Autour de la réduction d'une base aléatoire

Ali Akhavi [1] Jean-François Marckert [2] Alain Rouault [3]

22 mars 2007

ALEA'07 - Luminy

[1] LIAFA, Université Paris VII [akhavi@liafa.jussieu.fr]
[2] LABRI, Université Bordeaux I [marckert@labri.fr]
[3] LMV, Université de Versailles-Saint-Quentin [rouault@math.uvsq.fr]

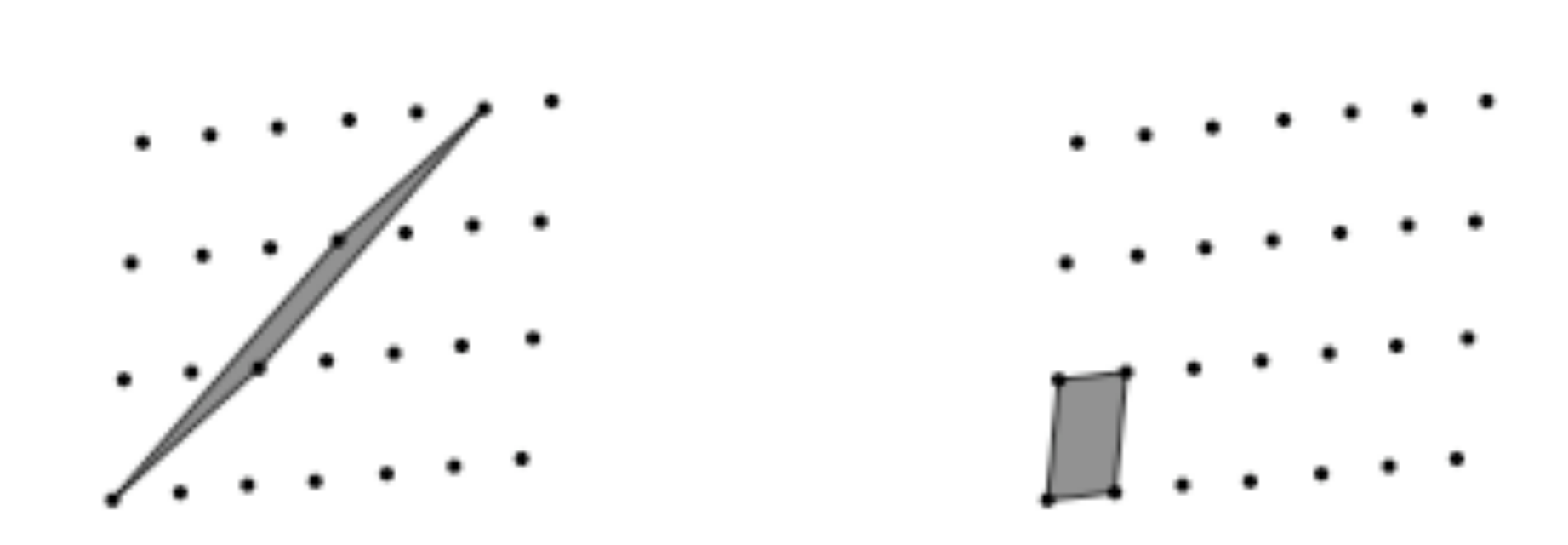
Sommaire

1. Le résultat : une version informelle
   - Réseau euclidien, base, le problème de la reduction
   - probabilité de réduction d'une base en fonction de la codimension
2. Le résultat : version plus précise
   - La LLL-réduction
   - modèle de base aléatoire
   - La probabilité asymptotique de la LLL-réduction d'une base aléatoire
3. Idée de la preuve

Réseau euclidien, base, Le problème de la reduction et ses motivations

- $(b) = b_1^{(n)}, b_2^{(n)}, \ldots, b_p^{(n)}$ (for $p \leq n$) is a linearly independent system of p vectors of $\mathbb{R}^n$.
- $\mathbb{R}^n$ with its classical Euclidean structure is the *ambient space*.
- $g := n - p$ is *the codimension* of the system (b).
- The set $\{\sum_{i=1}^{p} \lambda_i b_i^{(n)} : \lambda_i \in \mathbb{Z}\}$ is an additive discrete subgroup of $\mathbb{R}^n$ called *a lattice*.
- The system $b_1^{(n)}, b_2^{(n)}, \ldots, b_p^{(n)}$ is a *basis* of the lattice.
- The lattice basis reduction problem deals with finding a basis of a given lattice, whose vectors are "short enough" and "almost orthogonal".

Finding a nice basis of a lattice from an arbitrary basis



• On the first picture, an ugly basis, on the second, a reduced basis of the same lattice. A lattice has infinitely many bases.
• Numerous applications : cryptology, computationnal number theory, integer programming, computationnal group theory, ...
• Come to LLL+25, Caen 29,30 June, 1st and 2 nd July 07 !

An informal statement of the result

- $s \in (0,1)$ is an approximation parameter for the reduceness.
- The closer is s to 1, the better is the quality of the basis.

Theorem

Let $b_1^{(n)}, b_2^{(n)}, \ldots, b_p^{(n)}$ *be a* random basis of codimension $g = n - p$ under some natural random model . *Let* $s \in (0,1)$ *be a real parameter.*
(i) If $g = g(n)$ *tends to infinity, then the probability that a random basis is* $LLL(s)$*–reduced tends to* 1.
(ii) If g *is constant then the probability that a random basis is* $LLL(s)$*–reduced converges to a constant in* $(0,1)$ *(depending on* s *and* g*).*

Gram-Schmidt orthogonalization : $(b) \longrightarrow (\widehat{b})$:

$$\begin{cases} \widehat{b}_1 &= b_1 \\ \widehat{b}_2 &= b_{2\perp\langle b_1\rangle} \\ \vdots & \\ \widehat{b}_p &= b_{p\perp\langle b_1,\cdots,b_{p-1}\rangle} \end{cases} \longleftrightarrow \begin{cases} \widehat{b}_j^{(n)} = b_j^{(n)} - \sum_{i=1}^{j-1} \frac{\langle b_j^{(n)}, \widehat{b}_i^{(n)}\rangle}{\|\widehat{b}_i^{(n)}\|^2}\, \widehat{b}_i^{(n)} \\ \text{for } j \geq 2. \end{cases}$$

$$\begin{cases} (b) = (\widehat{b})\ R \\ R \text{ upper triangular :} \\ R_{j,j} = 1 \end{cases}$$

$$\begin{array}{c} \\ \widehat{b}_1 \\ \vdots \\ \widehat{b}_i \\ \widehat{b}_{i+1} \\ \vdots \\ \widehat{b}_p \end{array} \begin{array}{c} \begin{array}{cccccc} b_1 & \cdots & b_i & b_{i+1} & \cdots & b_p \end{array} \\ \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots & R_{1,p} \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 1 & R_{i,i+1} & & \vdots \\ 0 & \cdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \end{array}.$$

An LLL(s) reduced basis

$(b^{(n)}) = b_1^{(n)}, b_2^{(n)}, \ldots, b_p^{(n)}$ (for $p \leq n$) is a linearly independent system of p vectors of $\mathbb{R}^n$, with codimension $g := n - p$.

For all $i \in \{g+1, \ldots, n-1\}$, set : $\quad r_i^{(n)} := \dfrac{\|\widehat{b}_{n-i+1}^{(n)}\|^2}{\|\widehat{b}_{n-i}^{(n)}\|^2}$

Definition

- $(b^{(n)})$ *is an LLL(s)-reduced basis iff*

$$\forall i \in \{1, \ldots, p-1\}, \quad \frac{\|\widehat{b}_{i+1}^{(n)}\|^2}{\|\widehat{b}_i^{(n)}\|^2} > s^2.$$

$$\Leftrightarrow \forall i \in \{g+1, \ldots, n-1\} \quad r_i^{(n)} > s^2$$

$$\Leftrightarrow \min_{i \in \{g+1, \ldots, n-1\}} r_i^{(n)} > s^2$$

Important random variables

Definition

- *The* reduction level *of* $(b^{(n)})$ *is the quantity*

$$\mathcal{M}_n^g := \min_{i\in\{1,\dots,p-1\}} \frac{\|\widehat{b}_{i+1}^{(n)}\|^2}{\|\widehat{b}_i^{(n)}\|^2} = \min_{i\in\{g+1,\dots,n-1\}} r_i^{(n)}$$

- *The* index of worst local reduction *of* $(b^{(n)})$ *is*

$$\mathcal{I}_n^g := \min\left\{i : \ r_i^{(n)} = \mathcal{M}_n^g\right\}.$$

Models of random bases

- The vectors b_i's $(1 \leq i \leq p \leq n)$ are picked up randomly in $\mathbb{R}^n$, independently, and with the same distribution ν_n
- ν_n is invariant by rotation and satisfies $\nu_n(0) = 0$.
- A technical condition :

Assumption

There exists a deterministic sequence $(a_n)_n$ *and constants* $d_1, d_2, \alpha > 0$, $\rho_0 \in (0,1)$ *such that, for every* n *and* $\rho \in (0, \rho_0)$

$$\nu_n\left(\left|\frac{\|b_1^{(n)}\|^2}{a_n} - 1\right| \geq \rho\right) \leq d_1 e^{-n d_2 \rho^\alpha} .$$

In particular, $\sup\left\{\left|\frac{\|b_i^{(n)}\|^2}{a_n} - 1\right|, i \in \{1, \ldots, n\}\right\} \xrightarrow[n]{proba} 0.$

Three examples of random bases

- ν_n is the uniform distribution on $\mathbb{S}^{n-1}$. In this case $\|b_1^{(n)}\|^2 = 1$, and $a_n = 1$.
- $\nu_n = \mathbb{U}_n$. In this case, $a_n = 1$ and $\mathbb{U}_n(|\|b_1^{(n)}\|^2/a_n - 1| \geq \rho) = (1-\rho)^{n/2} \leq e^{-n\rho/2}$.
- ν_n is the n-variate standard normal (the coordinates are i.i.d. $\mathcal{N}(0,1)$). Then $\|b_1^{(n)}\|^2/2$ is $\gamma_{n/2}$-distributed. It can be shown that for $a_n = n$, the previous assumption holds in this case with $\alpha = 2$.
  Notice that these three models are cited in the second volume of Knuth's art of programming.

The result : Some notations

- $x = (x_i)_{i\geq 1}$ a sequence of real numbers,
- $\operatorname{argmin} x = \{i : \inf_{j\geq 1} x_j = x_i\}$.
- $\|x\|_q := \left(\sum_{i\geq 1} |x_i|^q\right)^{1/q}$
- $\ell_q := \{x, \|x\|_q < +\infty\}$.

Let $(\eta_i)_{i\geq 1}$ be a sequence of independent random variables such that $\eta_i \overset{(d)}{=} \gamma_{i/2}$ and set

$$\mathcal{R}_k = \eta_k/\eta_{k+1}\ ,\ k \geq 1\,,$$

$$\mathcal{M}_k = \min\{\mathcal{R}_k, k \geq 1\}\ \text{, and}$$

$$\mathcal{I}_k = \min\{\operatorname{argmin}\{\mathcal{R}_k, k \geq 1\}\},$$

The result

Proposition

For any $q > 2$, the following convergence in distribution holds in the metric space ℓ_q :

$$(r_k^n - 1)_{k\geq 1} \xrightarrow[n]{(d)} (\mathcal{R}_k - 1)_{k\geq 1}.$$

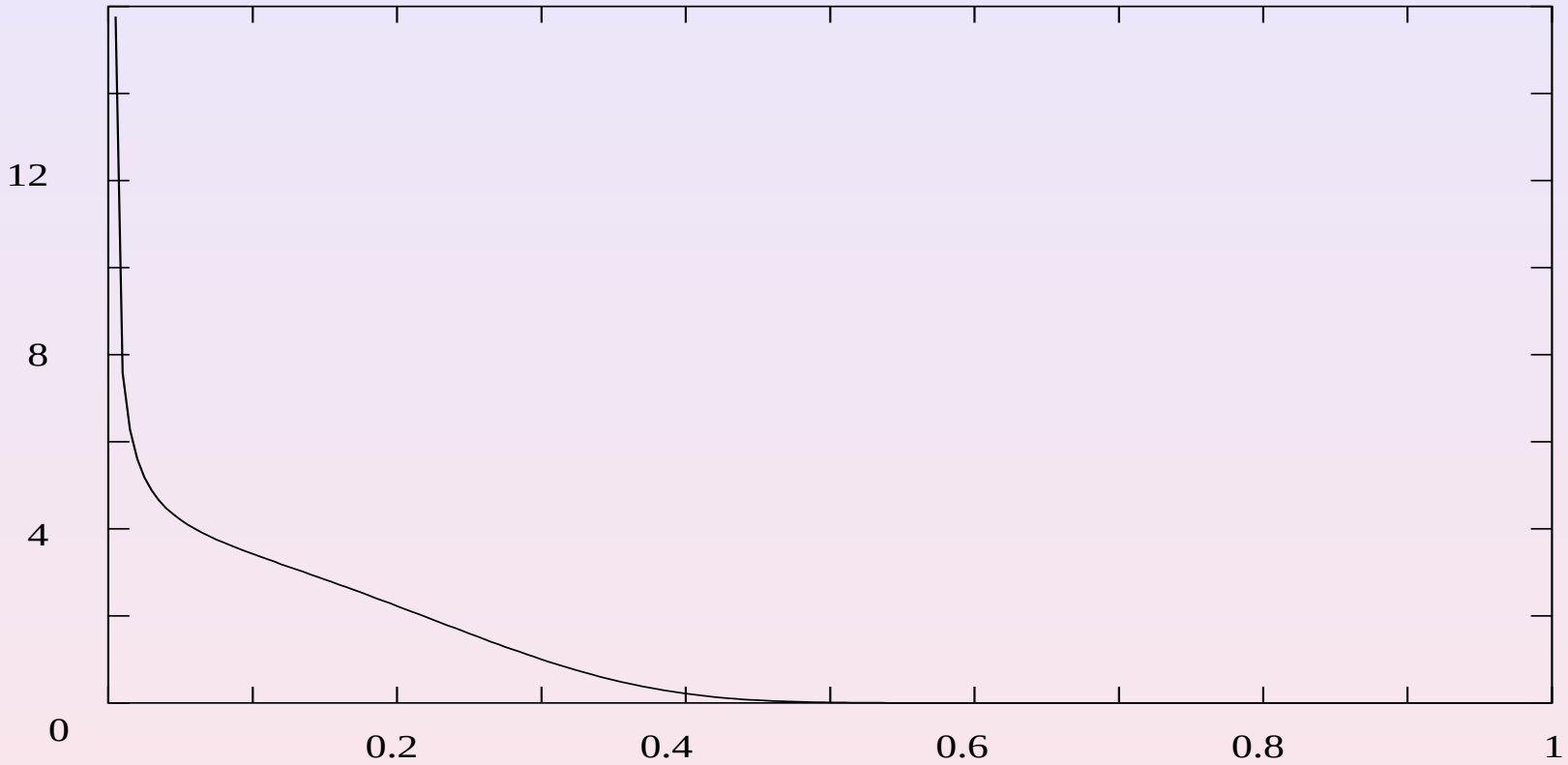
Theorem

If ν_n is spherical and satisfies Assumption 2.3 then,
(i) Let $g : \mathbb{N} \to \mathbb{N}$ such that $g(n) \leq n$ and $g(n) \to \infty$. Then $\mathcal{M}_n^{g(n)} \xrightarrow[n]{proba.} 1$.

(ii) For each $k \geq$, $\mathcal{M}_n^k \xrightarrow[n]{(d)} \mathcal{M}^k$.

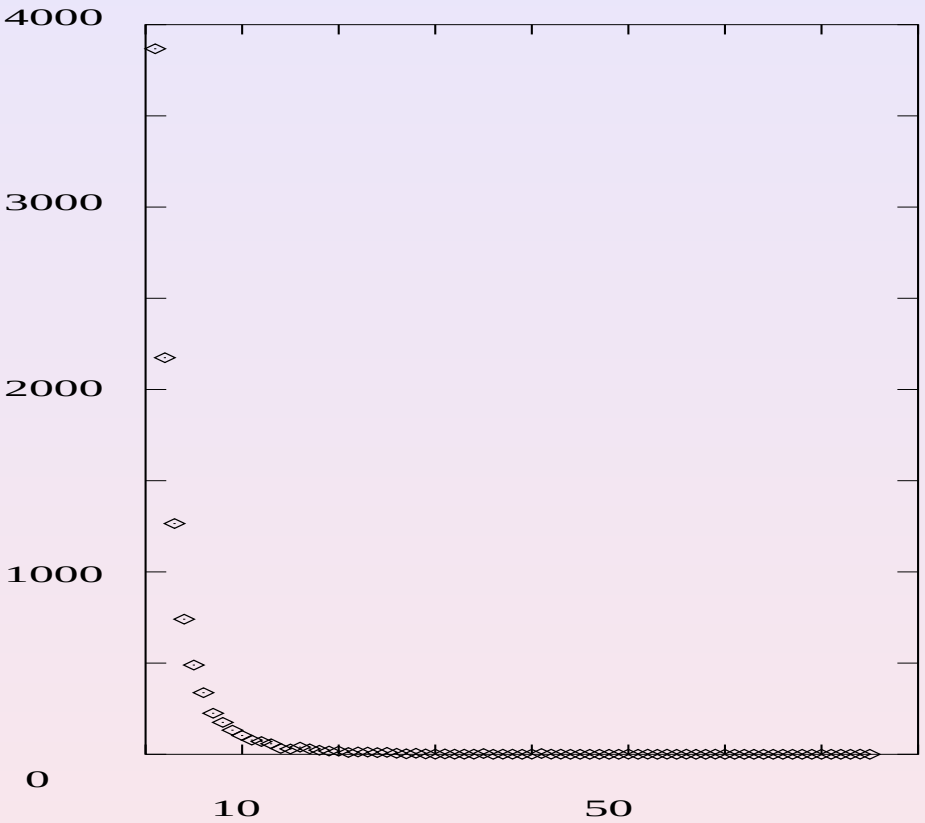
(iii) For any $k \geq 1$, $\mathcal{I}_n^k \xrightarrow[n]{(d)} \mathcal{I}^k$.

Simulation (I)



Simulation of the density of $\mathcal{M}^0$ with 10^8 data.

Simulation (II)



Histogram provided by 10000 simulations of $\mathcal{I}_\infty$.
The sequence $P(\mathcal{I}^0 = k)$ seems to be decreasing.

The Beta–Gamma algebra

- For $a > 0$, the gamma distribution of parameter a is

$$\gamma_a(dx) = \frac{e^{-x}x^{a-1}}{\Gamma(a)}\ \mathbb{1}_{[0,\infty)}(x)\ dx\,,$$

and its mean is a.

- For $(a,b) \in \mathbb{R}^{+\star}$, the beta distribution of parameters (a,b) denoted by $\beta_{a,b}$ is

$$\beta_{a,b}(dx) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}x^{a-1}(1-x)^{b-1}\ \mathbb{1}_{(0,1)}(x)\ dx.$$

- $$\gamma(a)+\gamma(b) \overset{(d)}{=} \gamma(a+b)\,,\ \frac{\gamma(a)}{\gamma(b)} \overset{(d)}{=} \frac{\beta(a,b)}{1-\beta(a,b)}\,,$$

- $$\mathbb{P}\big(\gamma(a)/\gamma(b) \in dx\big) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\frac{x^{a-1}}{(1+x)^{a+b}}\ \mathbb{1}_{[0,\infty[}(x)\ dx\,.$$

Idea of proof

1. $\|\widehat{b}_j^{(n)}\|^2 \overset{(d)}{=} \beta\left(\frac{n-j+1}{2}, \frac{j+1}{2}\right)$.
2. Convergence of the process $(r_j^{(n)})_{j\geq 1}$ with n.
   - for each j, $r_j^{(n)} \xrightarrow[n]{(d)} \gamma\left(\frac{j}{2}\right)/\gamma\left(\frac{j+1}{2}\right)$, and
   - $\gamma\left(\frac{j}{2}\right)/\gamma\left(\frac{j+1}{2}\right) \xrightarrow[j]{a.s.} 1$;
   - this suggests that the minimum $\mathcal{M}_n^g$ is reached by the firsts $r_j^{(n)}$ and motivated the time inversions
3. For any $q > 2$, $(\mathcal{R}_k - 1)$ is a.s. in ℓ_q, i.e. $\sum_k |\mathcal{R}_k - 1|^q < \infty$
4. Definition of a process $R^{(n)}$ equidistributed to $r^{(n)}$, but defined on a unique space probability
5. $(R_k^{(n)} - \mathcal{R}_k)_{k\geq 1} \xrightarrow[n]{a.s.} 0$ in ℓ_q, i.e. $\sum_k |R_k^{(n)} - \mathcal{R}_k|^q \xrightarrow[n]{a.s.} 0$.
6. Convergence of the reduction level and related quantities

Conclusion and perspectives

1. A non trivial result on random lattices
   - Other properties of random lattices -¿ [Rouault]
2. consequences in lattice reduction :
   A random basis with a high codimension is esay to reduce
   - To design efficient probabilistic reduction algorithms.
   - To analyse more precisely reduction algorithm (methods issued from dynamical systems)