PROBABILISTIC ANALYSES
OF LATTICE REDUCTION ALGORITHMS

Focus on the two–dimensional case

Brigitte Vallée and Antonio Vera
GREYC, CNRS and Université de Caen

– The two–dimensional case is a building block for the general case

– The probabilistic study has two characteristics...

  – It is based on a dedicated modelling,
  dependent on the potential application

  – It uses a dynamical system approach

The general problem of lattice reduction

A lattice of $\mathbb{R}^n$ = a discrete additive subgroup of $\mathbb{R}^n$.

A lattice $\mathcal{L}$ possesses a basis $B := (b_1, b_2, \ldots, b_p)$ with $p \leq n$,

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

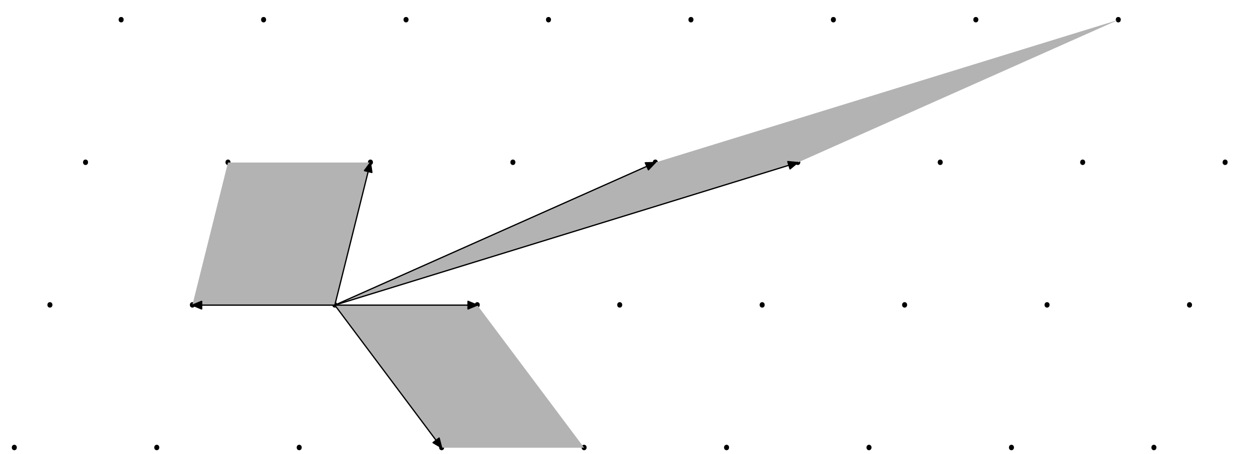
... and in fact, an infinite number of bases....

If now $\mathbb{R}^n$ is endowed with its (canonical) Euclidean structure, there exist bases (called reduced) with good Euclidean properties: their vectors are short enough and almost orthogonal.

Lattice reduction Problem : From a lattice $\mathcal{L}$ given by a basis B, construct from B a reduced basis $\hat{B}$ of $\mathcal{L}$.

Many applications of this problem in various domains:
number theory, arithmetics, discrete geometry..... and cryptology.

In two dimensions.



Summary of the talk

I– The algorithm in the general case

II– Probabilistic study in two dimensions

- complex version of the algorithm
- output distribution,
- output parameters,
- execution parameters.

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

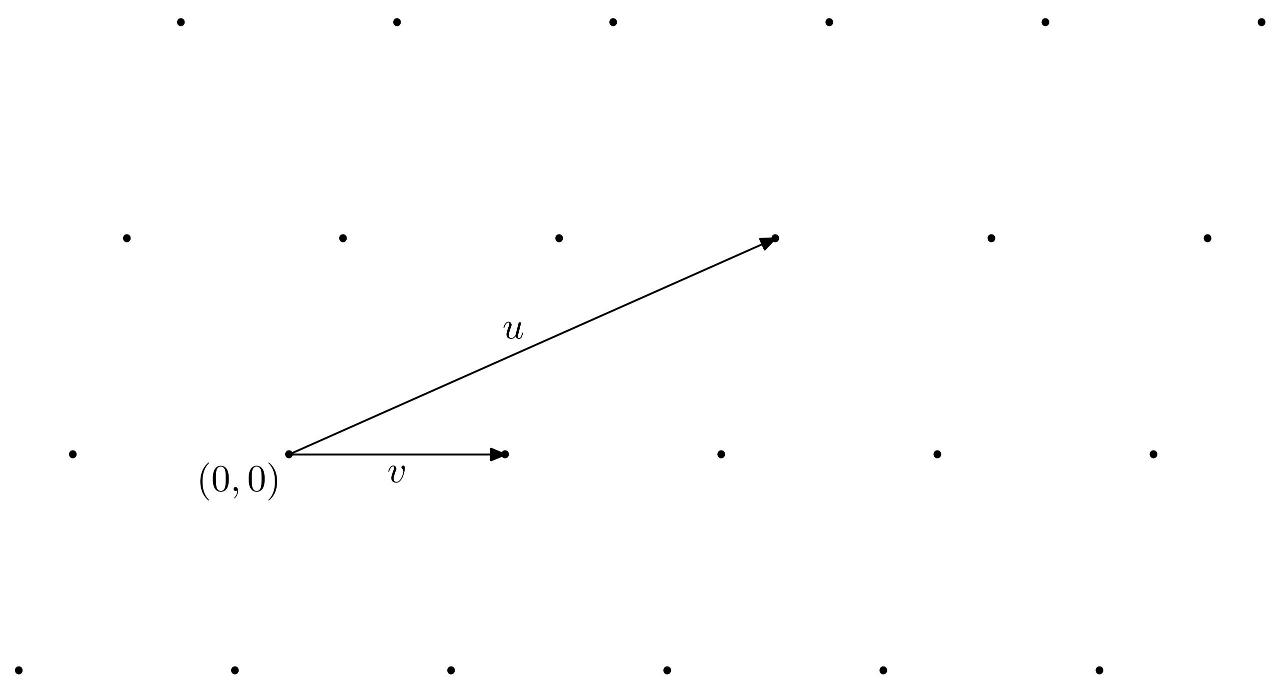
LLL algorithm = Reduction steps on successive (intersecting) local bases

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

Two main operations

— Integer translations – seen as "vectorial" divisions–

$$u = qv + r \quad \text{with} \quad q = q(u,v) = \left\lfloor \frac{u \cdot v}{|v|^2} \right\rceil, \quad \text{so that} \quad \left| \frac{r \cdot v}{|v|^2} \right| \le \frac{1}{2}$$



Here $q = 2$

— Exchanges: if $|r| \le |v|$, then exchange r and v......

LLL (t) $\quad$ $[t > 1]$

Input. A basis B of a lattice $\mathcal{L}$ of dimension p.

Output. A reduced basis $\hat{B}$ of $\mathcal{L}$.

`Gram` computes the basis $B^\star$ and the matrix $\mathcal{P}$.

$i := 1$;

`While` $i < p$ `do`

1– `Diagonal Size-Reduction` (b_{i+1})

2– **Test** if local basis U_i is `reduced` : Is $|v_i| \geq (1/t)|u_i|$?

if yes : `Other-size-reduction` (b_{i+1})

$i := i + 1$;

if not: `Exchange` b_i and b_{i+1}

`Recompute` $(B^\star, \mathcal{P})$;

`If` $i \neq 1$ `then` $i := i - 1$;

Main parameters of interest for the LLL(t) 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 $\det \mathcal{L}$:

$$\lambda(\mathcal{L}) \in [a, A\sqrt{p}], \qquad \det \mathcal{L} \in [a^p, A^p]$$

Three actions of the algorithm.

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

— 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,

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

Upper bounds for output parameters:

exponential wrt dimension p

the Hermite defect $\quad \gamma(B) := \dfrac{|\hat{b}_1|^2}{(\det \mathcal{L})^{2/p}} \quad \leq s^{p-1}$

the length defect $\quad \theta(B) := \dfrac{|\hat{b}_1|}{\lambda(\mathcal{L})} \quad \leq s^{p-1}$

the orthogonality defect $\quad \rho(B) := \dfrac{\prod_{i=1}^{p} |\hat{b}_i|}{\det \mathcal{L}} \quad \leq s^{p(p-1)/2}$

Upper bounds for the number of iterations K:

quadratic wrt dimension p

$$K \leq p^2 \log_t \frac{A}{a}, \qquad K \leq p^2 \log_t \frac{N\sqrt{p}}{\lambda(\mathcal{L})},$$

with $\quad a := \min \ell_i, \quad A := \max \ell_i, \quad N := \max |b_i|^2$

Previous slide: Study of the worst-case.

the LAREDA project is interested in the average–case,

more generally in a probabilistic study of the algorithm:

a more realistic study!

Are bounds in the average–case of the same type

as the bounds in the worst–case?

This answer a priori depends on the type of input bases...

which depends itself on the potential application....

for instance: cryptology, discrete geometry, modular arithmetics, etc

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 $B^{(p)} := (b_i^{(p)})$

already size-reduced with small Siegel ratios

associated to matrices with

$$m_{i,j}^{(p)} = \text{rand}\left(-\frac{1}{2}, \frac{1}{2}\right), \qquad r_i^{(p)} \to 0 \qquad \text{for } i, p \to \infty$$

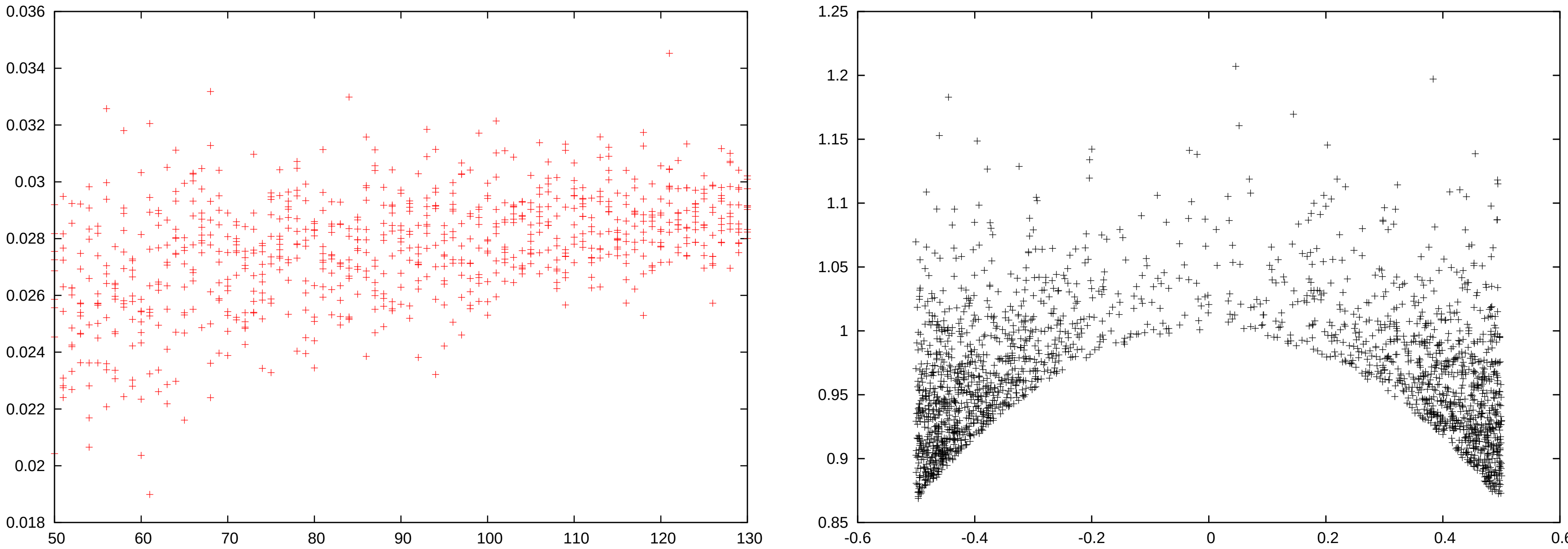
Experimental mean values versus proven upper bounds [Nguyen and Stehlé]

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)	$1/\alpha$	α^{p-1}	$\Theta(Mp^2)$
“Useful ” lattice bases Random knapsack–shape bases (Experimental mean values)	$1/\alpha$	α^{p-1}	$\Theta(Mp)$

The execution parameters depend on the type of the lattice basis.
The output configuration does not depend neither on index i nor on the type of bases and remains “exponential wrt p”.

What about the experimental value α?

Experiments on the LLL Alg. [Nguyen and Stehlé]



On the left, experimental results for $\log_2 \gamma$. The experimental value of parameter $[1/(2p)]\,\mathbb{E}[\log_2 \gamma]$ is close to 0.03, so that α is close to 1.04.

On the right, the output distribution of "local bases" shows an accumulation in the "corners", with $\mathbb{E}[\frac{1}{\hat{y}}] \sim 0.94$

I– The algorithm in the general case

II– Probabilistic study in two dimensions

- complex version of the algorithm
- output distribution,
- output parameters,
- execution parameters.

Three main facts for Lattice Reduction in two dimensions.

– The existence of a minimal basis (formed with two minima)

– A characterization of a minimal basis

– An efficient algorithm which finds it.

Up to an isometry, the lattice $\mathcal{L}$ is a subset of $\mathbb{R}^2$ or..... $\mathbb{C}$.

To a pair $(u, v) \in \mathbb{C}^2$, with $u \neq 0$, we associate a unique $z \in \mathbb{C}$:

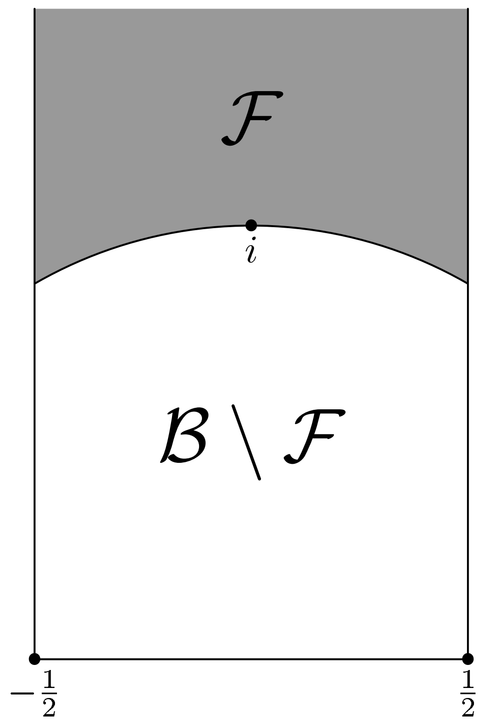
$$z := \frac{v}{u} = \frac{(u \cdot v)}{|u|^2} + i\frac{\det(u, v)}{|u|^2}.$$

Up to a similarity, the lattice $\mathcal{L}(u, v)$ becomes $\mathcal{L}(1, z) =: L(z)$

Positive basis (u, v)	$\det(u, v) > 0$	$\Im z > 0$
Acute basis (u, v)	$(u \cdot v) \geq 0$	$\Re z \geq 0$
Skew basis (u, v)	$\lvert\det(u, v)\rvert$ small wrt to $\lvert u\rvert^2$	small $\lvert\Im z\rvert$

Characterization of minimal bases.

A positive basis (u, v) is minimal iff $z = \dfrac{v}{u} \in \mathcal{F}$



$$\mathcal{B} := \{z; \quad |\Re(z)| \le 1/2\}$$

$$\mathcal{F} := \{z; \quad |z| \ge 1, \ |\Re(z)| \le 1/2, \}$$

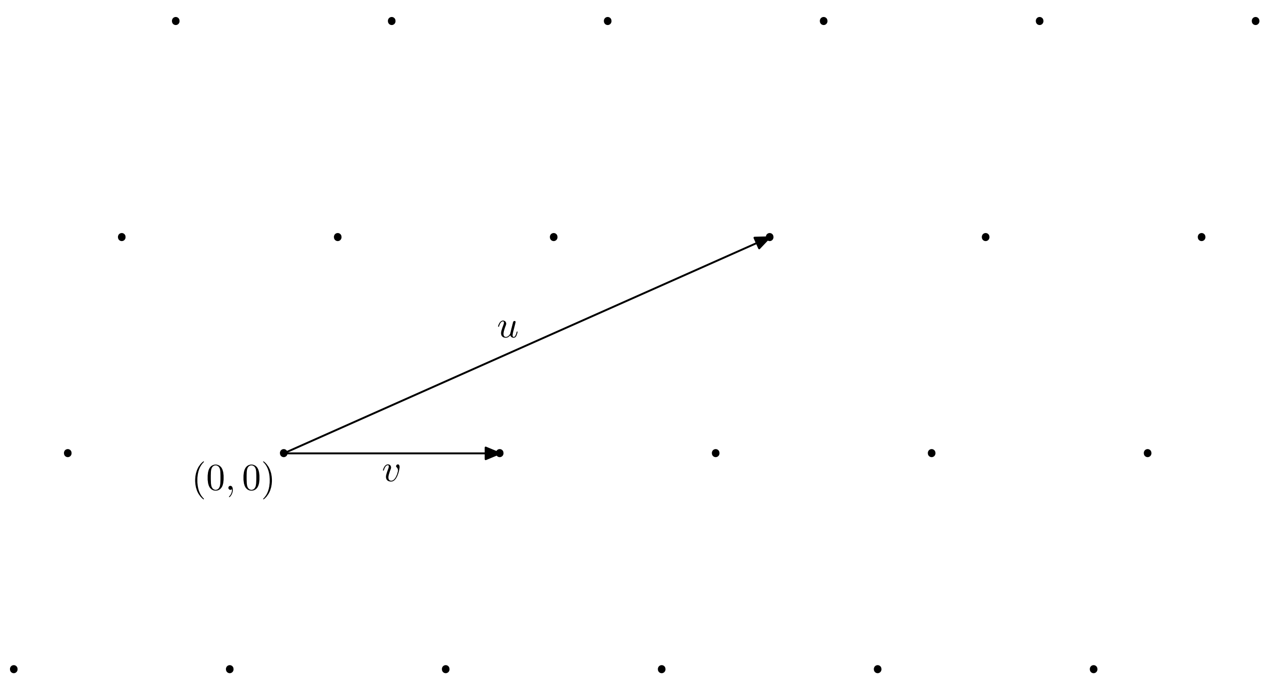
Vectorial version:

$$|v| \ge |u|, \qquad \frac{|(u.v)|}{|u|^2} \le \frac{1}{2}$$

The Gauss algorithm is an extension of the Euclid algorithm.

It performs integer translations – seen as "vectorial" divisions–

$$u = qv + r \quad \text{with} \quad q = \left\lfloor \Re\left(\frac{u}{v}\right)\right\rceil = \left\lfloor \frac{u \cdot v}{|v|^2} \right\rceil, \quad \left|\Re\left(\frac{r}{v}\right)\right| \le \frac{1}{2}$$



Here $q = 2$

The Gauss algorithm is an extension of the Euclid algorithm.

It performs integer translations – seen as "vectorial" divisions–, and exchanges.

Euclid's algorithm	Gauss' algorithm
Division between real numbers $u = qv + r$ with $q = \left\lfloor \frac{u}{v} \right\rceil$ and $\left\lvert \frac{r}{v} \right\rvert \leq \frac{1}{2}$	Division between complex vectors $u = qv + r$ with $q = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil$ and $\left\lvert \Re\left(\frac{r}{v}\right) \right\rvert \leq \frac{1}{2}$
Division + exchange $(v, u) \to (r, v)$ "read" on $x = v/u$ $U(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil$	Division + exchange $(v, u) \to (r, v)$ "read" on $z = v/u$ $U(z) = \frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right) \right\rceil$
Stopping condition: $x = 0$	Stopping condition: $z \in \mathcal{F}$

An execution of the Gauss Algorithm

– On the input (u, v) with $z = \dfrac{v}{u} \in \mathcal{B} \setminus \mathcal{F}$,

– The algorithm begins with vectors $(v_0 := u, v_1 := v)$,

it computes the sequence of divisions $v_{i-1} = q_i v_i + v_{i+1}$;

it produces vectors $(v_0, v_1, \ldots, v_p, v_{p+1})$ and quotients q_i,

– and obtains the output basis $(\hat{u} = v_p, \hat{v} = v_{p+1})$ with $\hat{z} = \dfrac{\hat{v}}{\hat{u}} \in \mathcal{F}$

Parameters of interest – of two types– describe the execution or the output

First: **execution parameters.**

Number of iterations $P(u, v)$

(Central) Bit–complexity $B(u, v) := \displaystyle\sum_{i=1}^{P(u,v)} \ell(q_i) \cdot \ell(|v_i|^2)$

An execution of the Gauss Algorithm

– On the input (u, v) with $z = \dfrac{v}{u} \in \mathcal{B} \setminus \mathcal{F}$,

– The algorithm begins with vectors $(v_0 := u, v_1 := v)$,

it computes the sequence of divisions $v_{i-1} = q_i v_i + v_{i+1}$;

it produces vectors $(v_0, v_1, \ldots, v_p, v_{p+1})$ and quotients q_i,

– and obtains the output basis $(\hat{u} = v_p, \hat{v} = v_{p+1})$ with $\hat{z} = \dfrac{\hat{v}}{\hat{u}} \in \mathcal{F}$

Parameters of interest – of two types– describe the execution or the output

The Gram–Schmidt **output** basis $(\hat{u}, \hat{v}^\star)$ is described with three parameters.

The first minimum λ and the Hermite defect γ are classical. The rôle of "the Gram–Schmidt second minimum" μ is central inside LLL.

$$\lambda(u, v) := |\hat{u}|, \qquad \mu(u, v) := |\hat{v}^\star|, \qquad \gamma(u, v) := \frac{|\hat{u}|}{|\hat{v}^\star|}.$$

Two main classes of probabilistic models....

described with their density $z \mapsto \nu(z)$ which only depends on $y := \Im z$

– The model with fixed determinant $\Im z = y_0$ (Ajtai bases)

$$\nu(z) \text{ proportional to } \mathbf{1}_{y=y_0}(z).$$

– The model with valuation r (random ball model)

$$\nu(z) \text{ proportional to } |\Im z|^r, \quad (\text{with } r > -1).$$

When $y_0 \to 0$ or $r \to -1$,

– these models give more weight to difficult instances:

complex numbers z with small $\Im z$, [skew bases]

– they provide a transition to the one–dimensional model [$\Im z = 0$]

Probabilistic Study of Execution parameters.

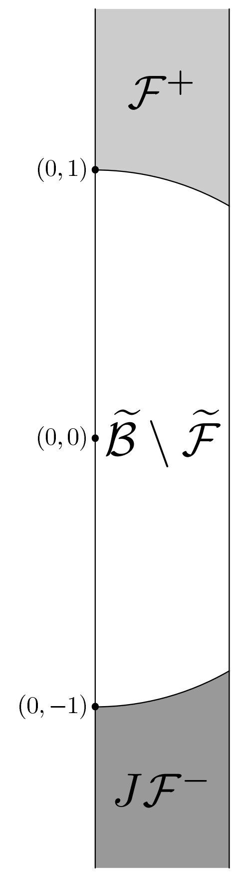
Easier with the acute version

which deals with the transformation $\tilde{U}$ and the fundamental domain $\tilde{\mathcal{F}}$.

$$\tilde{U}(z) := \epsilon\left(\frac{1}{z}\right)\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil\right)$$

with $\quad \epsilon(z) := \mathrm{sign}(\Re(z) - \lfloor \Re(z) \rceil),$

$$\widetilde{\mathcal{F}} := \mathcal{F}^+ \cup J\mathcal{F}^-$$



$$\tilde{U}(z) := \epsilon\left(\frac{1}{z}\right)\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil\right) \quad \text{with} \quad \epsilon(z) := \mathrm{sign}(\Re(z) - \lfloor \Re(z) \rceil)$$

AGAUSS = COREGAUSS followed with FINALGAUSS (at most 2 iterations).

COREGAUSS(z)

Input. A complex number in $\mathcal{D}$.

Output. A complex number in $\tilde{\mathcal{B}} \setminus \mathcal{D}$.

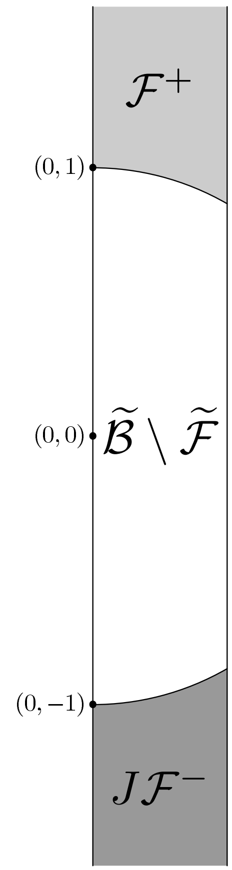
`While` $z \in \mathcal{D}$ `do` $z := \tilde{U}(z)$;

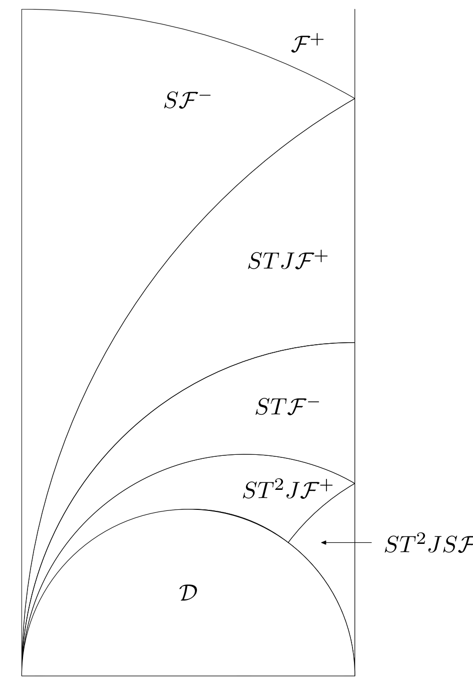
FINALGAUSS(z)

Input. A complex number in $\tilde{\mathcal{B}} \setminus \mathcal{D}$.

Output. A complex number in $\tilde{\mathcal{F}}$.

`While` $z \notin \tilde{\mathcal{F}}$ `do` $z := \tilde{U}(z)$





$S(z) = 1/z$, $T(z) = z + 1$

$J(z) = -z$

The CoreGauss Alg. is the central part of the AGauss Alg.

$$\text{Since} \quad \mathcal{D} = \text{ disk of diameter } [0, 1/2] = \{z; \quad \Re\left(\frac{1}{z}\right) \geq 2\},$$

the CoreGauss Alg uses at each step a quotient $(q, \epsilon) \geq (2, +1)$

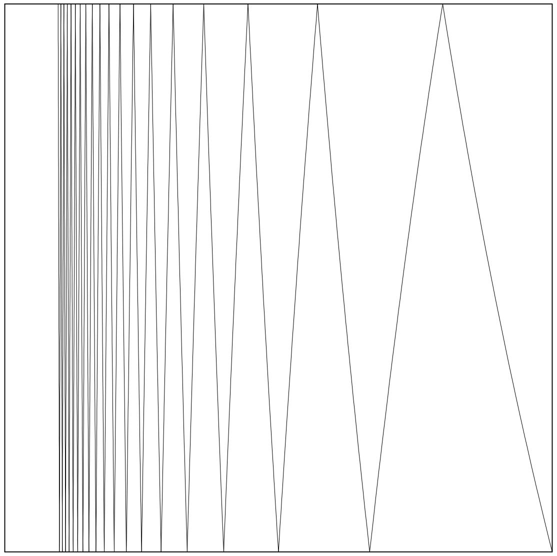
Exact generalisation

of the Centered Euclid Algorithm,

which deals with the map

$$[0, 1/2] \longrightarrow [0, 1/2],$$

$$x \mapsto \epsilon\left(\frac{1}{x}\right) \left(\frac{1}{x} - \left\lfloor \Re\left(\frac{1}{x}\right) \right\rceil\right)$$



The graph of the DS

of the Centered Euclid Alg.

The CoreGauss Alg. is regular and has a nice structure. It uses at each step a LFT of $\mathcal{H} := \{z \mapsto \dfrac{1}{q+\epsilon z}; \quad (q,\epsilon) \geq (2,+1)\}$

Study of its number of iterations R

[Daudé, Flajolet, Vallée (94, then 97)]

The domain $[R \geq k+1]$ is a union of disjoint disks,

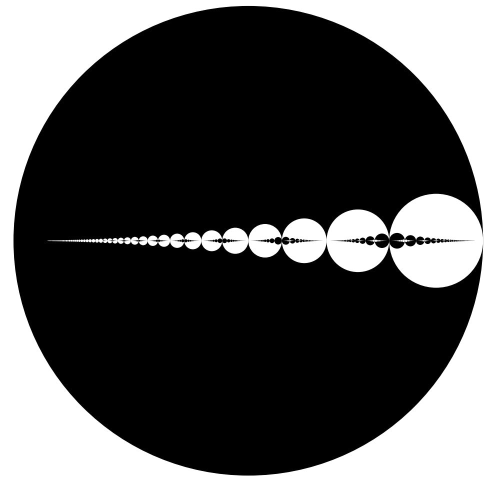
$$[R \geq k+1] = \bigcup_{h \in \mathcal{H}^k} h(\mathcal{D}),$$

For any valuation r,
R follows asymptotically a geometric law
with a ratio $\chi(2+r)$.

$$\mathbb{P}_{(r)}[R \geq k] \sim C_r \, \chi(2+r)^k$$

$$\chi(2) \sim 0.07738$$

When $r \to -1$, then $1 - \chi(2+r) \sim \dfrac{\pi^2}{6 \log \phi}(r+1)$.



The domains $[R = k]$ alternatively in black and white

Output distribution of the Gauss **algorithm.** [Vallée and Vera, 2007]

For an initial density of valuation r,

the output density on $\mathcal{F}$ is proportional to $F_{2+r}(x,y) \cdot \eta(x,y)$,

where η is the density of "random lattices"

and $F_s(x,y)$ is closely related to the classical Eisenstein series

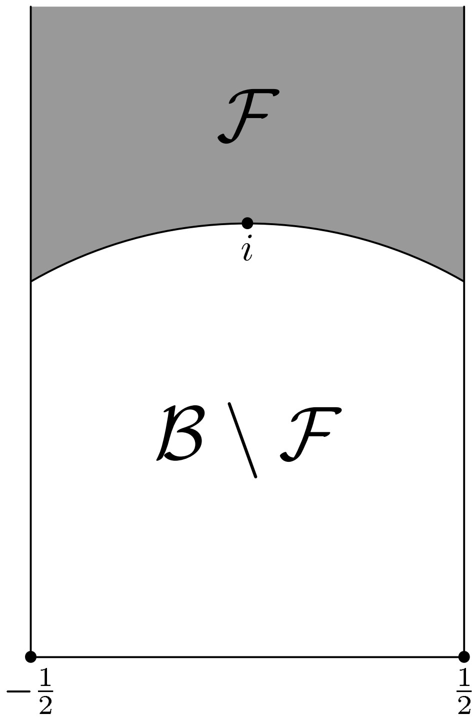
$$E_s(x,y) := \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{y^s}{|cz+d|^{2s}} = \zeta(2s) \cdot \left[F_s(x,y) + y^s\right].$$

When $r \to -1$, the output distribution relative to the input distribution of valuation r tends to the distribution of random lattices.

Output Parameters

for describing the output Gram–Schmidt basis.

Output parameter γ: the Hermite defect.



For an initial basis (u, v)
with an input $z := v/u$,
and an output $\hat{z} \in \mathcal{F}$,
the parameter $\gamma(u, v)$ satisfies

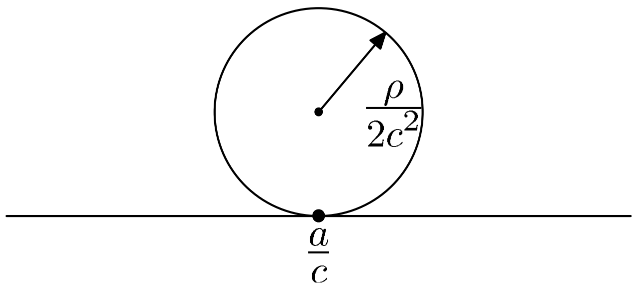
$$\gamma(u, v) := \frac{|\hat{u}|}{|\hat{v}^\star|} = \frac{|\hat{u}|^2}{\det \mathcal{L}} = \frac{1}{\hat{y}}$$

Then $\gamma(u, v) \leq \dfrac{2}{\sqrt{3}}$

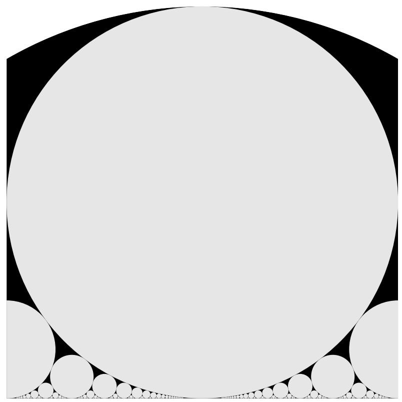
Output parameter γ [Laville, Vallée, Vera]

The domain $\{z;\ \gamma(z) \le \rho\}$ is described with Ford disks $\mathtt{Fo}(\frac{a}{c}, \rho)$,

$$\{z;\ \gamma(z) \le \rho\} = \{z;\ \hat{y} \ge \frac{1}{\rho}\} = \bigcup_{\frac{a}{c} \in [-\frac{1}{2}, \frac{1}{2}]} \mathtt{Fo}(\frac{a}{c}, \rho).$$



$\mathtt{Fo}(\frac{a}{c}, \rho)$



The domain $\{z;\ \gamma(z) \ge 1\}$ [in black]

For a density of valuation r,

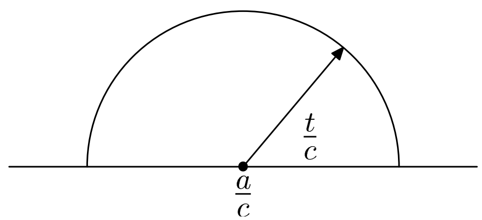
– Estimate of $\mathbb{P}_{(r)}[\gamma(z) \le \rho]$ as a function of ρ and r.

– Estimate of the "corner probability" $\mathbb{P}_{(r)}[\gamma(z) \ge 1]$

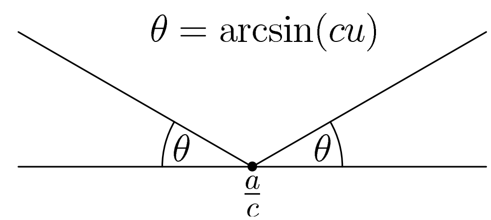
Output parameters λ and μ (Laville, Vallée, Vera, 1994 then 2007).

The domains $\Lambda(t) := \{z;\ \lambda(z)\ \le t\}$ and $M(u) := \{z\ \ \mu(z)\ \le u\}$ are described with Farey disks $\mathtt{Fa}(\frac{a}{c}, t)$ and angular sectors $\mathtt{Se}(\frac{a}{c}, u)$

$\mathtt{Fa}(\frac{a}{c}, t)$



$\mathtt{Se}(\frac{a}{c}, u)$

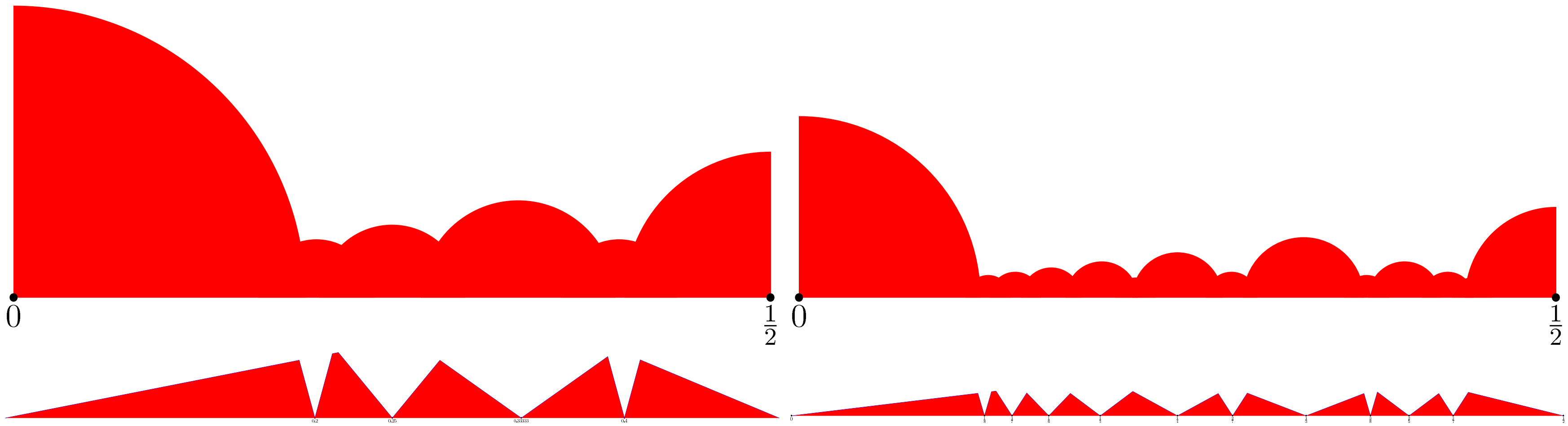


Consider the set $\mathcal{Q}(t)$ of rationals with denominator at most $1/t$.
Consider the vertical strip $\langle \frac{a}{c}, \frac{b}{d} \rangle$,
relative to two successive elements $\frac{a}{c}, \frac{b}{d}$ of $\mathcal{Q}(t)$.

Then, the intersections of $\Lambda(t)$ and $M(t)$ with the strip $\langle \frac{a}{c}, \frac{b}{d} \rangle$ are

$$\Lambda(t) \bigcap \langle \tfrac{a}{c}, \tfrac{b}{d} \rangle = \mathtt{Fa}_{+}(\tfrac{a}{c}, t) \bigcup \mathtt{Fa}_{-}(\tfrac{b}{d}, t) \bigcup \mathtt{Fa}(\tfrac{a+b}{c+d}, t)$$

$$M(t) \bigcap \langle \tfrac{a}{c}, \tfrac{b}{d} \rangle = \mathtt{Se}(\tfrac{a}{c}, t) \bigcap \mathtt{Se}(\tfrac{b}{d}, t) \bigcap \mathtt{Se}(\tfrac{b-a}{d-c}, t).$$



The description of domains $\Lambda(t) := \{z; \quad \lambda(z) \le t\}$ (on the top)

and $M(t) := \{z; \quad \mu(z) \le t\}$ (on the bottom)

for $t = 0.193$ (on the left) for $t = 0.12$ (on the right)

Involves rationals of the form

$\frac{a}{c}$ with $c \le 4$ (on the left) and $\frac{a}{c}$ with $c \le 8$ (on the right)

Distribution functions for parameters λ and μ (Vallée and Vera 2007)

For a density of valuation r,

various regimes for λ according to r, but always the same regime for μ.

$$\begin{array}{lcllr}
\mathbb{P}_{(r)}[\lambda(z) \le t] & = & \Theta(t^{r+2}) & \text{for} & r > 0, \\
\mathbb{P}_{(r)}[\lambda(z) \le t] & = & \Theta(t^2 |\log t|) & \text{for} & r = 0, \\
\mathbb{P}_{(r)}[\lambda(z) \le t] & = & \Theta(t^{2r+2}) & \text{for} & r < 0, \\
\mathbb{P}_{(r)}[\mu(z) \le u] & = & \Theta(u^{2r+2}). & &
\end{array}$$

Conclusion.

A probabilistic analysis of the Gauss algorithm,

the lattice reduction algorithm in two dimensions.

A first step towards....

the probabilistic analysis of lattice reduction alg. in the general case.

The main purpose of the LAREDA project...

A variant for the LLL Algorithm... [Villard (92)]

The ODD–EVEN version is a parallel version of the LLL algorithm with two phases,

– The ODD PHASE performs (in parallel) the GAUSS Alg. on all boxes of odd indices,

– The EVEN PHASE performs (in parallel) the GAUSS Alg. on all boxes of even indices

Between them, the (new) inputs of the Even Phase are computed from the (old) ouputs of the previous Odd Phase...

The Odd-Even Algorithm.

Odd–Even LLL (t) $[t > 1]$

Input. A basis B of a lattice $\mathcal{L}$ of dimension p.
Output. A reduced basis $\hat{B}$ of $\mathcal{L}$.

`Gram` computes the basis $B^\star$ and the matrix $\mathcal{P}$.
`While` B is not reduced `do`
  `Odd Phase` (B):= `Phase`$(B, 0)$;
  `Even Phase` (B):= `Phase`$(B, 1)$;

Phase(B, ϵ)
`For` $i = 1$ to $\lfloor (n-\epsilon)/2 \rfloor$ `do`
  `Diagonal-size-reduction` $(b_{2i+\epsilon})$;
  $\mathcal{M}_i$:= t–AGauss $(U_{2i+\epsilon-1})$;
  $(b_{2i+\epsilon-1}, b_{2i+\epsilon}) := (b_{2i+\epsilon-1}, b_{2i+\epsilon})^t \mathcal{M}_i$;
`For` $i = 1$ to n `do` `Other-size-reduction` (b_i);
`Recompute` $B^\star, \mathcal{P}$;

$$
\mathcal{P} := \begin{array}{c} \\ \vdots \\ b_{i-2} \\ b_{i-1} \\ b_i \\ b_{i+1} \\ \vdots \end{array}
\begin{array}{c}
\begin{array}{cccccc} \dots & b^\star_{i-2} & b^\star_{i-1} & b^\star_i & b^\star_{i+1} & \dots \end{array} \\
\begin{pmatrix}
\dots & \dots & \dots & \dots & \dots & \dots \\
\dots & 1 & 0 & \dots & \dots & \dots \\
\dots & m_{i-1,i-2} & 1|1 & 0 & \dots & \dots \\
\dots & \dots & m_{i,i-1} & 1|1 & 0 & \dots \\
\dots & \dots & \dots & m_{i+1,i} & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array}
$$

Two **contiguous** "odd" local bases : the green one and the red one. After reduction of the two bases, there are a new $|b^\star_{i-1}| = \mu$ and a new $|b^\star_i| = \lambda$. The initial Siegel ratio for the blue basis in the next Even Phase is

$$
r_{i-1} := \frac{\ell_i}{\ell_{i-1}} = \frac{\lambda}{\mu}
$$

$\Rightarrow$ Importance of the parallel study of the two parameters λ and μ.

Execution Parameters: Instance of a Dynamical Analysis.

The set $\mathcal{H} = \{z \mapsto \frac{1}{q+\epsilon z}; \quad (q,\epsilon) \geq (2,+1)\}$

describes one step of the Euclid Alg. or the CoreGauss Alg.

For studying cost $q \mapsto c(q)$, a weighted transfer operator is used,

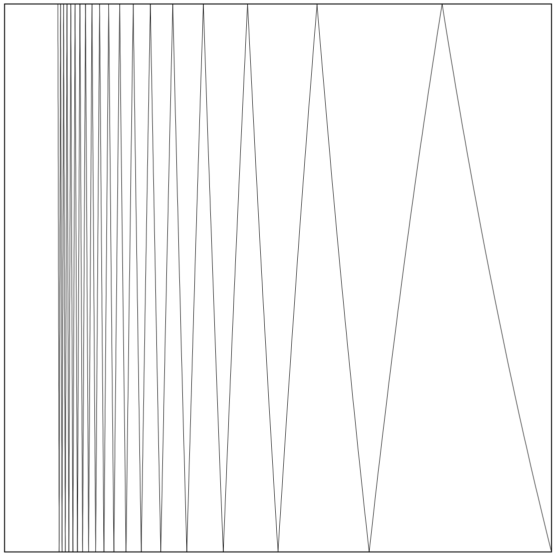
$$\mathbf{H}_{s,w,(c)}[f](x) := \sum_{(q,\epsilon)\geq(2,1)} \frac{\exp[wc(q)]}{(q+\epsilon x)^{2s}} \cdot f\left(\frac{1}{q+\epsilon x}\right).$$

For $s = 1, w = 0$, this is the density transformer.
All the recent results about the Euclid Algorithm
use this transfer operator

as a "generating operator":

it generates the generating functions of interest.

This is the Dynamic Analysis Method



Dynamical analysis of the Gauss algorithm

For the Gauss Alg, we use an extension of the transfer operator which deals with functions of two variables

$$\underline{\mathbf{H}}_{s,w,(c)}[F](u,v) := \sum_{(q,\epsilon)\geq(2,1)} \frac{\exp[wc(q)]}{(q+\epsilon u)^s(q+\epsilon v)^s} F\left(\frac{1}{q+\epsilon u}, \frac{1}{q+\epsilon v}\right).$$

All the constants which occur in the analysis are spectral constants, in particular the dominant eigenvalue $\chi_{(c)}(s,w)$ of the operator $\underline{\mathbf{H}}_{s,w,(c)}$ which is the same as for the plain operator $\mathbf{H}_{s,w,(c)}$.

The dynamics of the Euclid Algorithm is described with $s=1$.
The dynamics of the Gauss Algorithm is described with $s=2$.
Using a density of valuation r shifts the parameter $s \mapsto s+r$.

Rôle of parameters λ and μ in the LLL-Odd-Even Algorithm

Two contiguous "odd" local bases : the green one and the red one. After reduction of the two bases, there are a new $|b^\star_{i-1}| = \mu$ and a new $|b^\star_i| = \lambda$. The initial Siegel ratio for the blue basis in the next Even Phase is

$$r_{i-1} := \frac{\ell_i}{\ell_{i-1}} = \frac{\lambda}{\mu}$$

$$\mathcal{P} := \begin{array}{c} \\ \vdots \\ b_{i-2} \\ b_{i-1} \\ b_i \\ b_{i+1} \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccccc} \ldots & b^\star_{i-2} & b^\star_{i-1} & b^\star_i & b^\star_{i+1} & \ldots \end{array} \\ \begin{pmatrix} \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & 1 & 0 & \ldots & \ldots & \ldots \\ \ldots & m_{i-1,i-2} & 1|1 & 0 & \ldots & \ldots \\ \ldots & \ldots & m_{i,i-1} & 1|1 & 0 & \ldots \\ \ldots & \ldots & \ldots & m_{i+1,i} & 1 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix} \end{array}$$