Modélisations de l'algorithme LLL et de ses entrées par des systèmes dynamiques

Loïck Lhote

GREYC, ENSICAEN, CNRS-UMR 6072

Journées SDA 2

LORIA, Nancy, 9-10 avril 2014

Plan

Généralisations de l'algorithme d'Euclide

Une spécialité du GREYC : Analyse Dynamique d'algorithmes du PGCD

Généralisations de l'algorithme d'Euclide

Une spécialité du GREYC : Analyse Dynamique d'algorithmes du PGCD

PGCD
Approximation Rationnelle Simultanée

Problème :

Etant donné $\overrightarrow{y} \in \mathbb{R}^n$, trouver $q \in \mathbb{Z}$ avec $q \leq M$ et $\overrightarrow{p} \in \mathbb{Z}^n$ tels que $||q \cdot \overrightarrow{y} - \overrightarrow{p}||$ est petit.

Développement en fractions continues

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

Généralisations de l'algorithme d'Euclide

Une spécialité du GREYC : Analyse Dynamique d'algorithmes du PGCD

Réduction des réseaux

- Algorithmes LLL, HKZ, BKZ, ...
- Modélisation des algorithmes (tas de sable, CFG, etc.)
- Modélisation des entrées

PGCD
Approximation Rationnelle Simultanée

Problème :

Etant donné $\overrightarrow{y} \in \mathbb{R}^n$, trouver $q \in \mathbb{Z}$ avec $q \leq M$ et $\overrightarrow{p} \in \mathbb{Z}^n$ tels que $||q \cdot \overrightarrow{y} - \overrightarrow{p}||$ est petit.

Développement en fractions continues

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

Réseaux euclidiens

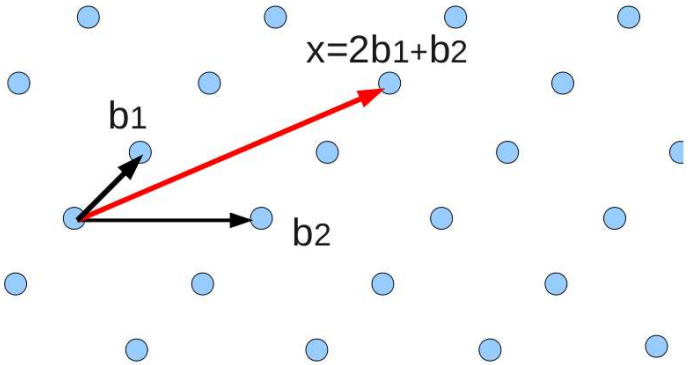
Un réseau euclidien de $\mathbb{R}^n$ est un sous-groupe discret de $\mathbb{R}^n$.

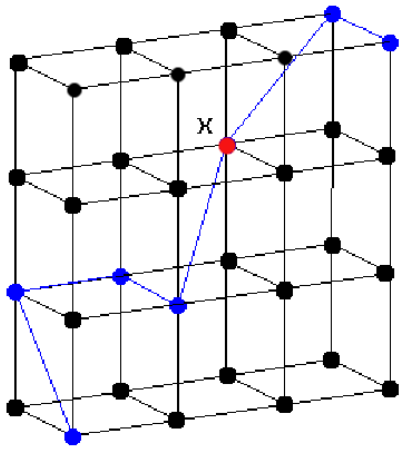
Si $B := (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d)$ est un système de d vecteurs linéairement indépendants de $\mathbb{R}^n$, le réseau engendré par B est

$$\mathcal{L} := \{\mathbf{x} \in \mathbb{R}^n; \quad \mathbf{x} = \sum_{i=1}^{d} x_i \mathbf{b}_i, \qquad x_i \in \mathbb{Z}\}$$

Le système $B := (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d)$ est une base du réseau $\mathcal{L}$

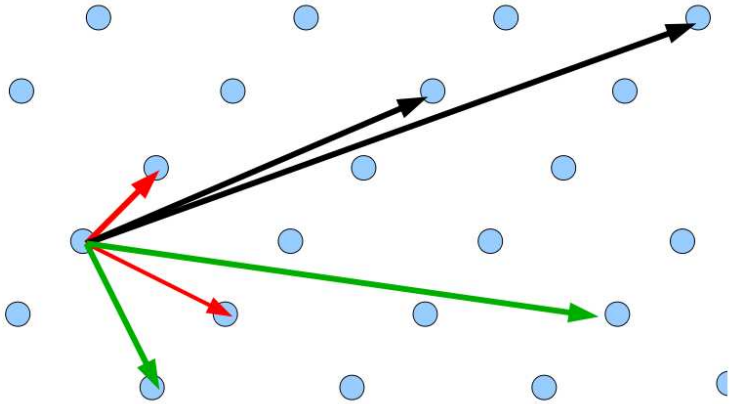
d : dimension du réseau.





Réseaux euclidiens

Un réseau possède
une infinité de bases



Problème essentiel :
Trouver une "bonne base" du réseau $\mathcal{L}$
avec des vecteurs assez courts et assez orthogonaux
à partir d'une base quelconque de $\mathcal{L}$.

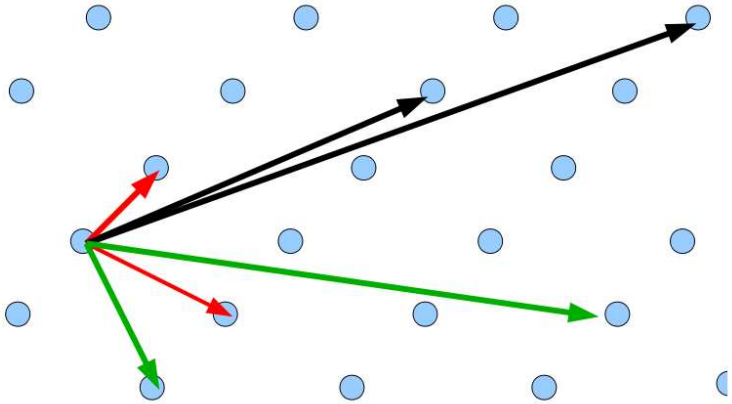
But de la réduction : trouver en un temps "raisonnable" une "assez bonne" base.

L'algorithme LLL conçu en 1982 par A. Lenstra, H. Lenstra et L. Lovász
trouve en temps polynomial une assez bonne base d'un réseau.

pour $d = 2$: l'algorithme de Gauss trouve la meilleure base
pour $d \geq 3$: l'algorithme LLL généralise l'algorithme de Gauss

Réseaux euclidiens

Un réseau possède
une infinité de bases



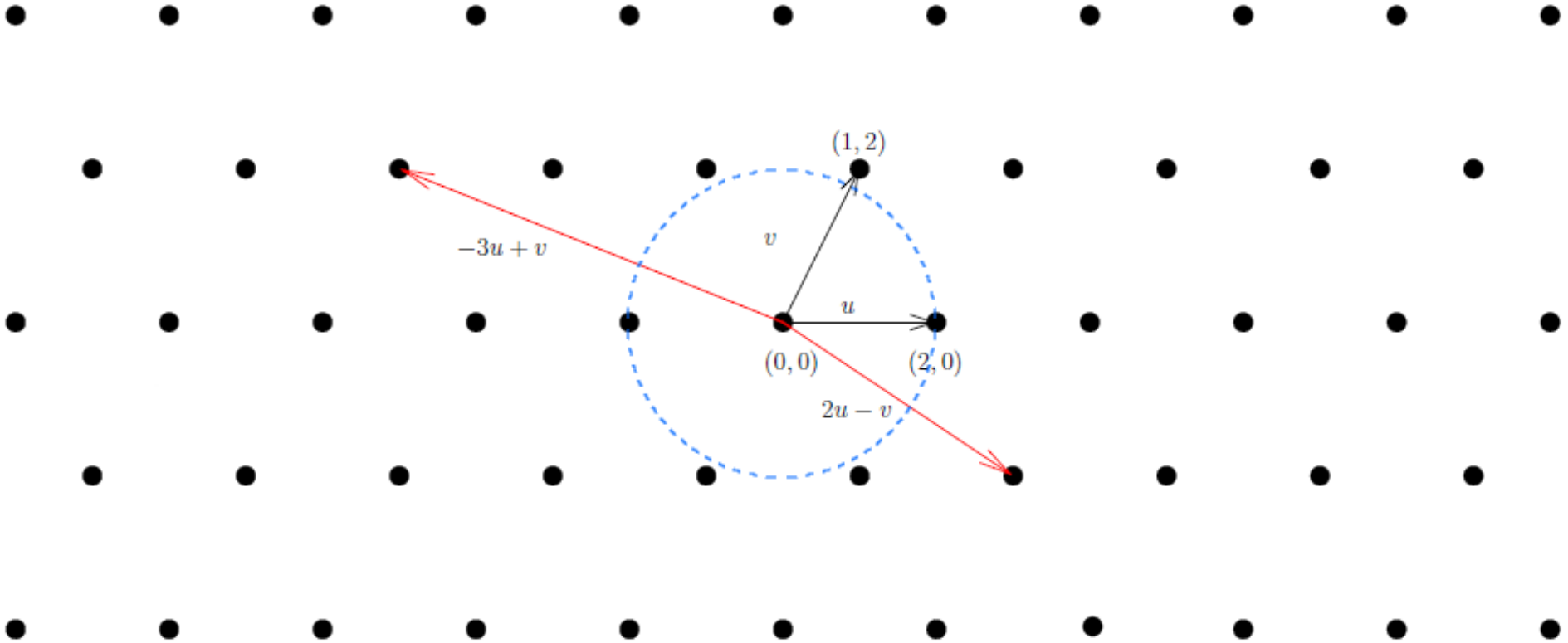
Problème essentiel :
Trouver une "bonne base" du réseau $\mathcal{L}$
avec des vecteurs assez courts et assez orthogonaux
à partir d'une base quelconque de $\mathcal{L}$.

But de la réduction : trouver en un temps "raisonnable" une "assez bonne" base.

L'algorithme LLL conçu en 1982 par A. Lenstra, H. Lenstra et L. Lovász
trouve en temps polynomial une assez bonne base d'un réseau.

pour $d = 2$: l'algorithme de Gauss trouve la meilleure base
pour $d \geq 3$: l'algorithme LLL généralise l'algorithme de Gauss

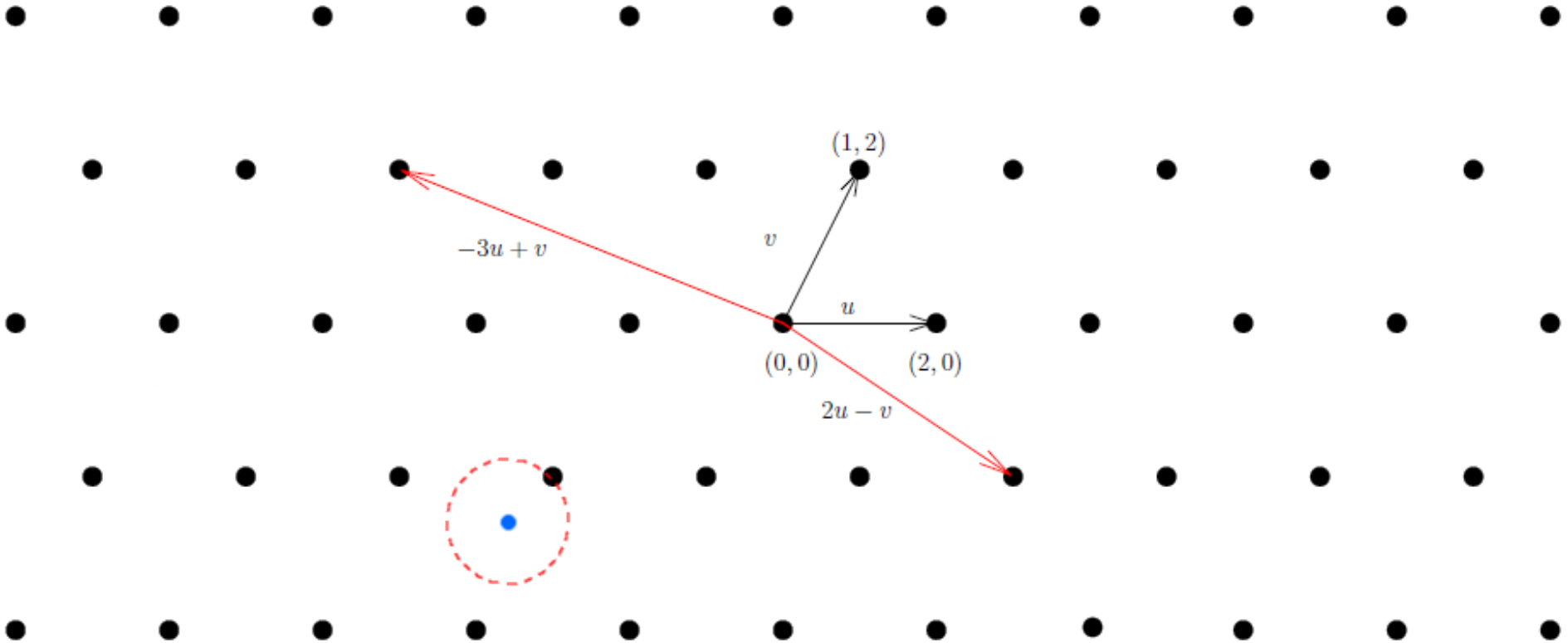
SVP : Shortest Vector Problem



Problème **SVP** : trouver un plus court vecteur non nul du réseau

Remarque : une base réduite donne une bonne approximation de la solution (pas toujours la solution).

CVP : Closest Vector Problem



Problème **CVP** : trouver un vecteur du réseau qui minimise la distance entre un vecteur et un réseau donnés.

Remarque : une base réduite donne "un bon domaine" où une solution peut être trouvée.

SVP et CVP

SVP (Shortest Vector Problem) et CVP (Closest Vector Problem) sont NP-difficiles.

L'algorithme LLL donne une solution approchée de SVP en temps polynômial.

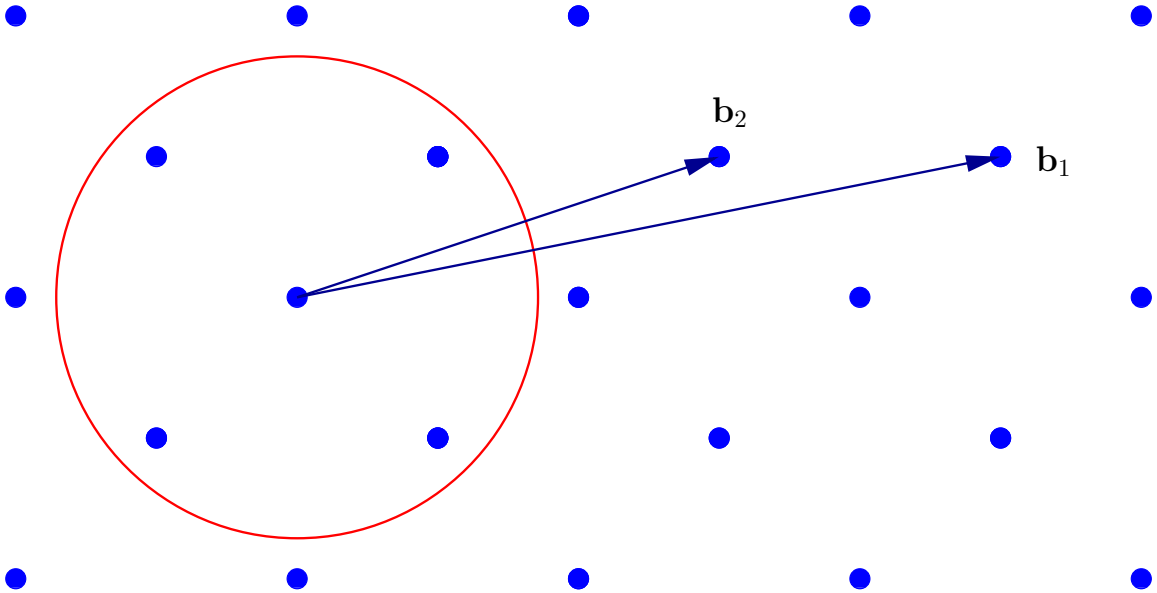
L'algorithme de Babai (basée sur LLL) donne une solution approchée de CVP en temps polynômial.

Plan

Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

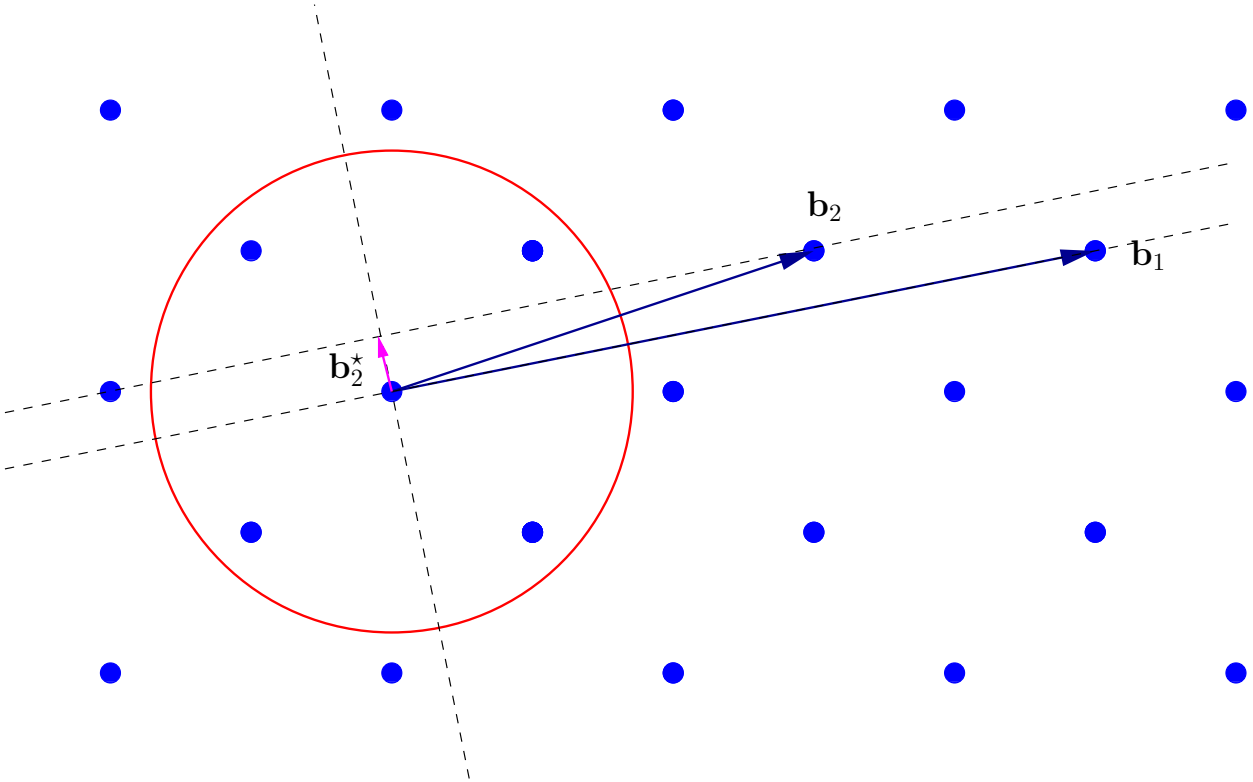
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

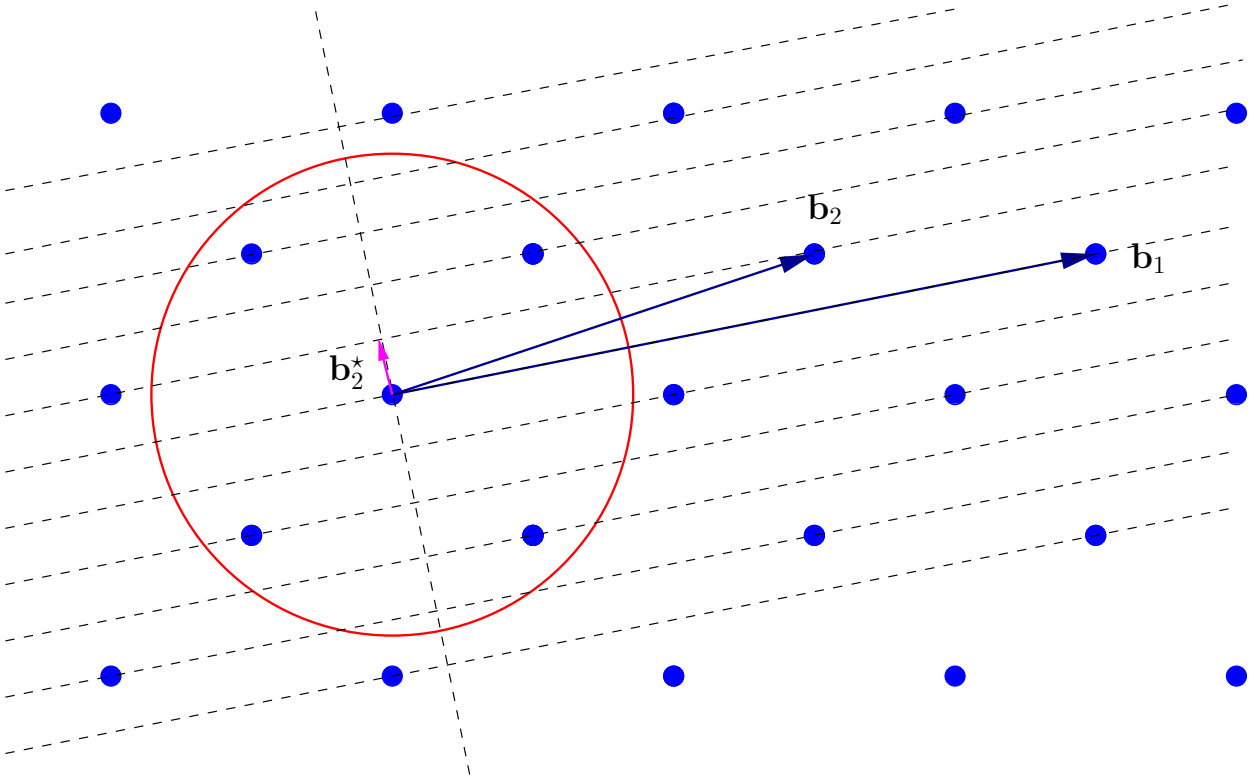
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

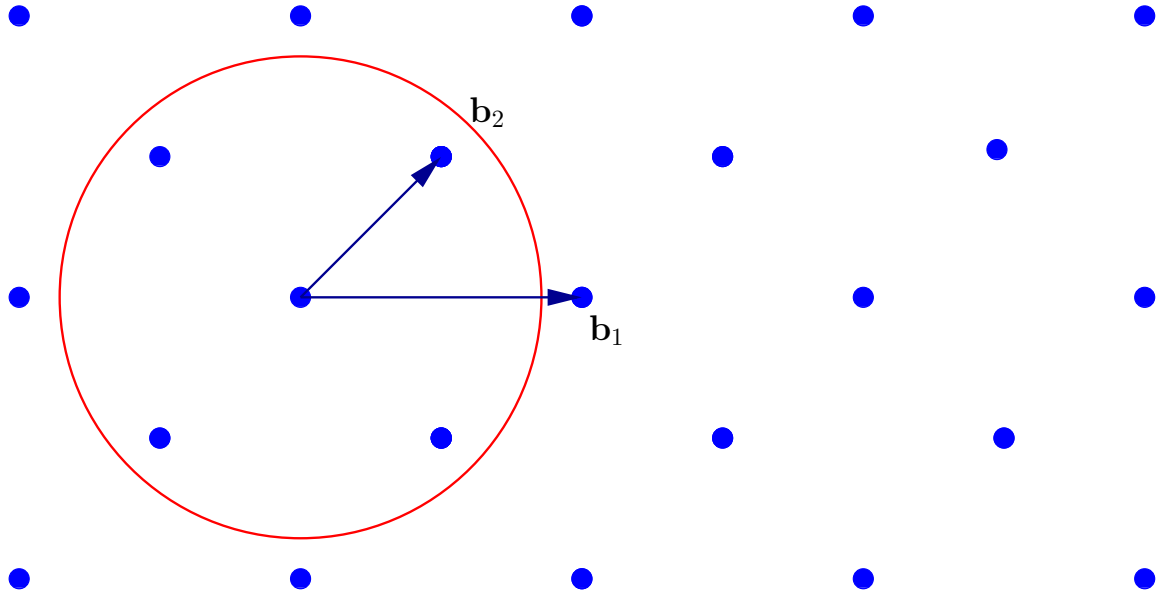
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

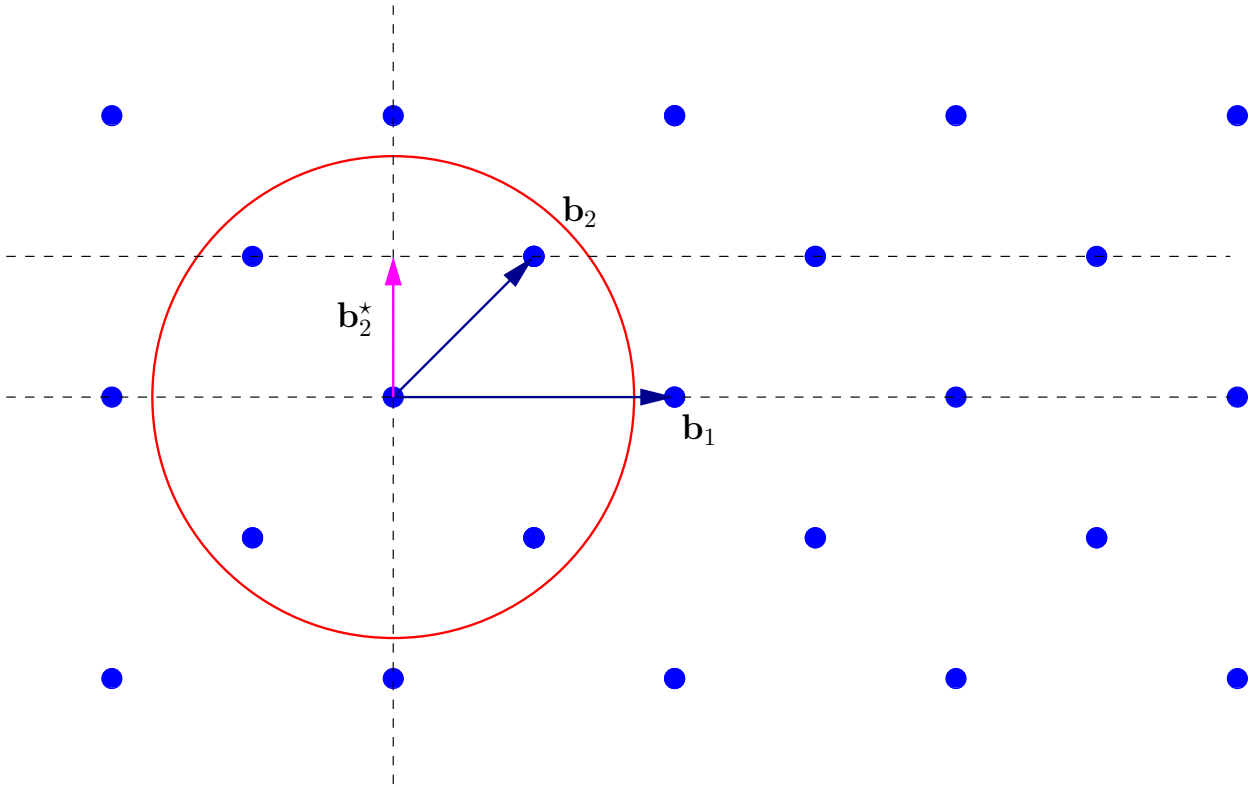
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

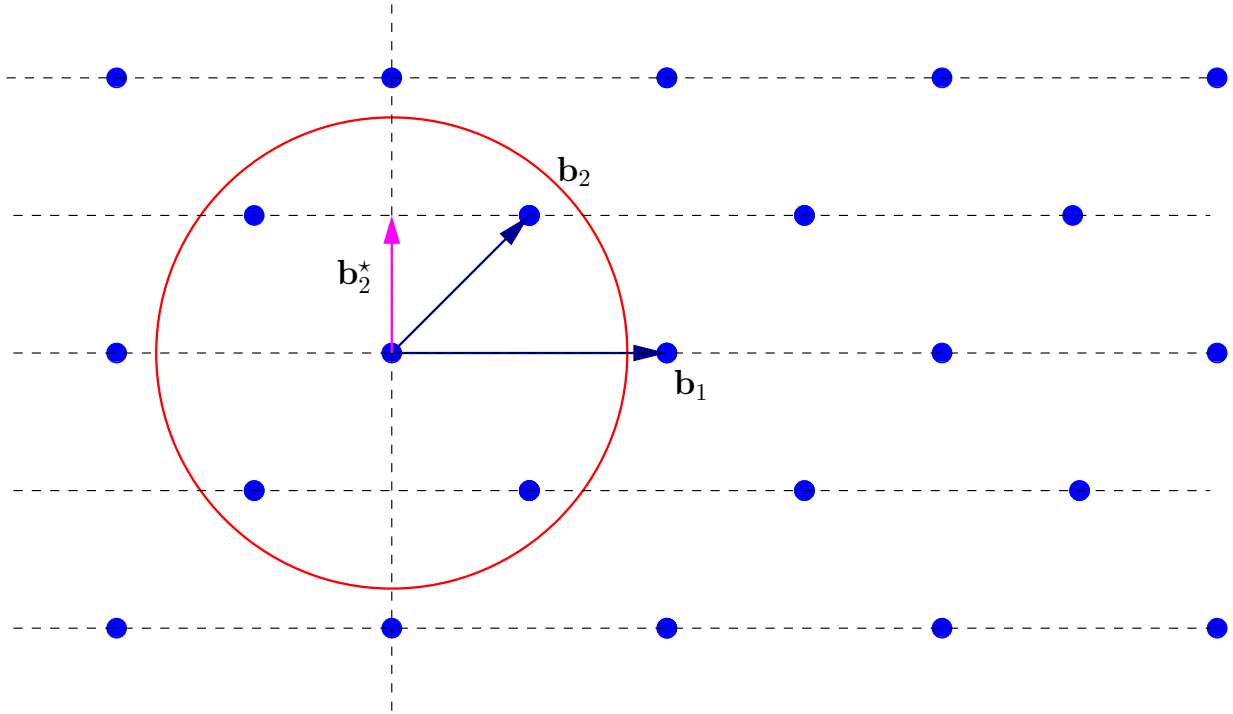
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

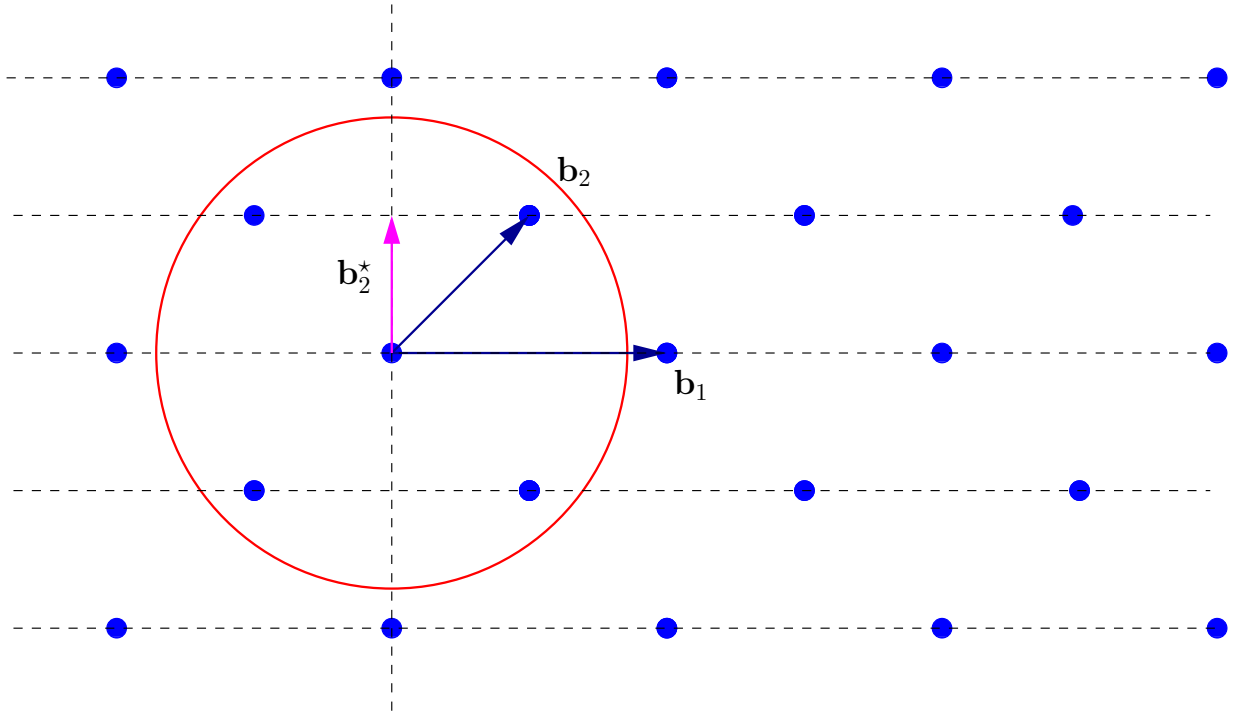
Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Programmation Linéaire Entière (H. Lenstra)

Une application importante pour utiliser une base réduite

Problème : Énumérer tous les vecteurs d'un réseau $\mathcal{L}$ à l'intérieur d'une boule.



Conclusion : utiliser une base réduite conduit à des calculs plus efficaces.

Remarque : $\mathbf{b}_2^\star$ doit être le plus long possible.

Absolute Error Problem

Évaluation d'une fonction f sur $[a, b]$ à une précision η donnée.

Méthode : Trouver un polynôme $p \in \mathcal{P}_{n,m}$ qui minimise $||f - q||$, $q \in \mathcal{P}_{n,m}$ où $m = (m_i)_{i=0..n}$ et

$$\mathcal{P}_{n,m} = \{q = \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} X + \ldots + \frac{q_n}{2^{m_n}} X^n \mid q_i \text{ entiers}\}$$

Méthodes naïves :

- Calculer de développement de Taylor et tronquer les coefficients
- Calculer le polynôme minimax et tronquer les coefficients

Absolute Error Problem

Idée : discrétiser le problème

Considérons $x_1, \ldots, x_d$ d points de $[a, b]$.

Calculons $q \in \mathcal{P}_{n,m}$ tel que pour tout $i = 1..d$,

$q(x_i)$ est aussi proche que possible de $f(x_i)$.

Absolute Error Problem

Idée : discrétiser le problème

Considérons $x_1, \ldots, x_d$ d points de $[a, b]$.

Calculons $q \in \mathcal{P}_{n,m}$ tel que pour tout $i = 1..d$,

$q(x_i)$ est aussi proche que possible de $f(x_i)$.

$$\Leftrightarrow$$

$$\begin{pmatrix} \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_1 + \ldots + \frac{q_n}{2^{m_n}} x_1^n \\ \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_2 + \ldots + \frac{q_n}{2^{m_n}} x_2^n \\ \vdots \\ \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_d + \ldots + \frac{q_n}{2^{m_n}} x_d^n \end{pmatrix} \text{ et } \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_d) \end{pmatrix}$$

des vecteurs aussi proches que possible

Absolute Error Problem

Idée : discrétiser le problème

Considérons $x_1, \ldots, x_d$ d points de $[a, b]$.

Calculons $q \in \mathcal{P}_{n,m}$ tel que pour tout $i = 1..d$,

$$q(x_i) \text{ est aussi proche que possible de } f(x_i).$$

$$\Leftrightarrow$$

$$\begin{pmatrix} \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_1 + \ldots + \frac{q_n}{2^{m_n}} x_1^n \\ \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_2 + \ldots + \frac{q_n}{2^{m_n}} x_2^n \\ \vdots \\ \frac{q_0}{2^{m_0}} + \frac{q_1}{2^{m_1}} x_d + \ldots + \frac{q_n}{2^{m_n}} x_d^n \end{pmatrix} \text{ et } \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_d) \end{pmatrix}$$

des vecteurs aussi proches que possible

$$\Leftrightarrow$$

$$q_0 \cdot \overrightarrow{v_0} + q_1 \cdot \overrightarrow{v_1} + \ldots + q_n \cdot \overrightarrow{v_n} \quad \text{and} \quad \overrightarrow{y} = \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_d) \end{pmatrix}$$

des vecteurs aussi proches que possible

Absolute Error Problem

Il faut minimiser $||q_0 \cdot \overrightarrow{v_0} + q_1 \cdot \overrightarrow{v_1} + \ldots + q_n \cdot \overrightarrow{v_n} - \overrightarrow{y}||$

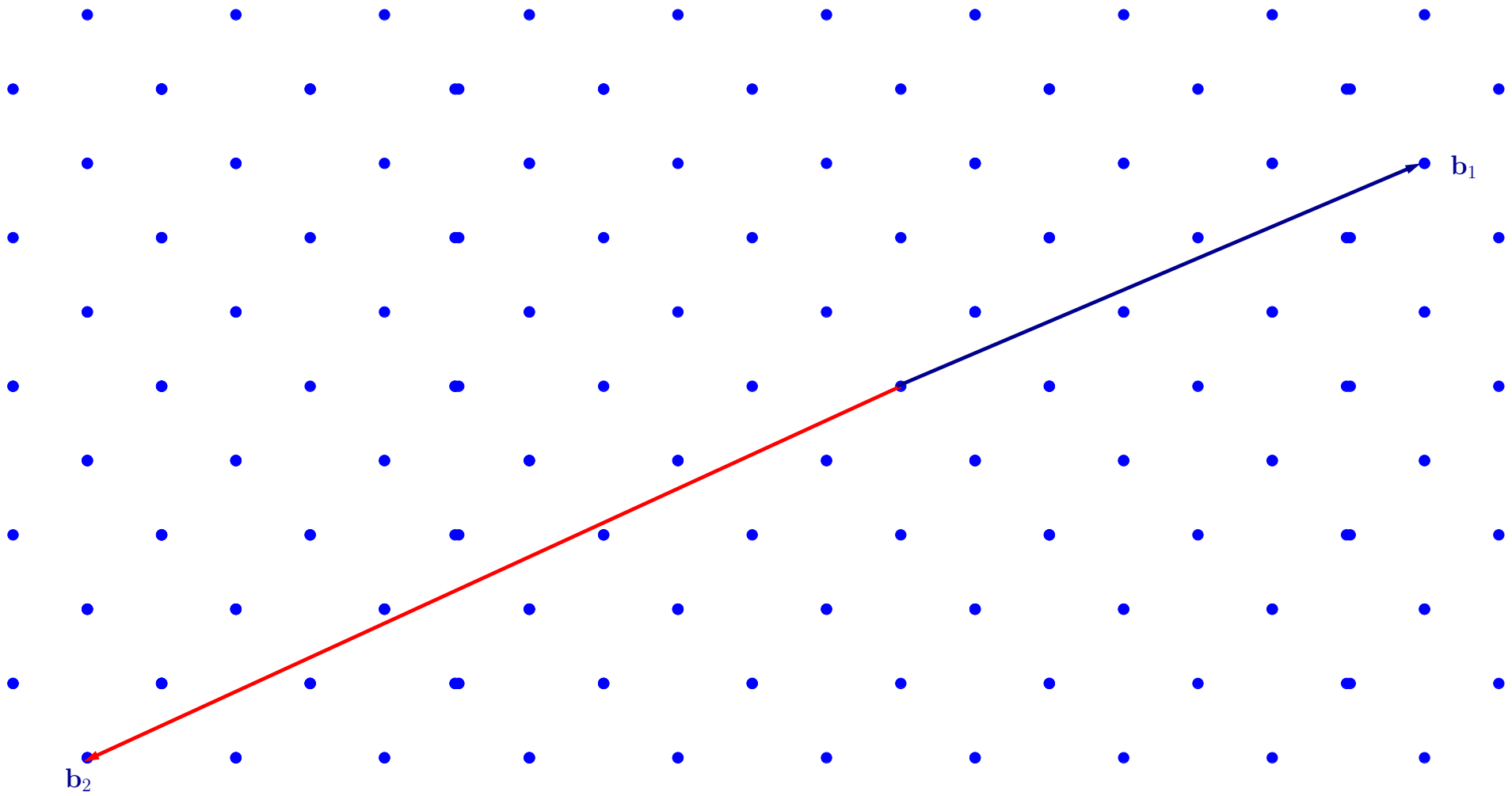
En d'autres mots, il faut trouver le plus proche vecteur de $\overrightarrow{y}$ dans le réseau $\mathcal{L}(\overrightarrow{v_0}, \overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$.

Autres applications

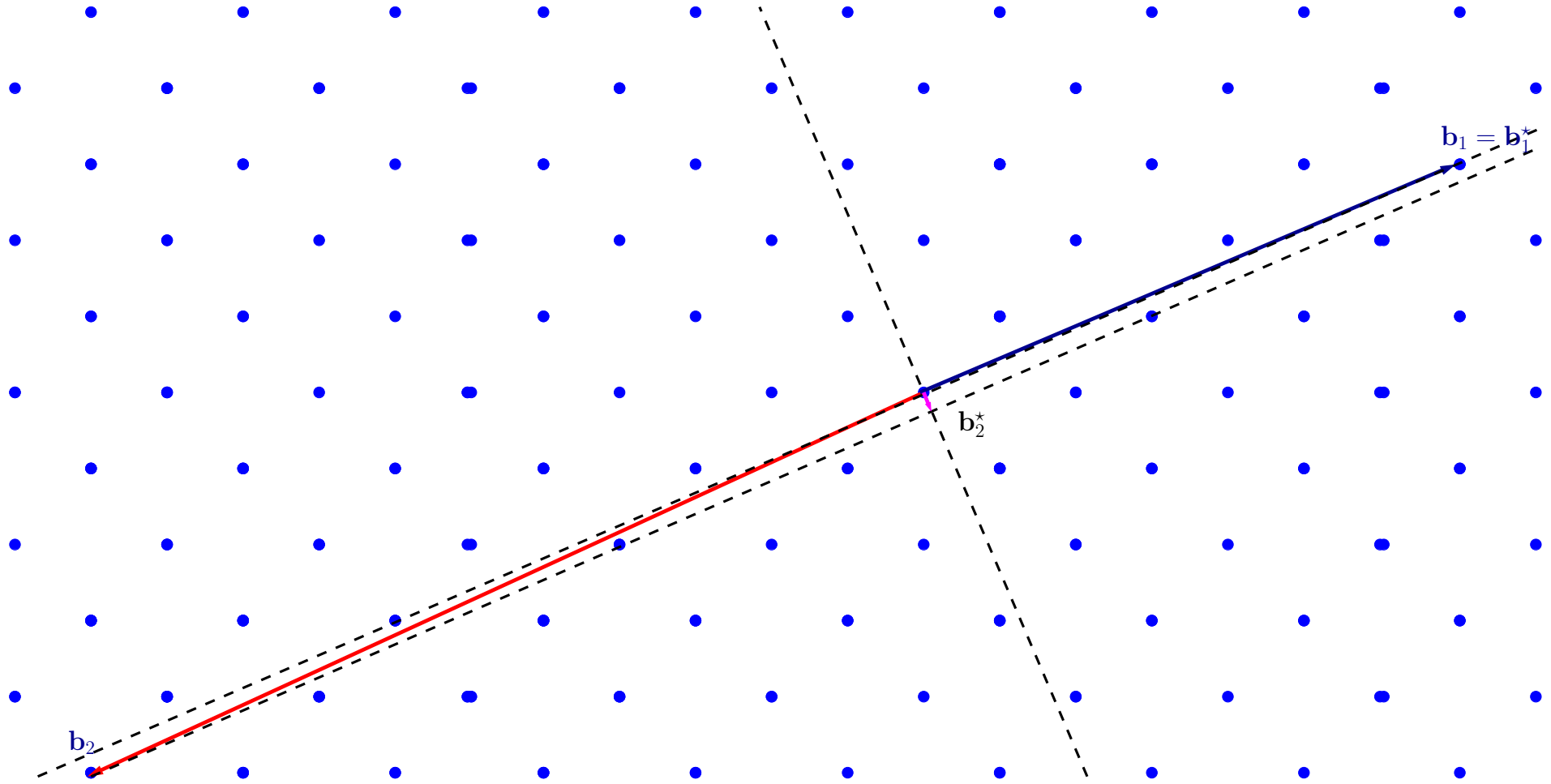
- Approximation diophantienne simultanée
- Cryptanalyses de protocoles de type RSA ou Sac-à-dos
- Conception de protocoles homomorphes
- Codage et télécommunications
- Théorie de la complexité
- ...

Plan

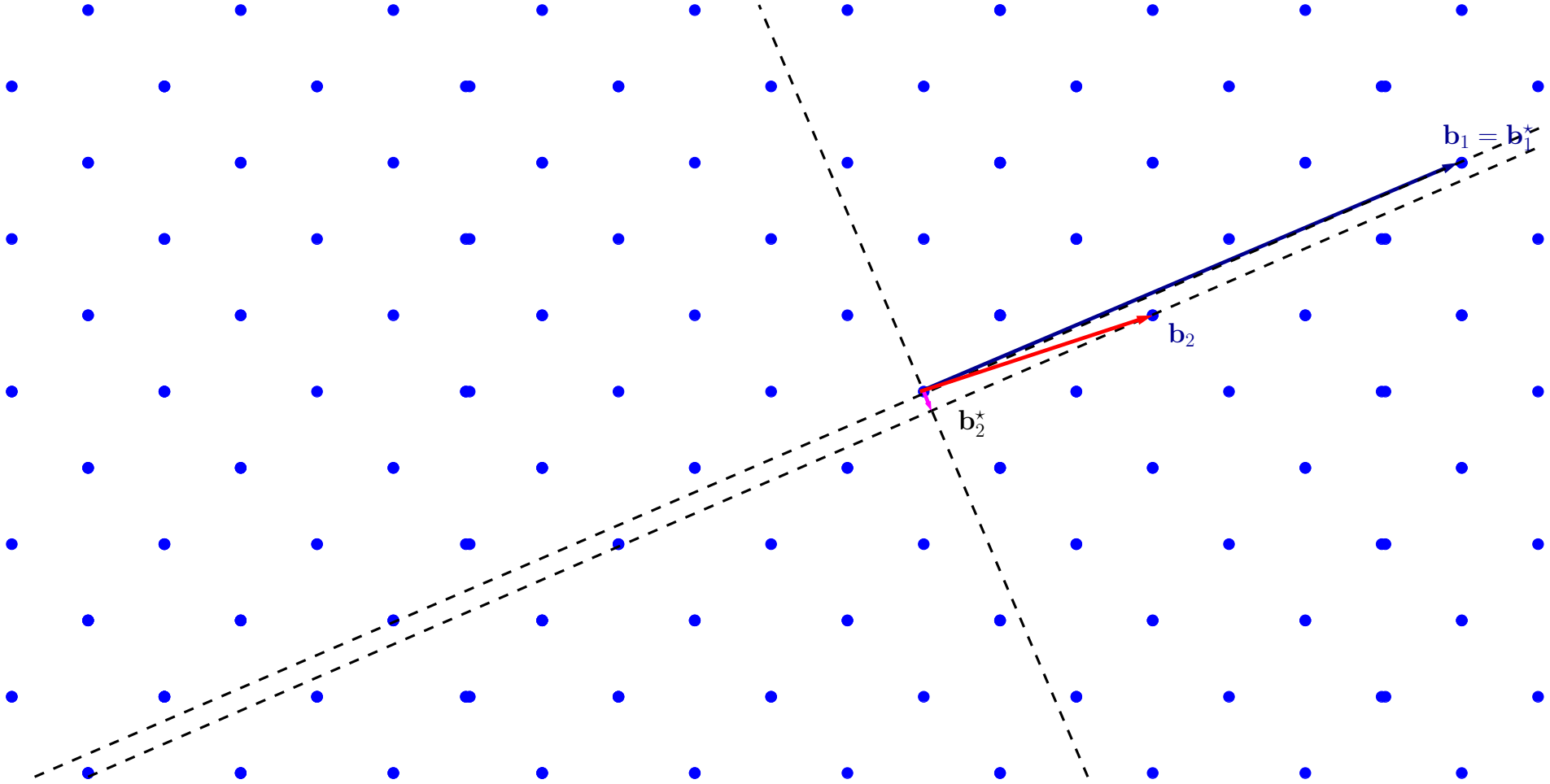
Principes de l'algorithme



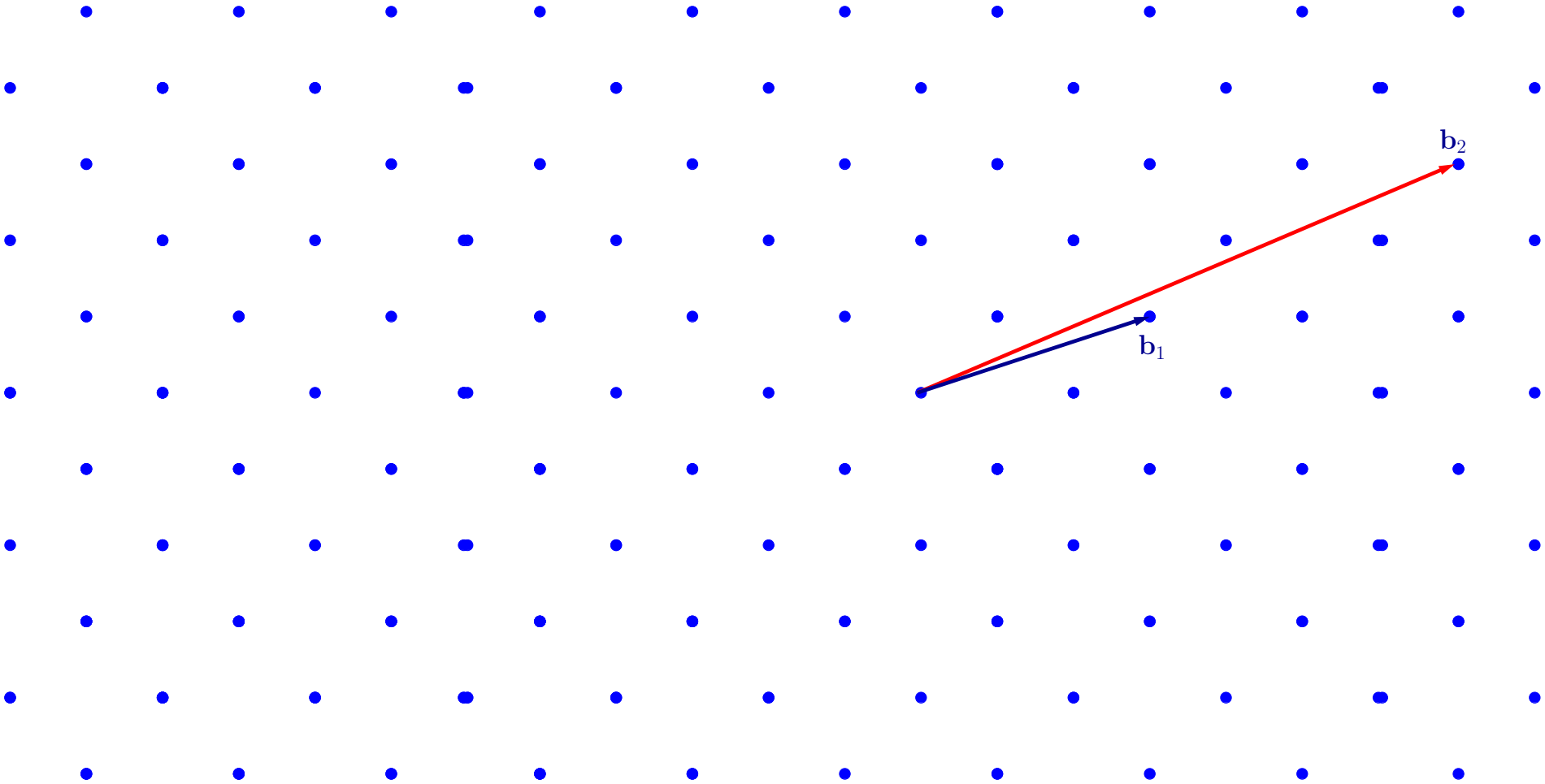
Principes de l'algorithme



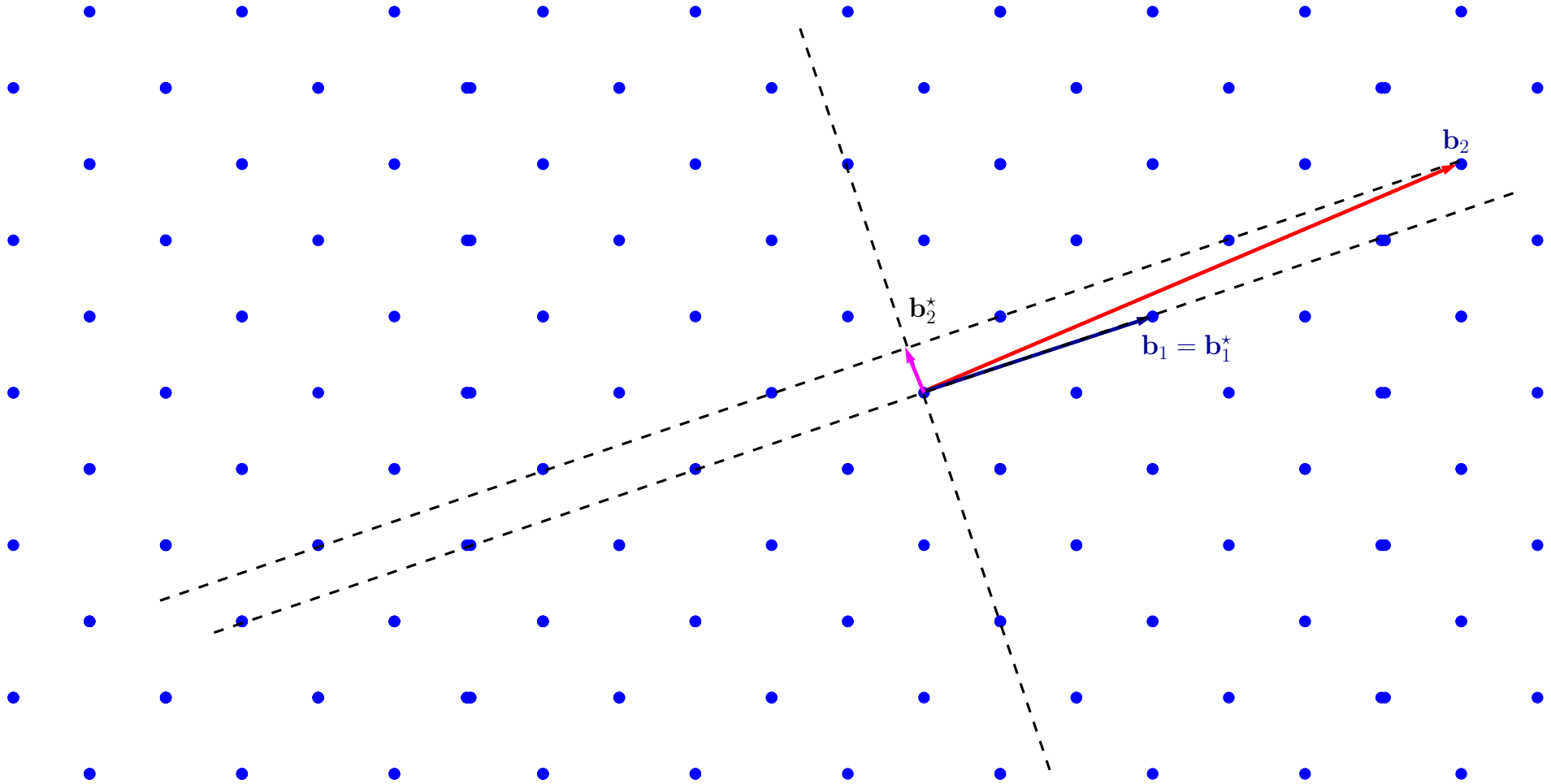
Principes de l'algorithme



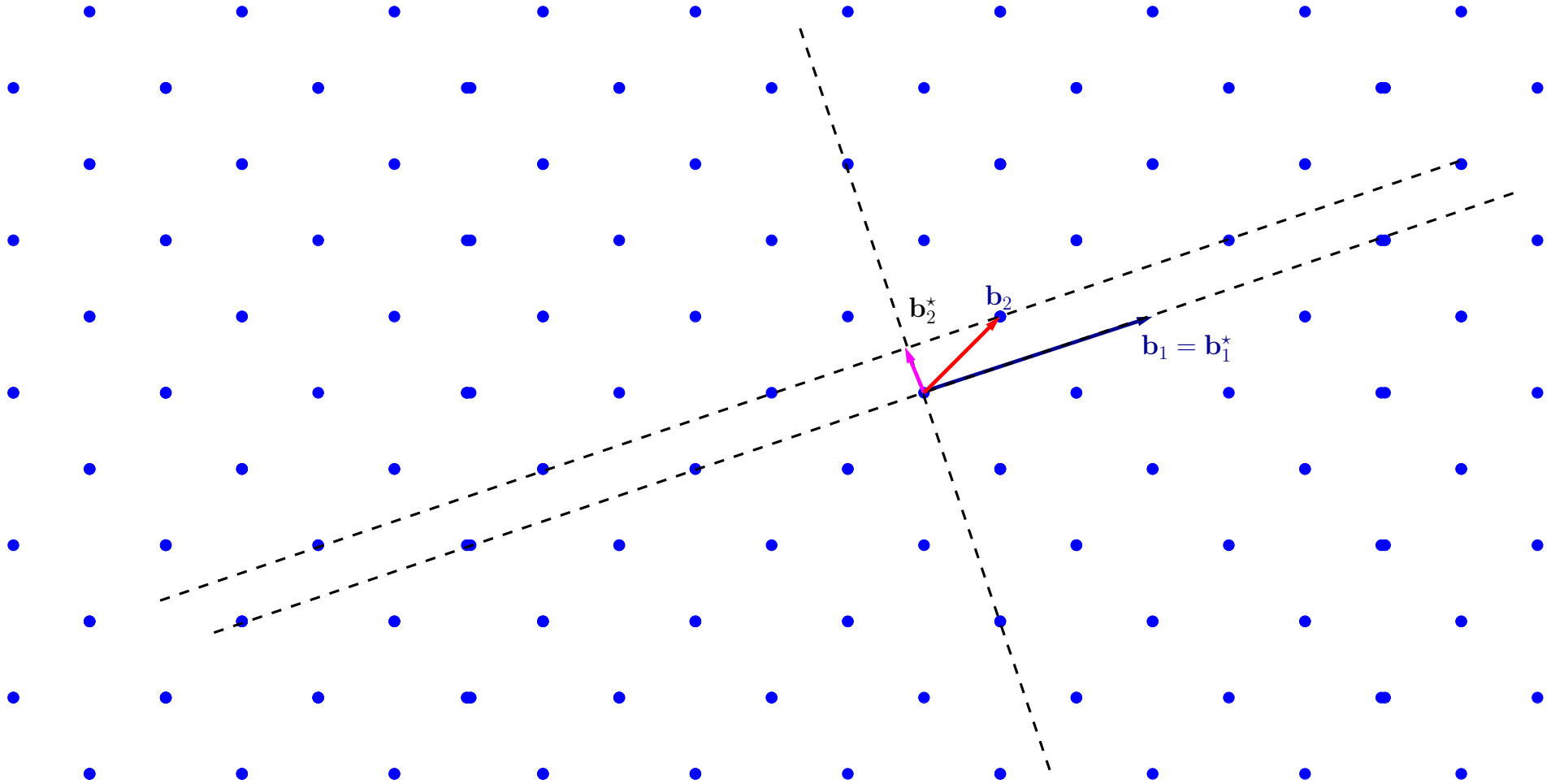
Principes de l'algorithme



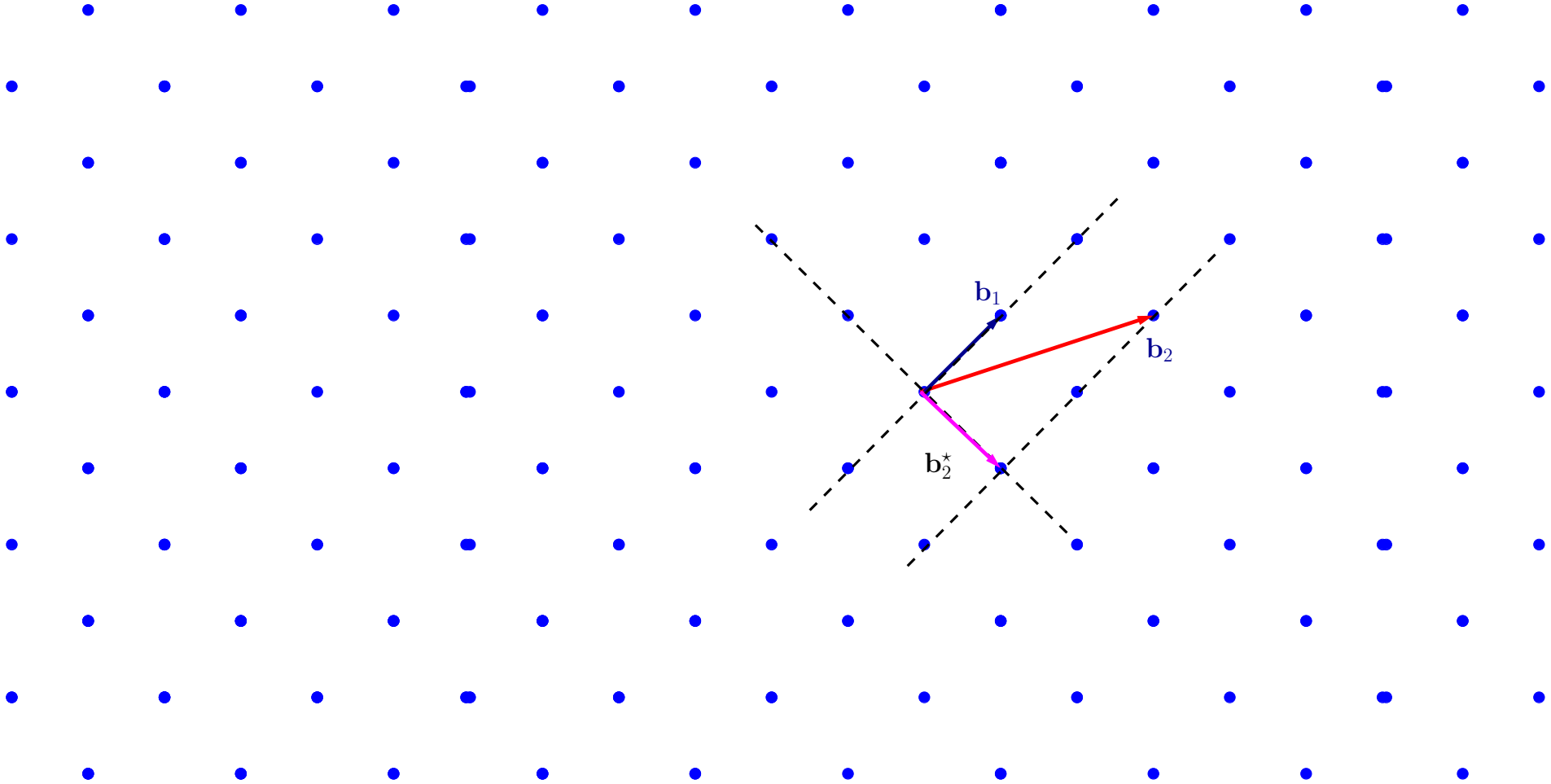
Principes de l'algorithme



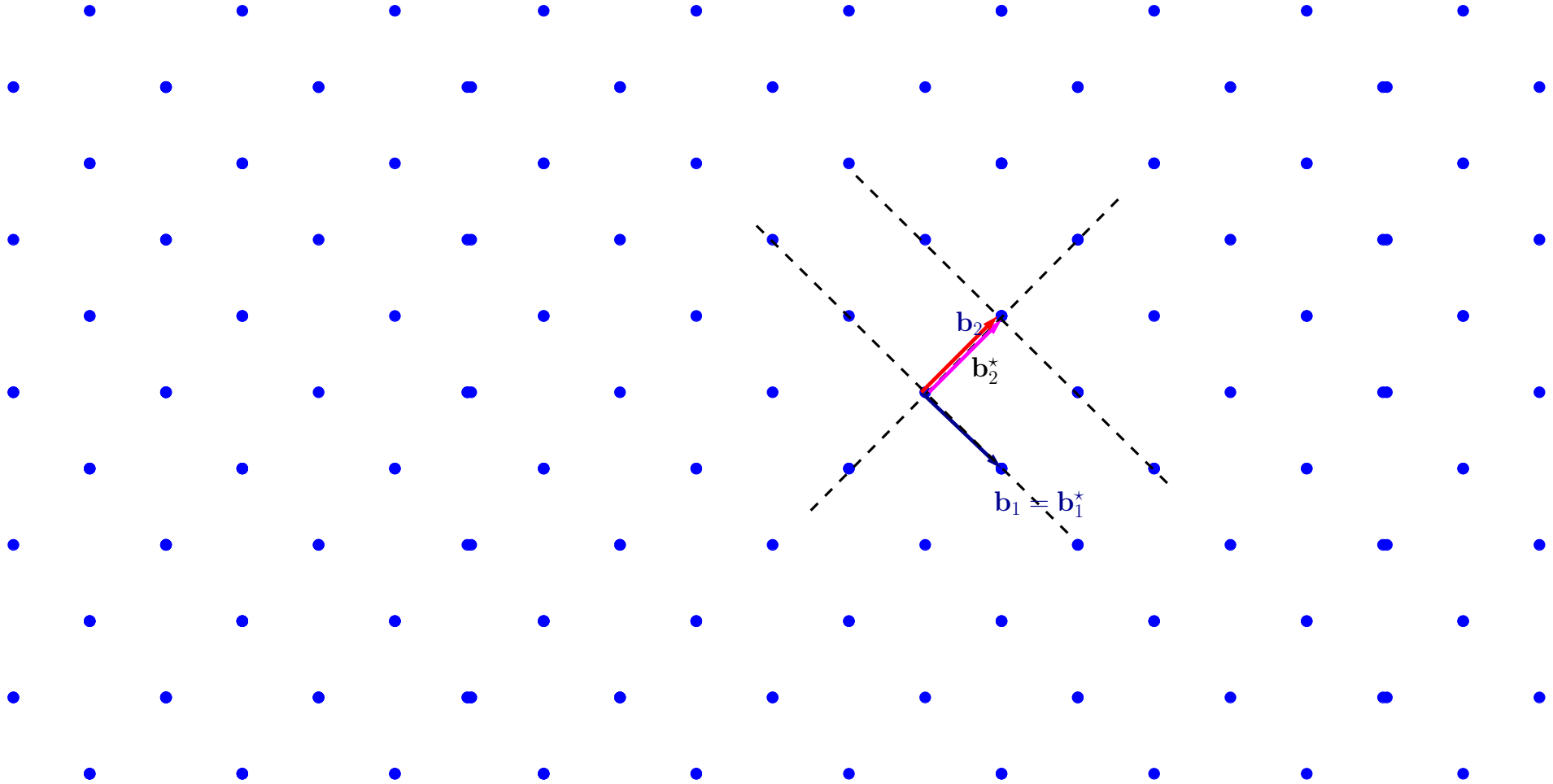
Principes de l'algorithme



Principes de l'algorithme



Principes de l'algorithme



$B^\star = (\mathbf{b}_1^\star, \ldots, \mathbf{b}_d^\star)$: la base des orthogonalisés de Gram Schmidt

$\mathcal{P} : B \to B^\star$ (la matrice de passage)

$$\begin{array}{c} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_i \\ \mathbf{b}_{i+1} \\ \vdots \\ \mathbf{b}_d \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{b}_1^\star & \mathbf{b}_2^\star & \ldots & \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star & \ldots & \mathbf{b}_d^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ m_{2,1} & 1 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & & & & \vdots \\ \ldots & \ddots & \ddots & & & & \vdots \\ \ldots & \ldots & \ldots & 1 & 0 & & \vdots \\ \ldots & \ldots & \ldots & m_{i+1,i} & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & 0 \\ m_{d,1} & m_{d,2} & \ldots & \ldots & \ldots & \ldots & 1 \end{pmatrix} \end{array}$$

Les translations :

- diminuent la norme des vecteurs
- rendent la base propre

Une base B est dite propre si la matrice de passage $\mathcal{P}$ vérifie :

$$|m_{i,j}| \leq 1/2 \text{ pour } 1 \leq j < i \leq n$$

$$B_i := \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}.$$

Les échanges :
(t paramètre de l'algorithme, $t > 1$)

- effectués si $\|\mathbf{v}_i\| < (1/t)\|\mathbf{u}_i\|$
- rendent la base plus orthogonale

$B^\star = (\mathbf{b}_1^\star, \ldots, \mathbf{b}_d^\star)$: la base des orthogonalisés de Gram Schmidt

$\mathcal{P} : B \to B^\star$ (la matrice de passage)

$$\begin{array}{c} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_i \\ \mathbf{b}_{i+1} \\ \vdots \\ \mathbf{b}_d \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{b}_1^\star & \mathbf{b}_2^\star & \ldots & \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star & \ldots & \mathbf{b}_d^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ m_{2,1} & 1 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & & & & \vdots \\ \ldots & \ddots & \ddots & & & & \vdots \\ \ldots & \ldots & \ldots & 1 & 0 & & \vdots \\ \ldots & \ldots & \ldots & m_{i+1,i} & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & 0 \\ m_{d,1} & m_{d,2} & \ldots & \ldots & \ldots & \ldots & 1 \end{pmatrix} \end{array}$$

Les translations :

- diminuent la norme des vecteurs
- rendent la base propre

Une base B est dite propre
si la matrice de passage $\mathcal{P}$ vérifie :

$$|m_{i,j}| \leq 1/2 \text{ pour } 1 \leq j < i \leq n$$

$$B_i := \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}.$$

Les échanges :
(t paramètre de l'algorithme, $t > 1$)

- effectués si $\|\mathbf{v}_i\| < (1/t)\|\mathbf{u}_i\|$
- rendent la base plus orthogonale

$B^\star = (\mathbf{b}_1^\star, \ldots, \mathbf{b}_d^\star)$: la base des orthogonalisés de Gram Schmidt

$\mathcal{P} : B \to B^\star$ (la matrice de passage)

$$\begin{array}{c} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_i \\ \mathbf{b}_{i+1} \\ \vdots \\ \mathbf{b}_d \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{b}_1^\star & \mathbf{b}_2^\star & \ldots & \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star & \ldots & \mathbf{b}_d^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ m_{2,1} & 1 & \ddots & & & & \vdots \\ \ldots & \ddots & \ddots & & & & \vdots \\ \ldots & \ldots & \ldots & 1 & 0 & & \vdots \\ \ldots & \ldots & \ldots & m_{i+1,i} & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & 0 \\ m_{d,1} & m_{d,2} & \ldots & \ldots & \ldots & \ldots & 1 \end{pmatrix} \end{array}$$

$$B_i := \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}.$$

Les translations :

- diminuent la norme des vecteurs
- rendent la base propre

Une base B est dite propre si la matrice de passage $\mathcal{P}$ vérifie :

$$|m_{i,j}| \leq 1/2 \text{ pour } 1 \leq j < i \leq n$$

Les échanges :
(t paramètre de l'algorithme, $t > 1$)

- effectués si $\|\mathbf{v}_i\| < (1/t)\|\mathbf{u}_i\|$
- rendent la base plus orthogonale

$B^\star = (\mathbf{b}_1^\star, \ldots, \mathbf{b}_d^\star)$: la base des orthogonalisés de Gram Schmidt

$\mathcal{P} : B \to B^\star$ (la matrice de passage)

$$\begin{array}{c} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_i \\ \mathbf{b}_{i+1} \\ \vdots \\ \mathbf{b}_d \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{b}_1^\star & \mathbf{b}_2^\star & \ldots & \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star & \ldots & \mathbf{b}_d^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ m_{2,1} & 1 & \ddots & & & & \vdots \\ \ldots & \ddots & \ddots & & & & \vdots \\ \ldots & \ldots & \ldots & 1 & 0 & & \vdots \\ \ldots & \ldots & \ldots & m_{i+1,i} & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & 0 \\ m_{d,1} & m_{d,2} & \ldots & \ldots & \ldots & \ldots & 1 \end{pmatrix} \end{array}$$

$$B_i := \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}.$$

Les translations :

- diminuent la norme des vecteurs
- rendent la base propre

Une base B est dite propre si la matrice de passage $\mathcal{P}$ vérifie :

$$|m_{i,j}| \leq 1/2 \text{ pour } 1 \leq j < i \leq n$$

Les échanges :
(t paramètre de l'algorithme, $t > 1$)

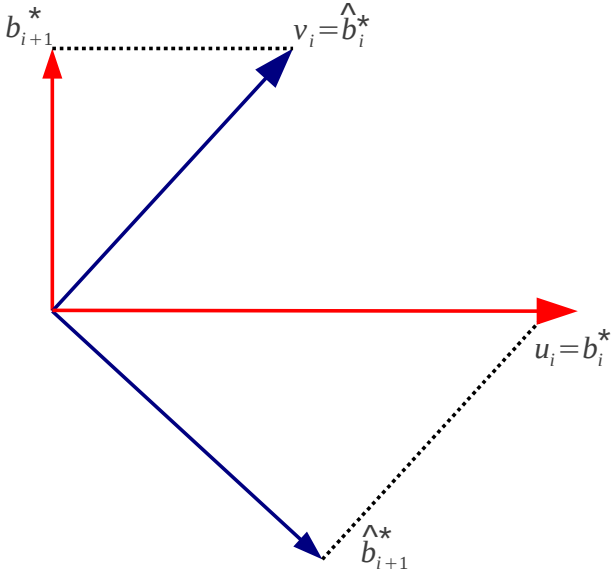
- effectués si $\|\mathbf{v}_i\| < (1/t)\|\mathbf{u}_i\|$
- rendent la base plus orthogonale

Les échanges rendent la base plus orthogonale

$$\ell_i := \|\mathbf{b}_i^\star\|, \qquad r_i := \frac{\ell_{i+1}}{\ell_i} \quad \text{(rapports de Siegel)} \qquad \text{et} \quad \nu_i := \{m_{i+1,i}\}$$

(partie fractionnelle centrée)

$$B_i = \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}$$



Si la base B_i n'est pas réduite,
un échange modifie la base $B_i^\star$.

Les nouveaux rapports de Siegel :

$$\check{r}_{i-1} = \rho . r_{i-1}$$

$$\check{r}_i = \frac{1}{\rho^2} . r_i$$

$$\check{r}_{i+1} = \rho . r_{i+1} .$$

avec un facteur de décroissance ρ

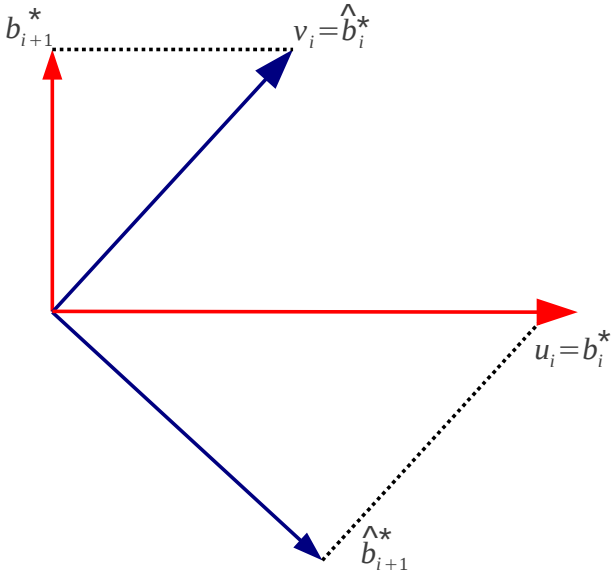
$$\rho^2 = r_i^2 + \nu_i^2 \leq 1$$

Les échanges rendent la base plus orthogonale

$$\ell_i := \|\mathbf{b}_i^\star\|, \qquad r_i := \frac{\ell_{i+1}}{\ell_i} \quad \text{(rapports de Siegel)} \qquad \text{et} \quad \nu_i := \{m_{i+1,i}\}$$

(partie fractionnelle centrée)

$$B_i = \begin{array}{c} \\ \mathbf{u}_i \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{b}_i^\star & \mathbf{b}_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}$$



Si la base B_i n'est pas réduite,
un échange modifie la base $B_i^\star$.

Les nouveaux rapports de Siegel :

$$\check{r}_{i-1} = \rho.r_{i-1}$$

$$\check{r}_i = \frac{1}{\rho^2}.r_i$$

$$\check{r}_{i+1} = \rho.r_{i+1}.$$

avec un facteur de décroissance ρ

$$\rho^2 = r_i^2 + \nu_i^2 \leq 1$$

Algorithme LLL(t), $t > 1$

Entrées: $B = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$
Résultat: $\widehat{B} = (\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_d)$ t-réduite.
Calculer $(B^\star, \mathcal{P})$;
$i \leftarrow 1$;
tant que $i < d$ **faire**
  Translater $\mathbf{b}_{i+1}$ // $\mathbf{b}_i$
    (t.q $|m_{i+1,i}| \leq 1/2$);
  Tester $\|\mathbf{v}_i\| > (1/t)\,\|\mathbf{u}_i\|$?
    Si oui
      Translater $\mathbf{b}_{i+1}$ // $\mathbf{b}_k$
        (t.q $|m_{k,i}| \leq 1/2$);
      $i \leftarrow i + 1$;
    Sinon
      Échanger $\mathbf{b}_i$ et $\mathbf{b}_{i+1}$;
      Recalculer $(B^\star, \mathcal{P})$;
      Si $i \neq 1$ alors $i \leftarrow i - 1$;
fin

Condition de Lovász

$$\mathcal{L}(t): \qquad r_i^2 \geq \frac{1}{t^2} - \nu_i^2$$

$$\|\mathbf{v}_i\| \geq (1/t)\|\mathbf{u}_i\|$$

Condition de Siegel

$$\mathcal{S}(s): \qquad r_i \geq \frac{1}{s}$$

Une base B d'un réseau $\mathcal{L}$ qui est propre est dite réduite au sens de t- Lovász (resp. s-Siegel) si vérifie la condition $\mathcal{L}(t)$ (resp. $\mathcal{S}(s)$)

si s et t vérifient

$$\frac{1}{s^2} = \frac{1}{t^2} - \frac{1}{4}, \text{ avec } s \geq \frac{2}{\sqrt{3}} \text{ et } t \geq 1$$

alors $\mathcal{L}(t) \Rightarrow \mathcal{S}(s)$

Algorithme LLL(t), $t > 1$

Entrées: $B = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$
Résultat: $\widehat{B} = (\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_d)$ t-réduite.
Calculer $(B^\star, \mathcal{P})$;
$i \leftarrow 1$;
tant que $i < d$ **faire**
  Translater $\mathbf{b}_{i+1}$ // $\mathbf{b}_i$ (t.q $|m_{i+1,i}| \leq 1/2$);
  Tester $\|\mathbf{v}_i\| > (1/t)\,\|\mathbf{u}_i\|$?
    Si oui
      Translater $\mathbf{b}_{i+1}$ // $\mathbf{b}_k$ (t.q $|m_{k,i}| \leq 1/2$);
      $i \leftarrow i + 1$;
    Sinon
      Échanger $\mathbf{b}_i$ et $\mathbf{b}_{i+1}$;
      Recalculer $(B^\star, \mathcal{P})$;
      Si $i \neq 1$ alors $i \leftarrow i - 1$;
fin

Condition de Lovász

$$\mathcal{L}(t): \qquad r_i^2 \geq \frac{1}{t^2} - \nu_i^2$$
$$\|\mathbf{v}_i\| \geq (1/t)\|\mathbf{u}_i\|$$

Condition de Siegel

$$\mathcal{S}(s): \qquad r_i \geq \frac{1}{s}$$

Une base B d'un réseau $\mathcal{L}$ qui est propre est dite réduite au sens de t- Lovász (resp. s-Siegel) si vérifie la condition $\mathcal{L}(t)$ (resp. $\mathcal{S}(s)$)

si s et t vérifient

$$\frac{1}{s^2} = \frac{1}{t^2} - \frac{1}{4}, \text{ avec } s \geq \frac{2}{\sqrt{3}} \text{ et } t \geq 1$$

alors $\mathcal{L}(t) \Rightarrow \mathcal{S}(s)$

Potentiel d'une base : $\Delta(B) = \prod_{i=1}^{d} \ell_i^{(d-i)}$.

À chaque échange $\Delta(B)$ décroît d'un facteur ρ ($\rho^{(j)}$: ρ à l'étape j).

$$\rho \leq \frac{1}{t} = \left(\frac{1}{s^2} + \frac{1}{4}\right)^{1/2} \leq 1$$

Le nombre d'échanges :

$$K(B) = \frac{1}{|\log \bar{\rho}|} \log \frac{\Delta(B)}{\Delta(\widehat{B})}, \qquad \text{avec} \qquad \log \bar{\rho} = \frac{1}{K} \sum_{j=1}^{K} \log \rho^{(j)}$$

Pire des cas (uniquement $t > 1$) :

$$K(B) \leq \frac{1}{\log t} \log \frac{\Delta(B)}{\Delta(\widehat{B})},$$

Remarque :

- Le pire des cas peut être rarement atteint
- L'analyse probabiliste rend mieux compte du comportement "générique"

Potentiel d'une base : $\Delta(B) = \prod_{i=1}^{d} \ell_i^{(d-i)}$.

À chaque échange $\Delta(B)$ décroît d'un facteur ρ ($\rho^{(j)}$: ρ à l'étape j).

$$\rho \leq \frac{1}{t} = \left(\frac{1}{s^2} + \frac{1}{4}\right)^{1/2} \leq 1$$

Le nombre d'échanges :

$$K(B) = \frac{1}{|\log \bar{\rho}|} \log \frac{\Delta(B)}{\Delta(\widehat{B})}, \qquad \text{avec} \qquad \log \bar{\rho} = \frac{1}{K} \sum_{j=1}^{K} \log \rho^{(j)}$$

Pire des cas (uniquement $t > 1$) :

$$K(B) \leq \frac{1}{\log t} \log \frac{\Delta(B)}{\Delta(\widehat{B})},$$

Remarque :

- Le pire des cas peut être rarement atteint
- L'analyse probabiliste rend mieux compte du comportement "générique"

Potentiel d'une base : $\Delta(B) = \prod_{i=1}^{d} \ell_i^{(d-i)}$.

À chaque échange $\Delta(B)$ décroît d'un facteur ρ ($\rho^{(j)}$: ρ à l'étape j).

$$\rho \leq \frac{1}{t} = \left(\frac{1}{s^2} + \frac{1}{4}\right)^{1/2} \leq 1$$

Le nombre d'échanges :

$$K(B) = \frac{1}{|\log \bar{\rho}|} \log \frac{\Delta(B)}{\Delta(\widehat{B})}, \qquad \text{avec} \qquad \log \bar{\rho} = \frac{1}{K} \sum_{j=1}^{K} \log \rho^{(j)}$$

Pire des cas (uniquement $t > 1$) :

$$K(B) \leq \frac{1}{\log t} \log \frac{\Delta(B)}{\Delta(\widehat{B})},$$

Remarque :

- Le pire des cas peut être rarement atteint
- L'analyse probabiliste rend mieux compte du comportement "générique"

Potentiel d'une base : $\Delta(B) = \prod_{i=1}^{d} \ell_i^{(d-i)}$.

À chaque échange $\Delta(B)$ décroît d'un facteur ρ ($\rho^{(j)}$: ρ à l'étape j).

$$\rho \leq \frac{1}{t} = \left(\frac{1}{s^2} + \frac{1}{4}\right)^{1/2} \leq 1$$

Le nombre d'échanges :

$$K(B) = \frac{1}{|\log \bar{\rho}|} \log \frac{\Delta(B)}{\Delta(\widehat{B})}, \qquad \text{avec} \qquad \log \bar{\rho} = \frac{1}{K} \sum_{j=1}^{K} \log \rho^{(j)}$$

Pire des cas (uniquement $t > 1$) :

$$K(B) \leq \frac{1}{\log t} \log \frac{\Delta(B)}{\Delta(\widehat{B})},$$

Remarque :

- Le pire des cas peut être rarement atteint
- L'analyse probabiliste rend mieux compte du comportement "générique"

Plan

Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$

Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

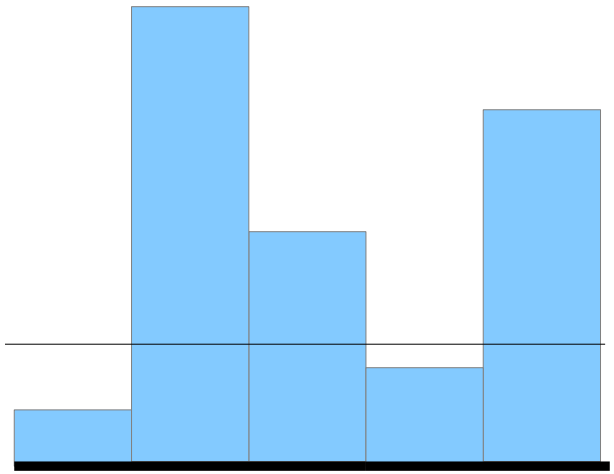
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

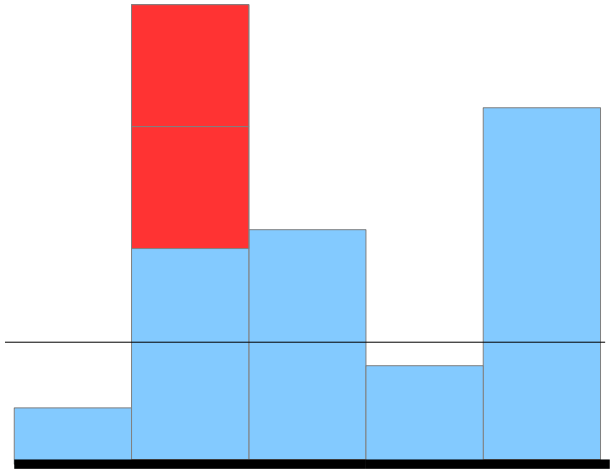
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

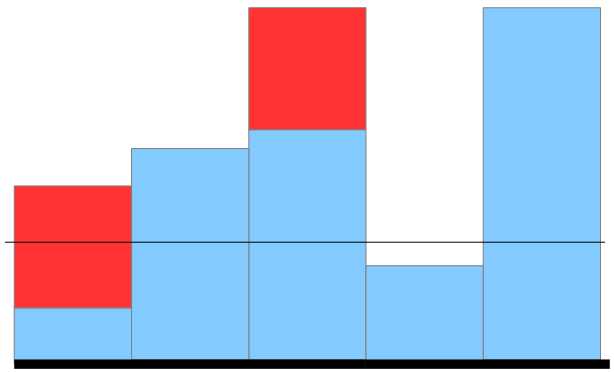
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

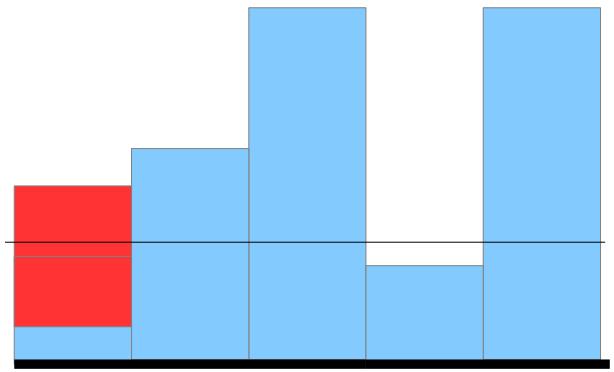
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

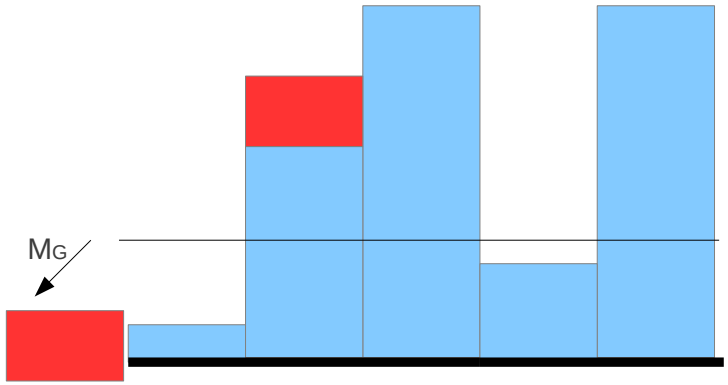
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

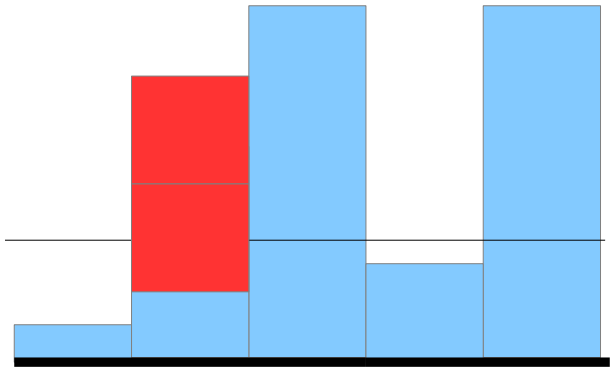
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

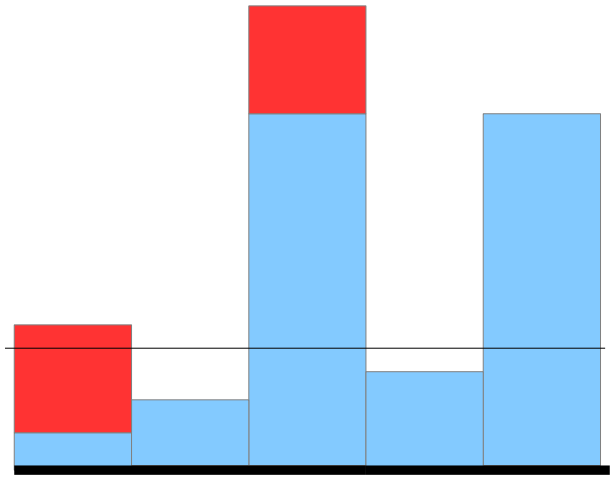
avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho . r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2} . r_i; \\ \check{r}_{i+1} := \rho . r_{i+1}; \end{cases}$$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

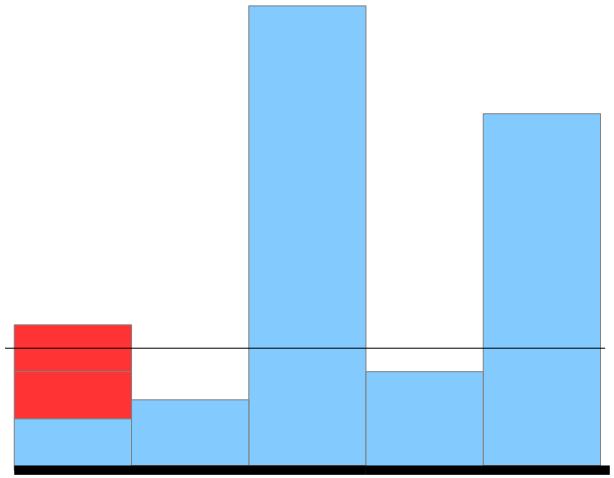
avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

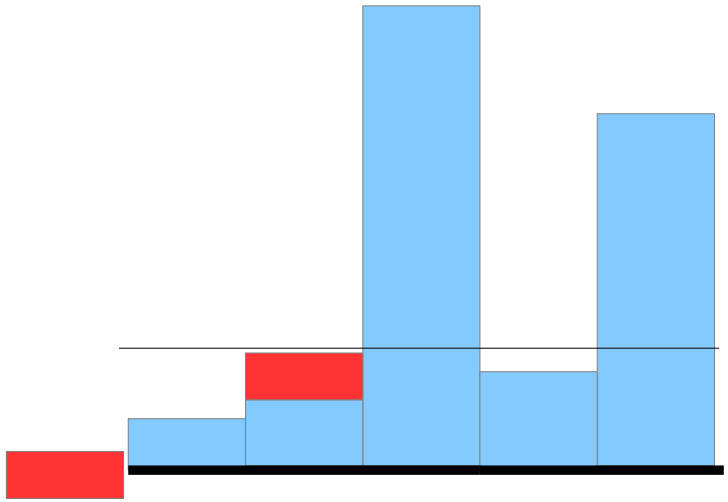
avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho . r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2} . r_i; \\ \check{r}_{i+1} := \rho . r_{i+1}; \end{cases}$$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

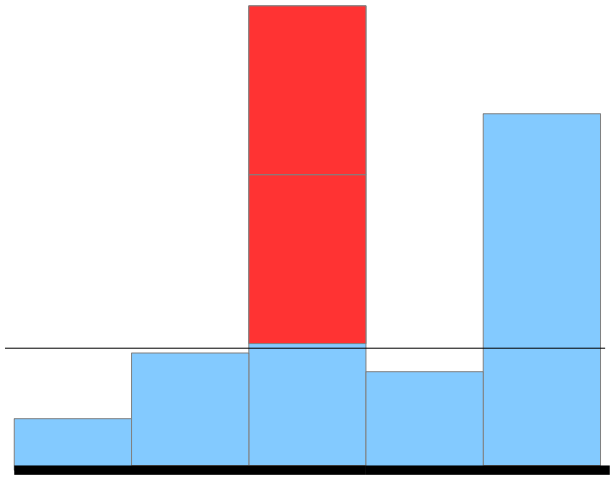
avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Notre approche :

le rôle essentiel est joué par les rapports

$$r_i = \frac{\ell_{i+1}}{\ell_i}$$

les coefficients ν_i ont un rôle secondaire

si $r_i < 1/s$ alors

$$\widetilde{T}_\rho^{(i)}(\mathbf{r}) = \begin{cases} \check{r}_{i-1} := \rho.r_{i-1}; \\ \check{r}_i := \dfrac{1}{\rho^2}.r_i; \\ \check{r}_{i+1} := \rho.r_{i+1}; \end{cases}$$

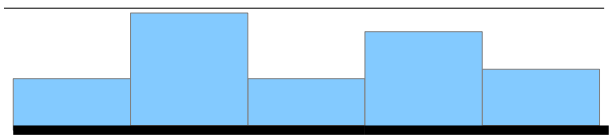
Point de vue additif :

$$\mathbf{c} := (c_1, \ldots, c_{d-1})$$

avec $c_i = -\log_s r_i$ et $\alpha = -\log_s \rho$

si $c_i > 1$ alors

$$T_\alpha^{(i)}(\mathbf{c}) = \begin{cases} \check{c}_{i-1} := c_{i-1} + \alpha \\ \check{c}_i := c_i - 2\alpha \\ \check{c}_{i+1} := c_{i+1} + \alpha \end{cases}$$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

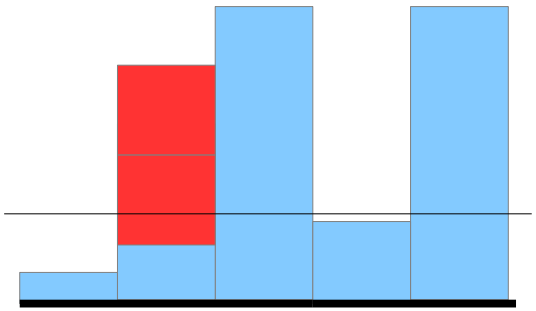
M1 : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

M2 : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

M3 : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

M4 : LLL avec la condition de Siegel ($c_i \leq 1$)

M5 : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

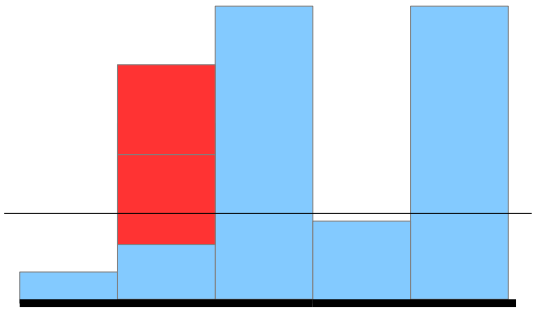
`M1` : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

`M2` : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

`M3` : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

`M4` : LLL avec la condition de Siegel ($c_i \leq 1$)

`M5` : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

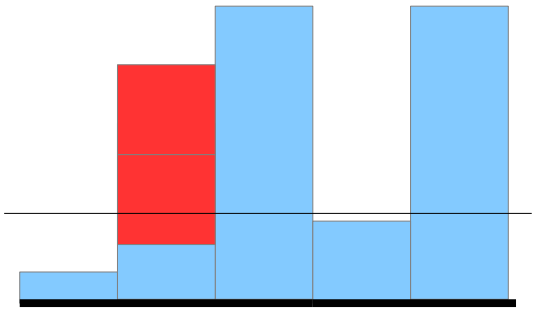
M1 : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

M2 : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

M3 : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

M4 : LLL avec la condition de Siegel ($c_i \leq 1$)

M5 : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

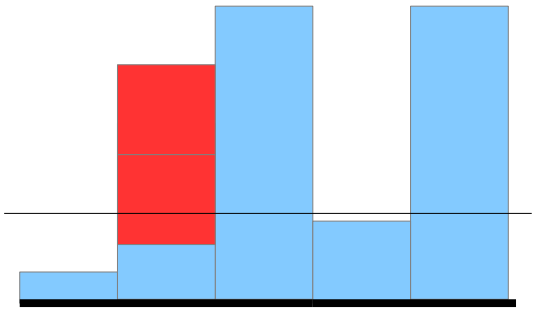
`M1` : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

`M2` : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

`M3` : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

`M4` : LLL avec la condition de Siegel ($c_i \leq 1$)

`M5` : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

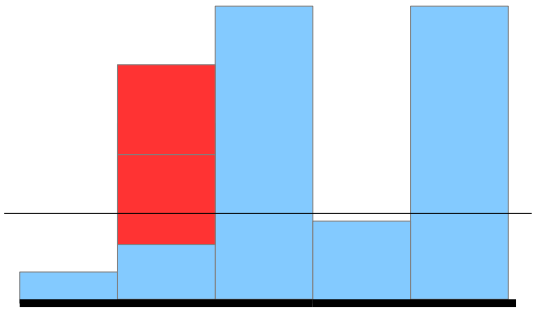
`M1` : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

`M2` : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

`M3` : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

`M4` : LLL avec la condition de Siegel ($c_i \leq 1$)

`M5` : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Entrées: $\mathbf{c} \in \mathcal{J}$
Sorties: $\mathbf{c} \in \mathcal{O} = \prod \mathcal{O}_i$

tant que $\mathbf{c} \notin \mathcal{O}$ **faire**
  `Choisir` i `tel que` $c_i \notin \mathcal{O}_i$;
  `Choisir` $\alpha \in \mathbb{R}^+$;
  $\mathbf{c} \leftarrow T_\alpha^{(i)}(\mathbf{c})$;
fin
Renvoyer $\mathbf{c}$

Deux principaux choix :

`Choisir` i : la stratégie
classique, gloutonne, aléatoire...

`Choisir` α : calculé, fixé...

$$\alpha_i = -\frac{1}{2}\log_s(s^{-2c_i} + \nu_i^2)$$

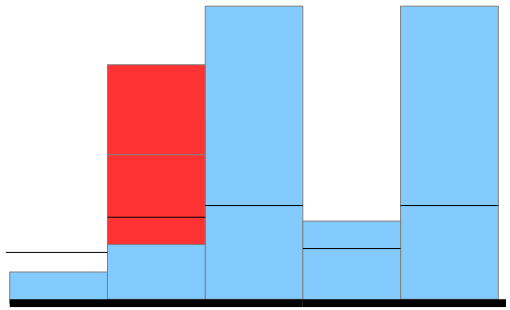
`M1` : $\alpha_i = \alpha$ est fixé au cours de l'algorithme

`M2` : α_i est fonction de c_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

`M3` : α_i est fonction de c_i, $\nu_i \in_{\mathcal{R}} [-\frac{1}{2}, \frac{1}{2}]$

`M4` : LLL avec la condition de Siegel ($c_i \leq 1$)

`M5` : vrai LLL avec la condition de Lovász
$c_i \leq \frac{1}{2}\log_s\left(\frac{1}{t^2} + \nu_i^2\right)$



Approche générale

$$\mathcal{B} = \begin{pmatrix} \ell_1 & 0 & \cdots & 0 \\ * & \ell_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \cdots & * & \ell_d \end{pmatrix}.$$

La longueur des orthogonalisés se lit sur la diagonale

Trois paramètres : (Υ, d, g)

- d : dimension du réseau
- densité g strictement positive définie sur $[0,1]$ qui vérifie donc $\int_0^1 g(t)dt = 1$
- Υ : masse moyenne totale du cfg

$$\mathbb{E}[c_i] = \frac{1}{d-1}\,\Upsilon\, g\left(\frac{i}{d}\right) \quad \text{et} \quad \mathbb{E}[\mathcal{M}] \approx \Upsilon$$

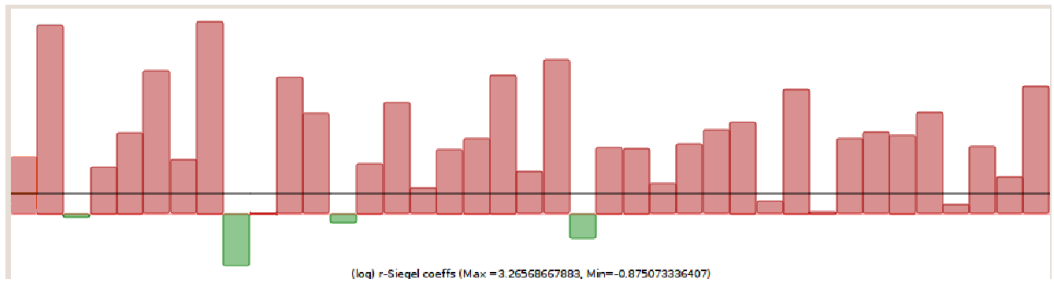
L'énergie moyenne vérifie

$$\mathbb{E}[\mathcal{E}] \sim d^2 \mathbb{E}[\mathcal{M}] \int_0^1 x(1-x)g(x)dx.$$

Les entrées "grand tas" (Ajtai)

Applications

- Preuve de la connection entre le pire des cas/le cas moyen (Ajtai '96)
- Les bases d'Ajtai modélisent des instances difficiles en moyenne, vis–à-vis du problème SVP



$\mathcal{A}(\Upsilon, d, g)$: des *cfg* défini par une densité g strictement positive définie sur $[0,1]$ et de classe $\mathcal{C}^1$ qui vérifie donc $\int_0^1 g(t)dt = 1$.

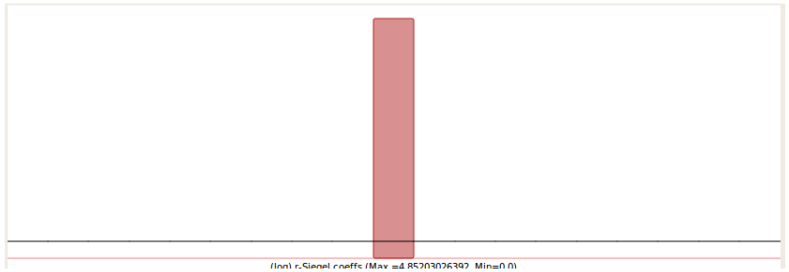
$$\mathbb{E}[c_i] = \frac{1}{d-1}\,\Upsilon\, g\left(\frac{i}{d}\right) \quad \text{et} \quad \mathbb{E}[\mathcal{M}] \approx \Upsilon$$

Réseaux uni-tas

Applications

- Cryptanalyse des protocoles de type sac à dos
- Factorisation des entiers par la méthode de Schnorr
- Cryptosystème NTRU

$$\mathcal{B} = \left(\begin{array}{c|c} X \cdot I_i & 0 \\ \hline A & Y \cdot I_{d-i} \end{array} \right).$$



(i) $d \in \mathbb{N}$,un réel $\beta \in [0,1]$ et l'entier $i \in [1\,..\,d-1]$ est défini par $i := [\beta d]$,

(iii) X et Y str. positives, avec $X \gg Y$,

$$\mathcal{U}(\Upsilon, d, \beta)$$

$$\mathbb{E}[c_i] = \Upsilon \quad \text{et} \quad \mathbb{E}[c_j] = 0 \quad j \neq i$$

L'énergie vérifie, pour $d \to \infty$,

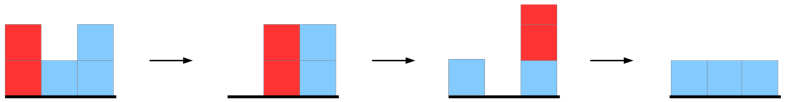
$$\mathbb{E}[\mathcal{E}] = \sum_{i=1}^{d-1} i(d-i)\mathbb{E}[c_i] \sim \begin{cases} d^2\beta(1-\beta)\,\Upsilon & \text{si } \beta \in]0,1[\\ d\,\Upsilon & \text{si } \beta \in \{0,1\} \end{cases}.$$

Plan

Chip Firing Game (M1) : α fixé

Chip Firing Game : le modèle $\mathcal{C}_d(\mathbf{c}, H, \alpha)$

si $c_i > H$ alors $\check{c}_{i-1} := c_{i-1} + \alpha \quad \check{c}_i := c_i - 2\alpha \quad \check{c}_{i+1} := c_{i+1} + \alpha$



$K(\mathbf{c} \mapsto \widehat{\mathbf{c}})$ est indépendante du chemin

Énergie d'un *cfg* : $\mathcal{E}(\mathbf{c}) := \sum_{i=1}^{d-1} i(d-i)c_i$

$$\mathcal{E}(\check{\mathbf{c}}) = \mathcal{E}(\mathbf{c}) - 2\alpha$$

$$K(\mathbf{c}) = \frac{1}{2\alpha}\left[\mathcal{E}(\mathbf{c}) - \mathcal{E}(\widehat{\mathbf{c}})\right] = \frac{1}{2\alpha}\sum_{i=1}^{d-1} i(d-i)(c_i - \widehat{c}_i).$$

La configuration finale est unique et ne dépend pas de la stratégie.

Déterminer

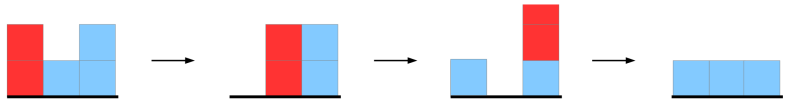
- le nombre d'itérations
- la configuration finale et son énergie

deux problèmes très liés

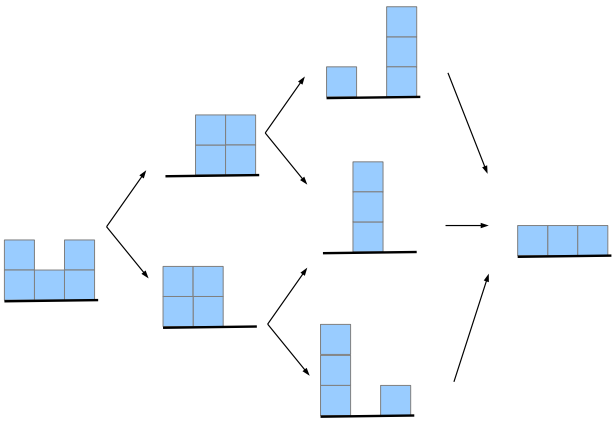
Chip Firing Game (M1) : α fixé

Chip Firing Game : le modèle $\mathcal{C}_d(\mathbf{c}, H, \alpha)$

si $c_i > H$ alors $\check{c}_{i-1} := c_{i-1} + \alpha \quad \check{c}_i := c_i - 2\alpha \quad \check{c}_{i+1} := c_{i+1} + \alpha$



La configuration finale est unique et ne dépend pas de la stratégie.



$K(\mathbf{c} \mapsto \widehat{\mathbf{c}})$ est indépendante du chemin

Énergie d'un *cfg* : $\mathcal{E}(\mathbf{c}) := \sum_{i=1}^{d-1} i(d-i)c_i$

$$\mathcal{E}(\check{\mathbf{c}}) = \mathcal{E}(\mathbf{c}) - 2\alpha$$

$$K(\mathbf{c}) = \frac{1}{2\alpha}\left[\mathcal{E}(\mathbf{c}) - \mathcal{E}(\widehat{\mathbf{c}})\right] = \frac{1}{2\alpha}\sum_{i=1}^{d-1} i(d-i)(c_i - \widehat{c}_i).$$

Déterminer

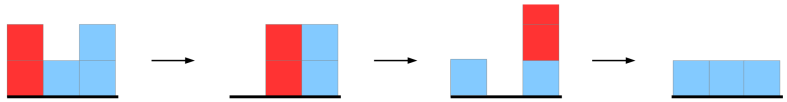
- le nombre d'itérations
- la configuration finale et son énergie

deux problèmes très liés

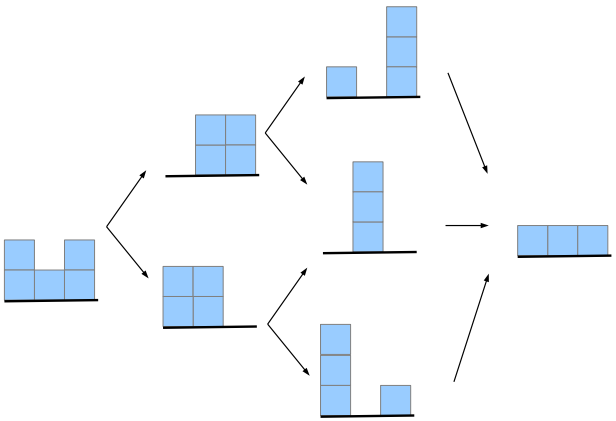
Chip Firing Game (M1) : α fixé

Chip Firing Game : le modèle $\mathcal{C}_d(\mathbf{c}, H, \alpha)$

si $c_i > H$ alors $\check{c}_{i-1} := c_{i-1} + \alpha \quad \check{c}_i := c_i - 2\alpha \quad \check{c}_{i+1} := c_{i+1} + \alpha$



La configuration finale est unique et ne dépend pas de la stratégie.



$K(\mathbf{c} \mapsto \widehat{\mathbf{c}})$ est indépendante du chemin

Énergie d'un *cfg* : $\mathcal{E}(\mathbf{c}) := \sum_{i=1}^{d-1} i(d-i)c_i$

$$\mathcal{E}(\check{\mathbf{c}}) = \mathcal{E}(\mathbf{c}) - 2\alpha$$

$$K(\mathbf{c}) = \frac{1}{2\alpha}\left[\mathcal{E}(\mathbf{c}) - \mathcal{E}(\widehat{\mathbf{c}})\right] = \frac{1}{2\alpha}\sum_{i=1}^{d-1} i(d-i)(c_i - \widehat{c}_i).$$

Déterminer

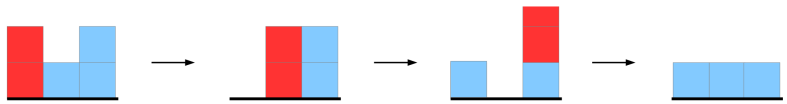
- le nombre d'itérations
- la configuration finale et son énergie

deux problèmes très liés

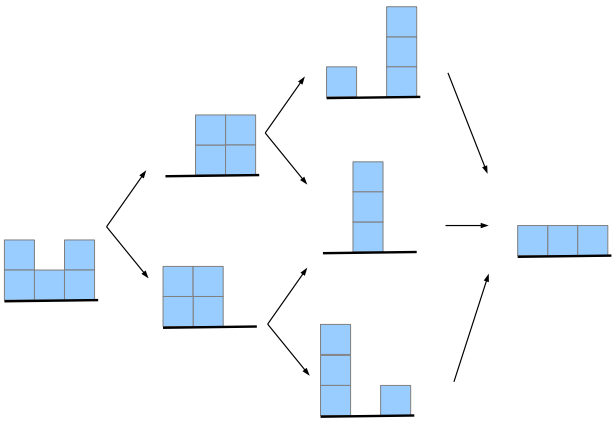
Chip Firing Game (M1) : α fixé

Chip Firing Game : le modèle $\mathcal{C}_d(\mathbf{c}, H, \alpha)$

si $c_i > H$ alors $\check{c}_{i-1} := c_{i-1} + \alpha \quad \check{c}_i := c_i - 2\alpha \quad \check{c}_{i+1} := c_{i+1} + \alpha$



La configuration finale est unique et ne dépend pas de la stratégie.



$K(\mathbf{c} \mapsto \widehat{\mathbf{c}})$ est indépendante du chemin

Énergie d'un *cfg* : $\mathcal{E}(\mathbf{c}) := \sum_{i=1}^{d-1} i(d-i)c_i$

$$\mathcal{E}(\check{\mathbf{c}}) = \mathcal{E}(\mathbf{c}) - 2\alpha$$

$$K(\mathbf{c}) = \frac{1}{2\alpha}\left[\mathcal{E}(\mathbf{c}) - \mathcal{E}(\widehat{\mathbf{c}})\right] = \frac{1}{2\alpha}\sum_{i=1}^{d-1} i(d-i)(c_i - \widehat{c}_i).$$

Déterminer

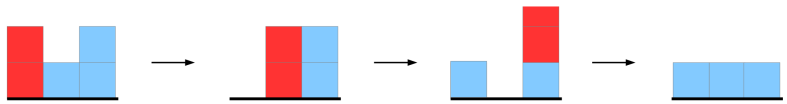
- le nombre d'itérations
- la configuration finale et son énergie

deux problèmes très liés

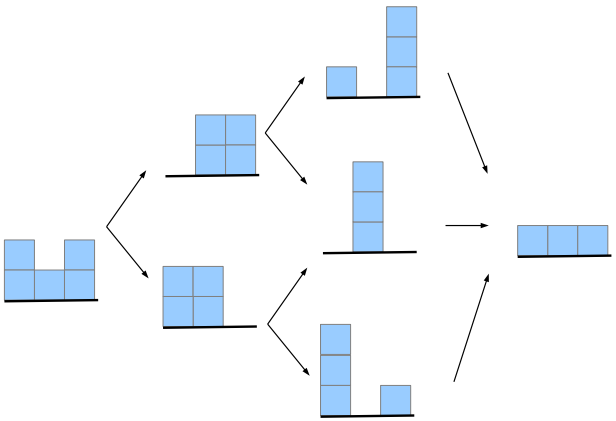
Chip Firing Game (M1) : α fixé

Chip Firing Game : le modèle $\mathcal{C}_d(\mathbf{c}, H, \alpha)$

si $c_i > H$ alors $\check{c}_{i-1} := c_{i-1} + \alpha \quad \check{c}_i := c_i - 2\alpha \quad \check{c}_{i+1} := c_{i+1} + \alpha$



La configuration finale est unique et ne dépend pas de la stratégie.



$K(\mathbf{c} \mapsto \widehat{\mathbf{c}})$ est indépendante du chemin

Énergie d'un *cfg* : $\mathcal{E}(\mathbf{c}) := \sum_{i=1}^{d-1} i(d-i)c_i$

$$\mathcal{E}(\check{\mathbf{c}}) = \mathcal{E}(\mathbf{c}) - 2\alpha$$

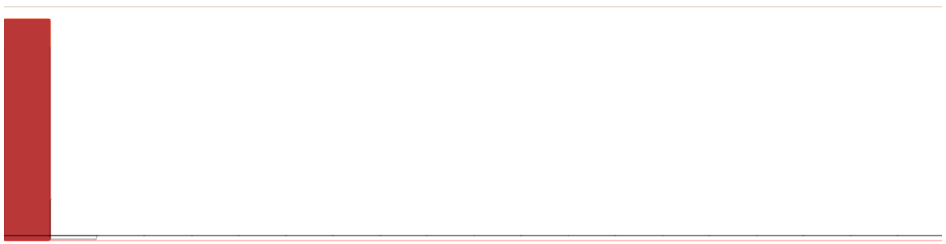
$$K(\mathbf{c}) = \frac{1}{2\alpha}\left[\mathcal{E}(\mathbf{c}) - \mathcal{E}(\widehat{\mathbf{c}})\right] = \frac{1}{2\alpha}\sum_{i=1}^{d-1} i(d-i)(c_i - \widehat{c}_i).$$

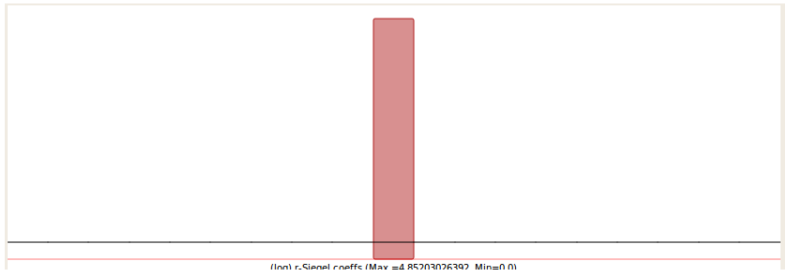
Déterminer

- le nombre d'itérations
- la configuration finale et son énergie

deux problèmes très liés

Réseaux uni-tas





Pour un cfg $\mathcal{C}_d(\mathbf{c}, h, H)$ avec une seule pile en position i de hauteur $\Upsilon = \Theta(d^a)$.

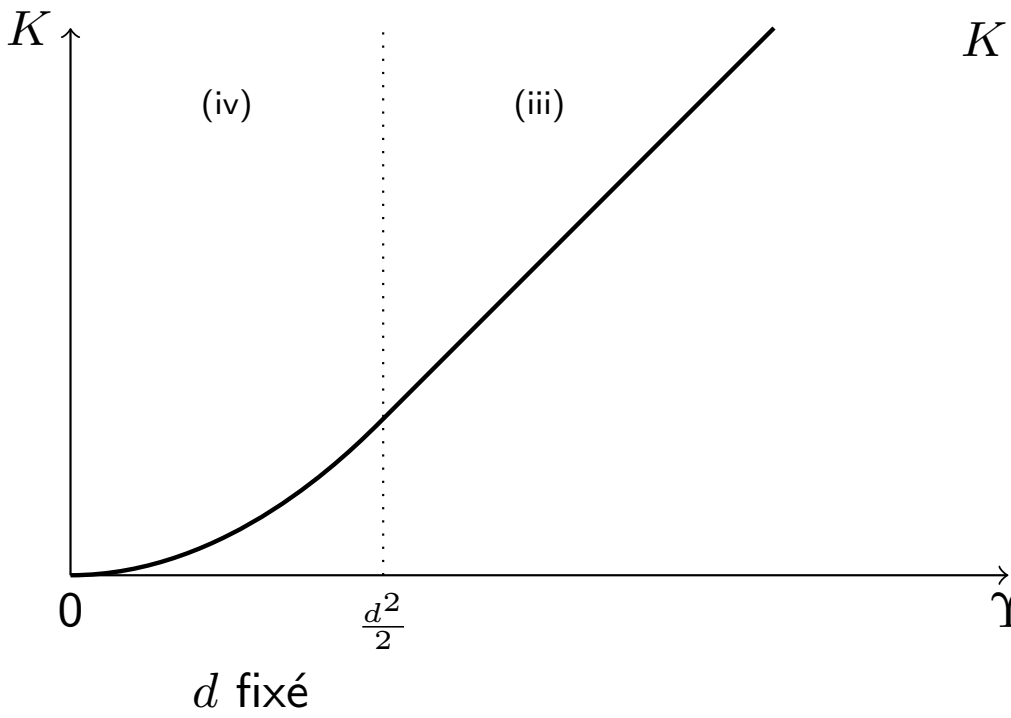
Si la pile n'est pas sur les bords, i.e., $i = \beta d$ avec $\beta \in]0, 1[$

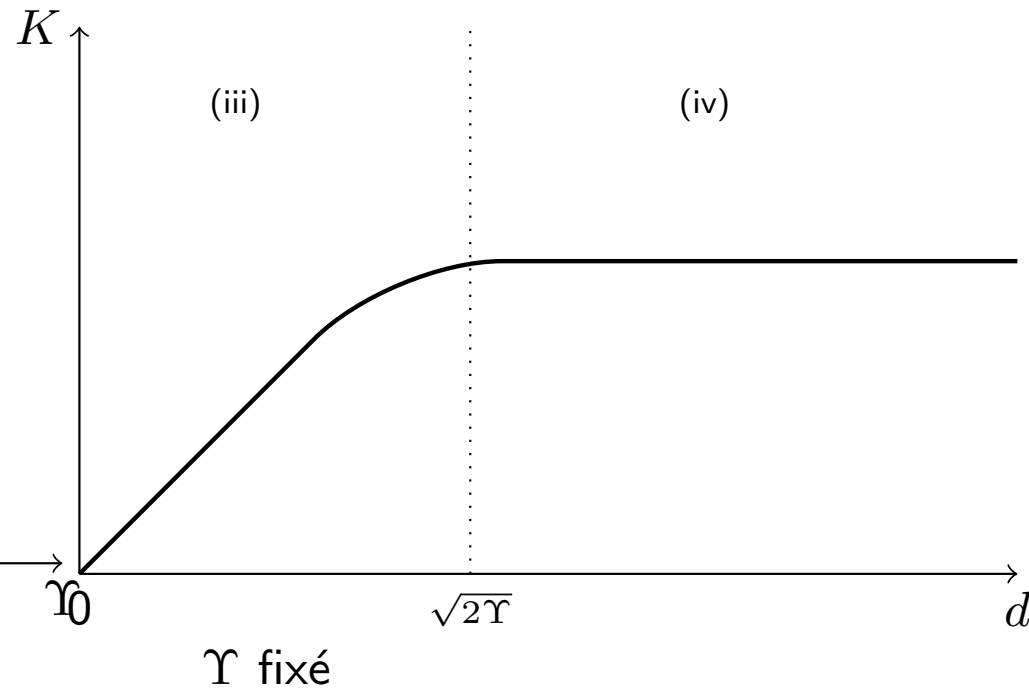
- Si $0 < a \leq 1$ (ne s'étale pas jusqu'au bord), alors $K = O(d^3)$
- Si $a > 1$ (s'étale jusqu'au bord), alors $K = \Theta(d^{2+a})$

Si la pile est sur les bords, en position $i \in \{1, d-1\}$:

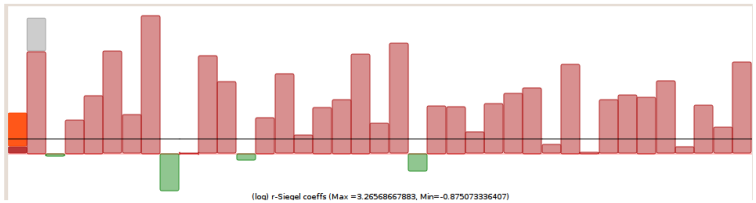
- Si $a \leq 2$ (ne s'étale pas jusqu'à l'autre bord), alors on a $K = O(d^3)$
- Si $a > 2$ (s'étale complètement), alors on a $K = \Theta(d^{a+1})$

"uni-tas" au début





Entrées "grand-tas" et cfg



Nombre d'itérations : dans le modèle $\mathcal{A}(\Upsilon, d, g)$, la masse moyenne Υ est une fonction au moins linéaire de d, et l'énergie initiale $\mathcal{E} = \mathcal{E}(\mathbf{c})$ moyenne vérifie

$$\mathbb{E}[\mathcal{E}] \sim d^2\, \Upsilon\, I(g), \qquad \text{avec} \quad I(g) = \int_0^1 x(1-x)g(x)dx.$$

Il y a deux cas principaux :

Cas où la masse moyenne Υ vérifie $\Upsilon = \Theta(d^a)$ avec $a > 1$.

$$\mathbb{E}[K] = \Theta(d^{a+2})$$

Cas où la masse moyenne Υ est linéaire en d et asymptotique à $C \cdot d$, avec $C > 1$.

$$\mathbb{E}[K] = \Theta(d^3)$$

$$\widetilde{\Upsilon} = \log \prod r_i = \frac{1}{\log s}\Upsilon \qquad s = \text{paramètre condition de Siegel}$$

Modèles	K **pire des cas**	K **pour** $\mathtt{M1}(\alpha)$	K **pour** $\mathtt{M2}(\mu)$	K **exp.**
$\mathcal{A}(\widetilde{\Upsilon}, d)$	$\frac{1}{12\log t} d(d+1)\widetilde{\Upsilon}$	$\frac{1}{12\alpha} d(d+1)\widetilde{\Upsilon}$		$\Theta(d^2\widetilde{\Upsilon})$
$\mathcal{N}(\widetilde{\Upsilon}, d)$	$\frac{1}{8\log t} d^2\widetilde{\Upsilon}$	$\frac{1}{8\alpha}\ d^2\widetilde{\Upsilon}$		$\Theta(d^2\widetilde{\Upsilon})$
$\mathcal{K}(\widetilde{\Upsilon}, d)$	$\frac{1}{2\log t} d\widetilde{\Upsilon}$	$\frac{1}{2\alpha} d\widetilde{\Upsilon}$		$\Theta(d\widetilde{\Upsilon})$

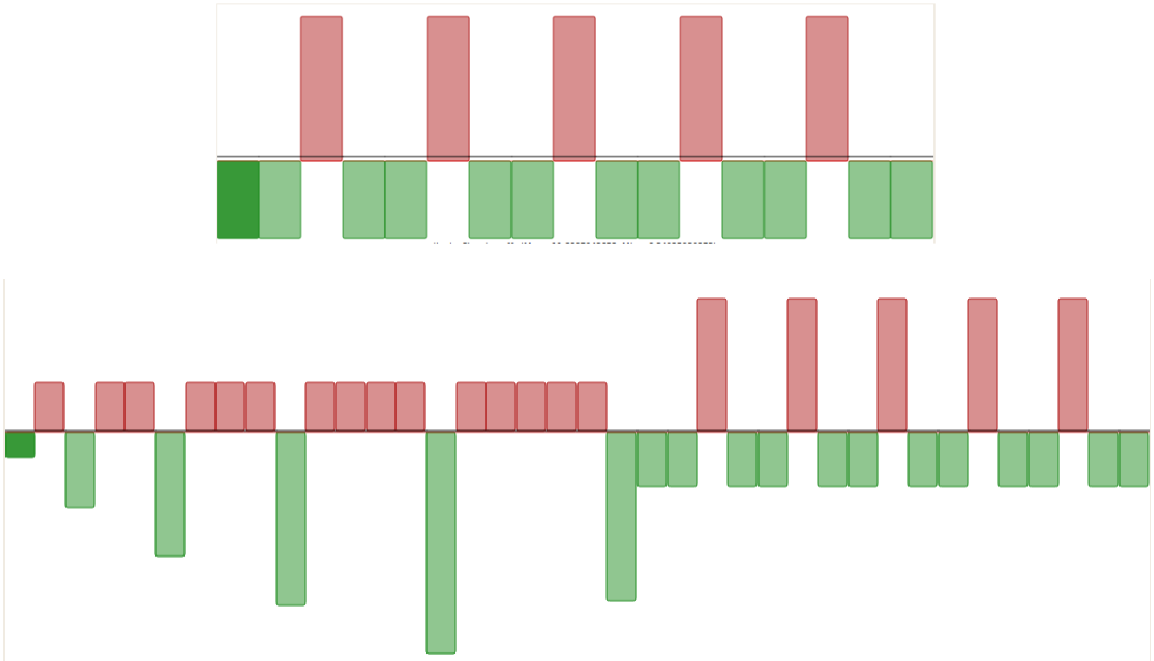
TABLE: La réduction est supposée difficile : $\widetilde{\Upsilon}/d^a \to \infty$ avec $a = 1$ pour les modèles $\mathcal{A}, \mathcal{N}$ et $a = 2$ pour le modèle $\mathcal{K}$.

$\mathcal{A}$=Ajtaï (grands-tas), $\mathcal{N}$=NTRU (uni-tas au milieu),
$\mathcal{K}$=Sac-à-dos (uni-tas au début)

CFG à trous : réseaux de Coppersmith

Interviennent dans la méthode de Coppersmith

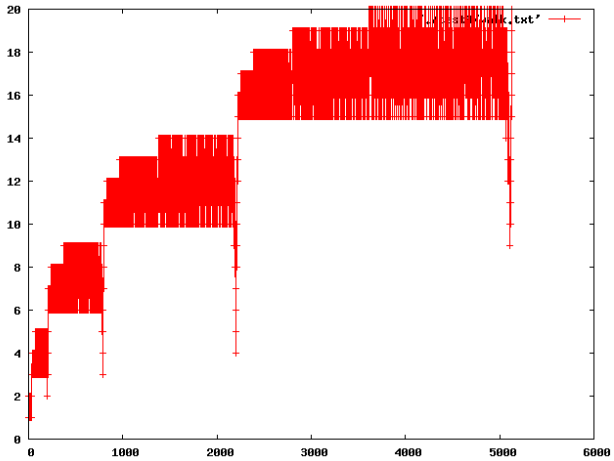
- qui permet de calculer les petites racines de polynômes multivariés modulo un entier
- utiliser dans les attaques de RSA

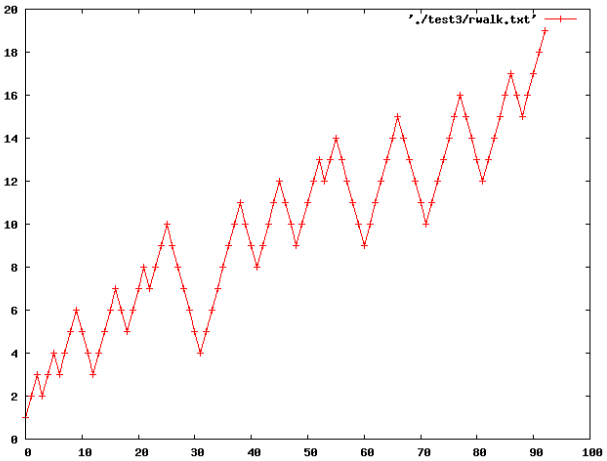


partie 1 partie 2

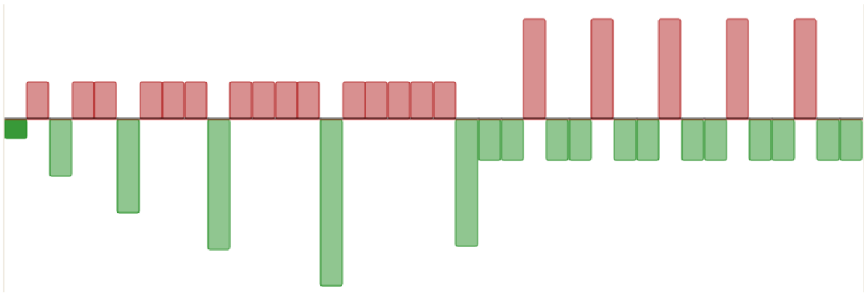
Les entrées "à trous"

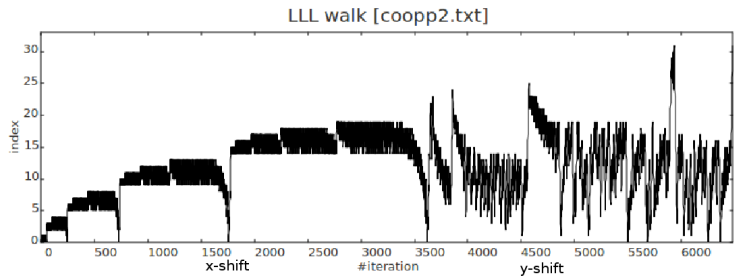
Marche aléatoire de l'indice sur le réseau de Coppersmith





Une grande partie de la réduction peut être effectuée indépendamment sur les blocs





CFG à trous : indépendance

$\mathbf{c}_g$ et $\mathbf{c}_d$: deux *cfg* avec des piles strictement positives à gauche et à droite, avec des configurations finales $\widehat{\mathbf{c}}_g$ et $\widehat{\mathbf{c}}_d$

$\mathbf{c}_m$: un cfg avec des piles négatives ou nulles au milieu

Indépendance

Les $\mathbf{c}_g$ et $\mathbf{c}_d$ sont indépendants dans le cfg composé des trois blocs s'il existe une configuration $\widehat{\mathbf{c}}_m$ réduite telle que la configuration finale du *cfg* total est $\widehat{\mathbf{c}}_g \cdot \widehat{\mathbf{c}}_m \cdot \widehat{\mathbf{c}}_d$

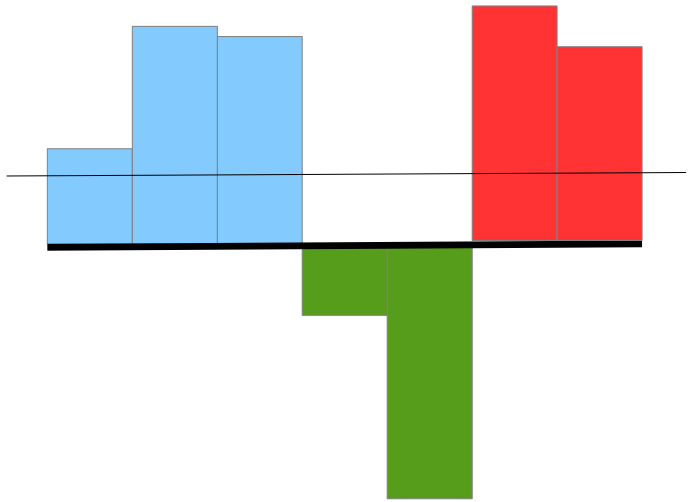
Des conditions suffisantes pour l'indépendance et la dépendance :

pour l'indépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} \leq \mathcal{M}$$

pour la dépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} > \mathcal{M}$$



CFG à trous : indépendance

$\mathbf{c}_g$ et $\mathbf{c}_d$: deux *cfg* avec des piles strictement positives à gauche et à droite, avec des configurations finales $\widehat{\mathbf{c}}_g$ et $\widehat{\mathbf{c}}_d$

$\mathbf{c}_m$: un cfg avec des piles négatives ou nulles au milieu

Indépendance

Les $\mathbf{c}_g$ et $\mathbf{c}_d$ sont indépendants dans le cfg composé des trois blocs s'il existe une configuration $\widehat{\mathbf{c}}_m$ réduite telle que la configuration finale du *cfg* total est $\widehat{\mathbf{c}}_g \cdot \widehat{\mathbf{c}}_m \cdot \widehat{\mathbf{c}}_d$

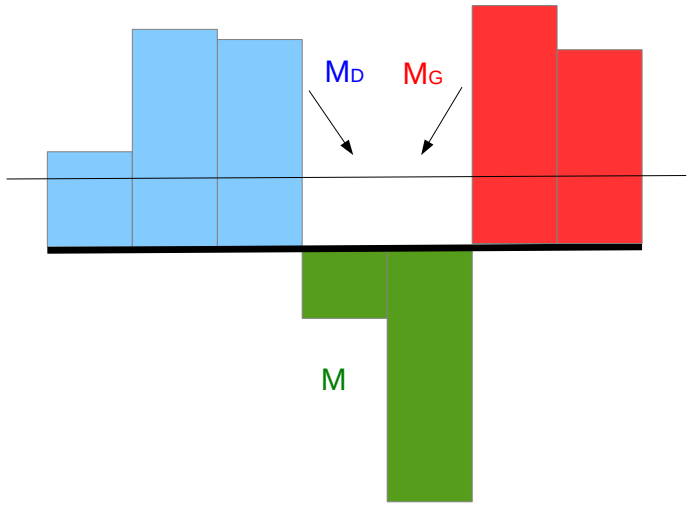
Des conditions suffisantes pour l'indépendance et la dépendance :

pour l'indépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} \leq \mathcal{M}$$

pour la dépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} > \mathcal{M}$$



CFG à trous : indépendance

$\mathbf{c}_g$ et $\mathbf{c}_d$: deux *cfg* avec des piles strictement positives à gauche et à droite, avec des configurations finales $\widehat{\mathbf{c}}_g$ et $\widehat{\mathbf{c}}_d$

$\mathbf{c}_m$: un cfg avec des piles négatives ou nulles au milieu

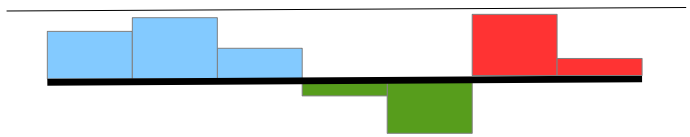
Indépendance

Les $\mathbf{c}_g$ et $\mathbf{c}_d$ sont indépendants dans le cfg composé des trois blocs s'il existe une configuration $\widehat{\mathbf{c}}_m$ réduite telle que la configuration finale du *cfg* total est $\widehat{\mathbf{c}}_g \cdot \widehat{\mathbf{c}}_m \cdot \widehat{\mathbf{c}}_d$

Des conditions suffisantes pour l'indépendance et la dépendance :

pour l'indépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} \leq \mathcal{M}$$



pour la dépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} > \mathcal{M}$$

CFG à trous : indépendance

$\mathbf{c}_g$ et $\mathbf{c}_d$: deux *cfg* avec des piles strictement positives à gauche et à droite, avec des configurations finales $\widehat{\mathbf{c}}_g$ et $\widehat{\mathbf{c}}_d$

$\mathbf{c}_m$: un cfg avec des piles négatives ou nulles au milieu

Indépendance

Les $\mathbf{c}_g$ et $\mathbf{c}_d$ sont indépendants dans le cfg composé des trois blocs s'il existe une configuration $\widehat{\mathbf{c}}_m$ réduite telle que la configuration finale du *cfg* total est $\widehat{\mathbf{c}}_g \cdot \widehat{\mathbf{c}}_m \cdot \widehat{\mathbf{c}}_d$

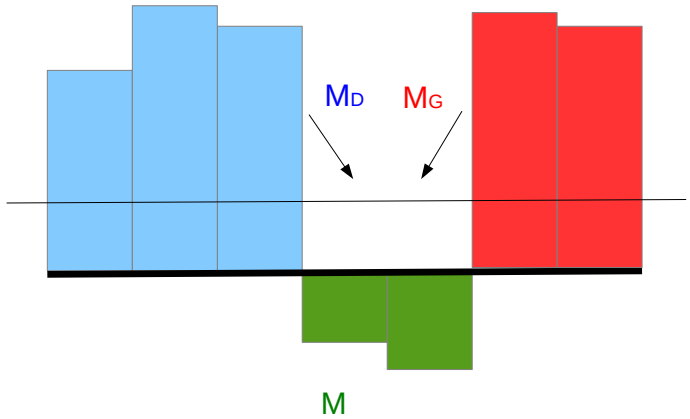
Des conditions suffisantes pour l'indépendance et la dépendance :

pour l'indépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} \leq \mathcal{M}$$

pour la dépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} > \mathcal{M}$$



CFG à trous : indépendance

$\mathbf{c}_g$ et $\mathbf{c}_d$: deux *cfg* avec des piles strictement positives à gauche et à droite, avec des configurations finales $\widehat{\mathbf{c}}_g$ et $\widehat{\mathbf{c}}_d$

$\mathbf{c}_m$: un cfg avec des piles négatives ou nulles au milieu

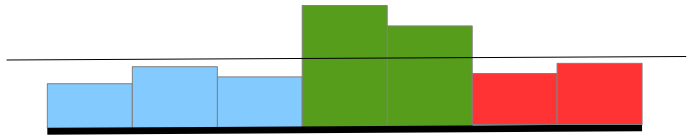
Indépendance

Les $\mathbf{c}_g$ et $\mathbf{c}_d$ sont indépendants dans le cfg composé des trois blocs s'il existe une configuration $\widehat{\mathbf{c}}_m$ réduite telle que la configuration finale du *cfg* total est $\widehat{\mathbf{c}}_g \cdot \widehat{\mathbf{c}}_m \cdot \widehat{\mathbf{c}}_d$

Des conditions suffisantes pour l'indépendance et la dépendance :

pour l'indépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} \leq \mathcal{M}$$

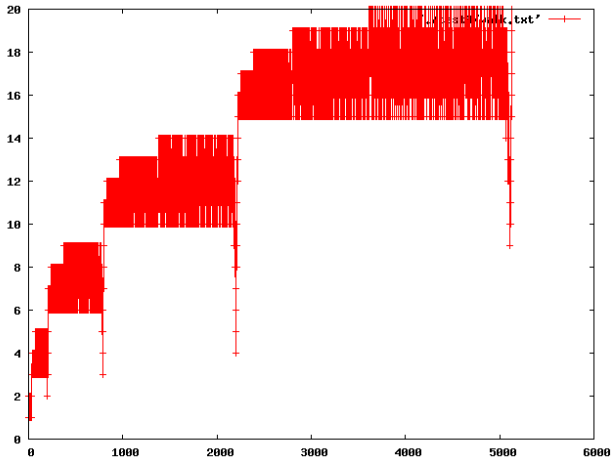


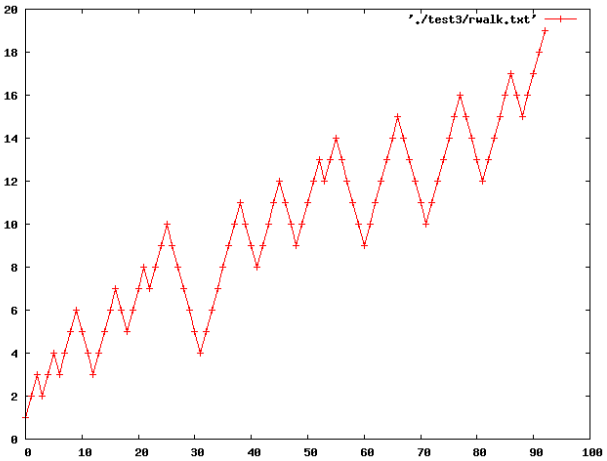
pour la dépendance :

$$\mathcal{M}_{\mathcal{D}} + \mathcal{M}_{\mathcal{G}} > \mathcal{M}$$

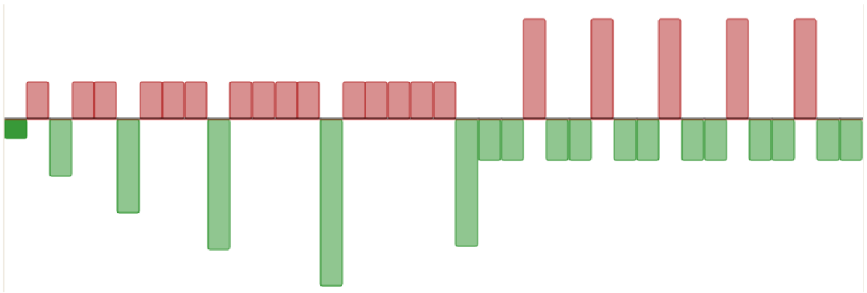
Les entrées "à trous"

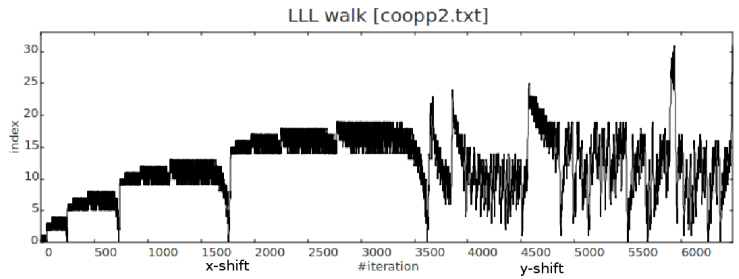
Marche aléatoire de l'indice sur le réseau de Coppersmith





Une grande partie de la réduction peut être effectuée indépendamment sur les blocs





Modèle M2 : systèmes dynamiques de $\mathbb{R}^{d-1}$

ρ est fonction de r_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu := \nu_i^2 \leftarrow \text{constant}$$

Le facteur de décroissance : $\rho = x_i + \mu$

M2$(t,\ \mu)$

Si $\quad r_i^2 < \dfrac{1}{t^2} - \mu$

$$\check{r}_{i-1} = \rho r_{i-1}$$
$$\check{r}_i = \frac{1}{\rho^2} r_i$$
$$\check{r}_{i+1} = \rho r_{i+1}.$$

Si $\quad x_i < \dfrac{1}{t^2} - \mu$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu)$$
$$\check{x}_i = \frac{x_i}{(x_i + \mu)^2}$$
$$\check{x}_{i+1} = x_{i+1}(x_i + \mu)$$

M2$(t,\ \mu)$ modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)

Le trou du système M2$(t,\ \mu)$ (condition d'arrêt) est $(x_1, \ldots, x_{d-1}) \in \left[\frac{1}{t^2} - \mu, +\infty\right[^{d-1}$.

Modèle M2 : systèmes dynamiques de $\mathbb{R}^{d-1}$

ρ est fonction de r_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu := \nu_i^2 \leftarrow \text{constant}$$

Le facteur de décroissance : $\rho = x_i + \mu$

M2(t, μ)

Si $r_i^2 < \frac{1}{t^2} - \mu$

$$\check{r}_{i-1} = \rho r_{i-1}$$
$$\check{r}_i = \frac{1}{\rho^2} r_i$$
$$\check{r}_{i+1} = \rho r_{i+1}.$$

Si $x_i < \frac{1}{t^2} - \mu$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu)$$
$$\check{x}_i = \frac{x_i}{(x_i + \mu)^2}$$
$$\check{x}_{i+1} = x_{i+1}(x_i + \mu)$$

M2(t, μ) modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)

Le trou du système M2(t, μ) (condition d'arrêt) est $(x_1, \ldots, x_{d-1}) \in \left[\frac{1}{t^2} - \mu, +\infty\right[^{d-1}$.

Modèle M2 : systèmes dynamiques de $\mathbb{R}^{d-1}$

ρ est fonction de r_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu := \nu_i^2 \leftarrow \text{constant}$$

Le facteur de décroissance : $\rho = x_i + \mu$ M2(t, μ)

Si $r_i^2 < \frac{1}{t^2} - \mu$

$$\check{r}_{i-1} = \rho r_{i-1}$$

$$\check{r}_i = \frac{1}{\rho^2} r_i$$

$$\check{r}_{i+1} = \rho r_{i+1}.$$

Si $x_i < \frac{1}{t^2} - \mu$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu)$$

$$\check{x}_i = \frac{x_i}{(x_i + \mu)^2}$$

$$\check{x}_{i+1} = x_{i+1}(x_i + \mu)$$

M2(t, μ) modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)

Le trou du système M2(t, μ) (condition d'arrêt) est $(x_1, \ldots, x_{d-1}) \in \left[\frac{1}{t^2} - \mu, +\infty\right[^{d-1}$.

Modèle M2 : systèmes dynamiques de $\mathbb{R}^{d-1}$

ρ est fonction de r_i, ν_i fixé dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu := \nu_i^2 \leftarrow \text{constant}$$

Le facteur de décroissance : $\rho = x_i + \mu$ M2(t, μ)

Si $r_i^2 < \frac{1}{t^2} - \mu$

$$\check{r}_{i-1} = \rho r_{i-1}$$
$$\check{r}_i = \frac{1}{\rho^2} r_i$$
$$\check{r}_{i+1} = \rho r_{i+1}.$$

Si $x_i < \frac{1}{t^2} - \mu$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu)$$
$$\check{x}_i = \frac{x_i}{(x_i + \mu)^2}$$
$$\check{x}_{i+1} = x_{i+1}(x_i + \mu)$$

M2(t, μ) modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)

Le trou du système M2(t, μ) (condition d'arrêt) est $(x_1, \ldots, x_{d-1}) \in \left[\frac{1}{t^2} - \mu, +\infty\right[^{d-1}$.

Étude du modèle M2

M2 n'est plus un tas de sable : c'est un système dynamique général, "à trou"

Nous analysons ce modèle avec $\mu \leq 1/4$:

- en dimension 2 : pour $t \geq 1$
  - des résultats similaires à ceux connus sur l'algorithme de Gauss
  - une distribution géométrique pour le nombre d'itérations
- en dimension 3 : (le premier cas où l'algorithme LLL(t) n'est pas bien connu)
  - pour $t \geq 1$: le nombre d'étapes suit toujours une loi géométrique sauf pour des densités particulières
- en dimension d :
  - pour $t > 1$: l'asymptotique du nombre d'itérations du modèle M2(t, μ), ce résultat n'étant pas connu pour LLL(t)
  - le passage entre LLL(t) et LLL(1) est conjecturé.

$$\widetilde{\Upsilon} = \log \prod r_i = \frac{1}{\log s}\Upsilon \qquad s = \text{paramètre condition de Siegel}$$

Modèles	K **pire des cas**	K **pour** $\mathtt{M1}(\alpha)$	K **pour** $\mathtt{M2}(\mu)$	K **exp.**
$\mathcal{A}(\widetilde{\Upsilon}, d)$	$\frac{1}{12\log t} d(d+1)\widetilde{\Upsilon}$	$\frac{1}{12\alpha} d(d+1)\widetilde{\Upsilon}$	$\frac{1}{6\lvert\log\mu\rvert} d(d+1)\widetilde{\Upsilon}$	$\Theta(d^2\widetilde{\Upsilon})$
$\mathcal{N}(\widetilde{\Upsilon}, d)$	$\frac{1}{8\log t} d^2\widetilde{\Upsilon}$	$\frac{1}{8\alpha} d^2\widetilde{\Upsilon}$	$\frac{1}{4\lvert\log\mu\rvert} d^2\widetilde{\Upsilon}$	$\Theta(d^2\widetilde{\Upsilon})$
$\mathcal{K}(\widetilde{\Upsilon}, d)$	$\frac{1}{2\log t} d\widetilde{\Upsilon}$	$\frac{1}{2\alpha} d\widetilde{\Upsilon}$	$\frac{1}{\lvert\log\mu\rvert} d\widetilde{\Upsilon}$	$\Theta(d\widetilde{\Upsilon})$

TABLE: La réduction est supposée difficile : $\widetilde{\Upsilon}/d^a \to \infty$ avec $a = 1$ pour les modèles $\mathcal{A}, \mathcal{N}$ et $a = 2$ pour le modèle $\mathcal{K}$.

$\mathcal{A}$=Ajtaï (grands-tas), $\mathcal{N}$=NTRU (uni-tas au milieu),
$\mathcal{K}$=Sac-à-dos (uni-tas au début)

Modèle M3 : systèmes dynamiques probabilistes

ρ est fonction de r_i, ν_i est uniforme dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu_i := \nu_i^2 \quad \text{avec} \quad \nu_i \in_R [-\frac{1}{2}, \frac{1}{2}]$$

$\mathtt{M3}(t)$

Si $x_i < \dfrac{1}{t^2} - \mu_i$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu_i)$$

$$\check{x}_i = \frac{x_i}{(x_i + \mu_i)^2}$$

$$\check{x}_{i+1} = x_{i+1}(x_i + \mu_i)$$

Générer un nouveau μ_i

- Le facteur de décroissance : $\rho = x_i + \mu_i$
- $\mathtt{M3}(t)$ modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)
- Le trou du système $\mathtt{M3}(t)$ (condition d'arrêt) est

$$(x_1, \ldots, x_{d-1}), \ (\mu_1, \ldots, \mu_{d_1}) \quad \text{tels que}$$

$$\forall i = 1, \ldots, d-1, \quad x_i \in \left[\frac{1}{t^2} - \mu_i, +\infty\right[.$$

C'est un système dynamique probabiliste dans $\mathbb{R}^{d-1}$, à trou, chaque transformation ayant un point fixe attractif

Modèle M3 : systèmes dynamiques probabilistes

ρ est fonction de r_i, ν_i est uniforme dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu_i := \nu_i^2 \quad \text{avec} \quad \nu_i \in_R [-\frac{1}{2}, \frac{1}{2}]$$

M3(t)

Si $x_i < \dfrac{1}{t^2} - \mu_i$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu_i)$$

$$\check{x}_i = \frac{x_i}{(x_i + \mu_i)^2}$$

$$\check{x}_{i+1} = x_{i+1}(x_i + \mu_i)$$

Générer un nouveau μ_i

- Le facteur de décroissance : $\rho = x_i + \mu_i$
- M3(t) modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)
- Le trou du système M3(t) (condition d'arrêt) est

$$(x_1, \ldots, x_{d-1}), \ (\mu_1, \ldots, \mu_{d_1}) \quad \text{tels que}$$

$$\forall i = 1, \ldots, d-1, \quad x_i \in \left[\frac{1}{t^2} - \mu_i, +\infty\right[.$$

C'est un système dynamique probabiliste dans $\mathbb{R}^{d-1}$, à trou, chaque transformation ayant un point fixe attractif

Modèle M3 : systèmes dynamiques probabilistes

ρ est fonction de r_i, ν_i est uniforme dans $[-\frac{1}{2}, \frac{1}{2}]$

On pose :

$$x_i := r_i^2 = \frac{\ell_{i+1}^2}{\ell_i^2} \leftarrow \text{variable}, \qquad \check{x}_i := \check{r}_i^2 = \frac{\check{\ell}_{i+1}^2}{\check{\ell}_i^2}, \qquad \mu_i := \nu_i^2 \quad \text{avec} \quad \nu_i \in_R [-\frac{1}{2}, \frac{1}{2}]$$

M3(t)

Si $x_i < \dfrac{1}{t^2} - \mu_i$

$$\check{x}_{i-1} = x_{i-1}(x_i + \mu_i)$$

$$\check{x}_i = \frac{x_i}{(x_i + \mu_i)^2}$$

$$\check{x}_{i+1} = x_{i+1}(x_i + \mu_i)$$

Générer un nouveau μ_i

- Le facteur de décroissance : $\rho = x_i + \mu_i$
- M3(t) modélise et analyse l'algorithme LLL(t) (également pour $t = 1$)
- Le trou du système M3(t) (condition d'arrêt) est

$$(x_1, \ldots, x_{d-1}), \ (\mu_1, \ldots, \mu_{d_1}) \quad \text{tels que}$$

$$\forall i = 1, \ldots, d-1, \quad x_i \in \left[\frac{1}{t^2} - \mu_i, +\infty\right[.$$

C'est un système dynamique probabiliste dans $\mathbb{R}^{d-1}$, à trou, chaque transformation ayant un point fixe attractif

Modèle M3 : résultats

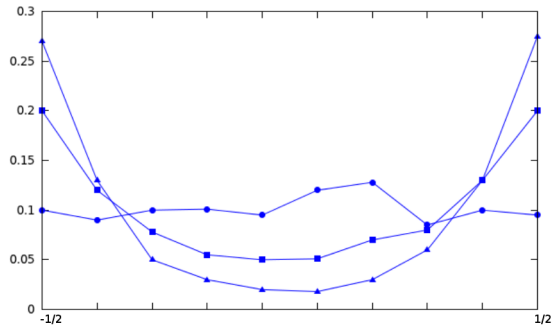
Aucun !

Conclusion

- Une classe de modèles simplifiés pour l'exécution de l'algorithme :
  - du plus simple : cfg
  - au plus compliqué : l'algorithme LLL
- Étude d'un modèle semi-simplifié d'exécution :
  - une analyse totale pour $d = 3$
    où l'analyse du véritable algorithme LLL est déjà mal comprise
  - analyse partielle en dimension générale.
- Modélisation des familles de réseaux cryptographiques, dans le cadre d'un cfg
  - "tas plein" : dit réseaux d'Ajtai
  - "uni-tas" : sac-à-dos ou réseaux NTRU
  - "tas à trous" : de Coppersmith :

Perspectives

- Modélisation d'autres algorithmes de réduction de réseaux (DeepLLL)
- Pour le modèle `M2`, prouver la conjecture, qui permettrait d'avoir un modèle simplifié pour l'algorithme LLL associé au paramètre $t = 1$
- Analyser le modèle `M3`
- Modèle de l'évolution du coefficient sous diagonal (Brigitte ?)



Merci pour votre attention !