Some steps for the probabilistic analysis of the LLL Algorithm

Brigitte Vallée
GREYC, CNRS and Université de Caen.

École de Printemps d'Informatique Théorique
Autrans, Mars 2013.

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sandpiles

– Returning to the LLL Algorithm

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sandpiles

– Returning to the LLL Algorithm

The LLL algorithm

Input : A lattice $\mathcal{L}$ given by a basis $B = (b_1, b_2, \ldots, b_n)$

The algorithm deals with the Gram–Schmidt orthogonalized system $B^\star = (b_1^\star, b_2^\star, \ldots, b_n^\star)$ with $b_i^\star :=$ proj. of b_i orth. to $< b_1, b_2, \ldots b_{i-1} >$ and the matrix $\mathcal{P} := (m_{i,j})$ which expresses B as a function of $B^\star$.

$$\mathcal{P} := \begin{array}{c} \\ b_1 \\ b_2 \\ \vdots \\ b_{i-1} \\ b_i \\ b_{i+1} \\ \vdots \\ b_p \end{array} \begin{array}{c} \begin{array}{ccccccccc} b_1^\star & b_2^\star & \ldots & b_{i-1}^\star & b_i^\star & b_{i+1}^\star & \ldots & b_p^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 \\ m_{2,1} & 1 & \ldots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{i-1,1} & m_{i-1,2} & \ldots & 1 & 0 & 0 & 0 & 0 \\ m_{i,1} & m_{i,2} & \ldots & m_{i,i-1} & 1 & 0 & 0 & 0 \\ m_{i+1,1} & m_{i+1,2} & \ldots & m_{i+1,i-1} & m_{i+1,i} & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{p,1} & m_{p,2} & \ldots & m_{p,i-1} & m_{p,i} & m_{p,i+1} & \ldots & 1 \end{pmatrix} \end{array}$$

LLL algorithm =

Gauss' reduction steps on local bases

$$U_i := \begin{array}{c} \\ u_i \\ v_i \end{array} \begin{array}{c} \begin{array}{cc} b_i^\star & b_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}$$

The LLL algorithm performs the GAUSS algorithm on local bases U_i, with three differences

(a) The output test is weaker and depends on a parameter $t > 1$: the test $|v_i| > |u_i|$ is replaced by the test $|v_i| > (1/t)|u_i|$.

(b) The operations first performed on the local basis (u_i, v_i) are then reflected on the system (b_i, b_{i+1}).

(c) The GAUSS algorithm is performed on the local basis U_i step by step. The index i begins at $i = 1$, ends at $i = p$, and is incremented $i := i + 1$ or decremented $i := i - 1$ at each step.

Main parameters of interest for the LLL algorithm.

The lengths $\ell_i := |b_i^\star|$, the Siegel ratios $r_i := \dfrac{\ell_{i+1}}{\ell_i}$

the interval $[a := \min \ell_i, A := \max \ell_i]$.

The interval $[a, A]$ provides an approximation of $\lambda(\mathcal{L})$ and $\det \mathcal{L}$:

$$\lambda(\mathcal{L}) \geq a, \qquad \lambda(\mathcal{L}) \leq A\sqrt{p}, \qquad a^p \leq \det \mathcal{L} \leq A^p$$

Three actions of the algorithm.

For $t > 1$ let $s := (2t)/\sqrt{4 - t^2}$. For $t = 1$, then $s = 2/\sqrt{3}$.

– The algorithm narrows the interval $[a, A]$

– It provides lower bounds for final ratios $\hat{r}_i$ that satisfy $\hat{r}_i \geq \dfrac{1}{s}$

– At each step where Test in 2. is negative,

$D := \displaystyle\prod_{i=1}^{p-1} \det \mathcal{L}(b_1, b_2, \ldots, b_i) = \prod_{i=1}^{p-1} \ell_i^{p-i}$ is decreased with a factor $\dfrac{1}{t}$.

Upper bounds for output parameters: exponential wrt dimension p

the Hermite defect	$\gamma(B) := \dfrac{\lvert\hat{b}_1\rvert^2}{(\det \mathcal{L})^{2/p}}$	$\leq s^{p-1}$
the lenght defect	$\theta(B) := \dfrac{\lvert\hat{b}_1\rvert}{\lambda(\mathcal{L})}$	$\leq s^{p-1}$
the orthogonality defect	$\rho(B) := \dfrac{\prod_{i=1}^{d} \lvert\hat{b}_i\rvert}{\det \mathcal{L}}$	$\leq s^{p(p-1)/2}$

Upper bounds for the number of iterations K: polynomial wrt to dimension p

$$K \leq (p-1) + p(p-1)\log_t \frac{A}{a}, \quad \text{with } a := \min \ell_i, A := \max \ell_i$$

$$K \leq \frac{p^2}{2}\log_t \frac{N\sqrt{p}}{\lambda(\mathcal{L})}, \quad \text{with } N := \max |b_i|^2 \text{ and } \lambda(\mathcal{L}),$$

$$K \leq (p-1) + p(p-1)\frac{M}{\lg t}, \quad \text{when } \mathcal{L} \subset \mathbb{Z}^n, \text{ with } M := \max_i \ell(|b_i|^2)$$

The LLL Algorithm – the Lovasz version.

A fundamental role played by the lengths ℓ_i and their ratios r_i

$$\ell_i := \|b_i^\star\|, \qquad r_i := \frac{\ell_{i+1}}{\ell_i}.$$

The algorithm aims at obtaining lower bounds on ratios r_i.

More precisely, the algorithm with $t > 1$ computes a basis $\hat{B}$ that

(i) is size–reduced: $\quad |\hat{m}_{i,j}| \leq 1/2$

(ii) fulfills the Lovasz conditions $\mathcal{L}_t(i)$:

$$\hat{v}_i \geq \frac{1}{t}\hat{u}_i \quad \text{or} \quad \hat{\ell}_{i+1}^2 + \hat{m}_{i+1,i}^2\,\hat{\ell}_i^2 \geq \frac{1}{t^2}\hat{\ell}_i^2.$$

Such a basis B is t–Lovasz reduced.

When t and s are related by the equality $(1/t^2) = (1/4) + (1/s^2)$,

such a basis fulfills the Siegel conditions $\mathcal{S}_s(i)$: $\quad \hat{r}_i \geq \frac{1}{s}$

Optimal value for s : $s = 2/\sqrt{3}$.

A weaker version for the LLL Algorithm – the Siegel version.

A fundamental role played by the lengths ℓ_i and their ratios r_i

$$\ell_i := \|b_i^\star\|, \qquad r_i := \frac{\ell_{i+1}}{\ell_i}.$$

The algorithm aims at obtaining lower bounds on ratios r_i.

The Siegel version (with a parameter $s > 2/\sqrt{3}$) computes a basis $\hat{B}$ that

(i) is size–reduced: $\quad |\hat{m}_{i,j}| \leq \frac{1}{2}$

(ii) fulfills the Siegel conditions $\mathcal{S}_s(i)$: $\quad \hat{r}_i \geq \frac{1}{s}$

Such a basis B is s–Siegel reduced. It has good euclidean properties.

$$\mathcal{P} := \begin{array}{c} \\ b_1 \\ b_2 \\ \vdots \\ b_{i-1} \\ b_i \\ b_{i+1} \\ \vdots \\ b_p \end{array} \begin{array}{c} \begin{array}{ccccccc} b_1^\star & b_2^\star & \dots & b_{i-1}^\star & b_i^\star & b_{i+1}^\star & \dots & b_p^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ m_{2,1} & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{i-1,1} & m_{i-1,2} & \dots & 1 & 0 & 0 & 0 & 0 \\ m_{i,1} & m_{i,2} & \dots & m_{i,i-1} & 1 & 0 & 0 & 0 \\ m_{i+1,1} & m_{i+1,2} & \dots & m_{i+1,i-1} & m_{i+1,i} & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{p,1} & m_{p,2} & \dots & m_{p,i-1} & m_{p,i} & m_{p,i+1} & \dots & 1 \end{pmatrix} \end{array}$$

LLL algorithm $=$

Gauss' reduction steps on local bases

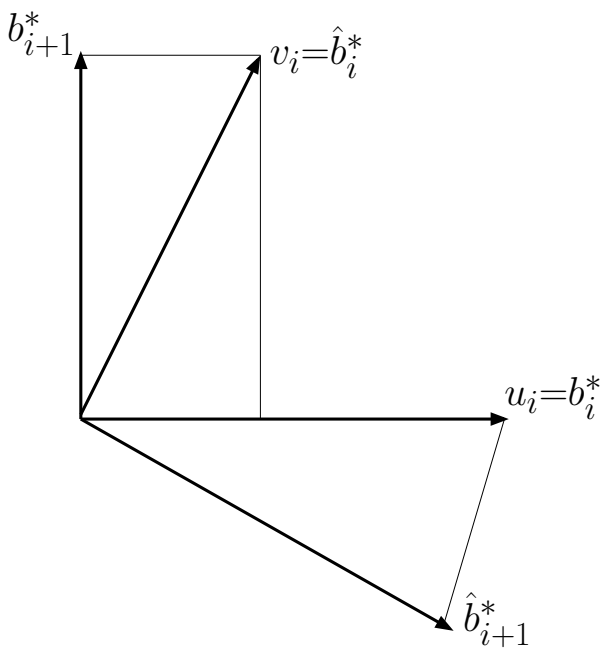
$$U_i := \begin{array}{c} \\ u_i \\ v_i \end{array} \begin{array}{c} \begin{array}{cc} b_i^\star & b_{i+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{i+1,i} & 1 \end{pmatrix} \end{array}$$

Two main types of operations performed:

(i) Translations $b_{i+1} := b_{i+1} - \lfloor m_{i+1,j} \rceil b_j$.

This does not change ℓ_{i+1}, and entails the inequality $|m_{i+1,j}| \leq (1/2)$.

(ii) Exchange between b_i and b_{i+1} when $\mathcal{S}_s(i)$ is not satisfied.



This modifies the lengths ℓ_i, ℓ_{i+1}.

The new values $\check{\ell}_i, \check{\ell}_{i+1}$ satisfy

$$\check{\ell}_i = \rho\, \ell_i \qquad \check{\ell}_{i+1} = \left(\frac{1}{\rho}\right) \ell_{i+1}$$

The factor ρ satisfies

$$\rho^2 = \frac{\ell^2_{i+1}}{\ell^2_i} + m^2_{i+1,i} \leq \frac{1}{s^2} + \frac{1}{4}$$

$$s > \frac{2}{\sqrt{3}} \Longrightarrow \rho < 1$$

LLL (s)
with $s > 2/\sqrt{3}$.

Input. A sequence $(\ell_1, \ell_2, \ldots \ell_n)$
Output. A sequence $(\hat{\ell}_1, \hat{\ell}_2, \ldots \hat{\ell}_n)$
with $\hat{\ell}_{i+1} \geq (1/s)\hat{\ell}_i$.

$i := 1$;
`While` $i < n$ `do`
If $\ell_{i+1} \geq (1/s)\,\ell_i$, **then** $i := i + 1$
else compute ρ ;
$\ell_i := \rho\,\ell_i$;
$\ell_{i+1} := (1/\rho)\,\ell_{i+1}$;
$i := \max(i - 1, 1)$;

The general scheme of the LLL Algorithm.

Main parameters of interest for the LLL Algorithm:

The number of iterations and the quality of the output basis.

Complexity bounds involve the potential $D(B)$ and the determinant $\det B$

$$D(B) = \prod_{i=1}^{n} \ell_i^i, \qquad \det B = \prod_{i=1}^{n} \ell_i.$$

During the execution, $D(B)$ is decreasing and $\det B$ is not modified.

Number of iterations. $$K(B) \leq \frac{1}{|\log \rho_0(s)|} \log \frac{D(B)}{D(\hat{B})},$$

where $\rho_0(s)$ is the maximal value of the decreasing factor ρ.

Quality of the output. The first output vector $\hat{b}_1$ is short enough;

$$\gamma(B) := \frac{||\hat{b}_1||}{(\det B)^{1/n}} \leq s^{(n-1)/2}.$$

What are the mean values of these two parameters?

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sand piles

– Returning to the LLL Algorithm

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.

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

(b) Ajtai "bad" bases $B^{(p)} := (b_i^{(p)})$ associated to a sequence $a_i^{(p)}$

$$b_i^{(p)} \in \mathbb{Z}^p, \quad b_i^{(p)} = a_i^{(p)}\, e_i + \sum_{j=1}^{i-1} a_{i,j}^{(p)}\, e_j \qquad (\Rightarrow \ell_i^{(p)} = a_i^{(p)})$$

with $$m_{i,j}^{(p)} = \frac{a_{i,j}^{(p)}}{a_j^{(p)}} = \text{rand}\left(-\frac{1}{2}, \frac{1}{2}\right) \qquad \text{[size-reduced]}$$

and $$r_i^{(p)} = \frac{a_{i+1}^{(p)}}{a_i^{(p)}} \to 0 \qquad \text{when } p \to \infty \qquad \text{[bad Siegel ratios]}$$

Experimental mean values .... versus proven upper bounds

[Nguyen and Stehlé]

Main parameters.	$\hat{r}_i$	γ	K
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}	$\Theta(Mp)$

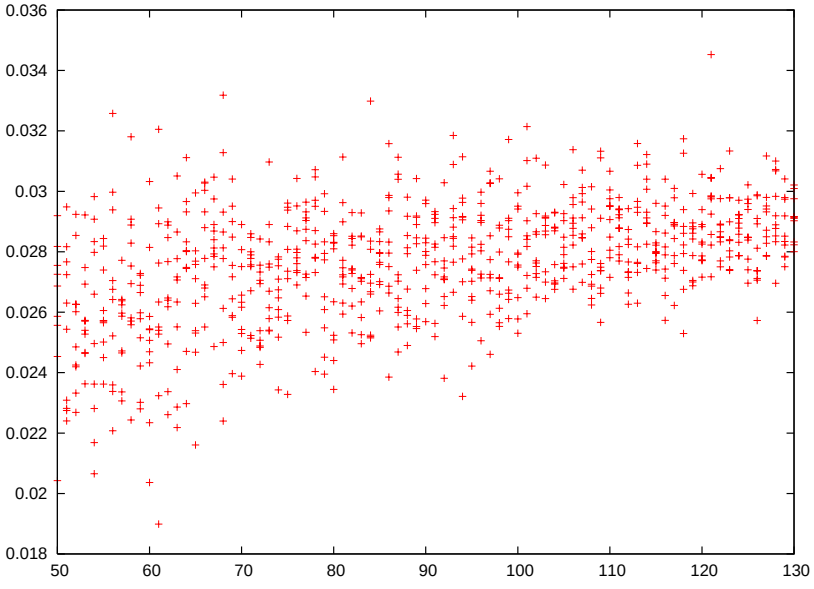
The execution parameters depend on the type of the lattice basis.

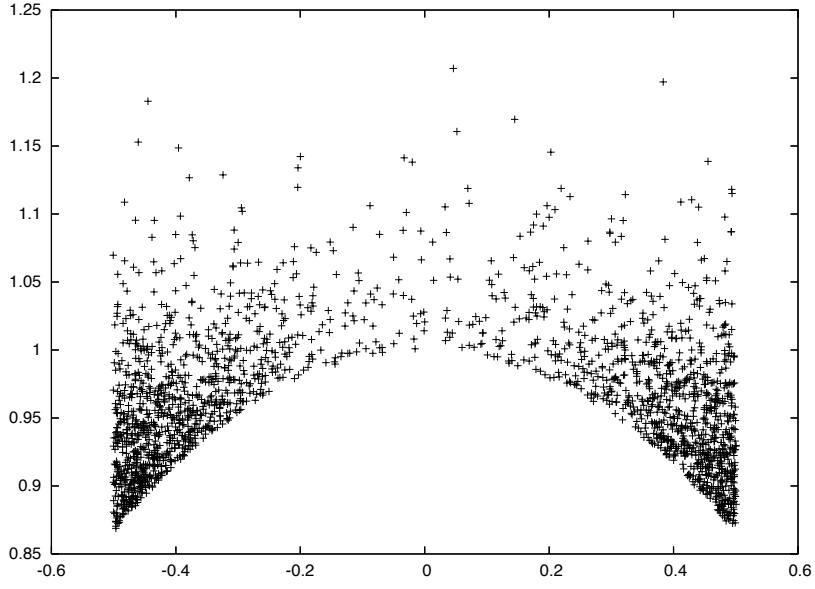
The output configuration does not depend strongly neither on index i nor on the type of bases.

It remains "exponential wrt p".

What about the "experimental" value β?

Experiments on the LLL Alg. [Nguyen and Stehlé]





On the left, experimental results for $\log_2 \gamma$.

The experimental value of parameter $[1/(2p)]\,\mathbb{E}[\log_2 \gamma] \approx 0.03$, so that $\beta \approx 1.04$.

On the right,

the output distribution of "local bases" shows an accumulation in the "corners".

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 in the spherical model.

A random basis $B_{p,(n)}$ of dimension p in the ambient space $\mathbb{R}^n$

- formed with p independent vectors
- drawn with the same distribution that is invariant by rotation.

Classical instances.

- uniform distribution in the ball or on the sphere
- gaussian distribution for coordinates

Probability of reduction.

For $s > 1$ and $n \to \infty$,

what is the probability $\pi_{p,(n),s}$ that $B_{p,(n)}$ is already s–reduced?

i.e., all the Siegel ratios $r_i := \dfrac{\ell_{i+1}}{\ell_i}$ already satisfy $r_i \geq \dfrac{1}{s}$ (for $i \leq p$)?

The answer depends on the position of p wrt n:

Two different behaviours!

Theorem. [Akhavi, Marckert, Rouault (2005)]

(i) If $n - p \to \infty$, then $\pi_{p,(n),s} \to 1$.

(ii) If $n - p = k$ is constant, then $\pi_{n-k,(n),s} \to \Pi_{k,s} \in (0, 1)$.

In particular: $\Pi_{0,s} \sim_{s\to\infty} 1 - \dfrac{1}{s}$,

$$\Pi_{0,s} \leq \exp\left[-\frac{\tau^2}{(s^2-1)^2}\right] \quad \text{when } s \to 1$$

For the LLL algorithm, and the first minimum too,
there are also two different behaviours.... according to the position of p wrt n:

Theorem. [Daudé and Vallée 1994] Under the random ball model,

– the number of iterations K of the LLL alg. on $B_{p,(n)}$,

– the first minimum λ of the lattice generated by $B_{p,(n)}$

satisfy "on average"

In the case of $p = n$

$$\mathbb{E}_{n,(n)}[K] \leq n^2 \left(\frac{1}{\log t}\right)\left[\frac{1}{2}\log n + 2\right], \quad \mathbb{E}_{n,(n)}[\lambda] \geq \frac{1}{4\sqrt{n}}$$

In the case when $p = cn$, with $c < 1$,

$$\mathbb{E}_{cn,(n)}[K] \leq \frac{cn}{1-c}\left(\frac{1}{\log t}\right)\left[\frac{1}{2}\log n + 2\right], \quad \mathbb{E}_{cn,(n)}[\lambda] \geq \exp\left[-\frac{4\log n}{2(1-c)n}\right].$$

Distribution of the last "local bases" $i = n - k$

[Akhavi, Marckert, Rouault (2005)]

For the last "local bases", at indices $i := n - k$, for fixed k and $n \to \infty$, the distribution of the ratio r_{n-k} admits a density φ_k,

$$\varphi_k(y) = 2B\left(\frac{k}{2}, \frac{k+1}{2}\right) \frac{y^{k-1}}{(1+y^2)^{k+(1/2)}} \mathbf{1}_{[0,\infty[}(y),$$

$$\text{with} \quad B(a,b) := \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}.$$

Near 0, the density φ_k behaves as a power function,

$$(ay)^{k-1} \leq \varphi_k(y) \leq (by)^{k-1}, \qquad \text{for some } a, b \text{ for } y \text{ near to 0.}$$

The last local bases, of index $n - k$ with k fixed, become

- more and more skew when k becomes smaller
- and thus more and more difficult to reduce

The first local bases, of index $n - k$ with $k \to \infty$, are already reduced....

A general probabilistic model for input bases.

Lattice bases B of full–rank whose matrix $B = (b_{i,j})$ is triangular.
The matrix $\mathcal{P}$ and the ratios r_i are easy to compute

$$r_i = \frac{b_{i+1,i+1}}{b_{i,i}}, \qquad m_{i,j} = \frac{b_{i,j}}{b_{j,j}}.$$

– Main parameters: the ratios r_i

The ratios r_i follow power laws : $\forall i \in [1..n-1],\ \exists \theta_i > 0$
for which $\Pr[r_i \leq x] = x^{1/\theta_i}$ for $x \in [0,1]$.

– Auxilliary parameters: the coefficients $m_{i,j}$.

For $j < i$, the coefficients $m_{i,j}$ are i.i.d in $[-1/2, +1/2]$.

Realistic instances whose difficulty increases with the parameters θ_i.

This distribution arises in a natural way in various frameworks,
– in the two dimensional case, and in the transition Euclid $\longrightarrow$ Gauss.
– when the initial basis is uniformly chosen in the unit ball.

Return to the LLL alg. with an additive point of view.

$$q_i := \log_s \ell_i, \qquad c_i := -\log_s r_i = q_i - q_{i+1}, \qquad \alpha := -\log_s \rho,$$

The Siegel condition becomes $q_i \le q_{i+1} + 1$ or $c_i \le 1$,

The exchange in the LLL algorithm becomes

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

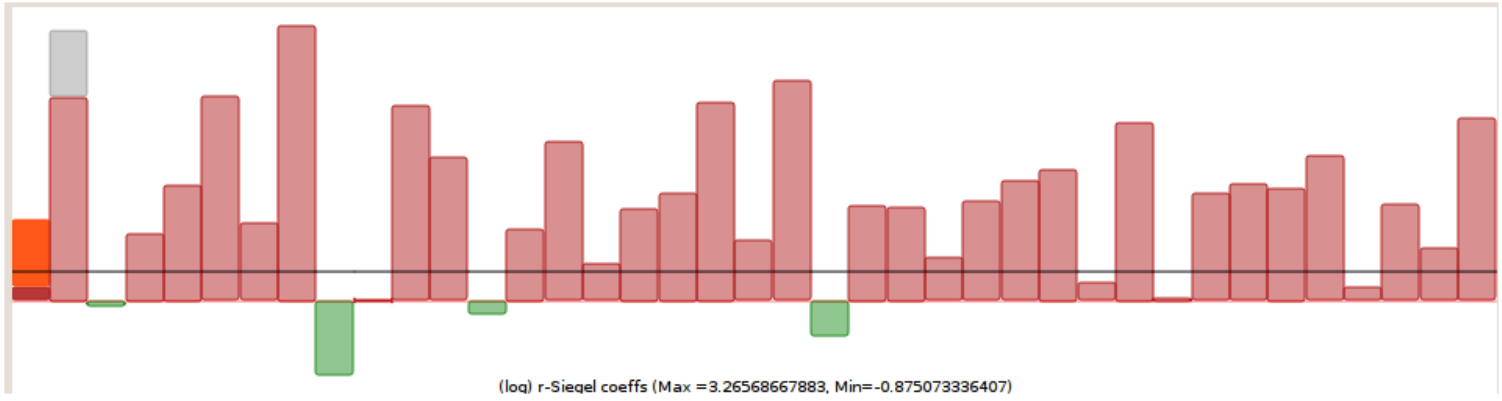
If $c_i > 1$, then $[\check{c}_i = c_i - 2\alpha, \quad \check{c_{i+1}} = c_{i+1} + \alpha, \quad \check{c_{i-1}} = c_{i-1} + \alpha,]$.

In our probabilistic model, each c_i follows an exponential law of the form

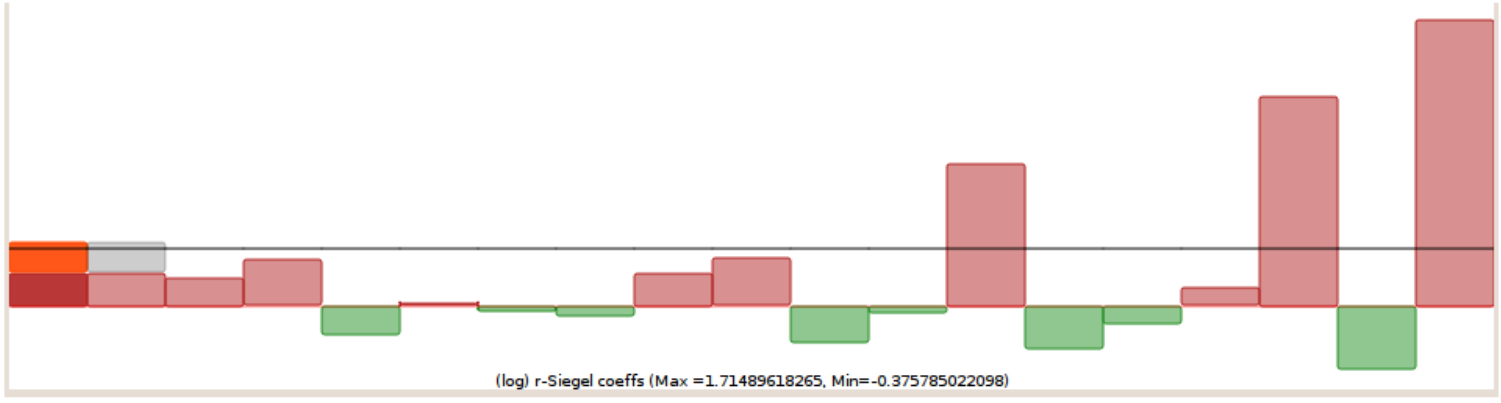
$$\Pr[c_i \ge y] = s^{-y/\theta_i} \qquad \text{for} \quad y \in [0, +\infty[\qquad \text{with} \quad \mathbb{E}[c_i] = \frac{\theta_i}{\log s}.$$

This model is then called the $\texttt{Exp-Ajtai}(\theta)$ model.

Some instances of cfg related to natural inputs



Some instances of cfg related to natural inputs



The regularized version of the LLL algorithm.

The main difficulty of the analysis of the LLL algorithm:

the decreasing factor ρ can vary throughout the interval $[0, \rho_0(s)]$.

$$\rho = \sqrt{\frac{\ell_{i+1}^2}{\ell_i^2} + m_{i+1,i}^2}.$$

We assume that the following Regularity Hypothesis holds (R):

The decreasing factor ρ (and thus its logarithm $\alpha := -\log_s \rho$) are constant.

Then, the equation

If $\quad q_i > q_{i+1} + 1, \quad$ then $\quad [\check{q_i} = q_i - \alpha, \quad q_{i\check{+}1} = q_{i+1} + \alpha]$.

defines a sandpile model.

The equation

If $\quad c_i > 1, \quad$ then $\quad [\check{c_i} = c_i - 2\alpha, \quad c_{i\check{+}1} = c_{i+1} + \alpha, \quad c_{i\check{-}1} = c_{i-1} + \alpha,]$.

defines a chip firing game.

RLLL (ρ, s)
with $s > 2/\sqrt{3}$, $\rho \leq \rho_0(s) < 1$

Input. A sequence $(\ell_1, \ell_2, \ldots \ell_n)$
Output. A sequence $(\hat{\ell}_1, \hat{\ell}_2, \ldots \hat{\ell}_n)$
with $\hat{\ell}_{i+1} \geq (1/s)\hat{\ell}_i$.

$i := 1$;
`While` $i < n$ `do`
  If $\ell_{i+1} \geq (1/s)\,\ell_i$, **then** $i := i+1$
    else $\ell_i := \rho\,\ell_i$;
      $\ell_{i+1} := (1/\rho)\,\ell_{i+1}$;
      $i := \max(i-1, 1)$;

ARLLL (α) with $\alpha > \alpha_0(s)$.

Input. A sequence $(q_1, q_2, \ldots q_n)$
Output. A sequence $(\hat{q}_1, \hat{q}_2, \ldots \hat{q}_n)$
with $\hat{q}_i - \hat{q}_{i+1} \leq 1$.

$i := 1$;
`While` $i < n$ `do`
  If $q_i - q_{i+1} \leq 1$, **then** $i := i+1$
    else $q_i := q_i - \alpha$;
      $q_{i+1} := q_{i+1} + \alpha$;
      $i := \max(i-1, 1)$;

Two versions of the regularized LLL algorithm.
On the left, the classical version, which depends on parameters s, ρ.
On the right, the additive version, which depends on the parameter $\alpha := -\log_s \rho$.

There are now three main questions:

– Is the Regularity Hypothesis (R) reasonable?

– What are the main features of the regularized versions of the LLL alg., namely sandpiles?

– What consequences can be deduced for the probabilistic behaviour of the LLL algorithm?

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sandpiles

– Returning to the LLL Algorithm

A general experimental study of parameter α.

We do not assume that there is a universal value for $\alpha := -\log_s \rho$.

Four variables may have an influence on the parameter α (for $n \to \infty$).

– The parameters θ_i of input distribution of `Exp-Ajtai` type.

– The position $i \in [1..n(B)-1]$: the index where the reduction occurs.

– The discrete time $j \in [1..K(B)]$: the index when the reduction occurs,

– The strategy defines the position i at the j–th iteration, inside the set

$$\mathcal{N}(j) := \{i; \quad \text{Condition } \mathcal{S}(i) \text{ not satisfied at the } j\text{–th iteration}\}$$

Three main strategies :

– The standard strategy chooses $i := \text{Min}\, \mathcal{N}(j)$

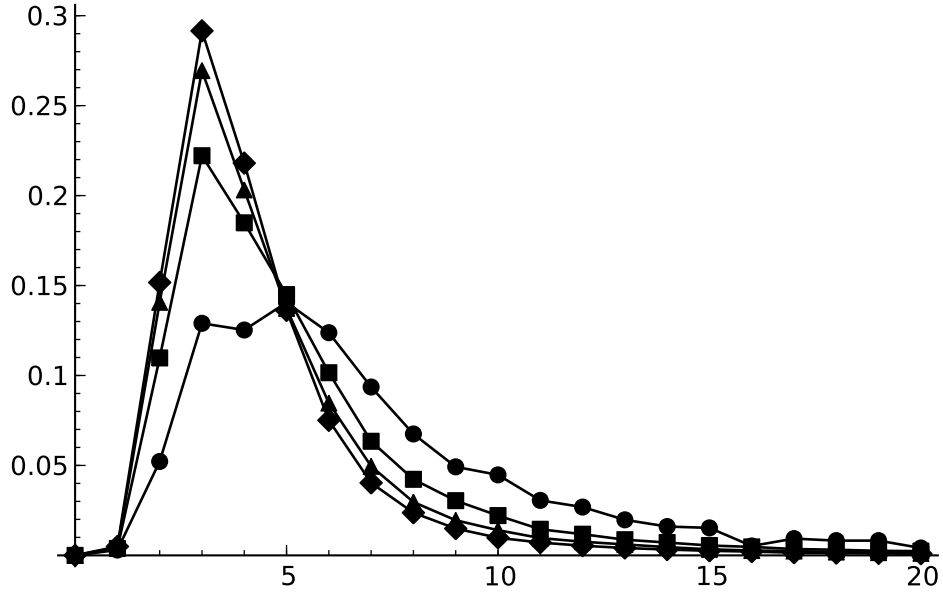
– The random strategy chooses $i \in_{\mathcal{R}} \mathcal{N}(j)$

– The greedy strategy chooses $i \in \mathcal{N}(j)$ for which the ratio r_i is minimum.

$$\mathcal{P} := \begin{array}{c} \\ b_1 \\ b_2 \\ \vdots \\ b_{i-1} \\ b_i \\ b_{i+1} \\ \vdots \\ b_p \end{array} \begin{array}{c} \begin{array}{cccccccc} b_1^\star & b_2^\star & \dots & b_{i-1}^\star & b_i^\star & b_{i+1}^\star & \dots & b_p^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ m_{2,1} & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{i-1,1} & m_{i-1,2} & \dots & 1 & 0 & 0 & 0 & 0 \\ m_{i,1} & m_{i,2} & \dots & m_{i,i-1} & 1 & 0 & 0 & 0 \\ m_{i+1,1} & m_{i+1,2} & \dots & m_{i+1,i-1} & m_{i+1,i} & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{p,1} & m_{p,2} & \dots & m_{p,i-1} & m_{p,i} & m_{p,i+1} & \dots & 1 \end{pmatrix} \end{array}$$

Distribution of the parameter α as a function of the dimension n

(Input distribution given by $\theta_i = 1.5$)



$n = 5\,(\bullet); n = 10\,(\blacksquare); n = 15\,(\blacktriangle); n = 20\,(\blacklozenge)$

When the dimension grows,

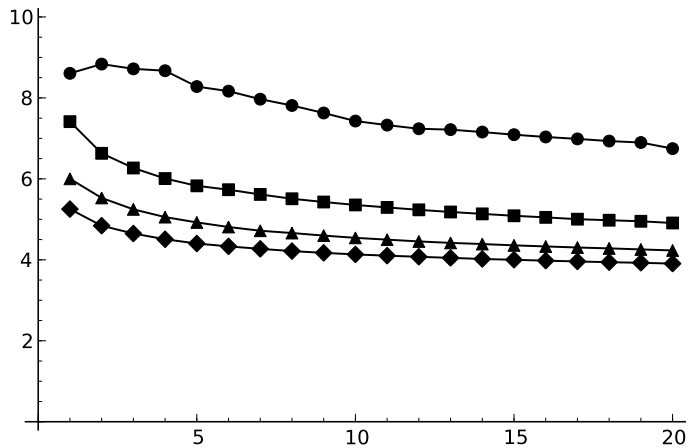
the distribution of α gets more and more concentrated,

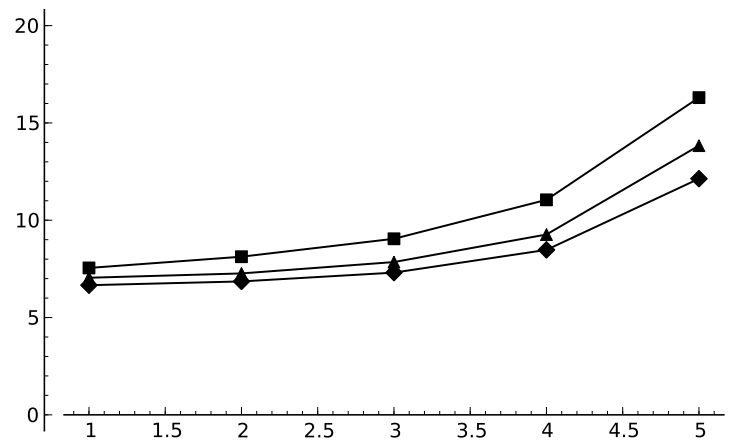
around a value which appears to tend to 2.5.

Influence of the discrete time and position on α.

$\bar{\alpha}^{\langle y \rangle}$:= mean value of α when the time is close to $(y/20)K$

$\bar{\alpha}_{\langle x \rangle}$:= mean value of α when the position is close to $(x/5)n$



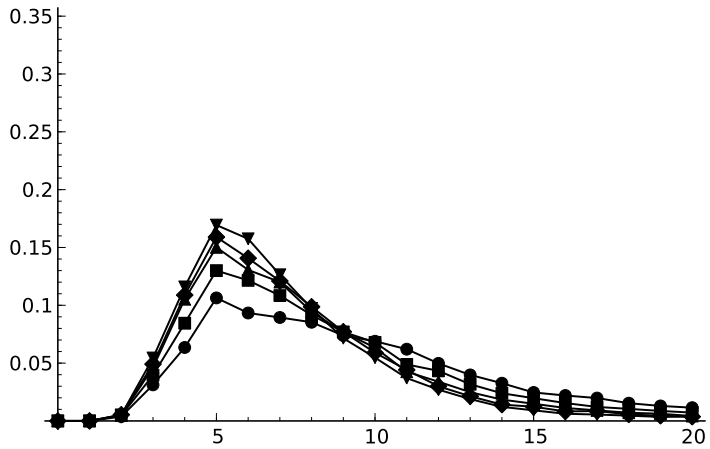


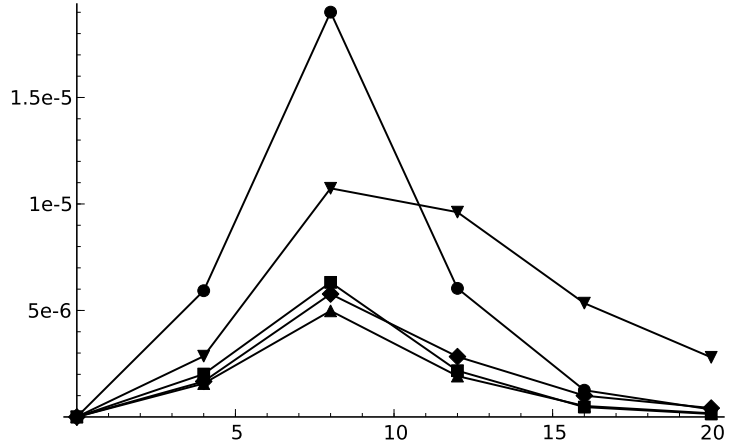
The functions $y \mapsto \bar{\alpha}^{\langle y \rangle}$ (left) and $x \mapsto \bar{\alpha}_{\langle x \rangle}$ (right),
for $n = 5$ (●); $n = 10$ (■); $n = 15$ (▲); $n = 20$ (♦)

The variations of the functions $y \mapsto \bar{\alpha}^{\langle y \rangle}$ and $x \mapsto \bar{\alpha}_{\langle x \rangle}$ are small,
and become smaller when the dimension n increases.

Distribution of $\alpha^{\langle y \rangle}$ and $\alpha_{\langle x \rangle}$

Remind: x refers to the position and y refers to the time.





Here $n = 20, Y = 20, X = 5$.

(left) the distribution of $\alpha^{\langle y \rangle}$ for $y = 2\,(\bullet); 5\,(\blacksquare); 10\,(\blacktriangle);\ 15\,(\blacklozenge); 20\,(\blacktriangledown)$

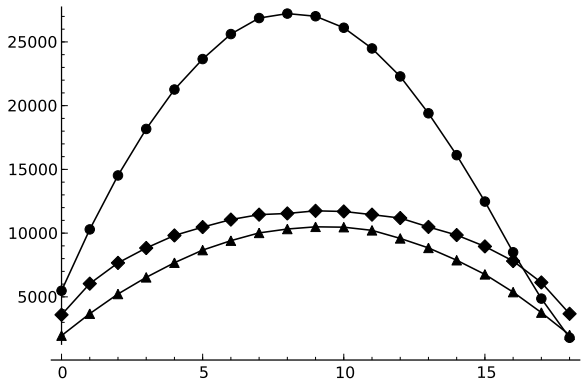
(right) the distribution of $\alpha_{\langle x \rangle}$ for $x = 1\,(\bullet); 2\,(\blacksquare); 3\,(\blacktriangle); 4\,(\blacklozenge); 5\,(\blacktriangledown)$

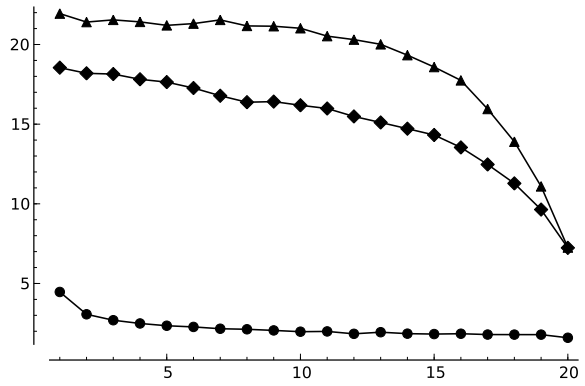
The distributions of $\alpha_{\langle x \rangle}$ and $\alpha^{\langle y \rangle}$ are concentrated,

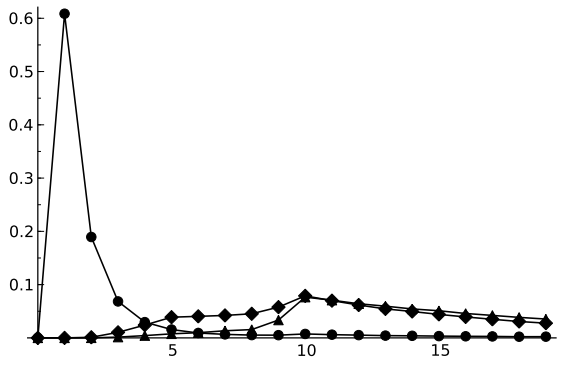
at least for y's not too small and for central values of x.

Influence of the strategy (not often studied):

• for standard, ▲ for greedy, and ♦ for random.







Here, $n = 20$.

(left): the functions $x \mapsto K_{\langle x \rangle}$ ($K_{\langle x \rangle}$ is the number of steps near the position x).

(middle) the functions $y \mapsto \bar{\alpha}^{\langle y \rangle}$. (right) the distribution of α.

– The standard strategy performs a larger number of steps.

The value of α is concentrated below $\alpha = 5$.

– The two other strategies perform a much smaller number of steps.

The values of α vary in $[5, 20]$ and decrease with the discrete time.

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sandpiles

– Returning to the LLL Algorithm

Three main questions about the RLLL algorithm.

$(Q1)$ Does the RLLL algorithm depend on the strategy?

$(Q2)$ Are there lower bounds on average for the number of iterations? the output configuration?

$(Q3)$ Does there exist a characterisation for two blocks to be independent? The two blocks B_- and B_+ are independent if the total basis formed by concatening the two reduced bases $\hat{B}_-$ and $\hat{B}_+$ is reduced.

The sandpile model is very well studied. However, ...
the RLLL algorithm gives rise to non classical instances of sandpile models.

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

The equation

If $\quad q_i > q_{i+1} + H, \quad$ 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).

Letting $c_i = q_i - q_{i+1}$, the equation

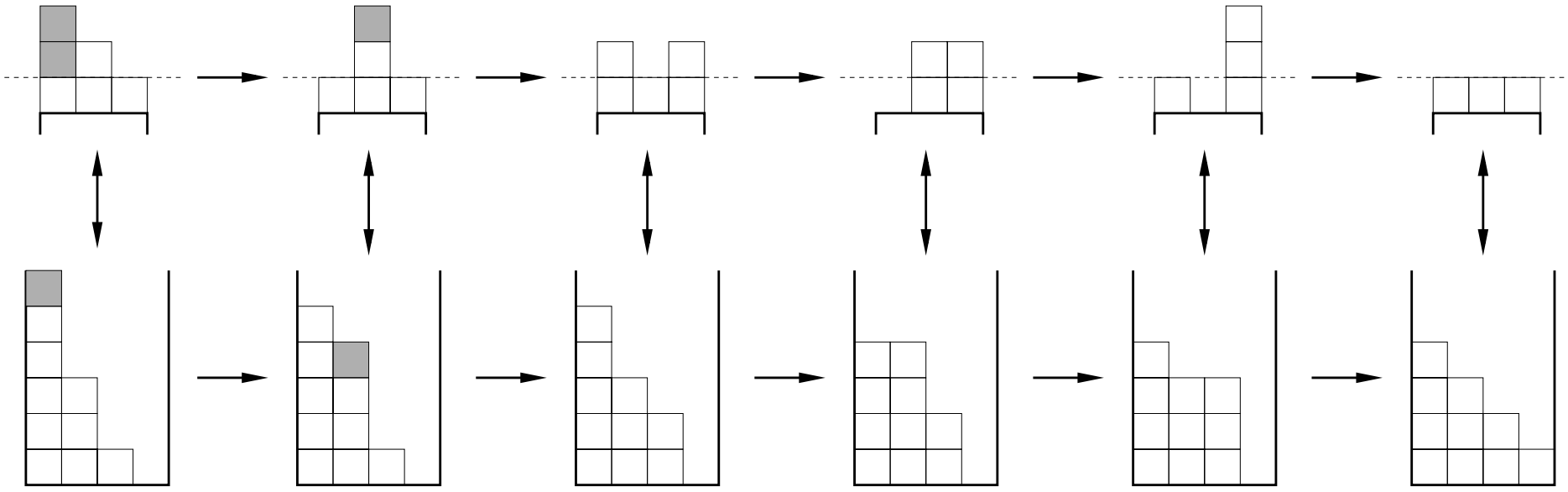
If $\quad c_i > H, \quad$ then $\quad [\check{c}_i = c_i - 2h, \quad \check{c_{i+1}} = c_{i+1} + h, \quad \check{c_{i-1}} = c_{i-1} + h,]$.

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

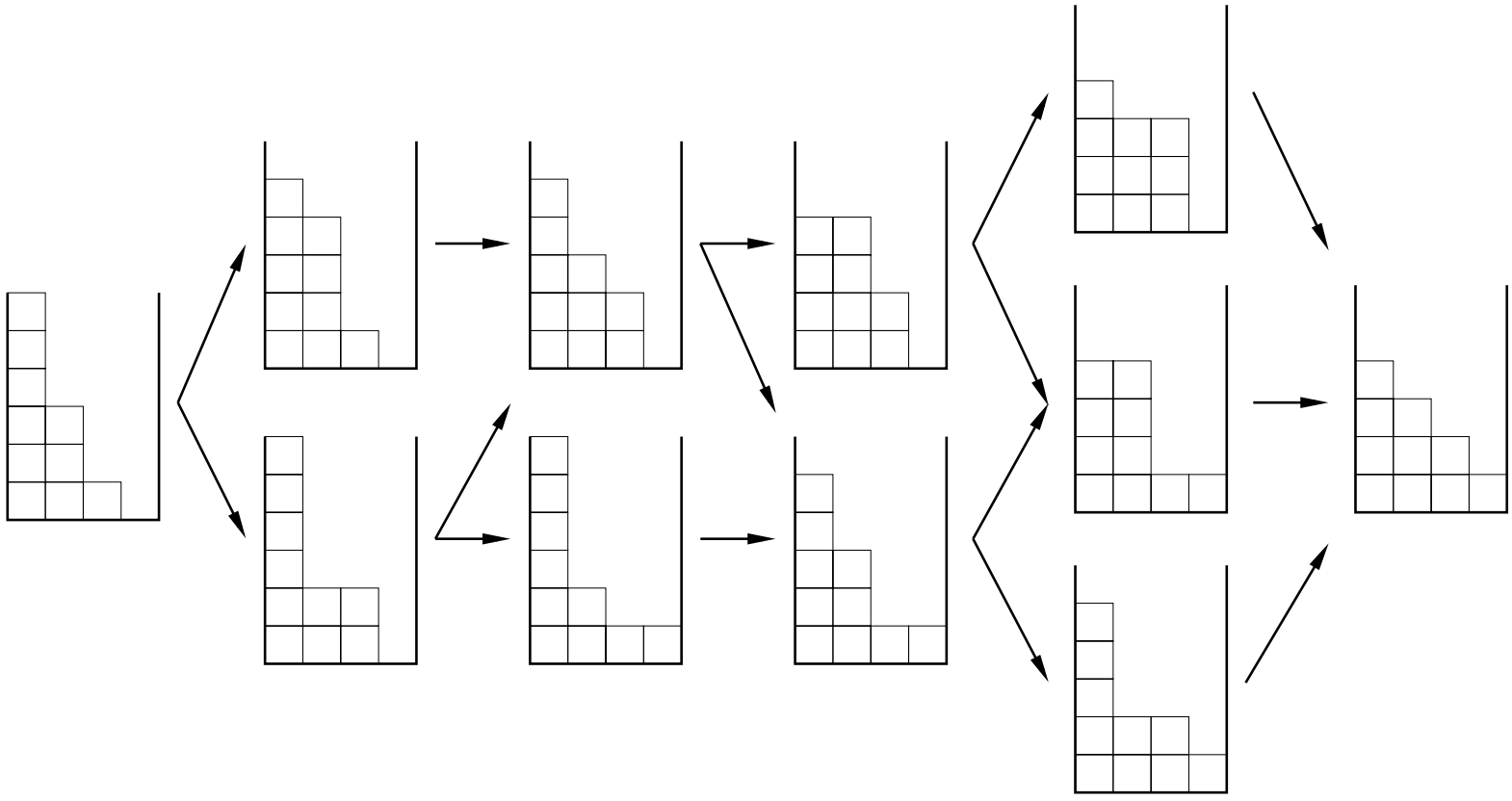
Classical instances studied: basic and decreasing.

– 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.



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



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

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

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

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

(iii) If the sandpile is strictly decreasing,

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

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

(iv) For a general sandpile,

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

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

(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)

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

Plan of the talk.

– Presentation of the LLL algorithm

– Probabilistic models of interest for the average-case analysis

– Testing the regularity hypothesis

– Results on sand piles

– Returning to the LLL Algorithm

Two interesting kinds of input bases.

(i) Totally non-reduced bases, for which Condition $\mathcal{S}_s(i)$ is never satisfied:
the sandpile is strictly decreasing.

(ii) A general input basis is a sequence of blocks,
some totally non-reduced, and other ones totally reduced.

Comparing two results:

– proven results for regular executions of the LLL algorithm.

– experimental results performed on general executions.

A good fitting between these two kinds of results, and thus:

– An indirect validation of the property :
"The executions of the LLL algorithm are very often regular enough".

– Long experiments on the LLL algorithm
can be simulated by fast computations in the sand pile model
(with a good choice of parameter α).

Output configuration: Study of the parameter $\gamma(\hat{B}) := \dfrac{\|\hat{b}_1\|}{\det B}$.

For a totally non reduced basis B on which the LLL algorithm is ρ–regular, the output parameter $\gamma(\hat{B})$ satisfies

$$\frac{2}{n-1}\log_s \gamma(\hat{B}) \in [1-\alpha, 1], \qquad \text{with } \alpha := -\log_s \rho.$$

Experiments done on general executions by Nguyen and Stehlé:
They show that, for most of the output bases $\hat{B}$, the ratio $\gamma(\hat{B})$ satisfies

$$\gamma(\hat{B}) \approx \beta^{(n-1)/2} \qquad \text{with } \beta \sim 1.04$$

The relation $\beta \sim s\sqrt{\rho}$ is then plausible,
so that the "usual" ρ would be close to 0.81.

Number of iterations.

Consider an input basis B, which follows the `Mod-Exp-Ajtai` distribution of parameter θ. If the execution of the LLL algorithm in dimension n is ρ–regular on the basis B, the number of iterations satisfies

$$K_n(\rho, \theta) \sim \frac{n^3}{12\alpha} \left(\frac{\rho^{1/\theta}}{1 - \rho^{1/\theta}} \right) \qquad (n \to \infty).$$

Experiments done for general executions by Nguyen and Stehlé.
For the historical choice of Ajtai, namely $\theta = n^a$, the experiments show a number of iterations of order n^{3+a}.

An instance of the independence property.

For breaking the RSA cryptosystem when the public exponent E is "small", Boneh and Durfee use the LLL algorithm on the following basis B:

The basis B is formed with blocks B_k, indexed from $k = 0$ to m.

- The block B_k has length $k + 1$,
- In each B_k, all the c_i's are equal to $L/2$ with $L := \log_s E$
- The total configuration is not totally decreasing,
- The independence condition holds.

An instance of the independence property.

For breaking the RSA cryptosystem when the public exponent E is "small", Boneh and Durfee use the LLL algorithm on the following basis B:

The basis B is formed with blocks B_k, indexed from $k = 0$ to m.

- The block B_k has length $k + 1$,
- In each B_k, all the c_i's are equal to $L/2$ with $L := \log_s E$
- The total configuration is not totally decreasing,
- The independence condition holds.

We can prove:

If the execution of the LLL algorithm is ρ-regular on the B-D basis, then:

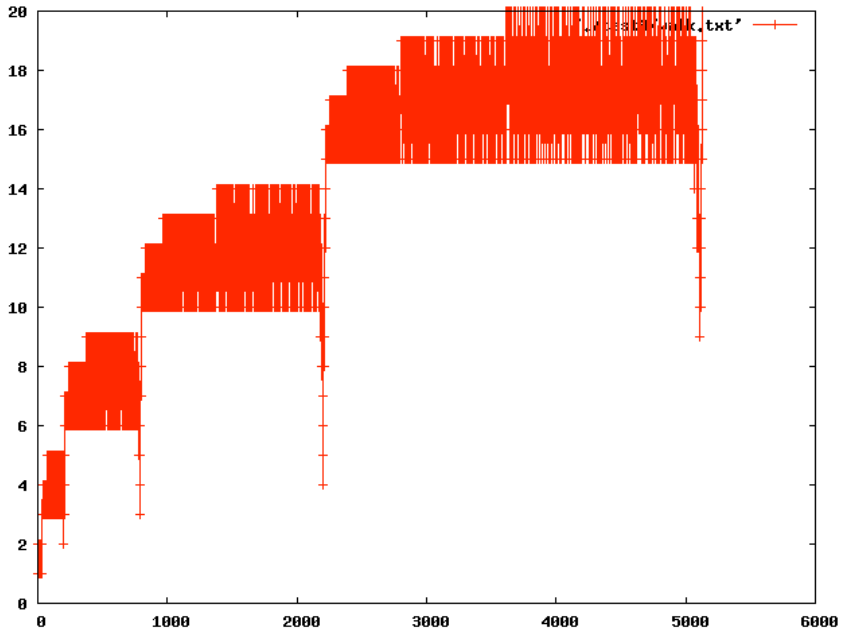
(i) the blocks B_k are independent,

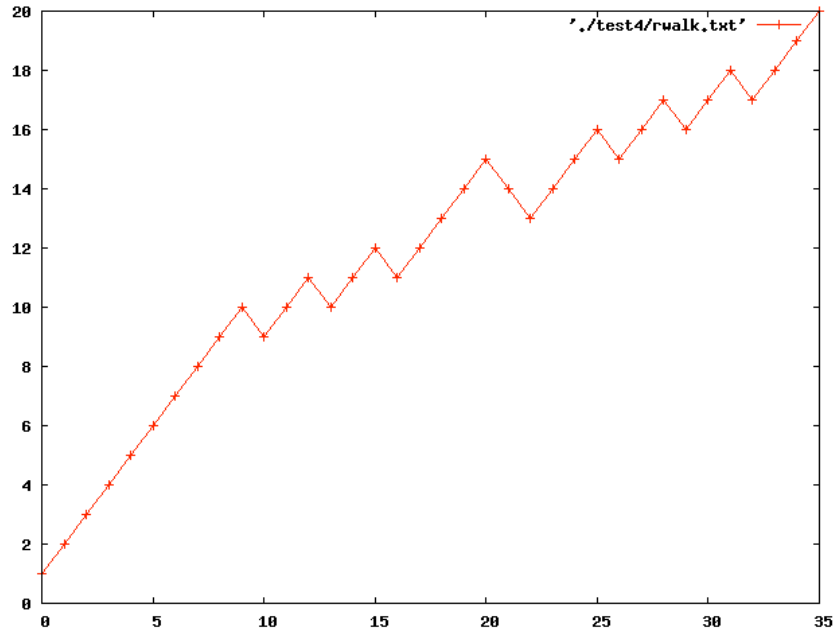
(ii) The number of iterations K_p (parallel) and K_s (sequential) satisfy

$$K_p = \frac{m^3}{12\alpha}\left(\frac{L}{2} - 1\right) \qquad K_s = \sum_{i=1}^{m} K_i \approx \frac{m^4}{48\alpha}\left(\frac{L}{2} - 1\right).$$

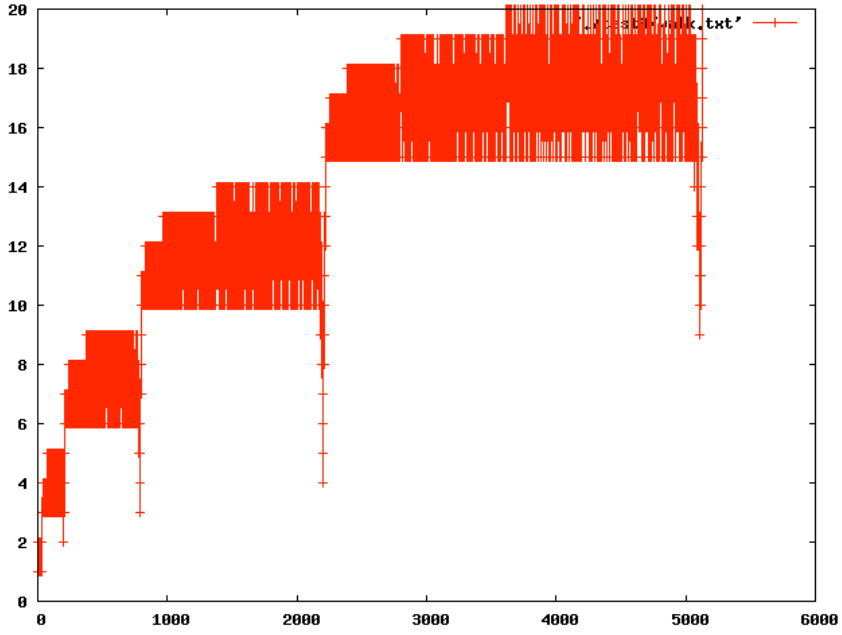
The execution of the LLL alg. on the BD lattice cannot be totally regular: In this case, the first vector of the reduced lattice basis would be the first vector of the initial basis, and the method would fail!

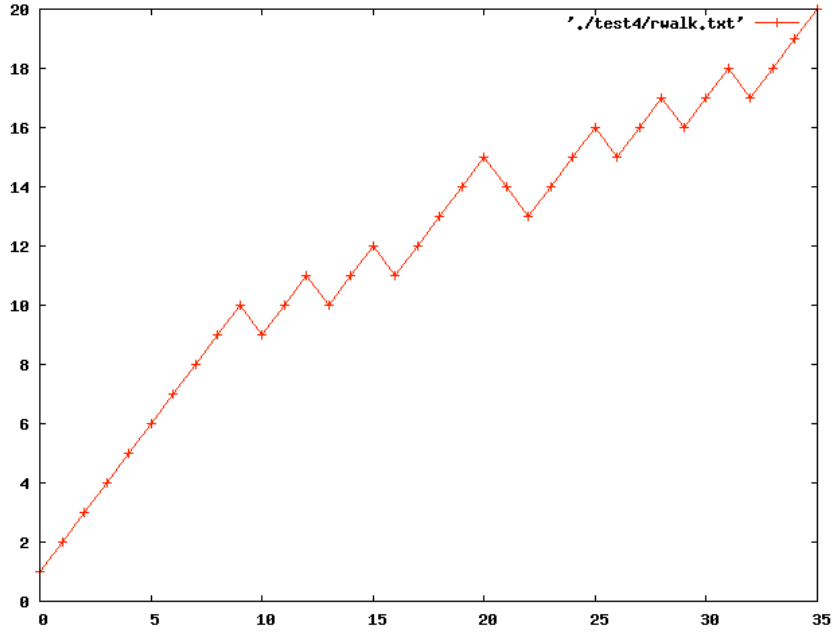
Comparing with an execution of the actual LLL algorithm on a BD lattice:





(left) The LLL alg. on a BD lattice (related to $m = 5$).
(right) The LLL alg. on the basis formed by the concatenation of the $\hat{B}_k$'s.





Each B_k is almost totally non reduced:

the number of iterations fits with the order $\Theta(k^3)$

which is proven for a ρ–regular execution.

The blocks are almost independent:

the basis obtained by concatening the $\hat{B}_k$ is not reduced,

but few reduction steps are needed for reducing it.

This strategy, whose first step is performed in parallel, is very efficient.

Conclusion

– A simplified model,

very useful for explaining, making experiments, finding conjectures.....

– Only qualitative similarities with the actual LLL algorithm.

– Possible (easy) proofs.

And now? A less simplified model ...

We can try to study an intermediary model, less simplified...
The factor ρ depends on the Siegel ratio r_i and the coefficient $m_{i+1,i}$.

$$\rho^2 = r_i^2 + m_{i+1,i}^2$$

We consider that the coefficient $m_{i+1,i}^2$ is fixed equal to θ,
so that ρ depends on c_i but only on c_i:

The LLL algorithm is now modelled as a dynamical system:
For instance, in two dimensions, the Siegel ratios

$$x := \frac{\ell_2^2}{\ell_1^2}, \qquad \hat{x} := \frac{\widehat{\ell}_2^2}{\widehat{\ell}_1^2},$$

are the main variables and define a mapping $f_\theta : x \mapsto \hat{x}$ as

$$f_\theta(x) = \frac{x}{(x+\theta)^2} \quad \text{if} \quad x < 1-\theta, \qquad f_\theta(x) = x \quad \text{if} \quad x \geq 1-\theta.$$

The first interesting case: Three dimensional case

There are two boxes and two Siegel ratios x and y.

The dynamical system is defined by two shifts,

A (governed by x), and B, (governed by y)

$$A(x,y) := \left(\frac{x}{(x+\theta)^2},\ y(x+\theta) \right) \quad \text{if } x < 1-\theta; \qquad A(x,y) = (x,y) \quad \text{else}$$

$$B(x,y) := \left(x(y+\theta),\ \frac{y}{(y+\theta)^2}, \right) \quad \text{if } y < 1-\theta; \qquad B(x,y) = (x,y) \quad \text{else}$$

Work in progress....