Modélisations de l'algorithme LLL et de ses entrées

Sur la base des travaux de:
B. Vallée, J. Clément, A. Vera, M. Georgieva, M. Madritsch, A. Akhavi,. . .
et bien d'autres encore!

Loïck Lhote
GREYC, UMR CNRS 6072,
ENSICAEN & Université de Caen Basse-Normandie

Projet ANR Dyna3S

Plan

Plan

GCD

Simultaneous Rational Approximation

Problem : Consider $\overrightarrow{y} \in \mathbb{R}^n$, find $q \in \mathbb{Z}$ with $q \leq M$ and $\overrightarrow{p} \in \mathbb{Z}^n$ such that $||q \cdot \overrightarrow{y} - \overrightarrow{p}||$ is small.

Continued Fraction Expansion

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots \, \cfrac{}{m_{p-1} + \cfrac{1}{m_p + 0}}}}}$$

This morning ...

Generalizations of the Euclid algorithm

Lattice reduction

- Algorithms : LLL, HKZ, BKZ, . . .
- Models for the algorithms (sandpile, CFG, . . .)
- Models for the inputs (cryptography, factorization, . . .)

This afternoon. . .

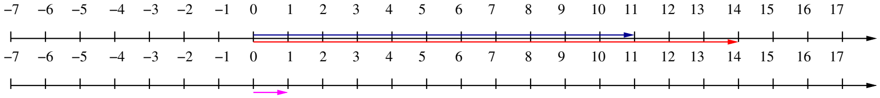
GCD
Simultaneous Rational Approximation

Problem : Consider $\overrightarrow{y} \in \mathbb{R}^n$, find $q \in \mathbb{Z}$ with $q \leq M$ and $\overrightarrow{p} \in \mathbb{Z}^n$ such that $||q \cdot \overrightarrow{y} - \overrightarrow{p}||$ is small.

Continued Fraction Expansion

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots \cfrac{}{m_{p-1} + \cfrac{1}{m_p + 0}}}}}$$

This morning . . .

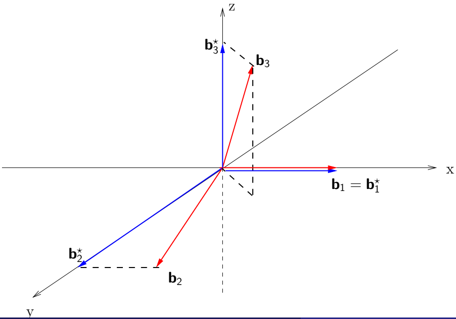


Plan

The LLL algorithm

Input : A lattice $\mathcal{L}$ given by a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$
$t > 1$

Output : A basis $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ of $\mathcal{L}$ such that the Gram-Schmidt Orthogonalization (GSO) satisfies ,



There exist a matrix M such that $\mathcal{B} = M\mathcal{B}^\star$ and

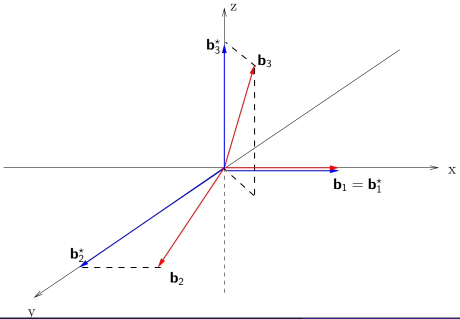
$$M = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \mu_{2,1} & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \mu_{m,1} & \cdots & \cdots & \mu_{m,m-1} & 1 \end{pmatrix}$$

The LLL algorithm

Input : A lattice $\mathcal{L}$ given by a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$
$t > 1$

Output : A basis $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ of $\mathcal{L}$ such that the Gram-Schmidt Orthogonalization (GSO) satisfies ,

1. for all $1 \leq j < i \leq m$, $|\mu_{i,j}| \leq \frac{1}{2}$ (size reduced)
2. for all $1 \leq i < m$, $||\mathbf{b}_{i+1}^\star||^2 + \mu_{i+1,i}^2||\mathbf{b}_i^\star||^2 \geq \frac{1}{t^2}||\mathbf{b}_i^\star||^2$ (Lovász conditions)



There exist a matrix M such that $\mathcal{B} = M\mathcal{B}^\star$ and

$$M = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \mu_{2,1} & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \mu_{m,1} & \cdots & \cdots & \mu_{m,m-1} & 1 \end{pmatrix}$$

The LLL algorithm

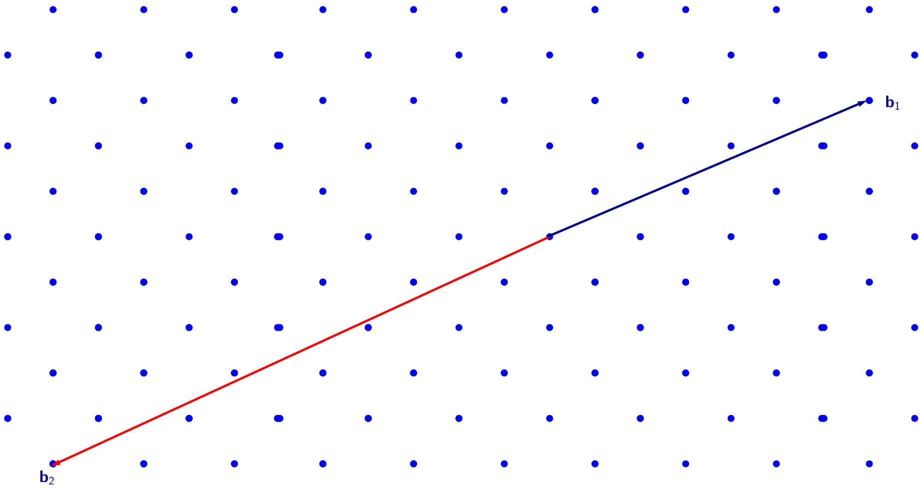
LLL performs translations and exchanges.

An exchange between two consecutive vectors is performed as soon as a Lovász condition is not satisfied.

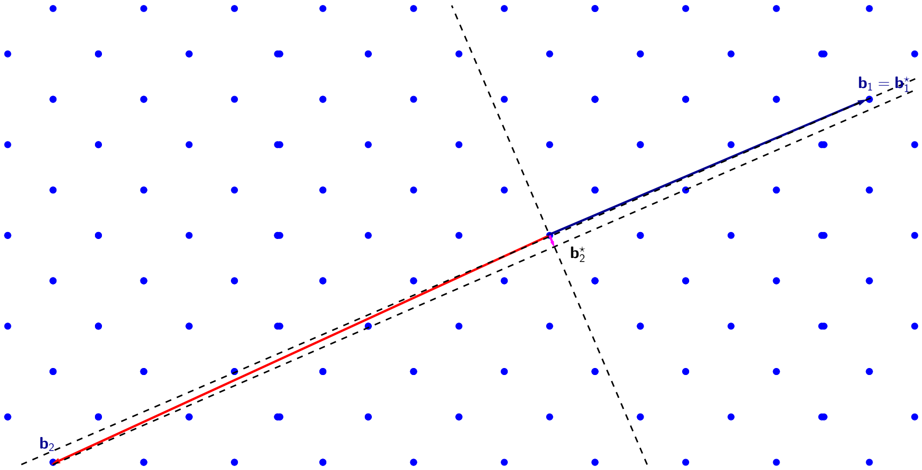
The exchanges improve the orthogonality and globally the ratios $\mathbf{b}_i^\star/\mathbf{b}_{i+1}^\star$ decrease.

Translations are performed for shortening the vectors (size-reduction)

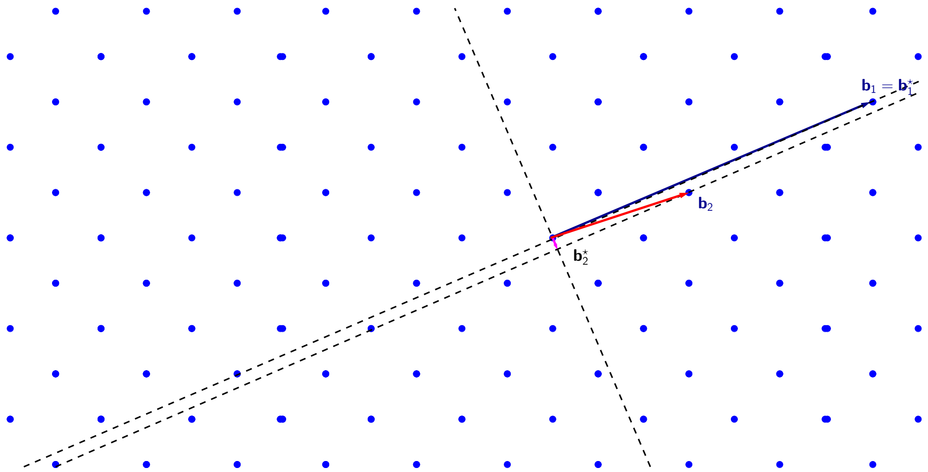
The LLL algorithm in dimension 2 (Gauss algorithm)



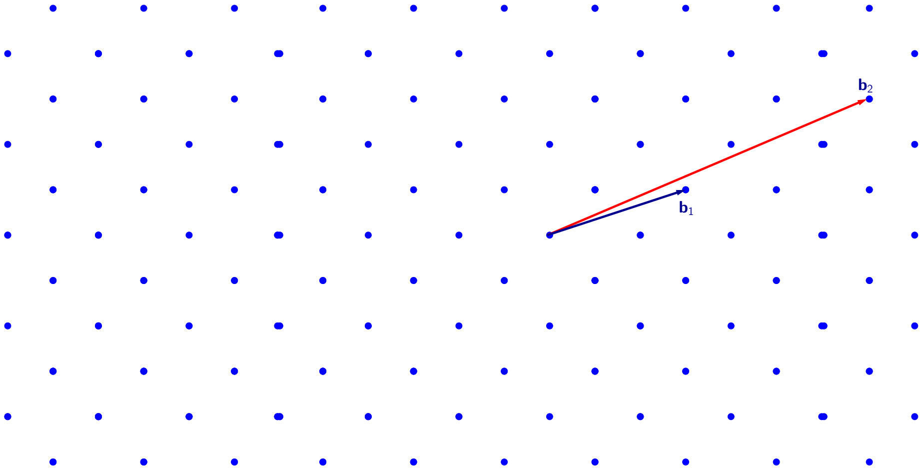
The LLL algorithm in dimension 2 (Gauss algorithm)



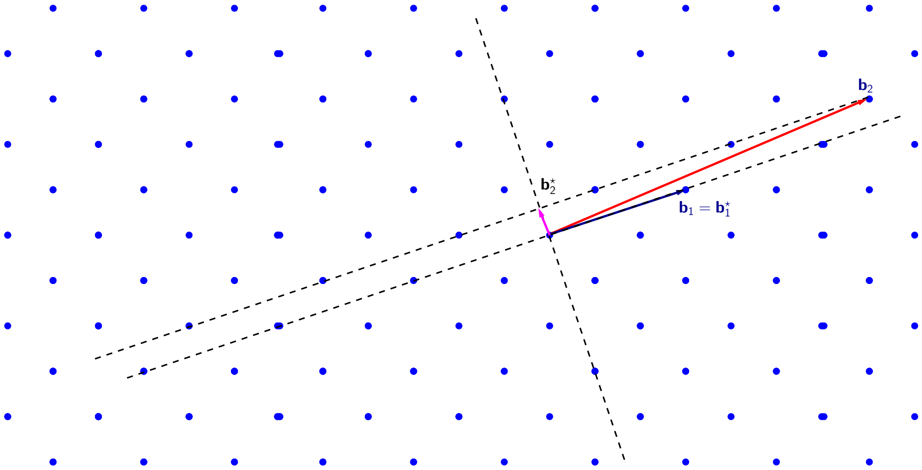
The LLL algorithm in dimension 2 (Gauss algorithm)



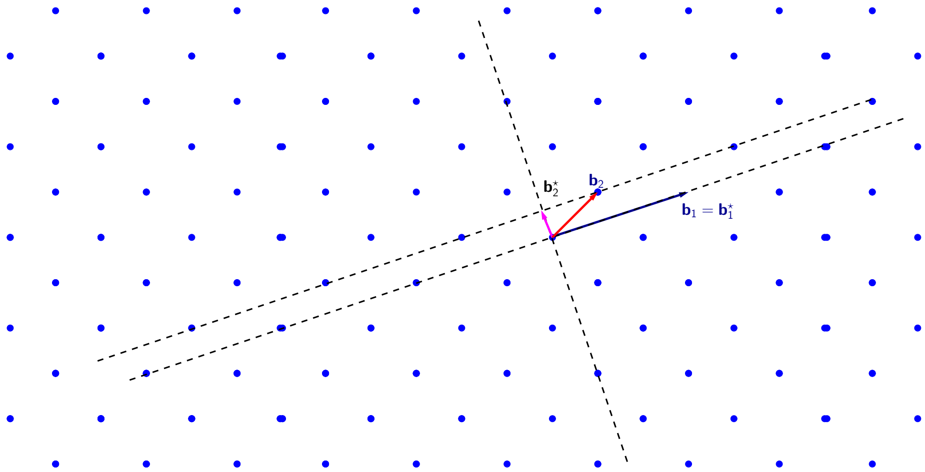
The LLL algorithm in dimension 2 (Gauss algorithm)



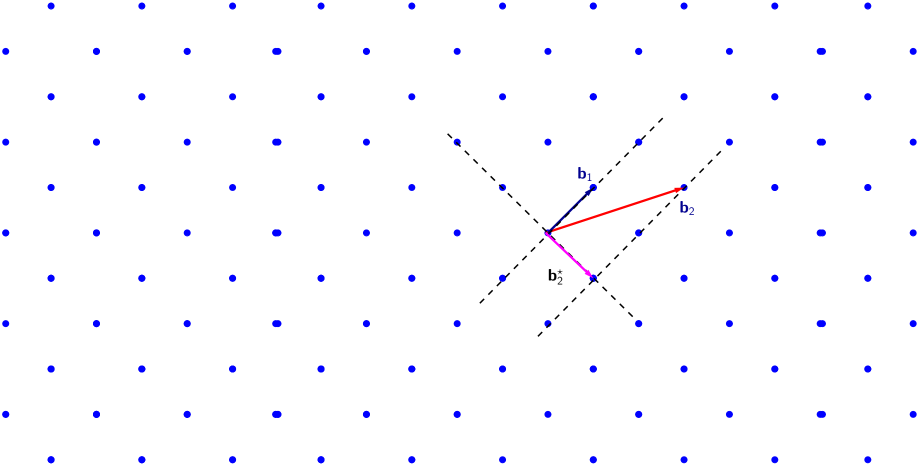
The LLL algorithm in dimension 2 (Gauss algorithm)



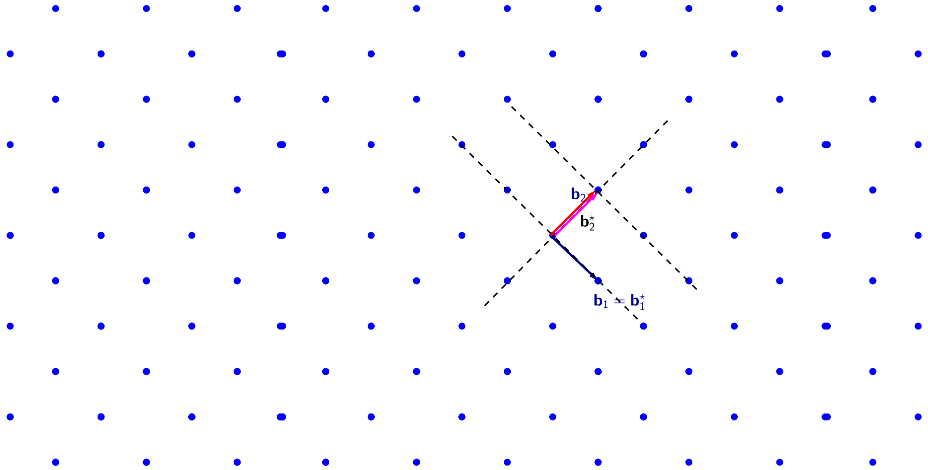
The LLL algorithm in dimension 2 (Gauss algorithm)



The LLL algorithm in dimension 2 (Gauss algorithm)



The LLL algorithm in dimension 2 (Gauss algorithm)

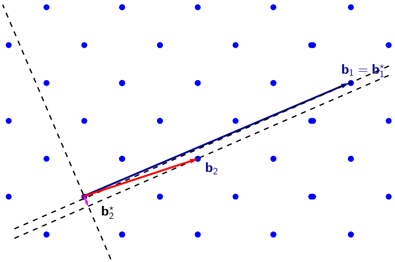


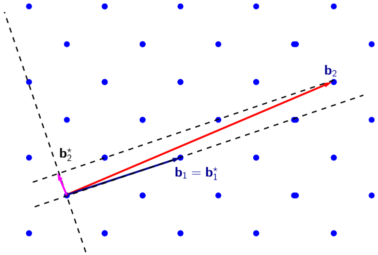
Translations and exchanges

Role of the translations (size-reduction):
The length of the vectors decreases with the translations.

Role of the exchanges:
Each exchange between $\mathbf{b}_i^\star$ and $\mathbf{b}_{i+1}^\star$ increases the length of $\mathbf{b}_{i+1}^\star$ and decreases the length of $\mathbf{b}_i^\star$.

The vectors are then more "orthogonal" and the ratio $||\mathbf{b}_i^\star||/||\mathbf{b}_{i+1}^\star||$ decreases.





The LLL algorithm

Input : A lattice $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_m)$
$t \geq 1$
Output : A t-LLL reduced basis of $\mathcal{L}$

Algorithm

```
Compute the GSO
size-reduce the basis using only translations (|μ_{i,j}| < 1/2)
while the basis is not t-LLL reduced do
    choose i such that ||b*_{i+1}||^2 + μ^2_{i+1,i}||b*_i||^2 < (1/t^2)||b*_i||^2
                                          according to a strategy
    exchange b_{i-1} and b_i
    size-reduce the basis using only translations
end while
return (b_1, ..., b_m)
```

Remark : The LLL algorithm only uses the orthogonal basis to make decision

Quality of the output

- The norms $||\mathbf{b}_i^\star||$ do not decrease too quickly since $||\mathbf{b}_i^\star|| \geq s^{i-1}||\mathbf{b}_1^\star||$ with

$$\frac{1}{t^2} = \frac{1}{4} + \frac{1}{s^2}.$$

- b_1 is a "short enough" vector of the lattice since

$$||b_1|| \leq 2^{(m-1)/2}\lambda(\mathcal{L})$$

[$\lambda(\mathcal{L})$ is the length of a shortest non zero vector of $\mathcal{L}$.]

Complexity

Theorem

LLL performs $O(n^3 m \log B)$ arithmetic operations with integers of size $O(n \log B)$ where $B = \max_{i=1..n} ||\mathbf{b}_i||$.

The real D

$$D = \prod_{i=1}^{n} ||\mathbf{b}_i^\star||^{n-i} \leq B^{n^2}, \quad \text{with} \quad B = \max_{i=1..n} ||\mathbf{b}_i||,$$

decreases by a factor $\delta = (\frac{1}{4} + s^2)^{1/2}$ at each exchange. Then LLL performs $O(n^2 \log B)$ exchanges.

Between two exchanges, there are at most $O(n^2)$ arithmetic operations.

The size of the integer increases quickly and the computations need multiprecision even for low dimensions (≈ 20).

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

Compute the GSO
size-reduce the basis using only translations $(|\mu_{i,j}| < \frac{1}{2})$
while the basis is not t-LLL reduced **do**
    choose i such that $||\mathbf{b}_{i+1}^\star||^2 + \mu_{i+1,i}^2 ||\mathbf{b}_i^\star||^2 < \frac{1}{t^2}||\mathbf{b}_i^\star||^2$
    according to a strategy
    exchange $\mathbf{b}_{i-1}$ and $\mathbf{b}_i$
    size-reduce the basis using only translations
end while
return $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

```
while the basis is not t-LLL reduced  do
    choose i such that ||b*_{i+1}||^2 + μ^2_{i+1,i}||b*_i||^2 < (1/t^2)||b*_i||^2
                                    according to a strategy
    exchange b_{i-1} and b_i
    size-reduce the basis using only translations
end while
return (b_1, ..., b_m)
```

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \dots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \dots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \dots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \dots, \hat{\mu}_{m-1})$ with for all $i = 1 \dots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

0 :

1 :

2 : **while** there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**

3 : choose i such that $||\mathbf{b}_{i+1}^\star||^2 + \mu_{i+1,i}^2||\mathbf{b}_i^\star||^2 < \frac{1}{t^2}||\mathbf{b}_i^\star||^2$
according to a strategy

4 : exchange $\mathbf{b}_{i-1}$ and $\mathbf{b}_i$

5 : size-reduce the basis using only translations

6 : **end while**

7 : **return** $(\mathbf{b}_1, \dots, \mathbf{b}_m)$

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \dots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \dots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \dots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \dots, \hat{\mu}_{m-1})$ with for all $i = 1 \dots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

while there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**
choose i such that $\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2$ according to a strategy
exchange $\mathbf{b}_{i-1}$ and $\mathbf{b}_i$
size-reduce the basis using only translations
end while
return $(\mathbf{b}_1, \dots, \mathbf{b}_m)$

The LLL algorithm : a new point of vue

<u>Input :</u> the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

<u>Output :</u> $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

<u>Algorithm</u>

while there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**
choose i such that $\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2$
according to a strategy
$\ell_i \leftarrow \rho\ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$
size-reduce the basis using only translations
end while
return $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

while there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**
  choose i such that $\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2$
  according to a strategy
  $\ell_i \leftarrow \rho \ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$
  call an oracle that recomputes μ_i and μ_{i+1}
end while
return $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$

The LLL algorithm : a new point of vue

Input : the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

0 :

1 :

2 : **while** there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**

3 : choose i such that $\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2$

according to a strategy

4 : $\ell_i \leftarrow \rho \ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$

5 : call an oracle that recomputes μ_i and μ_{i+1}

6 : **end while**

7 : **return** $(\ell_1, \ldots, \ell_m)$ and $(\mu_1, \ldots, \mu_{m-1})$

Plan

Simplified versions of the LLL algorithm

Updates in the LLL algorithm:

During an exchange, the norms of the vectors in the orthogonal basis become

$$||\mathbf{b}_i^\star|| \leftarrow \rho||\mathbf{b}_i^\star|| \quad \text{and} \quad ||\mathbf{b}_{i+1}^\star|| \leftarrow \frac{1}{\rho}||\mathbf{b}_{i+1}^\star|| \quad \text{with} \quad \rho^2 = \frac{||\mathbf{b}_{i+1}^\star||^2}{||\mathbf{b}_i^\star||^2} + \mu_{i+1,i}^2$$

Simplified versions of the LLL algorithm

Updates in the LLL algorithm:

During an exchange, the norms of the vectors in the orthogonal basis become

$$||\mathbf{b}_i^\star|| \leftarrow \rho||\mathbf{b}_i^\star|| \quad \text{and} \quad ||\mathbf{b}_{i+1}^\star|| \leftarrow \frac{1}{\rho}||\mathbf{b}_{i+1}^\star|| \quad \text{with} \quad \rho^2 = \frac{||\mathbf{b}_{i+1}^\star||^2}{||\mathbf{b}_i^\star||^2} + \mu_{i+1,i}^2$$

	LLL	Model 3	Model 2	Model 1
Conditions on ρ		- $\mu_{i+1,i}$ follows a uniform law on $[-\frac{1}{2}, \frac{1}{2}]$ - ρ depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$ and $\mu_{i+1,i}$	- the $\mu_{i+1,i}$ are supposed to be constant - ρ only depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$	ρ is supposed to be constant
Remarks	Too complicated	Open problem	Work in progress	True Chip Firing Game [Madritsch, Vallée]

Plan

The LLL algorithm : additive point of vue

Input : the real vector $(\ell_1, \ldots, \ell_m)$ with $\ell_i = ||\mathbf{b}_i^\star||$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{\ell}_1, \ldots, \hat{\ell}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{\ell}_{i+1}^2 \geq (\frac{1}{t^2} - \hat{\mu}_i^2)\hat{\ell}_i^2$

Algorithm

0 :

1 :

2 : **while** there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**

3 : choose i such that $||\mathbf{b}_{i+1}^\star||^2 + \mu_{i+1,i}^2||\mathbf{b}_i^\star||^2 < \frac{1}{t^2}||\mathbf{b}_i^\star||^2$
according to a strategy

4 : $\ell_i \leftarrow \rho\ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$

5 : call an oracle that recomputes μ_i and μ_{i+1}

6 : **end while**

7 : **return** $(\ell_1, \ldots, \ell_m)$ and $(\mu_1, \ldots, \mu_{m-1})$

The LLL algorithm : additive point of vue

Input : the real vector $(q_1, \ldots, q_m)$ with $q_i = \log \ell_i^2$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{q}_1, \ldots, \hat{q}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{q}_{i+1} \geq \log(\frac{1}{t^2} - \hat{\mu}_i^2) + \hat{q}_i$

Algorithm

0 :

1 :

2 : **while** there exists i such that $\boxed{\ell_{i+1}^2 < (\frac{1}{t^2} - \mu_i^2)\ell_i^2}$ **do**

3 : choose i such that $||\mathbf{b}_{i+1}^\star||^2 + \mu_{i+1,i}^2||\mathbf{b}_i^\star||^2 < \frac{1}{t^2}||\mathbf{b}_i^\star||^2$
according to a strategy

4 : $\ell_i \leftarrow \rho\ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$

5 : call an oracle that recomputes μ_i and μ_{i+1}

6 : **end while**

7 : **return** $(\ell_1, \ldots, \ell_m)$ and $(\mu_1, \ldots, \mu_{m-1})$

The LLL algorithm : additive point of vue

Input : the real vector $(q_1, \ldots, q_m)$ with $q_i = \log \ell_i^2$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{q}_1, \ldots, \hat{q}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{q}_{i+1} \geq \log(\frac{1}{t^2} - \hat{\mu}_i^2) + \hat{q}_i$

Algorithm

```
while there exists i such that [q_{i+1} < H + q_i] with H = log(1/t^2 − μ_i^2) do
    choose i such that ||b*_{i+1}||^2 + μ^2_{i+1,i}||b*_i||^2 < (1/t^2)||b*_i||^2
                                        according to a strategy
    ℓ_i ← ρℓ_i and ℓ_{i+1} ← (1/ρ)ℓ_{i+1} with [ρ^2 = ℓ^2_{i+1}/ℓ^2_i + μ_i^2]
    call an [oracle] that recomputes μ_i and μ_{i+1}
end while
return (ℓ_1, ..., ℓ_m) and (μ_1, ..., μ_{m−1})
```

The LLL algorithm : additive point of vue

Input : the real vector $(q_1, \ldots, q_m)$ with $q_i = \log \ell_i^2$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{q}_1, \ldots, \hat{q}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{q}_{i+1} \geq \log(\frac{1}{t^2} - \hat{\mu}_i^2) + \hat{q}_i$

Algorithm

while there exists i such that $\boxed{q_{i+1} < H + q_i}$ with $H = \log(\frac{1}{t^2} - \mu_i^2)$ **do**
    choose i such that $q_{i+1} < H + q_i$ with $H = \log(\frac{1}{t^2} - \mu_i^2)$
    according to a strategy
    $\ell_i \leftarrow \rho \ell_i$ and $\ell_{i+1} \leftarrow (1/\rho)\ell_{i+1}$ with $\boxed{\rho^2 = \frac{\ell_{i+1}^2}{\ell_i^2} + \mu_i^2}$
    call an oracle that recomputes μ_i and μ_{i+1}
end while
return $(\ell_1, \ldots, \ell_m)$ and $(\mu_1, \ldots, \mu_{m-1})$

The LLL algorithm : additive point of vue

Input : the real vector $(q_1, \ldots, q_m)$ with $q_i = \log \ell_i^2$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{q}_1, \ldots, \hat{q}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{q}_{i+1} \geq \log(\frac{1}{t^2} - \hat{\mu}_i^2) + \hat{q}_i$

Algorithm

```
while there exists i such that [q_{i+1} < H + q_i] with H = log(1/t^2 - mu_i^2) do
    choose i such that q_{i+1} < H + q_i with H = log(1/t^2 - mu_i^2)
                                          according to a strategy
    q_i <- q_i - h and q_{i+1} <- q_{i+1} + h with
            [h = -log rho^2 = -log e^{q_{i+1} - q_i} + mu_i^2]
    call an [oracle] that recomputes mu_i and mu_{i+1}
end while
return (l_1, ..., l_m) and (mu_1, ..., mu_{m-1})
```

The LLL algorithm : additive point of vue

Input : the real vector $(q_1, \ldots, q_m)$ with $q_i = \log \ell_i^2$
the subdiagonal coefficients $(\mu_1, \ldots, \mu_{m-1})$ with $|\mu_i| = |\mu_{i+1,i}| \leq \frac{1}{2}$
$t \geq 1$

Output : $(\hat{q}_1, \ldots, \hat{q}_m)$ and $(\hat{\mu}_1, \ldots, \hat{\mu}_{m-1})$ with for all $i = 1 \ldots m-1$,
$\hat{q}_{i+1} \geq \log(\frac{1}{t^2} - \hat{\mu}_i^2) + \hat{q}_i$

Algorithm

while there exists i such that $\boxed{q_{i+1} < H + q_i}$ with $H = \log(\frac{1}{t^2} - \mu_i^2)$ **do**
choose i such that $q_{i+1} < H + q_i$ with $H = \log(\frac{1}{t^2} - \mu_i^2)$
according to a strategy
$q_i \leftarrow q_i - h$ and $q_{i+1} \leftarrow q_{i+1} + h$ with
$\boxed{h = -\log \rho^2 = -\log e^{q_{i+1} - q_i} + \mu_i^2}$
call an oracle that recomputes μ_i and μ_{i+1}
end while
return $(q_1, \ldots, q_m)$ and $(\mu_1, \ldots, \mu_{m-1})$

Hypotheses

Model 1

H and h are supposed to be constant.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2 \qquad r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.
– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2$ $\qquad r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.
– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2$ $\qquad r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.

– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2 \qquad r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.
– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2 \qquad r_i = q_i - q_{i+1} = \log \dfrac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.

– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

General sandpiles and chip firing games with parameters (H, h).

In our context, $q_i = \log ||\mathbf{b}_i^\star||^2 \qquad r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

The equation

$$\text{If} \quad q_i > q_{i+1} + H, \quad \text{then} \quad [\check{q}_i = q_i - h, \quad \check{q_{i+1}} = q_{i+1} + h].$$

defines the sandpile model of parameters (H, h).

The equation

$$\text{If} \quad r_i > H, \quad \text{then} \quad [\check{r}_i = r_i - 2h, \quad \check{r_{i+1}} = r_{i+1} + h, \quad \check{r_{i-1}} = r_{i-1} + h,].$$

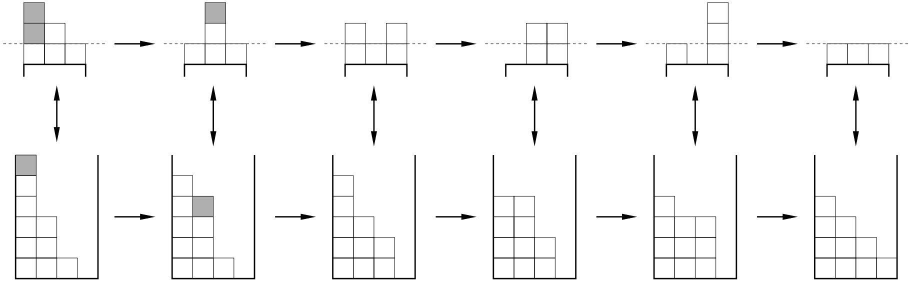
defines the chip firing game of parameters (H, h).

Classical instances studied : basic and decreasing.

– Basic instances : Initial integer q_i's and parameters H, h equal to 1.
– Basic (strictly) decreasing instances :
The sequence $i \mapsto q_i$ is (strictly) decreasing.

Here, we study general instances of sandpile models.

Evolution of a CFG and its sandpile

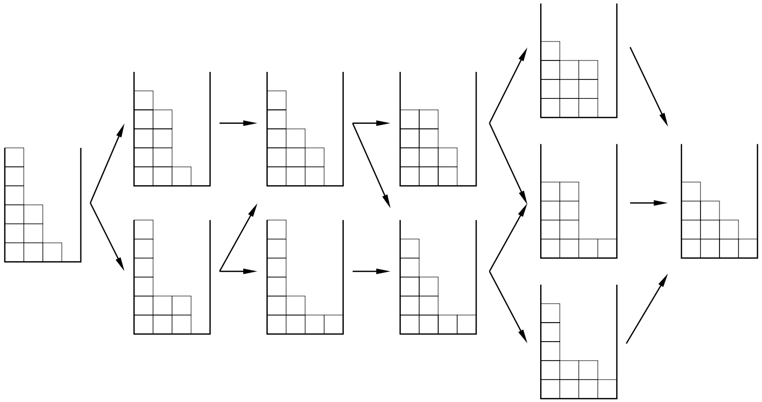


The evolution of a basic chip firing game (above),
and its associated sandpile (below).

above : $q_i = \log ||\mathbf{b}_i^\star||^2$

below : $r_i = q_i - q_{i+1} = \log \frac{||\mathbf{b}_i^\star||^2}{||\mathbf{b}_{i+1}^\star||^2}$

Evolutions of a basic sandpile



Possible evolutions of a basic sandpile.

For any sandpile of parameters (h, H)...

(i) There is a unique final $\hat{\mathbf{q}}$. The length of any path $\mathbf{q} \to \hat{\mathbf{q}}$ is

$$T(\mathbf{q}) = \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - \hat{r}_i)$$

(ii) If the sandpile is decreasing, $H - 2h < \hat{r}_i \leq H$,

$$0 \leq T(\mathbf{q}) - \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \leq 2A(n) \qquad \text{with} \quad A(n) := n\frac{n^2-1}{12}$$

(iii) If the sandpile is strictly decreasing,

$$\exists! j \quad \forall i \neq j,\; H - h < \hat{r}_i \leq H, \qquad \text{and} \quad H - 2h < \hat{r}_j \leq H - h,$$

$$0 \leq T(\mathbf{q}) - \left[A(n) + \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H)\right] \leq \frac{1}{8}n^2$$

(iv) For a general sandpile,

$$H - 2h < \hat{r}_i \leq H \quad \text{if} \quad r_i > H - h, \qquad \hat{r}_i \geq r_i \quad \text{if} \quad r_i \leq H - h$$

$$\frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)(r_i - H + h) \leq T(\mathbf{q}) \leq \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i) \max(r_i - H + h, 0)$$

For any sandpile of parameters (h, H)...

(i) There is a unique final $\hat{\mathbf{q}}$. The length of any path $\mathbf{q} \to \hat{\mathbf{q}}$ is

$$T(\mathbf{q}) = \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - \hat{r}_i)$$

(ii) If the sandpile is decreasing, $H - 2h < \hat{r}_i \leq H$,

$$0 \leq T(\mathbf{q}) - \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \leq 2A(n) \qquad \text{with} \quad A(n) := n\frac{n^2-1}{12}$$

(iii) If the sandpile is strictly decreasing,

$$\exists! j \quad \forall i \neq j,\ H - h < \hat{r}_i \leq H, \qquad \text{and} \quad H - 2h < \hat{r}_j \leq H - h,$$

$$0 \leq T(\mathbf{q}) - \left[A(n) + \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H)\right] \leq \frac{1}{8}n^2$$

(iv) For a general sandpile,

$$H - 2h < \hat{r}_i \leq H \quad \text{if} \quad r_i > H - h, \qquad \hat{r}_i \geq r_i \quad \text{if} \quad r_i \leq H - h$$

$$\frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)(r_i - H + h) \leq T(\mathbf{q}) \leq \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i) \max(r_i - H + h, 0)$$

For any sandpile of parameters (h, H)...

(i) There is a unique final $\hat{\mathbf{q}}$. The length of any path $\mathbf{q} \to \hat{\mathbf{q}}$ is

$$T(\mathbf{q}) = \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - \hat{r}_i)$$

(ii) If the sandpile is decreasing, $H - 2h < \hat{r}_i \le H$,

$$0 \le T(\mathbf{q}) - \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \le 2A(n) \qquad \text{with} \quad A(n) := n\frac{n^2-1}{12}$$

(iii) If the sandpile is strictly decreasing,

$$\exists! j \quad \forall i \ne j,\ H - h < \hat{r}_i \le H, \qquad \text{and} \quad H - 2h < \hat{r}_j \le H - h,$$

$$0 \le T(\mathbf{q}) - \left[A(n) + \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \right] \le \frac{1}{8} n^2$$

(iv) For a general sandpile,

$$H - 2h < \hat{r}_i \le H \quad \text{if} \quad r_i > H - h, \qquad \hat{r}_i \ge r_i \quad \text{if} \quad r_i \le H - h$$

$$\frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)(r_i - H + h) \le T(\mathbf{q}) \le \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i) \max(r_i - H + h, 0)$$

For any sandpile of parameters (h, H)...

(i) There is a unique final $\hat{\mathbf{q}}$. The length of any path $\mathbf{q} \to \hat{\mathbf{q}}$ is

$$T(\mathbf{q}) = \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - \hat{r}_i)$$

(ii) If the sandpile is decreasing, $H - 2h < \hat{r}_i \leq H$,

$$0 \leq T(\mathbf{q}) - \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \leq 2A(n) \qquad \text{with} \quad A(n) := n\frac{n^2-1}{12}$$

(iii) If the sandpile is strictly decreasing,

$$\exists! j \quad \forall i \neq j,\ H - h < \hat{r}_i \leq H, \qquad \text{and} \quad H - 2h < \hat{r}_j \leq H - h,$$

$$0 \leq T(\mathbf{q}) - \left[A(n) + \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)\,(r_i - H) \right] \leq \frac{1}{8} n^2$$

(iv) For a general sandpile,

$$H - 2h < \hat{r}_i \leq H \quad \text{if} \quad r_i > H - h, \qquad \hat{r}_i \geq r_i \quad \text{if} \quad r_i \leq H - h$$

$$\frac{1}{2h} \sum_{i=1}^{n-1} i(n-i)(r_i - H + h) \leq T(\mathbf{q}) \leq \frac{1}{2h} \sum_{i=1}^{n-1} i(n-i) \max(r_i - H + h, 0)$$

For any sandpile of parameters (h, H)...

(v) A sufficient condition for two adjacent strictly decreasing basic sandpiles

$$\mathbf{q}_- := (q_1, q_2, \ldots, q_p), \qquad \mathbf{q}_+ := (q_{p+1}, q_{p+2}, \ldots, q_{n+p})$$

to be independent is

$$\frac{1}{p}\left(\sum_{i=1}^{p} q_i\right) - \frac{1}{n}\left(\sum_{i=1}^{n} q_{p+i}\right) \leq \left(\frac{n+p}{2}\right) - 2.$$

In this case, the number of steps for the total sandpile $\mathbf{q}$ is (in parallel)

$$T(\mathbf{q}) = \max\left[T(\mathbf{q}_-), T(\mathbf{q}_+)\right]$$

For any sandpile of parameters (h, H)...

(v) A sufficient condition for two adjacent strictly decreasing basic sandpiles

$$\mathbf{q}_- := (q_1, q_2, \dots, q_p), \qquad \mathbf{q}_+ := (q_{p+1}, q_{p+2}, \dots, q_{n+p})$$

to be independent is

$$\frac{1}{p}\left(\sum_{i=1}^{p} q_i\right) - \frac{1}{n}\left(\sum_{i=1}^{n} q_{p+i}\right) \le \left(\frac{n+p}{2}\right) - 2.$$

In this case, the number of steps for the total sandpile $\mathbf{q}$ is (in parallel)

$$T(\mathbf{q}) = \max\left[T(\mathbf{q}_-), T(\mathbf{q}_+)\right]$$

Plan

Simplified versions of the LLL algorithm

Updates in the LLL algorithm:

During an exchange, the norms of the vectors in the orthogonal basis become

$$||\mathbf{b}_i^\star|| \leftarrow \rho||\mathbf{b}_i^\star|| \quad \text{and} \quad ||\mathbf{b}_{i+1}^\star|| \leftarrow \frac{1}{\rho}||\mathbf{b}_{i+1}^\star|| \quad \text{with} \quad \rho^2 = \frac{||\mathbf{b}_{i+1}^\star||^2}{||\mathbf{b}_i^\star||^2} + \mu_{i+1,i}^2$$

	LLL	Model 3	Model 2	Model 1
Conditions on ρ		- $\mu_{i+1,i}$ follows a uniform law on $[-\frac{1}{2}, \frac{1}{2}]$ - ρ depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$ and $\mu_{i+1,i}$	- the $\mu_{i+1,i}$ are supposed to be constant - ρ only depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$	ρ is supposed to be constant
Remarks	Too complicated	Open problem	Work in progress	True Chip Firing Game [Madritsch, Vallée]

Model M2(t, μ)

$$x_i = \frac{||\mathbf{b}^\star_{i+1}||^2}{||\mathbf{b}^\star_i||^2}, \qquad \rho^2 = x_i + \mu, \qquad \mathcal{O}_{t,\mu} = \left[\frac{1}{t^2} - \mu, +\infty\right[$$

Entrées: Le vecteur $\mathbf{x} = (x_1, \ldots, x_{d-1}) \in \mathbb{R}_+^{d-1}$
Résultat: Le vecteur final $\hat{\mathbf{x}} = (\hat{x}_1, \ldots, \hat{x}_{d-1}) \in \mathcal{O}_{\mu,t}^{d-1}$

tant que $\mathbf{x} \notin \mathcal{O}_{\mu,t}^{d-1}$ **faire**
Choisir i tel que $x_i \notin \mathcal{O}_{\mu,t}$;
Calculer $\mathbf{x} := T_{i,\mu}(\mathbf{x})$ vérifiant

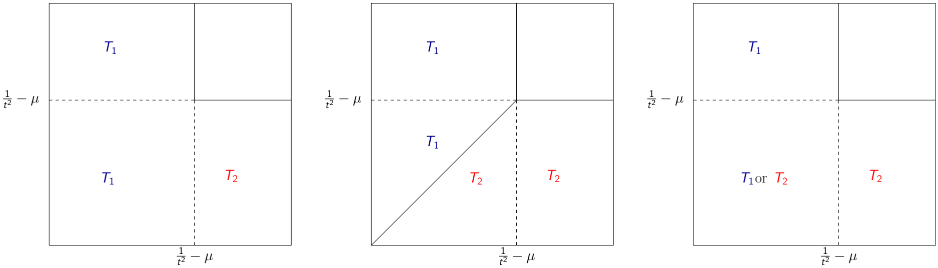
$$x_{i-1} := x_{i-1}(x_i + \mu), \qquad x_{i+1} := x_{i+1}(x_i + \mu), \qquad x_i = \frac{x_i}{(x_i + \mu)^2};$$

fintq

This is a general dynamical system in $\mathbb{R}^d$ with

- a hole $\mathcal{O}_{t,\mu}^{d-1}$
- and an attractive fixed point in $(1 - \mu, \ldots, 1 - \mu)$

Strategies



LLL strategy | Greedy strategy | Random strategy

First result when $t > 1$

Potential

$$P(\mathbf{x}) := \prod_{i=1}^{d-1} x_i^{i(d-i)}$$

With the greedy strategy, we have

$$P(T(\mathbf{x})) = \frac{P(\mathbf{x})}{\min_{i=1\ldots d-1} (x_i+\mu)^2} > P(\mathbf{x})$$

and if the basis is far from being reduced,

$$\min_{i=1\ldots d-1} (x_i+\mu)^2 \sim \mu^2, \qquad P(\mathbf{x}) \sim \mu P(T(\mathbf{x})), \qquad P(\mathbf{x}) \sim \mu^k P(T^k(\mathbf{x}))$$

But if the basis is close to be reduced,

$$\min_{i=1\ldots d-1} (x_i+\mu)^2 \approx \frac{1}{t^2} < 1 \quad \text{if } t > 1$$

First result when $t > 1$

Potential

$$P(\mathbf{x}) := \prod_{i=1}^{d-1} x_i^{i(d-i)}$$

With the greedy strategy, we have

$$P(T(\mathbf{x})) = \frac{P(\mathbf{x})}{\min_{i=1\ldots d-1} (x_i + \mu)^2} > P(\mathbf{x})$$

and if the basis is far from being reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \sim \mu^2, \qquad P(\mathbf{x}) \sim \mu P(T(\mathbf{x})), \qquad P(\mathbf{x}) \sim \mu^k P(T^k(\mathbf{x}))$$

But if the basis is close to be reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \approx \frac{1}{t^2} < 1 \quad \text{if } t > 1$$

First result when $t > 1$

Potential

$$P(\mathbf{x}) := \prod_{i=1}^{d-1} x_i^{i(d-i)}$$

With the greedy strategy, we have

$$P(T(\mathbf{x})) = \frac{P(\mathbf{x})}{\min_{i=1\ldots d-1} (x_i + \mu)^2} > P(\mathbf{x})$$

and if the basis is far from being reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \sim \mu^2, \qquad P(\mathbf{x}) \sim \mu P(T(\mathbf{x})), \qquad P(\mathbf{x}) \sim \mu^k P(T^k(\mathbf{x}))$$

But if the basis is close to be reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \approx \frac{1}{t^2} < 1 \quad \text{if } t > 1$$

First result when $t > 1$

Potential

$$P(\mathbf{x}) := \prod_{i=1}^{d-1} x_i^{i(d-i)}$$

With the greedy strategy, we have

$$P(T(\mathbf{x})) = \frac{P(\mathbf{x})}{\min_{i=1\ldots d-1} (x_i + \mu)^2} > P(\mathbf{x})$$

and if the basis is far from being reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \sim \mu^2, \qquad P(\mathbf{x}) \sim \mu P(T(\mathbf{x})), \qquad P(\mathbf{x}) \sim \mu^k P(T^k(\mathbf{x}))$$

But if the basis is close to be reduced,

$$\min_{i=1\ldots d-1} (x_i + \mu)^2 \approx \frac{1}{t^2} < 1 \quad \text{if } t > 1$$

First result when $t > 1$

Number of iterations when $t > 1$

Consider the dynamical system $\mathrm{M2}(\mu, t)$ with $t > 1$, $\mu \in [0, \frac{1}{4}]$ and $\mathbf{x} \notin \mathcal{O}_{t,\mu}^{d-1}$. The number of iterations of $\mathrm{M2}(\mu, t)$ on $\mathbf{x}$, denoted by $K_{t,\mu}(\mathbf{x})$ satisfies

$$K_{t,\mu}(\mathbf{x}) = \frac{1}{2} \log_\mu P(\mathbf{x}) + O(d^3).$$

Remark :

- the known results on the complexity of LLL involve $\log_t P(\mathbf{x})$,
- nothing is known when $t = 1$.

Model M2(t, μ) with $t = 1$

We did not succeed in generalizing the result except for $d = 2$ (Gauss) and $d = 3$ (LLL in dimension 3).

Number of iterations when $t = 1$ and $d = 2, 3$

Consider the dynamical system M2$(\mu, 1)$, $\mu \in [0, \frac{1}{4}]$, $\mathbf{x} \notin \mathcal{O}_{t,\mu}^{d-1}$ and $d = 2, 3$. The number of iterations of M2$(\mu, 1)$ on $\mathbf{x}$, denoted by $K_{1,\mu}(\mathbf{x})$ satisfies

$$K_{1,\mu}(\mathbf{x}) = \frac{1}{2} \log_\mu P(\mathbf{x}) + O(1).$$

Conjecture

$$K_{1,\mu}(\mathbf{x}) = \frac{1}{2} \log_\mu P(\mathbf{x}) + O(d^3).$$

Model M2(t, μ) with $t = 1$

We did not succeed in generalizing the result except for $d = 2$ (Gauss) and $d = 3$ (LLL in dimension 3).

Number of iterations when $t = 1$ and $d = 2, 3$

Consider the dynamical system M2(μ, 1), $\mu \in [0, \frac{1}{4}]$, $\mathbf{x} \notin \mathcal{O}_{t,\mu}^{d-1}$ and $d = 2, 3$. The number of iterations of M2(μ, 1) on $\mathbf{x}$, denoted by $K_{1,\mu}(\mathbf{x})$ satisfies

$$K_{1,\mu}(\mathbf{x}) = \frac{1}{2} \log_\mu P(\mathbf{x}) + O(1).$$

Conjecture

$$K_{1,\mu}(\mathbf{x}) = \frac{1}{2} \log_\mu P(\mathbf{x}) + O(d^3).$$

Plan

Simplified versions of the LLL algorithm

Updates in the LLL algorithm:
During an exchange, the norms of the vectors in the orthogonal basis become

$$||\mathbf{b}_i^\star|| \leftarrow \rho||\mathbf{b}_i^\star|| \quad \text{and} \quad ||\mathbf{b}_{i+1}^\star|| \leftarrow \frac{1}{\rho}||\mathbf{b}_{i+1}^\star|| \quad \text{with} \quad \rho^2 = \frac{||\mathbf{b}_{i+1}^\star||^2}{||\mathbf{b}_i^\star||^2} + \mu_{i+1,i}^2$$

	LLL	Model 3	Model 2	Model 1
Conditions on ρ		- $\mu_{i+1,i}$ follows a uniform law on $[-\frac{1}{2}, \frac{1}{2}]$ - ρ depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$ and $\mu_{i+1,i}$	- the $\mu_{i+1,i}$ are supposed to be constant - ρ only depends on the ratio $\frac{\lVert\mathbf{b}_{i+1}^\star\rVert^2}{\lVert\mathbf{b}_i^\star\rVert^2}$	ρ is supposed to be constant
Remarks	Too complicated	Open problem	Work in progress	True Chip Firing Game [Madritsch, Vallée]

Model M3(t, μ)

Entrées: Le vecteur $\mathbf{x} = (x_1, \ldots, x_{d-1}) \in \mathbb{R}_+^{d-1}$
Le vecteur $\mu = (\mu_1, \ldots, \mu_{d-1}) \in [0, \frac{1}{4}]^{d-1}$
Résultat: Les vecteurs $\hat{\mathbf{x}} = (\hat{x}_1, \ldots, \hat{x}_{d-1})$ et $\hat{\mu} = (\hat{\mu}_1, \ldots, \hat{\mu}_{d-1})$ tels que
$\hat{x}_i \geq \frac{1}{t^2} - \hat{\mu}_i$

tant que *il existe* i *tel que* $x_i < \frac{1}{t^2} - \mu_i$ **faire**
Choisir i tel que $x_i < \frac{1}{t^2} - \mu_i$
Calculer $\mathbf{x} := T_{i,\mu_i}(\mathbf{x})$ vérifiant

$$x_{i-1} := x_{i-1}(x_i + \mu_i), \qquad x_{i+1} := x_{i+1}(x_i + \mu_i), \qquad x_i = \frac{x_i}{(x_i + \mu_i)^2};$$

Générer aléatoirement un nouveau μ_i
fintq

This is a probabilistic dynamical system

Results

NONE !

Some ideas

$K(\mathbf{x})$ denotes the number of iterations on the input $\mathbf{x}$

Consider P_0 the potential such that $P(\mathbf{x}) \geq P_0 \Rightarrow \mathbf{x}$ is "reduced"

Consider a sequence of i.i.d. random variables $(\mu_i)_i$ that follow the same uniform law over $[0, \frac{1}{4}]$.

Consider the stopping time $T(\mathbf{x})$ defined as the minimum k such that

$$P_0 \prod_{i=1}^{k} \mu_i < P(\mathbf{x}).$$

my feeling : $K(\mathbf{x}) = T(\mathbf{x}) + O(d^3)$.

Some ideas

$K(\mathbf{x})$ denotes the number of iterations on the input $\mathbf{x}$

Consider P_0 the potential such that $P(\mathbf{x}) \geq P_0 \Rightarrow \mathbf{x}$ is "reduced"

Consider a sequence of i.i.d. random variables $(\mu_i)_i$ that follow the same uniform law over $[0, \frac{1}{4}]$.

Consider the stopping time $T(\mathbf{x})$ defined as the minimum k such that

$$P_0 \prod_{i=1}^{k} \mu_i < P(\mathbf{x}).$$

my feeling : $K(\mathbf{x}) = T(\mathbf{x}) + O(d^3)$.

Some ideas

$K(\mathbf{x})$ denotes the number of iterations on the input $\mathbf{x}$

Consider P_0 the potential such that $P(\mathbf{x}) \geq P_0 \Rightarrow \mathbf{x}$ is "reduced"

Consider a sequence of i.i.d. random variables $(\mu_i)_i$ that follow the same uniform law over $[0, \frac{1}{4}]$.

Consider the stopping time $T(\mathbf{x})$ defined as the minimum k such that

$$P_0 \prod_{i=1}^{k} \mu_i < P(\mathbf{x}).$$

my feeling : $\quad K(\mathbf{x}) = T(\mathbf{x}) + O(d^3).$

Some ideas

$K(\mathbf{x})$ denotes the number of iterations on the input $\mathbf{x}$

Consider P_0 the potential such that $P(\mathbf{x}) \geq P_0 \Rightarrow \mathbf{x}$ is "reduced"

Consider a sequence of i.i.d. random variables $(\mu_i)_i$ that follow the same uniform law over $[0, \frac{1}{4}]$.

Consider the stopping time $T(\mathbf{x})$ defined as the minimum k such that

$$P_0 \prod_{i=1}^{k} \mu_i < P(\mathbf{x}).$$

my feeling : $K(\mathbf{x}) = T(\mathbf{x}) + O(d^3)$.

Some ideas

$K(\mathbf{x})$ denotes the number of iterations on the input $\mathbf{x}$

Consider P_0 the potential such that $P(\mathbf{x}) \geq P_0 \Rightarrow \mathbf{x}$ is "reduced"

Consider a sequence of i.i.d. random variables $(\mu_i)_i$ that follow the same uniform law over $[0, \frac{1}{4}]$.

Consider the stopping time $T(\mathbf{x})$ defined as the minimum k such that

$$P_0 \prod_{i=1}^{k} \mu_i < P(\mathbf{x}).$$

my feeling : $\quad K(\mathbf{x}) = T(\mathbf{x}) + O(d^3).$

Plan

Plan

Various notions of a random basis of a lattice.

(a) "Useful" lattice bases arise in applications : variations around knapsack bases and their transposes with bordered identity matrices.

$$\begin{pmatrix} A \mid I_p \end{pmatrix} \quad \left(\begin{array}{c|c} y & 0 \\ \hline x & qI_p \end{array}\right) \quad \left(\begin{array}{c|c} I_p & H_p \\ \hline 0_p & qI_p \end{array}\right) \quad \left(\begin{array}{c|c} q & 0 \\ \hline x & I_{p-1} \end{array}\right)$$

(b) Ajtai "bad" bases $B_p := (b_{i,p})$ associated to a sequence $a_{i,p}$

$$b_{i,p} \in \mathbb{Z}^p, \quad b_{i,p} = a_{i,p}\, e_i + \sum_{j=1}^{i-1} a_{i,j,p}\, e_j \qquad (\Rightarrow ||b^\star_{i,p}|| = a_{i,p})$$

with $$\alpha_{i,j,p} = \frac{a^{(p)}_{i,j}}{a^{(p)}_j} = \text{rand}\left(-\frac{1}{2}, \frac{1}{2}\right) \qquad \text{[size-reduced]}$$

and $$\frac{||b^\star_{i+1,p}||}{||b^\star_{i,p}||} = \frac{a^{(p)}_{i+1}}{a^{(p)}_i} \to 0 \qquad \text{when } p \to \infty \qquad \text{[bad ratios - non reduced]}$$

Experimental mean values .... versus proven upper bounds [Nguyen and Stehlé]

Main parameters.	$\|\|b^\star_{i+1,p}\|\|/\|\|b^\star_{i,p}\|\|$	approx. factor	Nb. steps
Worst-case (Proven upper bounds)	$1/s$	s^{p-1}	$\Theta(Mp^2)$
"Bad" lattice bases Random Ajtai bases (Experimental mean values)	$1/\beta$	β^{p-1}	$\Theta(Mp^2)$
"Useful " lattice bases Random knapsack–shape bases (Experimental mean values)	$1/\beta$	β^{p-1}	$\Theta(Mp)$

The execution parameters depend on the type of the lattice basis.

The output configuration does not depend strongly neither on index i nor on the type of bases.

"experimental" value : $\beta \approx 1.04$
the

Other notions of a random basis of a lattice – reference models.

(c) Spherical model.
Choose independently each one of the p vectors in the ambient space $\mathbb{R}^n$, under a common distribution that is invariant by rotation.
Classical instances :

- uniform distribution in the ball, on the sphere
- gaussian distribution on coordinates

(d) Random lattices.
The space of (full-rank) lattices in $\mathbb{R}^n$ (modulo scale) is $X_n = SL_n(\mathbb{R})/SL_n(\mathbb{Z})$.
It possesses a unique probability measure
which is invariant under the action of $SL_n(\mathbb{R})$.
This gives rise to a natural notion of random lattices.

Probabilistic analyses of lattice reduction

- Akhavi, Marckert, Rouault (2005) [spherical model]
  - All the local bases are reduced except the last few ones
  - For the last few local bases, the length of the $\mathbf{b}_i^\star$ follows an explicit distribution

- Daudé and Vallée (1994) [random ball model]
  - The mean number of steps K satisfies

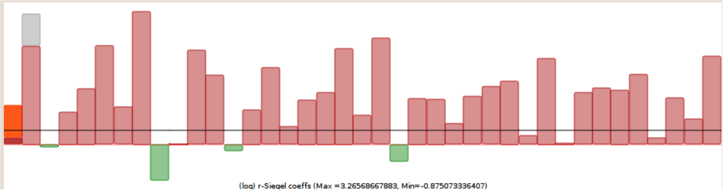
$$\mathrm{E}_n[K] \leq n^2 \left(\frac{1}{\log t} \right) \left[\frac{1}{2} \log n + 2 \right]$$

  - The mean size of the smallest nonzero vector of the lattice satisfies

$$\mathrm{E}_n[\lambda] \geq \frac{1}{4\sqrt{n}}$$

Plan

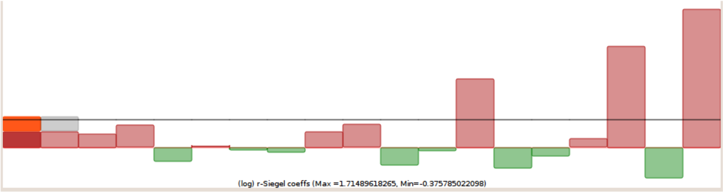
Some instances of cfg related to natural inputs



Ajtai type input

Knapsack type input

Some instances of cfg related to natural inputs



uniform distribution in the unit ball

Coppersmith's method

Plan

General model of Ajtai inputs

This is a general model of random cfg. Once a cfg is given, it is easy to compute a random lattice associated to the cfg.

The general model is based on 3 parameters

- Υ : the total mass of the cfg
- d : the dimension of the cfg
- g : density function over $[0, 1]$

The cfg $(c_1, \ldots, c_{d-1})$ satisfies

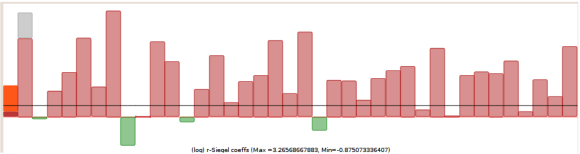
- for all i, c_i follows an exponential law
- $\mathbb{E}[c_i] = \dfrac{1}{d-1} \Upsilon g\left(\dfrac{i}{d}\right)$
- the total mass : $\mathbb{E}[\mathcal{M}] = \sum_{i=1}^{d-1} \mathbb{E}[c_i] \underset{d\to\infty}{\sim} \Upsilon$
- the energy (potential) :
  $$\mathbb{E}[\mathcal{E}] = \sum_{i=1}^{d-1} i(d-i)\mathbb{E}[c_i] \underset{d\to\infty}{\sim} d^2 \Upsilon \int_0^1 x(1-x)g(x)dx\Upsilon$$

model $\mathcal{A}(\Upsilon, d, g)$

The cfg $(c_1, \ldots, c_{d-1})$ satisfies

- for all i, c_i follows an exponential law
- $\mathbb{E}[c_i] = \dfrac{1}{d-1} \Upsilon g\left(\dfrac{i}{d}\right)$
- the total mass : $\mathbb{E}[\mathcal{M}] = \sum_{i=1}^{d-1} \mathbb{E}[c_i] \underset{d\to\infty}{\sim} \Upsilon$
- the energy (potential) :

$$\mathbb{E}[\mathcal{E}] = \sum_{i=1}^{d-1} i(d-i)\mathbb{E}[c_i] \underset{d\to\infty}{\sim} d^2\Upsilon \int_0^1 x(1-x)g(x)dx\Upsilon$$



In Ajtai work,

$$g(x) = \frac{a+1}{2^{a+1}-1}(2-x)^a.$$

"Uni-tas" general model : $\mathcal{U}(\Upsilon, d, \beta)$

The general model is based on 3 parameters

- Υ : the total mass of the cfg
- d : the dimension of the cfg
- $\beta \in [0, 1]$ related to the position of the unique "pile"

$$i = 1 + \lfloor \beta(d-2) \rfloor$$

The cfg $(c_1, \ldots, c_{d-1})$ satisfies

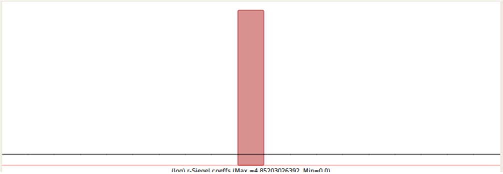
- $\mathbb{E}[c_i] = \Upsilon, \quad \mathbb{E}[c_j] = 0$ for $j \neq i$
- the total mass : $\mathbb{E}[\mathcal{M}] = \Upsilon$
- the energy (potential) :

$$\mathbb{E}[\mathcal{E}] \sim \begin{cases} d^2 \beta(1-\beta)\,\Upsilon & \text{si } \beta \in]0,1[\\ d\,\Upsilon & \text{si } \beta \in \{0,1\} \end{cases}.$$

“Uni-tas” general model : $\mathcal{U}(\Upsilon, d, \beta)$

Applications

- Knapsack problem : $\beta = 0$ (model $\mathcal{K}(\Upsilon, d)$)
- Schnorr factorization : $\beta = 0$
- protocol NTRU : $\beta = 1/2$ (model $\mathcal{N}(\Upsilon, d)$)
- ...



Coppersmith general model

A Coppersmith cfg can also be represented as the concatenation of several cfg

Results with the models M1/M2

Modèles	K **pire des cas**	K **pour** $\texttt{M1}(\alpha)$	K **pour** $\texttt{M2}(\mu)$	K **expérimental**
$\mathcal{A}(\Upsilon, d)$	$\frac{1}{12\log t} d(d+1)\tilde{\Upsilon}$	$\frac{1}{12\alpha} d(d+1)\tilde{\Upsilon}$	$\frac{1}{6\|\log\mu\|} d(d+1)\tilde{\Upsilon}$	$\Theta(d^2\tilde{\Upsilon})$
$\mathcal{N}(\Upsilon, d)$	$\frac{1}{8\log t} d^2\tilde{\Upsilon}$	$\frac{1}{8\alpha} d^2\tilde{\Upsilon}$	$\frac{1}{4\|\log\mu\|} d^2\tilde{\Upsilon}$	$\Theta(d^2\tilde{\Upsilon})$
$\mathcal{K}(\Upsilon, d)$	$\frac{1}{2\log t} d\tilde{\Upsilon}$	$\frac{1}{2\alpha} d\tilde{\Upsilon}$	$\frac{1}{\|\log\mu\|} d\tilde{\Upsilon}$	$\Theta(d\tilde{\Upsilon})$

- $\tilde{\Upsilon} = \alpha \cdot \Upsilon$ with α a known constant

Plan

Conclusion

- Simplified models,
  very useful for explaining, making experiments, finding conjectures......
- Only qualitative similarities with the actual LLL algorithm.
- Possible (easy) proofs.
- Some results in dimension $d \geq 3$ that do not exist for the LLL algorithm
- New challenges : model M3 which is a probabilistic dynamical system with a hole