Analyzing Blockwise Lattice Algorithms using Dynamical Systems

Guillaume Hanrot, Xavier Pujol, Damien Stehlé

ENS Lyon, LIP (CNRS – ENSL – INRIA – UCBL - ULyon)

Context

- Lattices provide exponentially hard problems suitable for public key cryptography.
- Best known attacks on lattice-based cryptosystems rely on blockwise lattice reduction algorithms.
- Understanding these algorithms helps assessing the security of LBC.
- The most widely used reduction algorithm is BKZ.
- No reasonable time bound was known about BKZ.

Context

- Lattices provide exponentially hard problems suitable for public key cryptography.
- Best known attacks on lattice-based cryptosystems rely on blockwise lattice reduction algorithms.
- Understanding these algorithms helps assessing the security of LBC.
- The most widely used reduction algorithm is BKZ.
- No reasonable time bound was known about BKZ.

Context

- Lattices provide exponentially hard problems suitable for public key cryptography.
- Best known attacks on lattice-based cryptosystems rely on blockwise lattice reduction algorithms.
- Understanding these algorithms helps assessing the security of LBC.
- The most widely used reduction algorithm is BKZ.
- No reasonable time bound was known about BKZ.

Context

- Lattices provide exponentially hard problems suitable for public key cryptography.
- Best known attacks on lattice-based cryptosystems rely on blockwise lattice reduction algorithms.
- Understanding these algorithms helps assessing the security of LBC.
- The most widely used reduction algorithm is BKZ.
- No reasonable time bound was known about BKZ.

Context

- Lattices provide exponentially hard problems suitable for public key cryptography.
- Best known attacks on lattice-based cryptosystems rely on blockwise lattice reduction algorithms.
- Understanding these algorithms helps assessing the security of LBC.
- The most widely used reduction algorithm is BKZ.
- No reasonable time bound was known about BKZ.

Contributions

- We give the first worst-case analysis of BKZ.
- We introduce a new BKZ model.
- It gives new tools for understanding lattice algorithms.

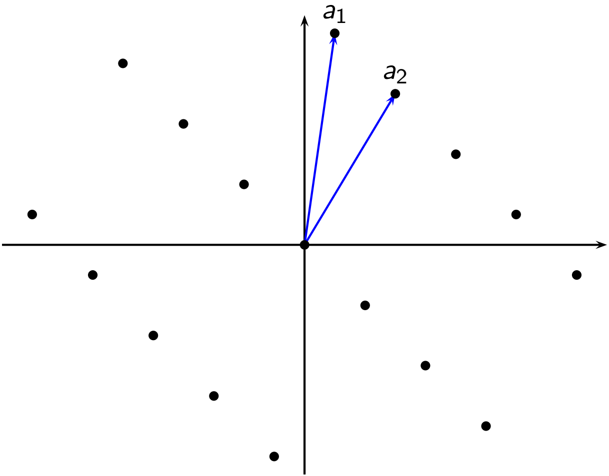
Contributions

- We give the first worst-case analysis of BKZ.
- We introduce a new BKZ model.
- It gives new tools for understanding lattice algorithms.

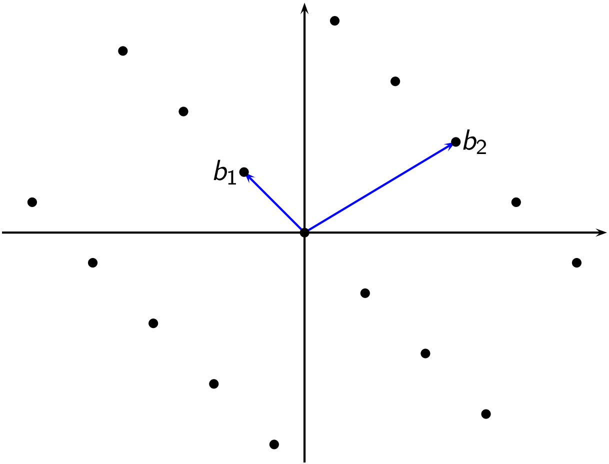
Contributions

- We give the first worst-case analysis of BKZ.
- We introduce a new BKZ model.
- It gives new tools for understanding lattice algorithms.

Lattices

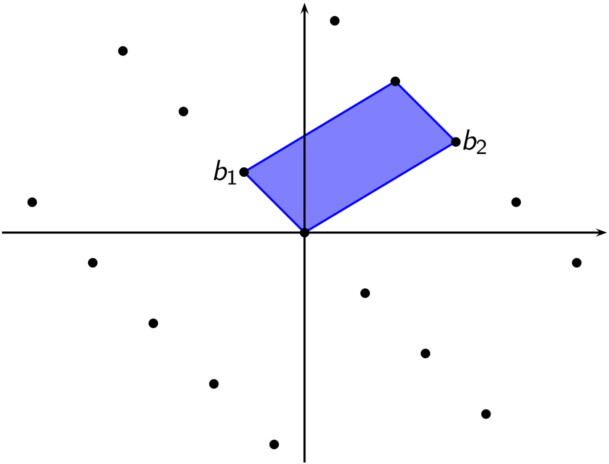


Lattices



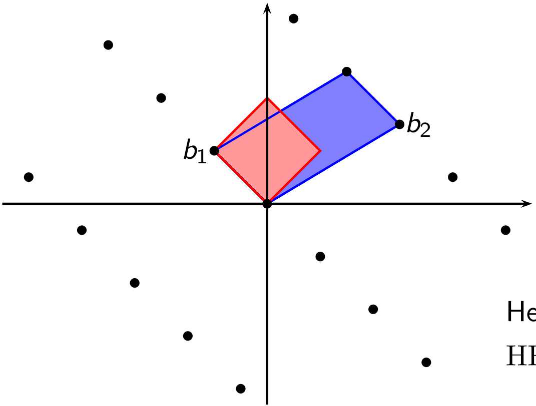
Lattice reduction

Lattices



Determinant

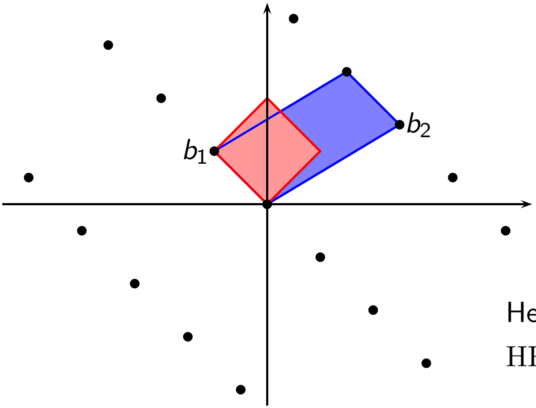
Lattices



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

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector $\neq 0$, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with γ_n = Hermite constant $\leq n$.

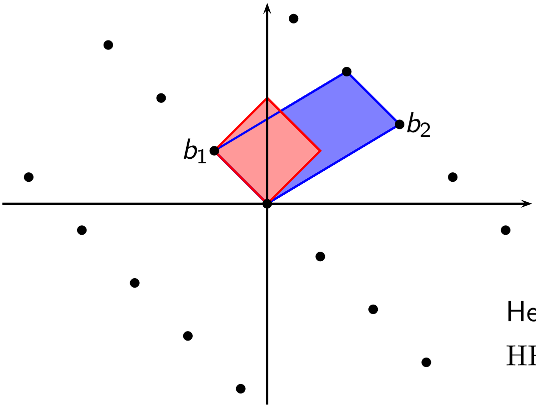
Lattices



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

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector $\neq 0$, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with γ_n = Hermite constant $\leq n$.

Lattices



Hermite factor of B:

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

- Goal of lattice reduction: find a basis with small HF.
- If b_1 is a shortest vector $\neq 0$, then $\mathrm{HF}(b_1, \ldots, b_n) \leq \sqrt{\gamma_n}$, with $\gamma_n =$ Hermite constant $\leq n$.

Hierarchy of lattice reductions in dimension n

$x_i = \log \|b_i^*\|$ for $i \leq n$ ($b_1^*, \ldots, b_n^* =$ Gram-Schmidt basis of B).

Hierarchy of lattice reductions in dimension n

$x_i = \log \|b_i^*\|$ for $i \le n$ ($b_1^*, \ldots, b_n^*$ = Gram-Schmidt basis of B).

HKZ
Hermite-Korkine-Zolorareff

HF: $\sqrt{\gamma_n}$

Time: $2^{O(n)}$

BKZ$_\beta$
Block Korkine-Zolotareff

$\simeq (\gamma_\beta)^{\frac{n}{2\beta}}$

$2^{O(\beta)} \times ?$

LLL
Lenstra-Lenstra-Lovász

$\simeq (\gamma_2)^{\frac{n}{2}}$

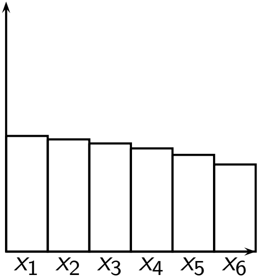
$\mathrm{Poly}(n)$

Hierarchy of lattice reductions in dimension n

$x_i = \log \|b_i^*\|$ for $i \le n$ ($b_1^*, \ldots, b_n^*$ = Gram-Schmidt basis of B).

HKZ

Hermite-Korkine-Zolorareff



HF: $\sqrt{\gamma_n}$

Time: $2^{O(n)}$

BKZ$_\beta$

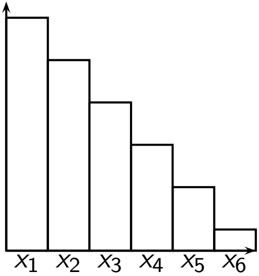
Block Korkine-Zolotareff

$\simeq (\gamma_\beta)^{\frac{n}{2\beta}}$

$2^{O(\beta)} \times ?$

LLL

Lenstra-Lenstra-Lovász



$\simeq (\gamma_2)^{\frac{n}{2}}$

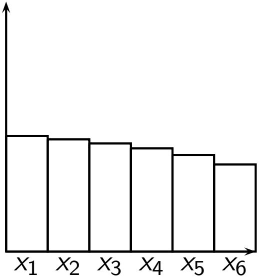
$\mathrm{Poly}(n)$

Hierarchy of lattice reductions in dimension n

$$x_i = \log \|b_i^*\| \text{ for } i \leq n \; (b_1^*, \ldots, b_n^* = \text{Gram-Schmidt basis of } B).$$

HKZ

Hermite-Korkine-Zolorareff

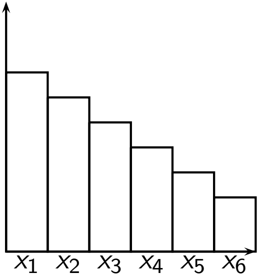


HF: $\sqrt{\gamma_n}$

Time: $2^{O(n)}$

BKZ$_\beta$

Block Korkine-Zolotareff



$\simeq (\gamma_\beta)^{\frac{n}{2\beta}}$

$2^{O(\beta)} \times ?$

LLL

Lenstra-Lenstra-Lovász

$\simeq (\gamma_2)^{\frac{n}{2}}$

$\mathrm{Poly}(n)$

Known results on blockwise algorithms

BKZ

- Schnorr (1987): first hierarchies between LLL and HKZ.
- Schnorr and Euchner (1994): algorithm for BKZ-reduction.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Other reductions in time $2^{O(\beta)} \times \mathrm{Poly}(n)$:

- Schnorr (1987) : Semi-block-2β-reduction.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

...but BKZ remains the most efficient in practice.

Known results on blockwise algorithms

BKZ

- Schnorr (1987): first hierarchies between LLL and HKZ.
- Schnorr and Euchner (1994): algorithm for BKZ-reduction.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Other reductions in time $2^{O(\beta)} \times \mathrm{Poly}(n)$:

- Schnorr (1987) : Semi-block-2β-reduction.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

...but BKZ remains the most efficient in practice.

Known results on blockwise algorithms

BKZ

- Schnorr (1987): first hierarchies between LLL and HKZ.
- Schnorr and Euchner (1994): algorithm for BKZ-reduction.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Other reductions in time $2^{O(\beta)} \times \mathrm{Poly}(n)$:

- Schnorr (1987) : Semi-block-2β-reduction.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

...but BKZ remains the most efficient in practice.

Known results on blockwise algorithms

BKZ

- Schnorr (1987): first hierarchies between LLL and HKZ.
- Schnorr and Euchner (1994): algorithm for BKZ-reduction.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Other reductions in time $2^{O(\beta)} \times \mathrm{Poly}(n)$:

- Schnorr (1987) : Semi-block-2β-reduction.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

...but BKZ remains the most efficient in practice.

Known results on blockwise algorithms

BKZ

- Schnorr (1987): first hierarchies between LLL and HKZ.
- Schnorr and Euchner (1994): algorithm for BKZ-reduction.
- Gama and Nguyen (2008): BKZ behaves badly when the block size is ≥ 25.

Other reductions in time $2^{O(\beta)} \times \mathrm{Poly}(n)$:

- Schnorr (1987) : Semi-block-2β-reduction.
- Gama *et al.* (2006): Block-Rankin-reduction.
- Gama and Nguyen (2008): Slide-reduction.

...but BKZ remains the most efficient in practice.

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 a projection of the block $(b_i, \ldots, b_{i+\beta-1})$.
    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 a projection of the block $(b_i, \ldots, b_{i+\beta-1})$.
    Report the transformation on B.

Termination?

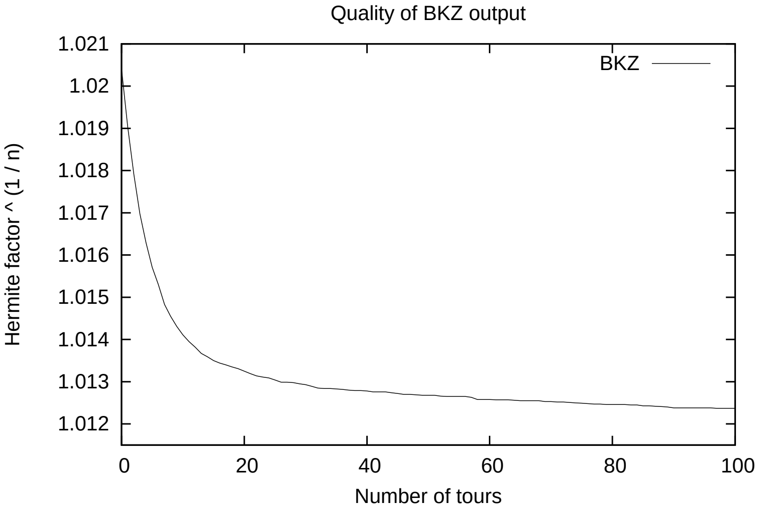
BKZ

Algorithm (BKZ_β, modified version)

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

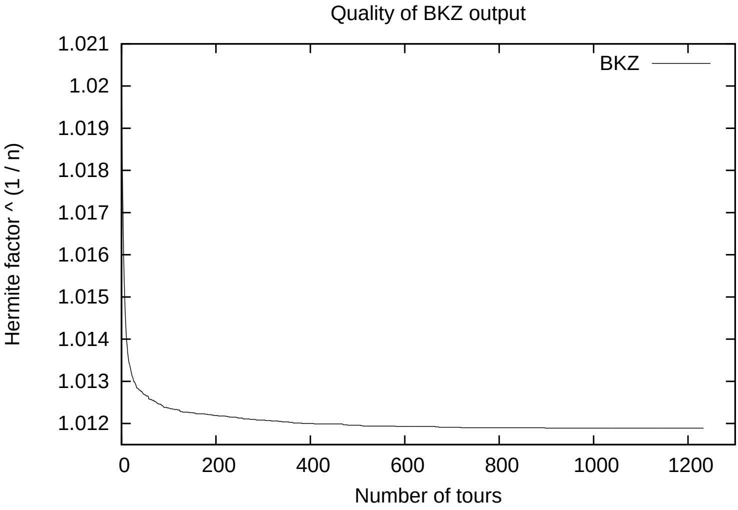
Termination?

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:*

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

Sandpile model

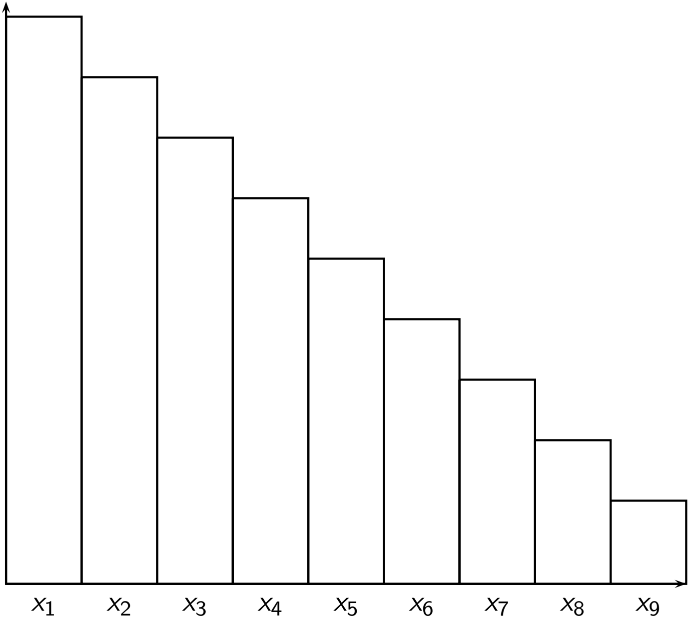
- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- We assume that HKZ-reductions correspond to a fixed pattern.
- The information on the initial x_i's fully determines the x_i's after a call to HKZ.

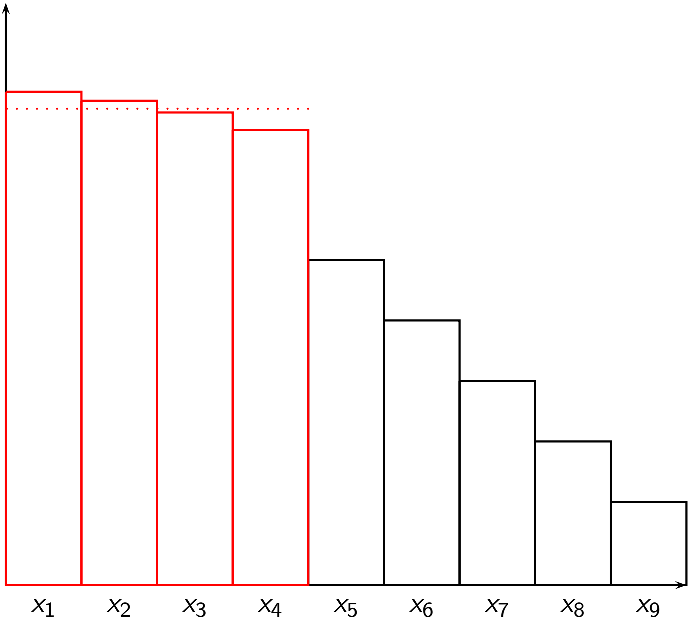
Sandpile model

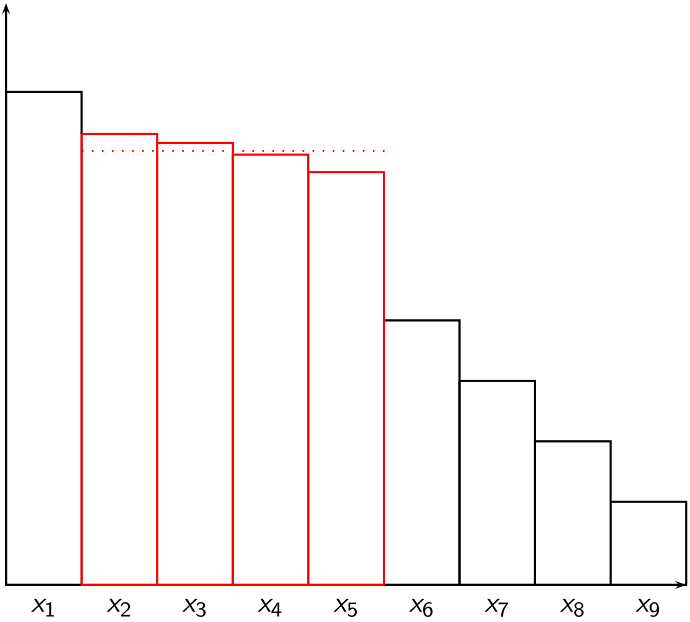
- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- We assume that HKZ-reductions correspond to a fixed pattern.
- The information on the initial x_i's fully determines the x_i's after a call to HKZ.

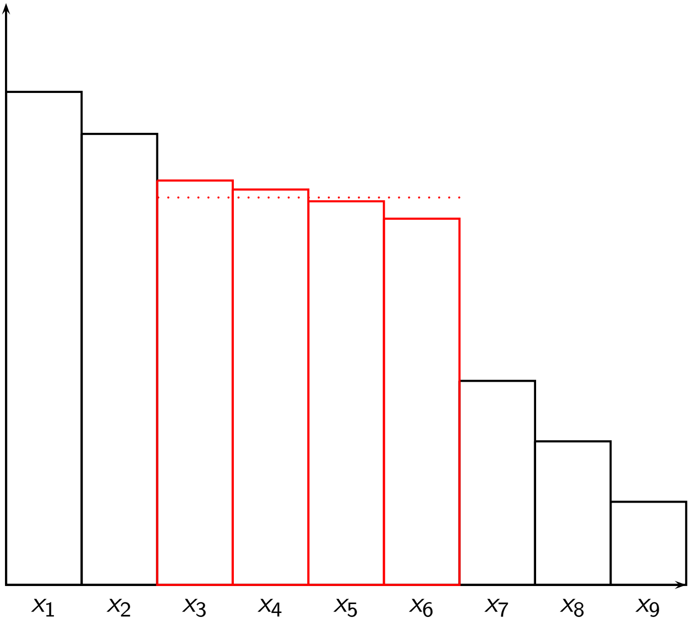
Sandpile model

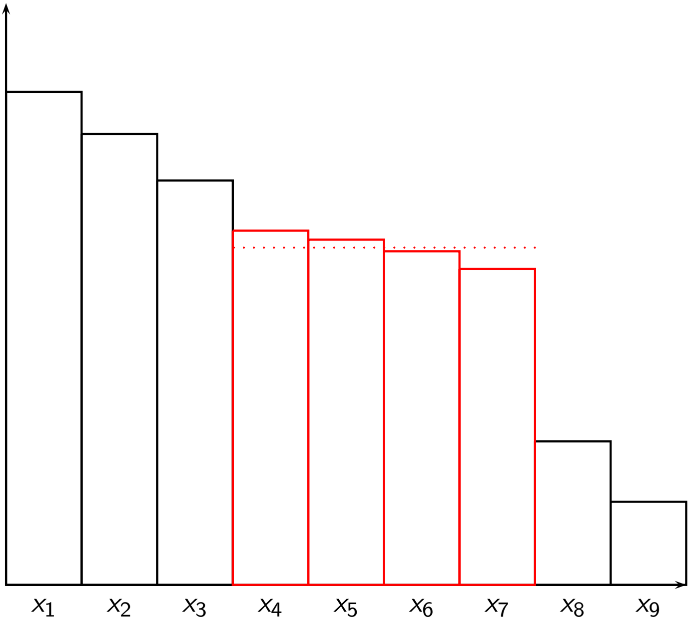
- We consider only $x_i = \log \|b_i^*\|$ for $i \leq n$.
- We assume that HKZ-reductions correspond to a fixed pattern.
- The information on the initial x_i's fully determines the x_i's after a call to HKZ.

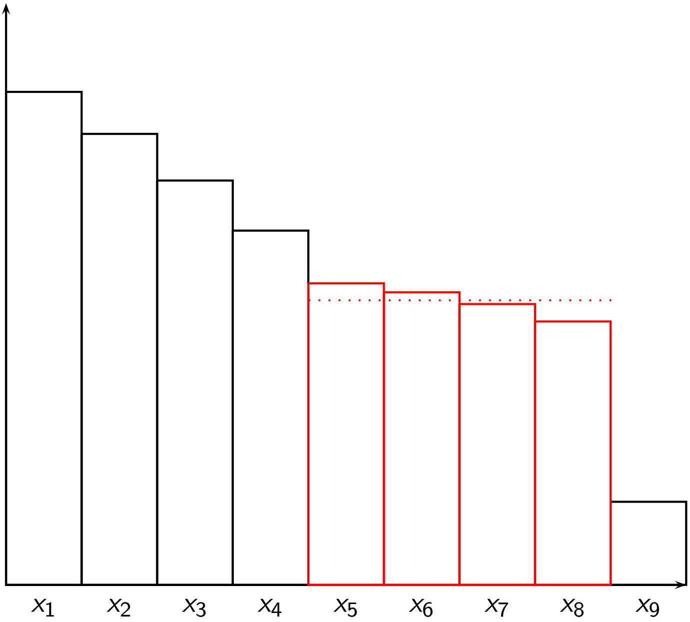

x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9

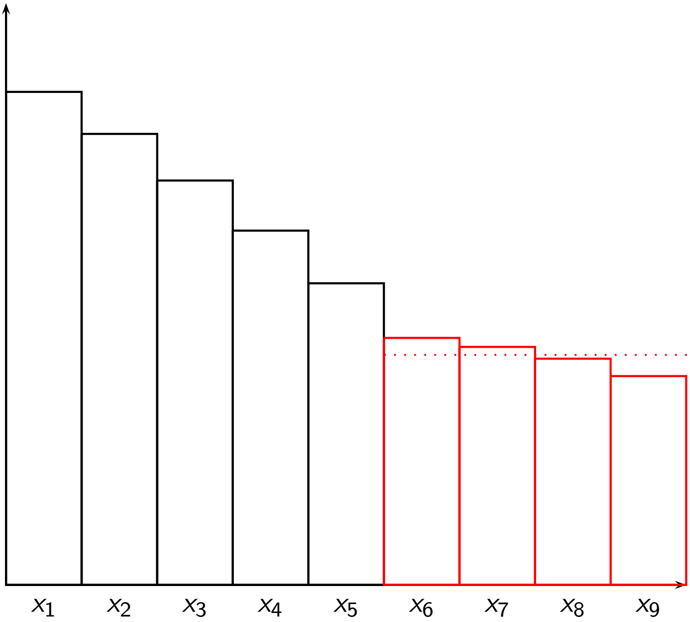

x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9

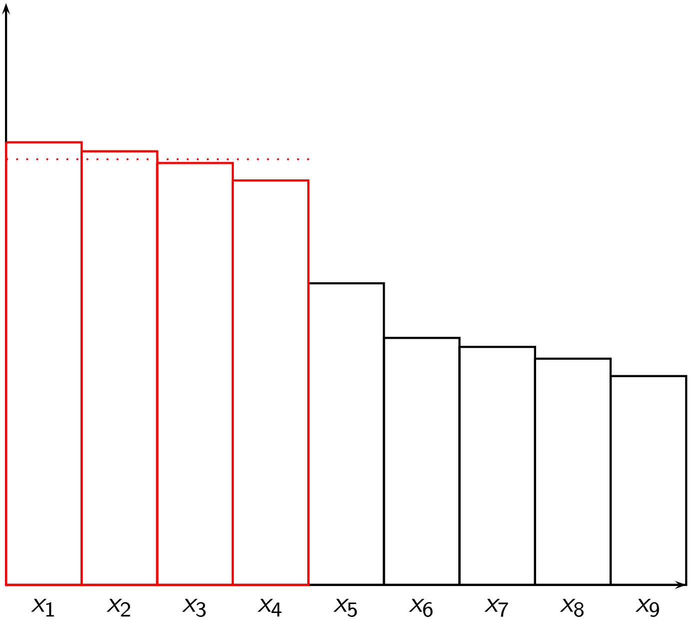

x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9


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

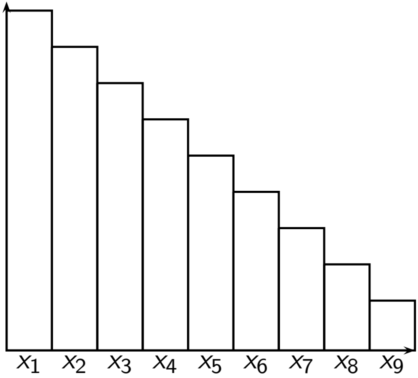

x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9


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

Matrix interpretation



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

$X_{0.5} \leftarrow A_1 X$

$X_1 \leftarrow A_1 X + \Gamma_1$

$X_2 \leftarrow A_2 X_1 + \Gamma_2$

$\ldots$

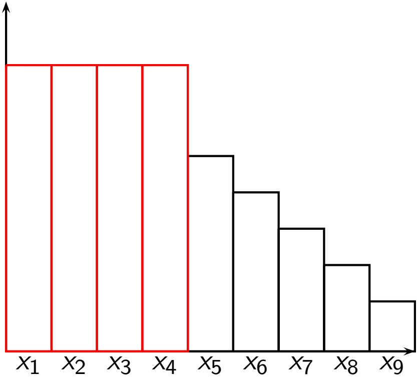
$X_k = A_k X_k + \Gamma_k$

with $k = n - \beta + 1$

A full tour:

$X' \leftarrow AX + \Gamma$

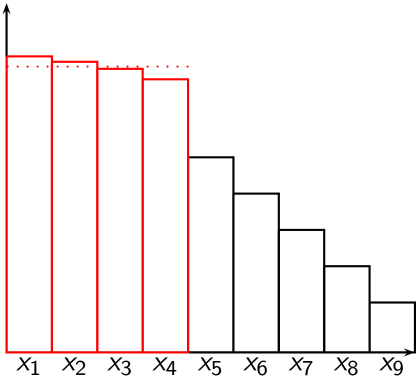
Matrix interpretation



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

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

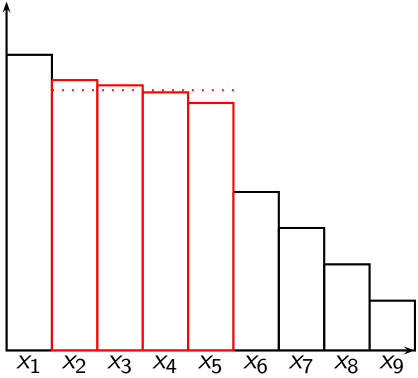
Matrix interpretation



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

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

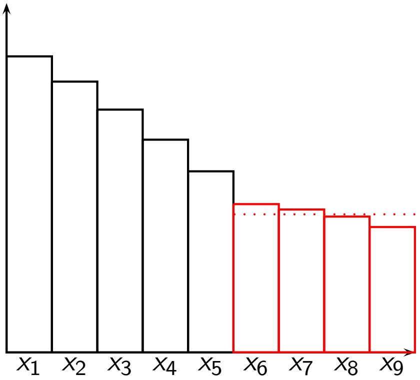
Matrix interpretation



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

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

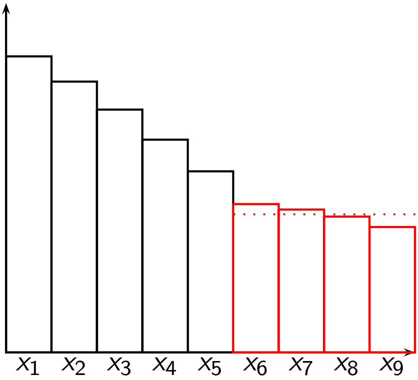
Matrix interpretation



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

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

Matrix 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 $k = n - \beta + 1$

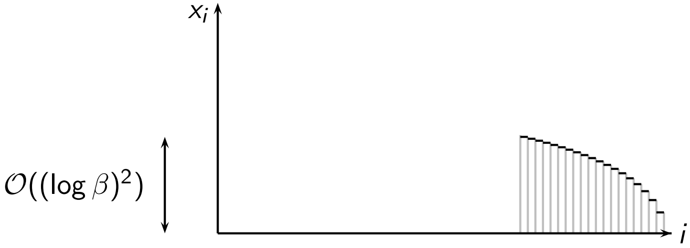
A full tour:
$X' \leftarrow AX + \Gamma$

Quality of the output

Method: study the fixed point of:

$$X = AX + \Gamma$$

- The β last x_i's have the shape of an HKZ-reduced basis.
- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta - 1}$.



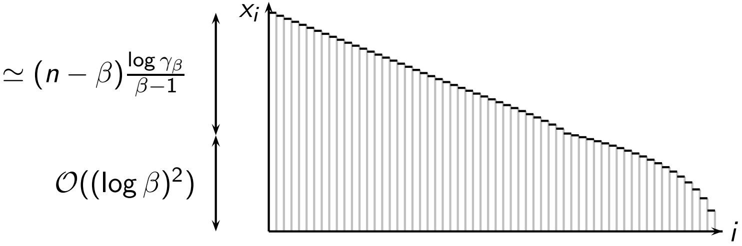
Corresponds to a Hermite factor close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.

Quality of the output

Method: study the fixed point of:

$$X = AX + \Gamma$$

- The β last x_i's have the shape of an HKZ-reduced basis.
- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta - 1}$.



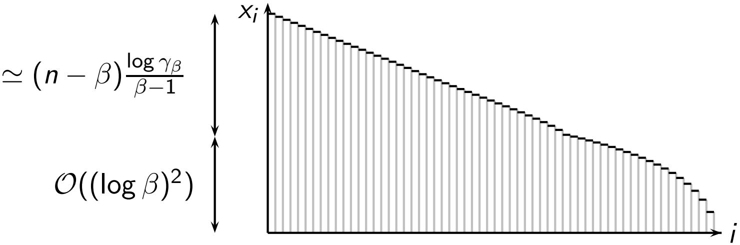
Corresponds to a Hermite factor close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.

Quality of the output

Method: study the fixed point of:

$$X = AX + \Gamma$$

- The β last x_i's have the shape of an HKZ-reduced basis.
- Asymptotically, line of slope $-\frac{\log \gamma_\beta}{\beta-1}$.



Corresponds to a Hermite factor close to $\gamma_\beta^{\frac{n-1}{2(\beta-1)}}$.

Fast convergence

Dynamical system:

$$X \leftarrow AX + \Gamma$$

Method: study of the eigenvalues of $A^T A$.

Result: the largest eigenvalue of $A^T A$ smaller than 1 is

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

$\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours.
$\rightarrow$ leads to the claimed complexity bound.

Fast convergence

Dynamical system:

$$X \leftarrow AX + \Gamma$$

Method: study of the eigenvalues of $A^T A$.

Result: the largest eigenvalue of $A^T A$ smaller than 1 is

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

$\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours.
$\rightarrow$ leads to the claimed complexity bound.

Fast convergence

Dynamical system:

$$X \leftarrow AX + \Gamma$$

Method: study of the eigenvalues of $A^T A$.

Result: the largest eigenvalue of $A^T A$ smaller than 1 is

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

$\|X - X^\infty\|$ decreases by a constant factor every $\frac{n^2}{\beta^2}$ tours.
$\rightarrow$ leads to the claimed complexity bound.

From the model to the real algorithm

- The results from the previous section cannot be used directly.
- By averaging the x_i's, a rigorous adaptation becomes possible.
- Working on the averages suffices to get the result.

From the model to the real algorithm

- The results from the previous section cannot be used directly.
- By averaging the x_i's, a rigorous adaptation becomes possible.
- Working on the averages suffices to get the result.

From the model to the real algorithm

- The results from the previous section cannot be used directly.
- By averaging the x_i's, a rigorous adaptation becomes possible.
- Working on the averages suffices to get the result.

Conclusion

- First analysis of BKZ.
- New methodology for analysing blockwise algorithms.

- Better strategies for reducing?
- The worst-case analysis does not fully explains the practical behaviour.
- Predictive model?

Conclusion

- First analysis of BKZ.
- New methodology for analysing blockwise algorithms.

- Better strategies for reducing?
- The worst-case analysis does not fully explains the practical behaviour.
- Predictive model?

Conclusion

- First analysis of BKZ.
- New methodology for analysing blockwise algorithms.

- Better strategies for reducing?
- The worst-case analysis does not fully explains the practical behaviour.
- Predictive model?

Conclusion

- First analysis of BKZ.
- New methodology for analysing blockwise algorithms.

- Better strategies for reducing?
- The worst-case analysis does not fully explains the practical behaviour.
- Predictive model?

Conclusion

- First analysis of BKZ.
- New methodology for analysing blockwise algorithms.

- Better strategies for reducing?
- The worst-case analysis does not fully explains the practical behaviour.
- Predictive model?