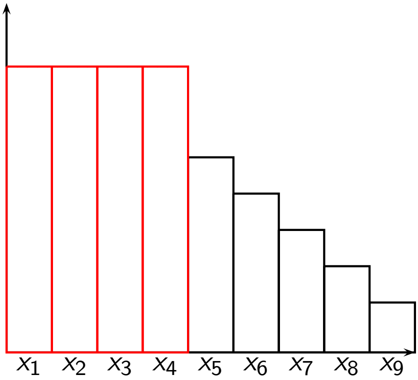
$X_k = A_k X_k + \Gamma_k$

with $k = n - \beta + 1$

A full tour:

$X' \leftarrow AX + \Gamma$

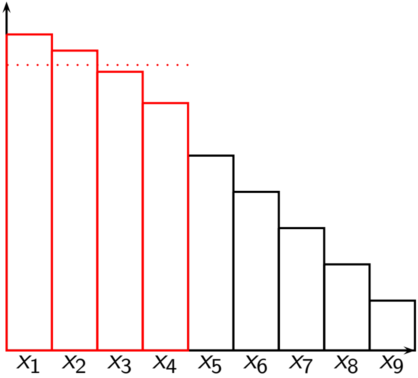
Matricial interpretation



$X = (x_1, \ldots, x_n)^T$
$X_{0.5} \leftarrow A_1 X$
$X_1 \leftarrow A_1 X + \Gamma_1$
$X_2 \leftarrow A_2 X_1 + \Gamma_2$
$\ldots$
$X_k = A_k X_k + \Gamma_k$
with $k = n - \beta + 1$

A full tour:
$X' \leftarrow AX + \Gamma$

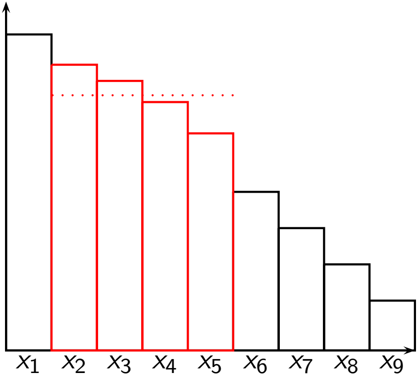
Matricial interpretation



$X = (x_1, \ldots, x_n)^T$
$X_{0.5} \leftarrow A_1 X$
$X_1 \leftarrow A_1 X + \Gamma_1$
$X_2 \leftarrow A_2 X_1 + \Gamma_2$
$\ldots$
$X_k = A_k X_k + \Gamma_k$
with $k = n - \beta + 1$

A full tour:
$X' \leftarrow AX + \Gamma$

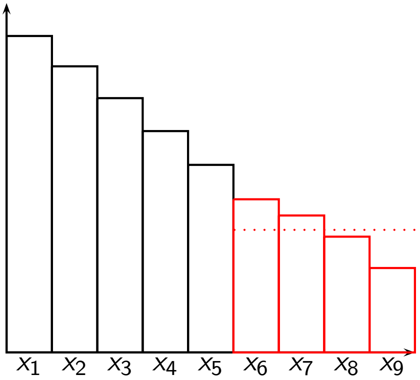
Matricial interpretation



$X = (x_1, \ldots, x_n)^T$
$X_{0.5} \leftarrow A_1 X$
$X_1 \leftarrow A_1 X + \Gamma_1$
$X_2 \leftarrow A_2 X_1 + \Gamma_2$
$\ldots$
$X_k = A_k X_k + \Gamma_k$
with $k = n - \beta + 1$

A full tour:
$X' \leftarrow AX + \Gamma$

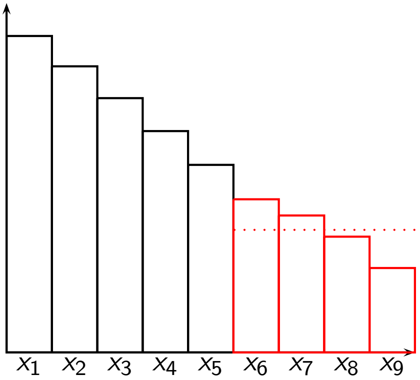
Matricial interpretation



$X = (x_1, \ldots, x_n)^T$
$X_{0.5} \leftarrow A_1 X$
$X_1 \leftarrow A_1 X + \Gamma_1$
$X_2 \leftarrow A_2 X_1 + \Gamma_2$
$\ldots$
$X_k = A_k X_k + \Gamma_k$
with $k = n - \beta + 1$

A full tour:
$X' \leftarrow AX + \Gamma$

Matricial interpretation



$X = (x_1, \ldots, x_n)^T$
$X_{0.5} \leftarrow A_1 X$
$X_1 \leftarrow A_1 X + \Gamma_1$
$X_2 \leftarrow A_2 X_1 + \Gamma_2$
$\ldots$
$X_k = A_k X_k + \Gamma_k$
with $k = n - \beta + 1$

A full tour:
$X' \leftarrow AX + \Gamma$

Expected properties of the model

$$X \leftarrow AX + \Gamma$$

- Well-reduced output:
  $\rightarrow$ study of fixed points ($X^\infty = AX^\infty + \Gamma$).
- Convergence in a polynomial number of steps:
  $\rightarrow$ study of eigenvalues of $A^T A$
  (so that $\|A^k X\|_2$ is bounded).

Expected properties of the model

$$X \leftarrow AX + \Gamma$$

- Well-reduced output:
  $\rightarrow$ study of fixed points ($X^\infty = AX^\infty + \Gamma$).
- Convergence in a polynomial number of steps:
  $\rightarrow$ study of eigenvalues of $A^T A$
  (so that $\|A^k X\|_2$ is bounded).

Expected properties of the model

$$X \leftarrow AX + \Gamma$$

- Well-reduced output:
  $\rightarrow$ study of fixed points ($X^\infty = AX^\infty + \Gamma$).
- Convergence in a polynomial number of steps:
  $\rightarrow$ study of eigenvalues of $A^T A$
  (so that $\|A^k X\|_2$ is bounded).

Fixed point X^∞ - Uniqueness

$$X^\infty = AX^\infty + \Gamma$$

- What matters is the rank of A.
- The solutions of $AX^\infty = X^\infty$ are vectors in $\mathrm{Span}(1, \ldots, 1)$.
- Unique solution if we consider only $\{X | \sum x_i = 0\}$.

Fixed point X^∞ - Uniqueness

$$X^\infty = AX^\infty + \Gamma$$

- What matters is the rank of A.
- The solutions of $AX^\infty = X^\infty$ are vectors in $\mathrm{Span}(1, \ldots, 1)$.
- Unique solution if we consider only $\{X | \sum x_i = 0\}$.

Fixed point X^∞ - Uniqueness

$$X^\infty = AX^\infty + \Gamma$$

- What matters is the rank of A.
- The solutions of $AX^\infty = X^\infty$ are vectors in $\mathrm{Span}(1, \ldots, 1)$.
- Unique solution if we consider only $\{X | \sum x_i = 0\}$.

Fixed point X^∞ - Existence

- The last β vectors have the shape of an HKZ-reduced basis.
- Recursive formula for the previous vectors:

$$x_i^\infty = \frac{\beta}{2(\beta-1)} \log \gamma_\beta + \sum_{j=i+1}^{i+\beta} \frac{x_j^\infty}{\beta - 1}.$$

- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta-1}$.

Fixed point X^∞ - Existence

- The last β vectors have the shape of an HKZ-reduced basis.
- Recursive formula for the previous vectors:

$$x_i^\infty = \frac{\beta}{2(\beta-1)} \log \gamma_\beta + \sum_{j=i+1}^{i+\beta} \frac{x_j^\infty}{\beta - 1}.$$

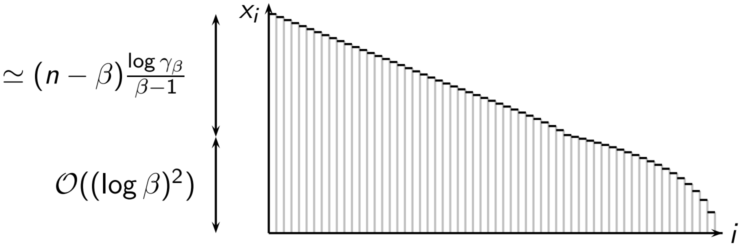
- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta-1}$.

Fixed point X^∞ - Existence

- The last β vectors have the shape of an HKZ-reduced basis.
- Recursive formula for the previous vectors:

$$x_i^\infty = \frac{\beta}{2(\beta-1)} \log \gamma_\beta + \sum_{j=i+1}^{i+\beta} \frac{x_j^\infty}{\beta - 1}.$$

- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta-1}$.



Eigenvalues of $A^T A$

- Method: study of the roots of the characteristic polynomial of $A^T A$.
- Let $\chi_n(\lambda) = \det(\lambda I_n - A_n^T A_n)$.
  Recurrence formula:

$$\chi_{n+2}(\lambda) = \frac{[2\beta(\beta-1)+1]\,\lambda - 1}{\beta^2}\chi_{n+1} - \left(\frac{\beta-1}{\beta}\right)^2 \lambda^2 \chi_n$$

- By a change of variable, it becomes a classical recurrence (Chebyshev polynomials):

$$\psi_{n+2}(\mu) = 2\mu\psi_{n+1}(\mu) - \psi_n(\mu)$$

(change of variable: $\tau(\mu) = 2\beta(\beta-1)(\mu-1)$ et $\psi_n(\mu) = \left(\frac{\beta}{\beta-1}\right)^{n-\beta} \cdot \frac{\bar{\chi}_n(1-\tau(\mu))}{\tau(\mu)}$)

Eigenvalues of $A^T A$

- Method: study of the roots of the characteristic polynomial of $A^T A$.
- Let $\chi_n(\lambda) = \det(\lambda I_n - A_n^T A_n)$.
  Recurrence formula:

$$\chi_{n+2}(\lambda) = \frac{[2\beta(\beta-1)+1]\,\lambda - 1}{\beta^2}\chi_{n+1} - \left(\frac{\beta-1}{\beta}\right)^2 \lambda^2 \chi_n$$

- By a change of variable, it becomes a classical recurrence (Chebyshev polynomials):

$$\psi_{n+2}(\mu) = 2\mu\psi_{n+1}(\mu) - \psi_n(\mu)$$

(change of variable: $\tau(\mu) = 2\beta(\beta-1)(\mu-1)$ et $\psi_n(\mu) = \left(\frac{\beta}{\beta-1}\right)^{n-\beta} \cdot \frac{\bar{\chi}_n(1-\tau(\mu))}{\tau(\mu)}$)

Eigenvalues of $A^T A$

- Method: study of the roots of the characteristic polynomial of $A^T A$.
- Let $\chi_n(\lambda) = \det(\lambda I_n - A_n^T A_n)$.
  Recurrence formula:

$$\chi_{n+2}(\lambda) = \frac{[2\beta(\beta-1)+1]\,\lambda - 1}{\beta^2}\chi_{n+1} - \left(\frac{\beta-1}{\beta}\right)^2 \lambda^2 \chi_n$$

- By a change of variable, it becomes a classical recurrence (Chebyshev polynomials):

$$\psi_{n+2}(\mu) = 2\mu\psi_{n+1}(\mu) - \psi_n(\mu)$$

(change of variable: $\tau(\mu) = 2\beta(\beta-1)(\mu-1)$ et $\psi_n(\mu) = \left(\frac{\beta}{\beta-1}\right)^{n-\beta} \cdot \frac{\bar{\chi}_n(1-\tau(\mu))}{\tau(\mu)}$)

- Explicit expression for ψ_n:

$$\psi_n = U_{n-\beta+1} - \frac{\beta-1}{\beta} U_{n-\beta}$$

with $U_n(\cos x) = \frac{\sin(nx)}{\sin x}$.

- Studying this function leads to the following results:
  - 1 is a simple root of the characteristic polynomial.
  - The second largest eigenvalue of $A^T A$ is

$$\leq 1 - \frac{1}{2}\frac{\beta^2}{n^2}.$$

- Explicit expression for ψ_n:

$$\psi_n = U_{n-\beta+1} - \frac{\beta - 1}{\beta} U_{n-\beta}$$

with $U_n(\cos x) = \frac{\sin(nx)}{\sin x}$.

- Studying this function leads to the following results:
  - 1 is a simple root of the characteristic polynomial.
  - The second largest eigenvalue of $A^T A$ is

$$\leq 1 - \frac{1}{2}\frac{\beta^2}{n^2}.$$

Results on the sandpile model

- The slope $-\frac{\log \gamma_\beta}{\beta-1}$ of the fixed point corresponds to a Hermite factor $\frac{\|b_1\|}{(\det L)^{1/n}}$ close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.
- Geometric convergence: $\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours, *i.e.* $\frac{n^3}{\beta^2}$ calls to HKZ_β.
- $\frac{n^3}{\beta^2}(\log \frac{n}{\epsilon} + \log\log \frac{\max \|b_i\|}{(\det L)^{1/n}})$ calls to HKZ_β are enough to obtain $\|X - X^\infty\| < \epsilon$.

Results on the sandpile model

- The slope $-\frac{\log \gamma_\beta}{\beta - 1}$ of the fixed point corresponds to a Hermite factor $\frac{\|b_1\|}{(\det L)^{1/n}}$ close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.
- Geometric convergence: $\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours, *i.e.* $\frac{n^3}{\beta^2}$ calls to HKZ$_\beta$.
- $\frac{n^3}{\beta^2}(\log \frac{n}{\epsilon} + \log\log \frac{\max \|b_i\|}{(\det L)^{1/n}})$ calls to HKZ$_\beta$ are enough to obtain $\|X - X^\infty\| < \epsilon$.

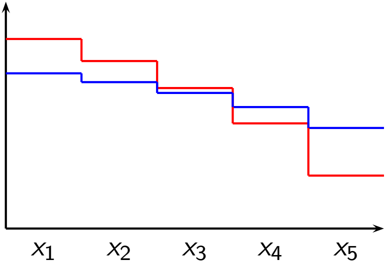
Results on the sandpile model

- The slope $-\frac{\log \gamma_\beta}{\beta - 1}$ of the fixed point corresponds to a Hermite factor $\frac{\|b_1\|}{(\det L)^{1/n}}$ close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.
- Geometric convergence: $\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours, *i.e.* $\frac{n^3}{\beta^2}$ calls to HKZ_β.
- $\frac{n^3}{\beta^2}(\log \frac{n}{\epsilon} + \log\log \frac{\max \|b_i\|}{(\det L)^{1/n}})$ calls to HKZ_β are enough to obtain $\|X - X^\infty\| < \epsilon$.

Comparison between the model and BKZ

When the determinant is fixed, there is no vector inequality on the x_i's between:

- a worst-case HKZ-reduced basis (equalities in Minkowski inequalities)
- an arbitrary HKZ-reduced basis (strict inequalities).

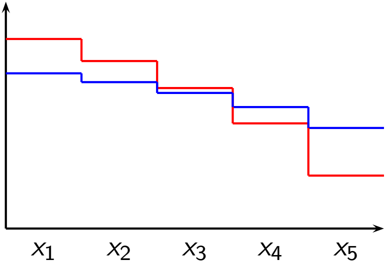


→ The previous results cannot be transposed directly.

Comparison between the model and BKZ

When the determinant is fixed, there is no vector inequality on the x_i's between:

- a worst-case HKZ-reduced basis (equalities in Minkowski inequalities)
- an arbitrary HKZ-reduced basis (strict inequalities).



$\rightarrow$ The previous results cannot be transposed directly.

Change of basis

- Obtaining information on the individual x_i's is difficult.
- The model can give some information on $\pi_i = \frac{1}{i}\sum_{j=1}^{i} x_j$, the mean of the first x_j's.
- New dynamical system: $\Pi \leftarrow \widetilde{A}\Pi + \widetilde{\Gamma} \quad (\widetilde{A} = PAP^{-1})$
- In the real world, we still have $\Pi \leftarrow \Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ (coefficient-wise).

Change of basis

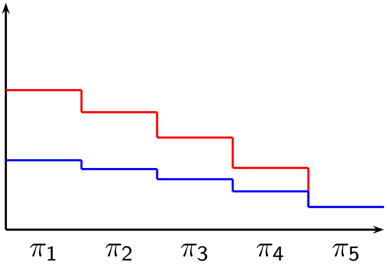
- Obtaining information on the individual x_i's is difficult.
- The model can give some information on $\pi_i = \frac{1}{i}\sum_{j=1}^{i} x_j$, the mean of the first x_j's.
- New dynamical system: $\Pi \leftarrow \widetilde{A}\Pi + \widetilde{\Gamma} \quad (\widetilde{A} = PAP^{-1})$
- In the real world, we still have $\Pi \leftarrow \Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ (coefficient-wise).

Change of basis

- Obtaining information on the individual x_i's is difficult.
- The model can give some information on $\pi_i = \frac{1}{i}\sum_{j=1}^{i} x_j$, the mean of the first x_j's.
- New dynamical system: $\Pi \leftarrow \widetilde{A}\Pi + \widetilde{\Gamma} \quad (\widetilde{A} = PAP^{-1})$
- In the real world, we still have $\Pi \leftarrow \Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ (coefficient-wise).

Change of basis

- Obtaining information on the individual x_i's is difficult.
- The model can give some information on $\pi_i = \frac{1}{i}\sum_{j=1}^{i} x_j$, the mean of the first x_j's.
- New dynamical system: $\Pi \leftarrow \widetilde{A}\Pi + \widetilde{\Gamma} \quad (\widetilde{A} = PAP^{-1})$



- In the real world, we still have $\Pi \leftarrow \Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ (coefficient-wise).

Results on BKZ_β

Using the inequality $\Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ recursively gives:

$$\Pi^{[k]} - \Pi^{\infty} \leq \widetilde{A}^{k}(\Pi^{[0]} - \Pi^{\infty}).$$

The upper bound on the eigenvalues of $A^T A$ is used to bound the 2-norm of the right term.

$$\Pi^{[k]} - \Pi^{\infty} \leq (1 + \log n)^{\frac{1}{2}} \left(1 - \frac{\beta^2}{2n^2}\right)^{\frac{k}{2}} \|\Pi^{[0]} - \Pi^{\infty}\|_2$$

Results on BKZ_β

Using the inequality $\Pi' \leq \widetilde{A}\Pi + \widetilde{\Gamma}$ recursively gives:

$$\Pi^{[k]} - \Pi^{\infty} \leq \widetilde{A}^{k}(\Pi^{[0]} - \Pi^{\infty}).$$

The upper bound on the eigenvalues of $A^T A$ is used to bound the 2-norm of the right term.

$$\Pi^{[k]} - \Pi^{\infty} \leq (1 + \log n)^{\frac{1}{2}} \left(1 - \frac{\beta^2}{2n^2}\right)^{\frac{k}{2}} \|\Pi^{[0]} - \Pi^{\infty}\|_2$$

Meaning of the Π_i's:

- $\pi_1 = x_1 = \log \|b_1\|$
- $\pi_n = \sum_{i=1}^{n} x_i = \log \det L$

$$\Pi^{[k]} - \Pi^{\infty} \leq (1 + \log n)^{\frac{1}{2}} \left(1 - \frac{\beta^2}{2n^2}\right)^{\frac{k}{2}} \|\Pi^{[0]} - \Pi^{\infty}\|_2$$

$\rightarrow \frac{\|b_1\|}{(\det L)^{1/n}} \leq (1+\epsilon)\gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}}$ in $\widetilde{\mathcal{O}}(\frac{n^2}{\beta^2} \cdot n)$ calls to HKZ_β.

Meaning of the Π_i's:

- $\pi_1 = x_1 = \log \|b_1\|$
- $\pi_n = \sum_{i=1}^{n} x_i = \log \det L$

$$\Pi^{[k]} - \Pi^{\infty} \leq (1 + \log n)^{\frac{1}{2}} \left(1 - \frac{\beta^2}{2n^2}\right)^{\frac{k}{2}} \|\Pi^{[0]} - \Pi^{\infty}\|_2$$

$\rightarrow \frac{\|b_1\|}{(\det L)^{1/n}} \leq (1 + \epsilon)\gamma_{\beta}^{\frac{n-1}{2(\beta-1)} + \frac{3}{2}}$ in $\widetilde{\mathcal{O}}(\frac{n^2}{\beta^2} \cdot n)$ calls to HKZ_{β}.

Differences between LLL and BKZ_2

- Swaps in LLL / HKZ_2 = Gauss-reductions in BKZ_2.
  $\rightarrow$ the complexity of both operations is $\widetilde{\mathcal{O}}(\text{size}(B))$.
- Different, non-adaptative order in BKZ_2.

Differences between LLL and BKZ_2

- Swaps in LLL / HKZ_2 = Gauss-reductions in BKZ_2.
  $\rightarrow$ the complexity of both operations is $\widetilde{\mathcal{O}}(\text{size}(B))$.
- Different, non-adaptative order in BKZ_2.

Differences between LLL and BKZ_2

- Swaps in LLL / HKZ_2 = Gauss-reductions in BKZ_2.
  $\rightarrow$ the complexity of both operations is $\widetilde{\mathcal{O}}(\mathrm{size}(B))$.
- Different, non-adaptative order in BKZ_2.

Quasi-linear LLL

In BKZ_2:

- Each Gauss-reduction costs $\widetilde{\mathcal{O}}(\log \max \|b_i\|)$.
- $\mathcal{P}oly(n) \times \log \log \max_i \frac{\|b_i^*\|}{(\det L)^{1/n}}$ Gauss-reductions.
- A basis such that $\frac{\|b_1\|}{(\det L)^{1/n}} \leq \sqrt{\frac{4}{3}}^{n-1}(1+\epsilon)$ is returned.
- With more work, it is possible to obtain an LLL-reduced basis.

Conclusion

- The optimal quality that can be proven for BKZ_β is reached in a polynomial number of calls to HKZ_β.
- Binary complexity of BKZ_2?
- Adaptive strategies.
- In practice, the algorithm reaches better approximation factors than expected.
  $\rightarrow$ For how long is it interesting to continue the execution once we go beyond the theorical factor?