Lattice Reduction Algorithms:

EUCLID, GAUSS, LLL

Description and Probabilistic Analysis

Brigitte Vallée
(CNRS and Université de Caen, France)

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

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....

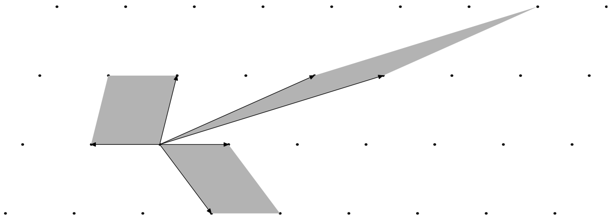
If now $\mathbb{R}^n$ is endowed with its (canonical) Euclidean structure,
there exist bases (called reduced) with good Euclidean properties:
their vectors are short enough and almost orthogonal.

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.

Lattice reduction algorithms in the two dimensional case.



Three main cases,
according to the increasing dimension p of the lattice.

$p = 1$: the Euclid algorithm
computes the greatest common divisor $\gcd(u, v)$

$p = 2$: the Gauss algorithm
computes a minimal basis of a lattice of two dimensions

$p \geq 3$: the LLL algorithm
computes a reduced basis of a lattice of any dimensions.

Each algorithm can be viewed
as an extension of the previous one

Probabilistic Analysis of Algorithms

An algorithm with a set of inputs Ω,
and a parameter (or a cost) C defined on Ω which describes

– the execution of the algorithm (number of iterations, bit–complexity)

– the geometry of the output
(the length of the vectors, their orthogonality)

Gather the inputs wrt to their sizes (here, their number of bits)

$$\Omega_k := \{\omega \in \Omega, \quad \mathrm{size}(\omega) = k\}.$$

Consider a distribution on Ω_k (for instance the uniform distribution),
Study the cost C on Ω_k in a probabilistic way:

Estimate the mean value of C, its variance, its distribution...
in an asymptotic way (for $k \to \infty$)

Main tools for probabilistic analysis of algorithms

1– Interaction between the discrete world and the continuous world.

Three steps.

(a) The discrete algorithm is extended into a continuous process.....
(b) .... which is studied – more easily, using all the analytic tools.
(c) Coming back to the discrete algorithm,
with various principles of transfer from continuous to discrete.

Dimension 1 is different from the other ones $(p \geq 2)$ –more difficult

In any case,
the discrete data are of zero measure amongst the continuous data.

Main tools for probabilistic analysis of algorithms
2– Generating functions ?

A classical tool : Generating functions of various types

$$A(z) := \sum_{n \geq 0} a_n z^n, \qquad \hat{A}(z) := \sum_{n \geq 0} a_n \frac{z^n}{n!}, \qquad \tilde{A}(s) := \sum_{n \geq 1} \frac{a_n}{n^s}$$

Useful when the distribution of data does not change too much
during the execution of the algorithm
(for instance: the Euclid Algorithm on polynomials)

Here, this is not the case .... due to the existence of carries
and the study of the dynamical system underlying the algorithm explains
how the distribution of data evolves during the execution of the algorithm.

This leads to the paradigm of
Dynamical Analysis :=
Analysis of Algorithms + Dynamical Systems

Main tools for probabilistic analysis of algorithms
3- Dynamical Analysis –main principles.

Input.- A discrete algorithm.

Step 1.- Extend the discrete algorithm into a continuous process, i.e. a dynamical system. (X, V) X compact, $V : X \to X$, where the discrete alg. gives rise to particular trajectories.

Step 2.- Study this (continuous) dynamical system, via its generic trajectories. A main tool: the transfer operator.

Step 3.- Coming back to the algorithm: we need proving that the discrete trajectories behave like the generic trajectories.

- Euclid: Use the transfer operator as a generating operator,
  which generates itself ..... the generating functions
- Gauss: Replace areas by number of points

Output.- Probabilistic analysis of the Algorithm.

The Euclid Algorithm: the grand father of all the algorithms.

On the input (u, v), it computes the gcd of u and v,

together with the Continued Fraction Expansion of u/v.

if $v \geq u$, then $u_0 := v;\ u_1 := u$

$$\left\{\begin{array}{ccccccc} u_0 & = & m_1 u_1 & + & u_2 & & 0 < u_2 < u_1 \\ u_1 & = & m_2 u_2 & + & u_3 & & 0 < u_3 < u_2 \\ \ldots & = & \ldots & + & & & \\ u_{p-2} & = & m_{p-1} u_{p-1} & + & u_p & & 0 < u_p < u_{p-1} \\ u_{p-1} & = & m_p u_p & + & 0 & & u_{p+1} = 0 \end{array}\right\}$$

u_p is the gcd of u and v, the m_i's are the digits. p is the depth.

CFE of $\frac{u}{v}$:

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

The Euclidean dynamical system (I).

The trace of the execution of the Euclid Algorithm on (u_1, u_0) is:

$$(u_1, u_0) \to (u_2, u_1) \to (u_3, u_2) \to \ldots \to (u_{p-1}, u_p) \to (u_{p+1}, u_p) = (0, u_p)$$

Replace the integer pair (u_i, u_{i-1}) by the rational $x_i := \dfrac{u_i}{u_{i-1}}$.

The division $u_{i-1} = m_i u_i + u_{i+1}$ is then written as

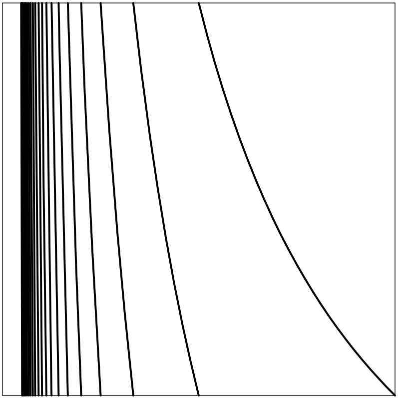
$$x_{i+1} = \frac{1}{x_i} - \left\lfloor \frac{1}{x_i} \right\rfloor \qquad \text{or} \qquad x_{i+1} = V(x_i), \qquad \text{where}$$

$$V : [0,1] \longrightarrow [0,1], \quad V(x) := \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor \quad \text{for} \;\; x \neq 0, \quad V(0) = 0$$

An execution of the Euclidean Algorithm $(x, V(x), V^2(x), \ldots, 0)$

$=$ A rational trajectory of the Dynamical System $([0,1], V)$

$=$ a trajectory that reaches 0.



The Euclidean dynamical system (II).

A dynamical system with a denumerable system of branches $(V_{[m]})_{m\geq 1}$,

$$V_{[m]} :]\frac{1}{m+1}, \frac{1}{m}[\longrightarrow]0,1[, \qquad V_{[m]}(x) := \frac{1}{x} - m$$

The set $\mathcal{H}$ of the inverse branches of V is

$$\mathcal{H} := \{\ h_{[m]} :]0,1[\longrightarrow]\frac{1}{m+1}, \frac{1}{m}[; \qquad h_{[m]}(x) := \frac{1}{m+x}\}$$

The set $\mathcal{H}$ builds one step of the CF's.

The set $\mathcal{H}^n$ of the inverse branches of V^n builds CF's of depth n.

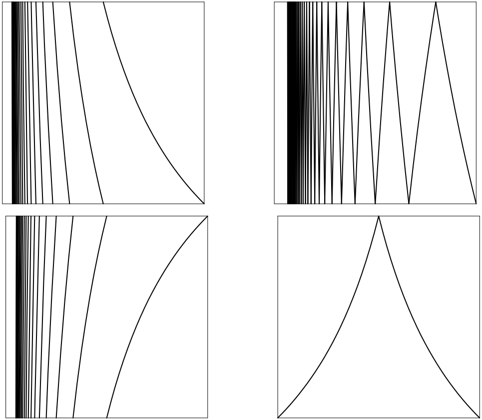
The set $\mathcal{H}^\star := \bigcup \mathcal{H}^n$ builds all the (finite) CF's.

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_p}}}} = h_{[m_1]} \circ h_{[m_2]} \circ \ldots \circ h_{[m_p]}(0)$$

For other Euclidean Algorithms, related to other Euclidean divisions

, replace the rational u/v by a generic real x:

A continuous dynamical system extends each discrete division

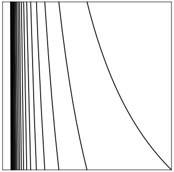


Above, Standard and Centered; On the bottom, By-Excess and Subtractive.

On the bottom, there are indifferent points : $x = 1$ or 0, for which $V(x) = x, |V'(x)| = 1$.

A main tool: the transfer operator.

The density transformer $\mathbf{H}$ expresses the new density f_1 as a function of the old density f_0, as $f_1 = \mathbf{H}[f_0]$.
It involves the set $\mathcal{H}$ of inverse branches of V,



$$\mathbf{H}[f](x) := \sum_{h \in \mathcal{H}} |h'(x)| \cdot f \circ h(x)$$

With a cost $c : \mathcal{H} \to \mathbf{R}^+$, and a parameter s, and extended to $\mathcal{H}^\star$ by additivity, it gives rise to the weighted transfer operator

$$\mathbf{H}_{s,w,(c)}[f](x) := \sum_{h \in \mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x)$$

The main costs of interest for Euclidean Algorithms

– The additive costs, which depend on the digits

$$C(u,v) := \sum_{i=1}^{p} c(m_i)$$

if $c = 1$, then $C :=$ the number of iterations
if $c = \mathbf{1}_{m_0}$, then $C :=$ the number of digits equal to m_0
if $c = \ell$ (the binary length), then $C :=$ the length of the CFE

– The bit complexity (not an additive cost)

$$C(u,v) := \sum_{i=1}^{p} \ell(u_i)\,\ell(m_i)$$

Here, focus on average-case results ($n :=$ input size $:= \log M$)

– For the Standard, Centered Euclidean Algorithms,

– the mean values of costs P, C are linear wrt n,

– the mean bit-complexity is quadratic.

$$\mathbb{E}_n[P] \sim \frac{2\log 2}{h(\mathcal{S})} n, \qquad \mathbb{E}_n[C] \sim \frac{2\log 2}{h(\mathcal{S})} \mu[c]\, n, \qquad \mathbb{E}_n[B] \sim \frac{\log 2}{h(\mathcal{S})} \mu[\ell]\, n^2.$$

– The main constant $h(\mathcal{S})$ is the entropy of the Dynamical System.

A well-defined mathematical object, computable.

$$h(\mathcal{S}) = \frac{\pi^2}{6\log 2} \sim 2.37 \ \ \text{[Standard]}, \quad h(\mathcal{S}) = \frac{\pi^2}{6\log\phi} \sim 3.41 \ \ \text{[Centered]}.$$

– The constant $\mu[c]$ is the mean value of cost c. For the binary length ℓ,

$$\mu(\ell) = 3 + \frac{\log 2}{\log\phi} + \frac{1}{\log\phi} \prod_{k\geq 3} \frac{(2^k-1)\phi^2 + 2\phi}{(2^k-1)\phi^2 - 2}$$

Relation between the transfer operator and the Dirichlet series.

Due to the fact that branches are LFT's,
There is an alternative expression for the Dirichlet series

$$S_C(s) := \sum_{(u,v)\in\Omega} \frac{C(u,v)}{v^{2s}} = (I - \mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} \circ (I - \mathbf{H}_s)^{-1}[1](\eta)$$

as a function of two transfer operators : the weighted one

$$\mathbf{H}_s^{[c]}[f](x) = \sum_{h\in\mathcal{H}} c(h) \cdot |h'(x)|^s \cdot f \circ h(x)$$

and the quasi-inverse $(I - \mathbf{H}_s)^{-1}$ of the plain transfer operator $\mathbf{H}_s$,

$$\mathbf{H}_s[f](x) := \sum_{h\in\mathcal{H}} |h'(x)|^s \cdot f \circ h(x).$$

Singularities of $s \mapsto (I - \mathbf{H}_s)^{-1}$ are related to spectral properties of $\mathbf{H}_s$
..... on a convenient functional space .... which depends on the DS (and the algo)...

We used the general framework

Geometric properties of the Dynamical System

$\Downarrow$

Spectral properties for the Transfer Operator

in a convenient functional space.

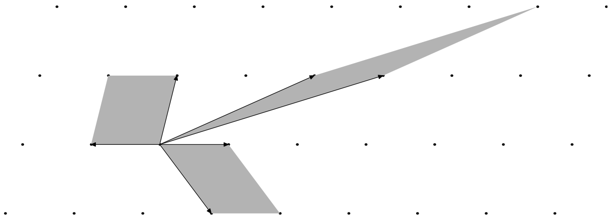
$\Downarrow$

Analytical properties of the (Dirichlet) Gen. Functions

$\Downarrow$

Asymptotic Analysis of the Algorithm

Lattice reduction algorithms in the two dimensional case.



Lattice Reduction in two dimensions.

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 $\mathcal{L}(1, z) =: L(z)$.

All the main notions and main operations in lattice reduction can only be expressed with $z = v/u$.

- Positive basis (u, v) [or $\det(u, v) > 0$] $\rightarrow \Im z > 0$
- Acute basis (u, v) [or $(u.v) \geq 0$] $\rightarrow \Re z \geq 0$
- Skew basis (u, v) [or $|\det(u, v)|$ small wrt $|u|^2$] $\rightarrow \Im z$ small

Three main facts in two dimensions.

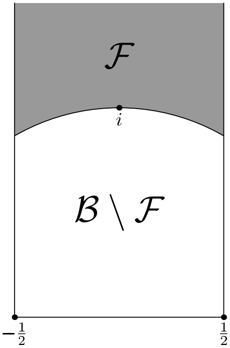
– The existence of an optimal basis = a minimal basis

– A characterization of an optimal basis.

– An efficient algorithm which finds it = The Gauss Algorithm.

Characterization of minimal bases.

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



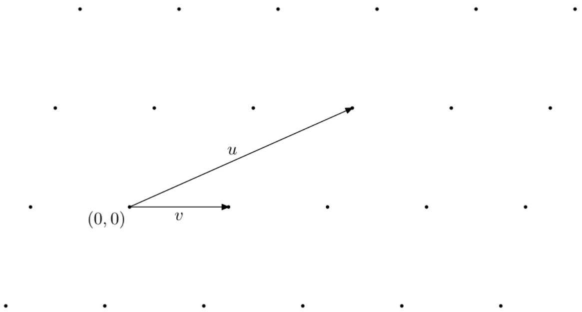
$$\mathcal{B} := \{z; \quad |\Re(z)| \leq 1/2\}$$

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

The Gauss algorithm is an extension of the Euclid algorithm.

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

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



Here $m = 2$

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 $v = mu + r$ with $m = \left\lfloor \frac{u}{v} \right\rceil$ and $\left\lvert \frac{r}{v} \right\rvert \leq \frac{1}{2}$	Division between complex vectors $v = mu + r$ with $m = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil$ and $\left\lvert \Re\left(\frac{r}{v}\right) \right\rvert \leq \frac{1}{2}$
Division + exchange $(v, u) \to (r, v)$ "read" on $x = v/u$ $V(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil$	Division + exchange $(v, u) \to (r, v)$ "read" on $z = v/u$ $V(z) = \frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right) \right\rceil$
Stopping condition: $x = 0$	Stopping condition: $z \in \mathcal{F}$

An essential difference between the two algorithms

– The (continuous) Euclid Algorithm never stops .....

..... except for rationals.

– The (continuous) Gauss Algorithm always stops ....

..... except for irrational flat bases z

for which $\Im z = 0$ and $\Re z \notin \mathbb{Q}$

Difference due to the various "holes":

– The Euclid hole $\{0\}$ is of zero measure

– The Gauss hole $\mathcal{F}$ is a fundamental domain

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 $v_{i-1} = m_i v_i + v_{i+1}$;

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

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

The main parameters of interest describe the execution or the output

First: execution parameters.

Number of iterations $\quad P(u, v)$

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

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 $v_{i-1} = m_i v_i + v_{i+1}$;

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

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

The main parameters of interest describe the execution or the output

Now : output parameters.

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

– the first minimum λ

– the orthogonalized second minimum μ

– the Hermite defect γ

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

$$\lambda^2(u, v) = \frac{y}{\hat{y}}, \qquad \mu^2(u, v) = y\hat{y}, \qquad \gamma(u, v) = \frac{1}{\hat{y}}$$

Probabilistic study in the two dimensional case

To a pair $(u, v) \in \mathbb{C}^2$, 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) [or $\det(u, v) > 0$] $\to \Im z > 0$
- Acute basis (u, v) [or $(u, v) \geq 0$] $\to \Re z \geq 0$
- Skew basis (u, v) [or $|\det(u, v)|$ small wrt $|u|^2$] $\to \Im z$ small

Two complex versions of the Gauss Algorithm,

where all the operations are expressed with $z = v/u$,

PGauss (with positive bases) or AGauss (with acute bases)

Not the same algorithm, but close algorithms,

PGauss used for Output studies, AGauss for Execution studies

A main class of probabilistic models....

The model with valuation r (with $r > -1$)

where the input density $z \mapsto \nu(z)$ only depends on $y := \Im z$

and is proportional to $|\Im z|^r$

When $r \to -1$,

– this model gives more weight to difficult instances:

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

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

The acute version

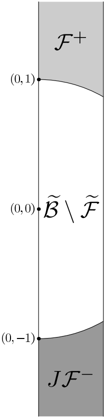
deals with the transformation $\tilde{U}$ and the fundamental domain $\tilde{\mathcal{F}}$.

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

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

The hole is $\tilde{\mathcal{F}} := \mathcal{F}^+ \cup J\mathcal{F}^-$.

$J : z \mapsto -z$



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

$\mathcal{D}$:= disk with diameter $[0, 1/2]$

AGAUSS = CoreGauss followed with FinalGauss (at most 2 iterations).

CoreGauss(z)

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

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

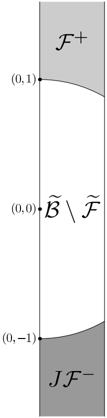
```
While z ∈ D do z := Ũ(z);
```

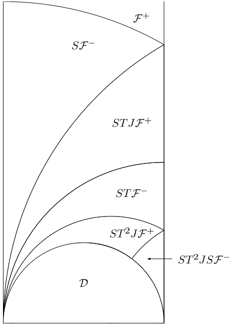
FinalGauss(z)

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

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

```
While z ∉ F̃ do z := Ũ(z)
```





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

$J(z) = -z$

The $\textsc{CoreGauss}$ Alg. is the central part of the $\textsc{AGauss}$ Alg.

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

the $\textsc{CoreGauss}$ Alg uses at each step a quotient $(m, \epsilon) \geq (2, +1)$

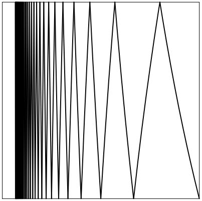
Exact generalisation

of the $\textsc{Centered Euclid}$ Algorithm,

which deals with the map

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

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



The graph of the DS

of the Centered Euclid Alg.

The $\textsc{CoreGauss}$ Alg. is regular and has a nice structure. It uses at

each step a LFT of $\mathcal{H} := \{z \mapsto \frac{1}{m + \epsilon z}; \quad (m, \epsilon) \geq (2, +1)\}$

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,

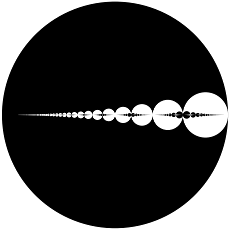
R follows asymptotically a geometric law

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 $1 - \chi(2+r) \sim \frac{\pi^2}{6 \log \phi}(r+1)$.



The domains $[R = k]$

alternatively

in black and white

Bit–complexity. [Vallée and Vera (2007)]

On the set Ω_M of inputs (u, v) with $\ell(|v|^2) = M$, endowed with a density of valuation r, the central execution of the Gauss algorithm has a mean bit–complexity which is linear with respect to size M,

$$\mathbb{E}_{M,(r)}[B] = q(r)M + O_{(r)}(1) \qquad \text{as} \qquad M \to \infty$$

The constant $q(r)$ is the mean value of the additive cost Q relative to the binary length ℓ,

$$Q := \sum_{i=1}^{p} \ell(m_i),$$

wrt the density of valuation r. Q follows an asympt. geometric law.

When $r \to -1$ and $M \to \infty$ with $(r + 1)M \to 1$,

the measure of Ω_M is concentrated near the real axis, and

$$\mathbb{E}_{M,(r)}[B] = O(M^2).$$

The same complexity as the Euclid Alg!

Execution Parameters: Instance of a Dynamical Analysis.

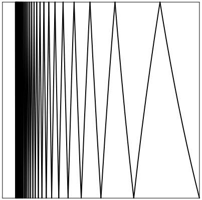
The set $\mathcal{H} = \{z \mapsto \frac{1}{m + \epsilon z}; \quad (m, \epsilon) \geq (2, +1)\}$

describes one step of the EUCLID Alg. or the COREGAUSS Alg.

For studying cost $m \mapsto c(m)$ for the Euclid Algorithm,

a weighted transfer operator is used,

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



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

The GAUSS Alg, is described with an extension of the transfer operator which deals with functions of two variables

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

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 $s \mapsto s+r$.

Output Parameters for describing the output Gram–Schmidt basis.

The three main output parameters,

– the first minimum $\lambda(z) := \lambda(1, z)$,

– the orthogonalized second minimum $\mu(z) := \mu(1, z)$,

– the Hermite defect $\gamma(z) := \gamma(1, z)$

Two steps

– Determination of the "distribution" domains

$$\Gamma(\rho) := \{z;\ \gamma(z) \le \rho\}, \quad \Lambda(t) := \{z;\ \lambda(z)\ \le t\}, \quad M(u) := \{z;\ \mu(z)\ \le u\}$$

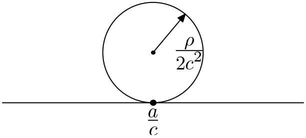
– Computation of the measures of these domains.....

...... in a probabilistic model of valuation r.

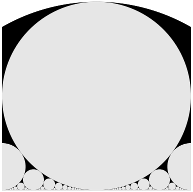
Output parameter γ [Laville, Vallée, Vera]

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

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



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



The domain $\{z;\ \gamma(z) \le 1\}$ [in white]

For $\rho \le 1$, Ford disks are disjoint.

Output accumulation in the corners of the fundamental domain?

The inputs which “fall” in the corners are in black. Their measure depends on the input density. For an initial density of valuation r,
the probability for an output basis to lie on the corners of $\mathcal{F}$ is

$$C(r) := 1 - A_1(r) \cdot \frac{\zeta(2r+3)}{\zeta(2r+4)}.$$

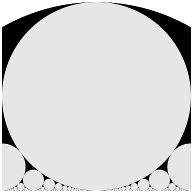
Three main cases of interest for $C(r)$

$$[r \to -1] : \quad 1 - \frac{3}{\pi} \approx 0.045$$

$$[r = 0] : \quad 1 - \frac{3\pi}{2\pi + 3\sqrt{3}} \frac{\zeta(3)}{\zeta(4)} \approx 0.088$$

$$[r \to \infty] : \quad 1 - \sqrt{\frac{\pi}{r}} e^{-3/2}$$

$$[r = 20] \quad \approx 0.911 \quad [r = 100] \quad \approx 0.960$$



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

Output accumulation in the corners of the fundamental domain?

The inputs which "fall" in the corners are in black. Their measure depends on the input density. For an initial density of valuation r,
the probability for an output basis to lie on the corners of $\mathcal{F}$ is

$$C(r) := 1 - A_1(r) \cdot \frac{\zeta(2r+3)}{\zeta(2r+4)}.$$

Three main cases of interest for $C(r)$

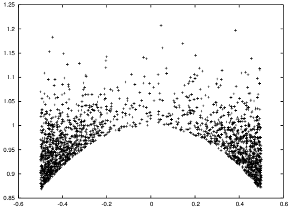
$$[r \to -1]: \quad 1 - \frac{3}{\pi} \approx 0.045$$

$$[r = 0]: \quad 1 - \frac{3\pi}{2\pi + 3\sqrt{3}} \frac{\zeta(3)}{\zeta(4)} \approx 0.088$$

$$[r \to \infty]: \quad 1 - \sqrt{\frac{\pi}{r}} e^{-3/2}$$

$[r = 20] \quad \approx 0.911 \quad [r = 100] \quad \approx 0.960$

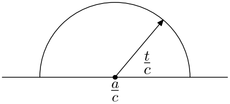
To be compared with.....

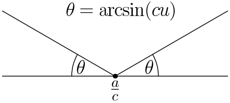


The accumulation in the "corners" for the LLL output distribution of "local bases"

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

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

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

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

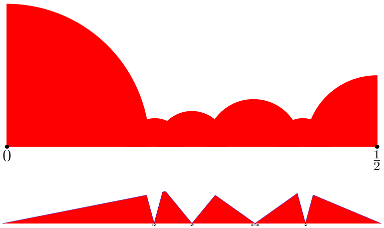
Consider the set $\mathcal{Q}(t)$ of rationals with denominator at most $1/t$.
Consider the vertical strip $\langle \frac{a}{c}, \frac{b}{d} \rangle$,

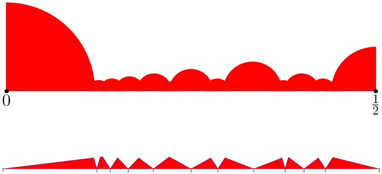
relative to two successive elements $\frac{a}{c}, \frac{b}{d}$ of $\mathcal{Q}(t)$.

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 $\Lambda(t) := \{z; \quad \lambda(z) \leq t\}$ (on the top)

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

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

Involves rationals of the form

$\dfrac{a}{c}$ with $c \leq 4$ (on the left) and $\dfrac{a}{c}$ with $c \leq 8$ (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.

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

In the case when $r \ge 0$ and $t \to 0$, precise estimates for parameter λ,

$$\mathbb{P}_{(r)}[\lambda(z) \le t] \quad \sim_{t\to 0} \quad A_2(r)\frac{\zeta(r+1)}{\zeta(r+2)} \cdot t^{r+2} \quad \text{for} \quad r > 0,$$

$$\mathbb{P}_{(r)}[\lambda(z) \le t] \quad \sim_{t\to 0} \quad A_2(0)\frac{1}{\zeta(2)} t^{2}|\log t| \quad \text{for} \quad r = 0.$$

where A_2 involves various Γ functions....

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".

Here, in two dimensions,

$$\eta(x,y) = \frac{3}{\pi}\frac{1}{y^2}$$

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

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

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