Lattice Reduction Algorithms:

EUCLID, GAUSS, LLL

Description and Probabilistic Analysis

Brigitte Vallée
(CNRS and Université de Caen, France)

Mauritanie, February 2016

The general problem of lattice reduction

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

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

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

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

If now $\mathbb{R}^p$ 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 $\widehat{B}$ of $\mathcal{L}$.

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

The general problem of lattice reduction

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

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

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

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

If now $\mathbb{R}^p$ 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 $\widehat{B}$ of $\mathcal{L}$.

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

The general problem of lattice reduction

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

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

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

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

If now $\mathbb{R}^p$ 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 $\widehat{B}$ of $\mathcal{L}$.

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

The general problem of lattice reduction

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

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

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

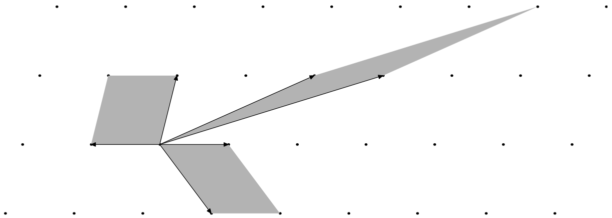
... and in fact, an infinite number of bases....

If now $\mathbb{R}^p$ 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 $\widehat{B}$ 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 n of the lattice.

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

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

$n \geq 3$: 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

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

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

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

$n \geq 3$: 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

Three main cases,

according to the increasing dimension n of the lattice.

$n = 1$: the Euclid algorithm

computes the greatest common divisor $\gcd(u, v)$

$n = 2$: the Gauss algorithm

computes a minimal basis of a lattice of two dimensions

$n \geq 3$: the LLL algorithm

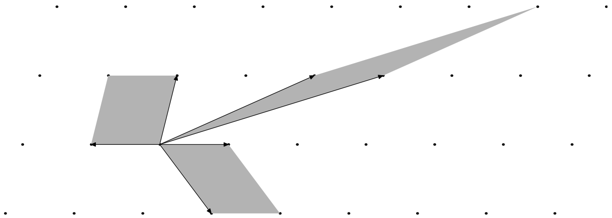
computes a reduced basis of a lattice of any dimensions.

Each algorithm can be viewed

as an extension of the previous one

II- The Gauss 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 $z \in \mathbb{C}$:

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

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

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 $z \in \mathbb{C}$:

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

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

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 $z \in \mathbb{C}$:

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

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

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 $z \in \mathbb{C}$:

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

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.

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.

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.

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.

Successive minima.

First minimum of $\mathcal{L}$:

a nonzero vector $u \in \mathcal{L}$ that has a smallest Euclidean norm;

$$||u|| \leq ||v|| \quad \forall v \in \mathcal{L}$$

the length of a first minimum of $\mathcal{L}$ is denoted by $\lambda_1(\mathcal{L})$.

Second minimum of $\mathcal{L}$:

any shortest vector amongst the vectors of $\mathcal{L}$ that are linearly independent of a first minimum u;

the length of a second minimum is denoted by $\lambda_2(\mathcal{L})$.

A basis is minimal if it comprises a first and a second minimum.

For instance, the basis on the left of Figure is minimal.

Successive minima.

First minimum of $\mathcal{L}$:

a nonzero vector $u \in \mathcal{L}$ that has a smallest Euclidean norm;

$$||u|| \leq ||v|| \quad \forall v \in \mathcal{L}$$

the length of a first minimum of $\mathcal{L}$ is denoted by $\lambda_1(\mathcal{L})$.

Second minimum of $\mathcal{L}$:

any shortest vector amongst the vectors of $\mathcal{L}$ that are linearly independent of a first minimum u;

the length of a second minimum is denoted by $\lambda_2(\mathcal{L})$.

A basis is minimal if it comprises a first and a second minimum.

For instance, the basis on the left of Figure is minimal.

Successive minima.

First minimum of $\mathcal{L}$:

a nonzero vector $u \in \mathcal{L}$ that has a smallest Euclidean norm;

$$||u|| \leq ||v|| \quad \forall v \in \mathcal{L}$$

the length of a first minimum of $\mathcal{L}$ is denoted by $\lambda_1(\mathcal{L})$.

Second minimum of $\mathcal{L}$:

any shortest vector amongst the vectors of $\mathcal{L}$ that are linearly independent of a first minimum u;

the length of a second minimum is denoted by $\lambda_2(\mathcal{L})$.

A basis is minimal if it comprises a first and a second minimum.

For instance, the basis on the left of Figure is minimal.

Characterization of a minimal acute basis.

Let (u, v) be an acute basis. The conditions (a) and (b) are equivalent:

(a) the basis (u, v) is minimal;

(b) the pair (u, v) satisfies the two simultaneous inequalities:

$$\left|\frac{v}{u}\right| \geq 1, \qquad \text{and} \qquad 0 \leq \Re\left(\frac{v}{u}\right) \leq \frac{1}{2}.$$

Then,

– the angle $\theta(u, v)$ between the two vectors u and v of a minimal basis

– and the imaginary part $y := \Im(v/u)$ satisfy

$$|\theta| \in [\pi/3, \pi/2] \qquad \left|\Im\left(\frac{v}{u}\right)\right| \geq \frac{\sqrt{3}}{2}$$

Characterization of a minimal acute basis.

Let (u, v) be an acute basis. The conditions (a) and (b) are equivalent:

(a) the basis (u, v) is minimal;

(b) the pair (u, v) satisfies the two simultaneous inequalities:

$$\left|\frac{v}{u}\right| \geq 1, \qquad \text{and} \qquad 0 \leq \Re\left(\frac{v}{u}\right) \leq \frac{1}{2}.$$

Then,

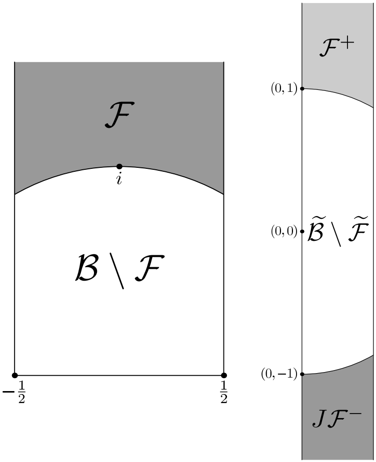
– the angle $\theta(u, v)$ between the two vectors u and v of a minimal basis

– and the imaginary part $y := \Im(v/u)$ satisfy

$$|\theta| \in [\pi/3, \pi/2] \qquad \left|\Im\left(\frac{v}{u}\right)\right| \geq \frac{\sqrt{3}}{2}$$

Characterization of minimal bases.

An acute basis (u, v) is minimal iff $z = \dfrac{v}{u} \in \tilde{\mathcal{F}}$



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

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

$\mathcal{B}^\epsilon := \{z \in \mathcal{B}, \quad \operatorname{sign} \Re(z) = \epsilon\}$

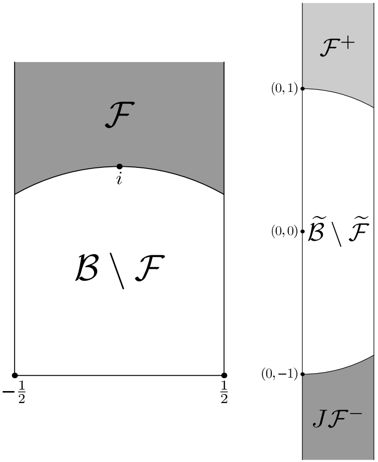
$\mathcal{F}^\epsilon := \{z \in \mathcal{F}, \quad \operatorname{sign} \Re(z) = \epsilon\}$

With $J : z \mapsto -z$

$\tilde{\mathcal{B}} := \mathcal{B}^+ \bigcup J\mathcal{B}^-, \ \tilde{\mathcal{F}} := \mathcal{F}^+ \bigcup J\mathcal{F}^-$

Characterization of minimal bases.

An acute basis (u, v) is minimal iff $z = \dfrac{v}{u} \in \tilde{\mathcal{F}}$



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

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

$$\mathcal{B}^\epsilon := \{z \in \mathcal{B}, \quad \operatorname{sign} \Re(z) = \epsilon\}$$

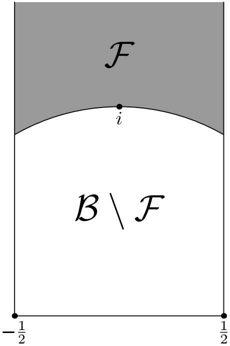
$$\mathcal{F}^\epsilon := \{z \in \mathcal{F}, \quad \operatorname{sign} \Re(z) = \epsilon\}$$

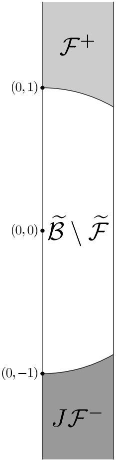
With $J : z \mapsto -z$

$$\tilde{\mathcal{B}} := \mathcal{B}^+ \bigcup J\mathcal{B}^-, \ \tilde{\mathcal{F}} := \mathcal{F}^+ \bigcup J\mathcal{F}^-$$

Characterization of minimal bases.

An acute basis (u, v) is minimal iff $z = \dfrac{v}{u} \in \tilde{\mathcal{F}}$





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

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

$$\mathcal{B}^\epsilon := \{z \in \mathcal{B}, \quad \operatorname{sign} \Re(z) = \epsilon\}$$

$$\mathcal{F}^\epsilon := \{z \in \mathcal{F}, \quad \operatorname{sign} \Re(z) = \epsilon\}$$

With $J : z \mapsto -z$

$$\tilde{\mathcal{B}} := \mathcal{B}^+ \bigcup J\mathcal{B}^-, \ \ \tilde{\mathcal{F}} := \mathcal{F}^+ \bigcup J\mathcal{F}^-$$

Vectorial version of the Gauss Algorithm

A-Gauss(u, v)

Input. An acute basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \leq |u|,\ \tau(v, u) \in [0, 1/2]$.

Output. An acute minimal basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \geq |u|$

While $|v| < |u|$ do
$(u, v) := (v, u)$;
Replace v by the smallest vector amongst
$\{w = \epsilon(v - mu) \mid \epsilon = \pm 1,\ m \in \mathbb{Z}\}$

The replacement operation is done as follows:

$$\tau(v, u) = \Re\left(\frac{v}{u}\right) = \frac{\langle u \cdot v \rangle}{|u|^2}$$

$$m := \lfloor \tau(v, u) \rceil ; \epsilon := \mathtt{sign}\left(\tau(v, u) - \lfloor \tau(v, u) \rceil\right);$$
$$v := \epsilon(v - mu);$$

Vectorial version of the Gauss Algorithm

$\texttt{A-Gauss}(u, v)$

Input. An acute basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \leq |u|,\ \tau(v, u) \in [0, 1/2]$.

Output. An acute minimal basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \geq |u|$

$\texttt{While}\ \ |v| < |u|\ \texttt{do}$
$(u, v) := (v, u)$;
Replace v by the smallest vector amongst
$\{w = \epsilon(v - mu) \mid \epsilon = \pm 1,\ m \in \mathbb{Z}\}$

The replacement operation is done as follows:

$$\tau(v, u) = \Re\left(\frac{v}{u}\right) = \frac{\langle u \cdot v \rangle}{|u|^2}$$

$$m := \lfloor \tau(v, u) \rceil ; \epsilon := \texttt{sign}\left(\tau(v, u) - \lfloor \tau(v, u) \rceil\right);$$
$$v := \epsilon(v - mu);$$

Vectorial version of the Gauss Algorithm

A-Gauss(u, v)

Input. An acute basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \leq |u|$, $\tau(v, u) \in [0, 1/2]$.

Output. An acute minimal basis (u, v) of $\mathcal{L}(u, v)$
with $|v| \geq |u|$

While $|v| < |u|$ do
$(u, v) := (v, u)$;
Replace v by the smallest vector amongst
$\{w = \epsilon(v - mu) \mid \epsilon = \pm 1,\ m \in \mathbb{Z}\}$

The replacement operation is done as follows:

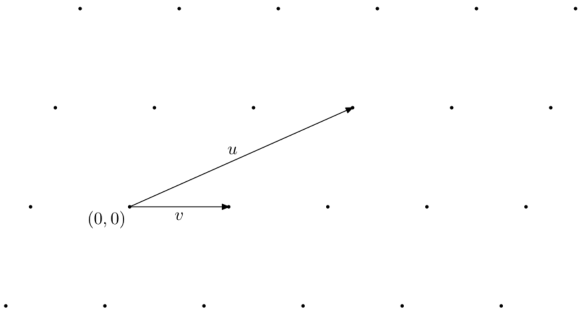
$$\tau(v, u) = \Re\left(\frac{v}{u}\right) = \frac{\langle u \cdot v \rangle}{|u|^2}$$

$$m := \lfloor \tau(v, u) \rceil ; \epsilon := \mathtt{sign}\left(\tau(v, u) - \lfloor \tau(v, u) \rceil\right);$$
$$v := \epsilon(v - mu);$$

The Gauss algorithm is an extension of the Euclid algorithm.

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

$$u = mv + \epsilon r \quad \text{with} \quad m = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil = \left\lfloor \frac{\langle u \cdot v \rangle}{|v|^2} \right\rceil, \quad 0 \leq \Re\left(\frac{r}{v}\right) \leq \frac{1}{2}$$



Here $m = 2$ and $\epsilon = 1$.

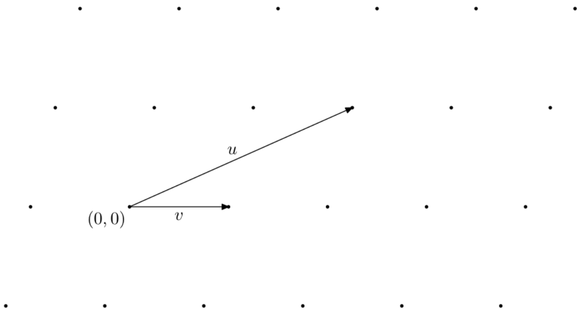
The vector r is the smallest amongst all the vectors which belong to

$$\{w = \epsilon(u - mv); \quad \epsilon = \pm 1, m \in \mathbb{Z}\}$$

The Gauss algorithm is an extension of the Euclid algorithm.

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

$$u = mv + \epsilon r \quad \text{with} \quad m = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil = \left\lfloor \frac{\langle u \cdot v \rangle}{|v|^2} \right\rceil, \quad 0 \le \Re\left(\frac{r}{v}\right) \le \frac{1}{2}$$



Here $m = 2$ and $\epsilon = 1$.

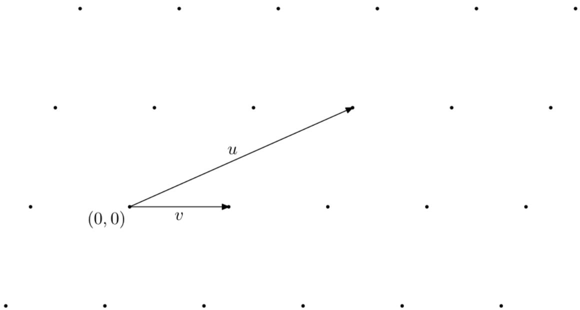
The vector r is the smallest amongst all the vectors which belong to

$$\{w = \epsilon(u - mv); \quad \epsilon = \pm 1, m \in \mathbb{Z}\}$$

The Gauss algorithm is an extension of the Euclid algorithm.

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

$$u = mv + \epsilon r \quad \text{with} \quad m = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil = \left\lfloor \frac{\langle u \cdot v \rangle}{|v|^2} \right\rceil, \quad 0 \le \Re\left(\frac{r}{v}\right) \le \frac{1}{2}$$



Here $m = 2$ and $\epsilon = 1$.

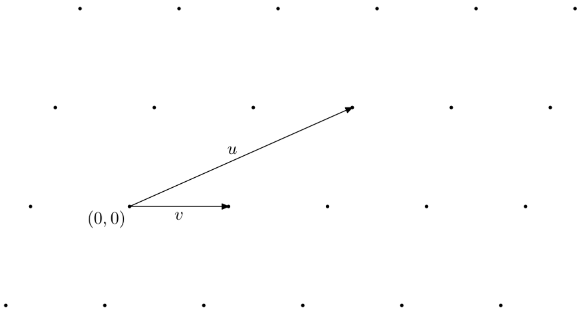
The vector r is the smallest amongst all the vectors which belong to

$$\{w = \epsilon(u - mv); \quad \epsilon = \pm 1, m \in \mathbb{Z}\}$$

The Gauss algorithm is an extension of the Euclid algorithm.

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

$$u = mv + \epsilon r \quad \text{with} \quad m = \left\lfloor \Re\left(\frac{u}{v}\right) \right\rceil = \left\lfloor \frac{\langle u \cdot v \rangle}{|v|^2} \right\rceil, \quad 0 \le \Re\left(\frac{r}{v}\right) \le \frac{1}{2}$$



Here $m = 2$ and $\epsilon = 1$.

The vector r is the smallest amongst all the vectors which belong to

$$\{w = \epsilon(u - mv); \quad \epsilon = \pm 1, m \in \mathbb{Z}\}$$

Complex version of the Gauss Algorithm

`A-Gauss`(z)

Input. z with $|z| \le 1, \ \Re z \in [0, 1/2], \ \Im z \neq 0$

Output. $z \in \tilde{\mathcal{F}}$

While $|z| \le 1$ do

$z := 1/z;$

$m := \lfloor \Re z \rceil; \epsilon := \mathtt{sign}\,(z - \lfloor \Re z \rceil);$

$z := \epsilon(z - m);$

The three steps are summarized as

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

Complex version of the Gauss Algorithm

$\texttt{A-Gauss}(z)$

Input. z with $|z| \le 1,\ \Re z \in [0, 1/2],\ \Im z \neq 0$

Output. $z \in \tilde{\mathcal{F}}$

While $|z| \le 1$ do

$z := 1/z;$

$m := \lfloor \Re z \rceil ; \epsilon := \mathbf{sign}\,(z - \lfloor \Re z \rceil);$

$z := \epsilon(z - m);$

The three steps are summarized as

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

Complex version of the Gauss Algorithm

```
A-Gauss(z)
```

Input. z with $|z| \le 1,\ \Re z \in [0, 1/2],\ \Im z \neq 0$

Output. $z \in \tilde{\mathcal{F}}$

$\texttt{While}\ \ |z| \le 1\ \texttt{do}$

$\quad z := 1/z;$

$\quad m := \lfloor \Re z \rceil ; \epsilon := \mathbf{sign}\,(z - \lfloor \Re z \rceil);$

$\quad z := \epsilon(z - m);$

The three steps are summarized as

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

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

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

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

An essential difference between the two algorithms

– The continuous extension of the 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 essential difference between the two algorithms

– The continuous extension of the 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 essential difference between the two algorithms

– The continuous extension of the 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 $v_{i-1} = m_i v_i + \epsilon_i \, v_{i+1}$;

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

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

The main parameters of interest describe

– the execution, for instance the number of iterations

– the output, for instance the distribution inside the 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 $v_{i-1} = m_i v_i + \epsilon_i\, v_{i+1}$;

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

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

The main parameters of interest describe

– the execution, for instance the number of iterations

– the output, for instance the distribution inside the 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 $v_{i-1} = m_i v_i + \epsilon_i \, v_{i+1}$;

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

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

The main parameters of interest describe

– the execution, for instance the number of iterations

– the output, for instance the distribution inside the fundamental domain

An execution of the Gauss Algorithm

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

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

it computes the sequence of divisions $v_{i-1} = m_i v_i + \epsilon_i\, v_{i+1}$;

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

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

The main parameters of interest describe

– the execution, for instance the number of iterations

– the output, for instance the distribution inside the 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 $v_{i-1} = m_i v_i + \epsilon_i \, v_{i+1}$;

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

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

The main parameters of interest describe

– the execution, for instance the number of iterations

– the output, for instance the distribution inside the fundamental domain

Study of the Gauss Algorithm.

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

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

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

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

Our version of the Gauss Algorithm (which uses the shift U)
deal with acute bases

Study of the Gauss Algorithm.

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

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

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 $\langle u \cdot v \rangle \geq 0$] $\to \Re z \geq 0$
- Skew basis (u, v) [or $|\det(u, v)|$ small wrt $|u|^2$] $\to \Im z$ small

Our version of the Gauss Algorithm (which uses the shift U)
deal with acute bases

The acute version

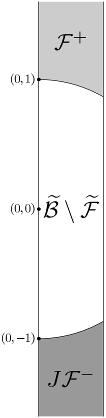
deals with the transformation U and the fundamental domain $\tilde{\mathcal{F}}$.

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

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

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

$J : z \mapsto -z$



The acute version

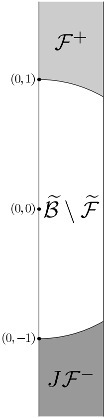
deals with the transformation U and the fundamental domain $\tilde{\mathcal{F}}$.

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

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

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

$J : z \mapsto -z$



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

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

`A-Gauss` = `CoreGauss` followed with `FinalGauss` (at most 2 iterations).

`CoreGauss`(z)

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

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

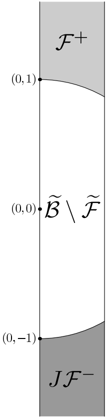
`While` $z \in \mathcal{D}$ do $z := U(z)$;

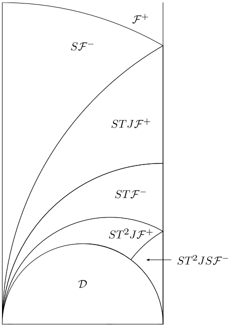
`FinalGauss`(z)

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 $z := U(z)$





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

$J(z) = -\bar{z}$

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

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

A-Gauss $=$ CoreGauss followed with FinalGauss (at most 2 iterations).

CoreGauss(z)

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

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

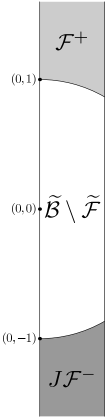
While $z \in \mathcal{D}$ do $z := U(z)$;

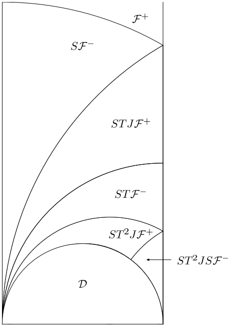
FinalGauss(z)

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 $z := U(z)$





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

$J(z) = -\bar{z}$

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

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

`A-Gauss` $=$ `CoreGauss` followed with `FinalGauss` (at most 2 iterations).

`CoreGauss`(z)

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

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

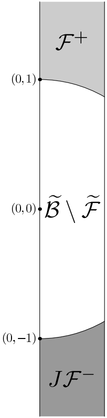
`While` $z \in \mathcal{D}$ `do` $z := U(z)$;

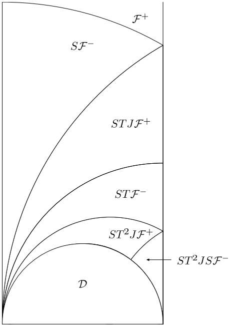
`FinalGauss`(z)

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` $z := U(z)$





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

$J(z) = -\bar{z}$

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

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

`A-Gauss` = `CoreGauss` followed with `FinalGauss` (at most 2 iterations).

`CoreGauss`(z)

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

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

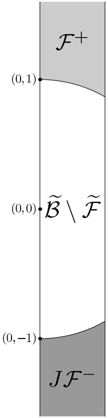
`While` $z \in \mathcal{D}$ `do` $z := U(z)$;

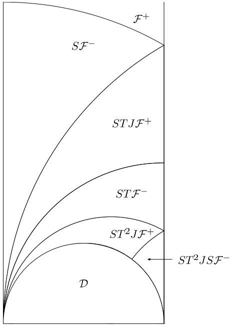
`FinalGauss`(z)

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` $z := U(z)$





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

$J(z) = -z$

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

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

A-Gauss $=$ CoreGauss followed with FinalGauss (at most 2 iterations).

CoreGauss(z)

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

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

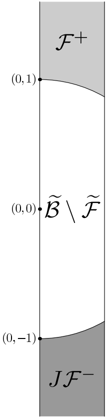
While $z \in \mathcal{D}$ do $z := U(z)$;

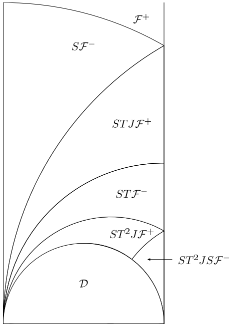
FinalGauss(z)

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 $z := U(z)$





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

$J(z) = -z$

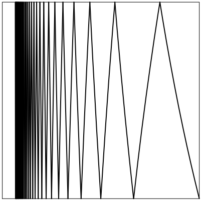
The CoreGauss Alg. is the central part of the AGauss Alg.

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

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

Exact generalisation
of the C-Euclid Algorithm,
which deals with the map
$[0, 1/2] \to [0, 1/2]$,

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



The graph of the DS
of the Centered Euclid Alg.

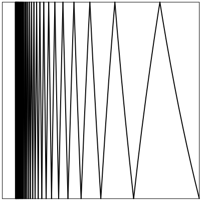
The `CoreGauss` Alg. is the central part of the AGAUSS Alg.

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

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

Exact generalisation
of the `C-Euclid` Algorithm,
which deals with the map
$[0, 1/2] \to [0, 1/2]$,

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



The graph of the DS
of the Centered Euclid Alg.

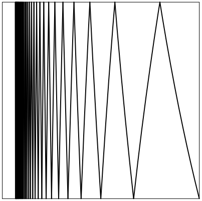
The `CoreGauss` Alg. is the central part of the AGAUSS Alg.

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

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

Exact generalisation
of the `C-Euclid` Algorithm,
which deals with the map
$[0,1/2] \to [0,1/2]$,

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



The graph of the DS
of the Centered Euclid Alg.

Number of iterations of the Core-Gauss Algorithm

The `CoreGauss` Alg. is regular and has a nice structure.

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

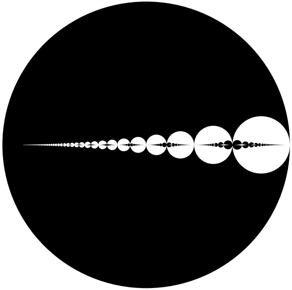
The domain $[R \geq k+1]$ is a union of disjoint disks,

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

Then: $$\mathbb{E}[R] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^\star} ||h(\mathcal{D})||$$

$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$)



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

Number of iterations of the Core-Gauss Algorithm

The `CoreGauss` Alg. is regular and has a nice structure.

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

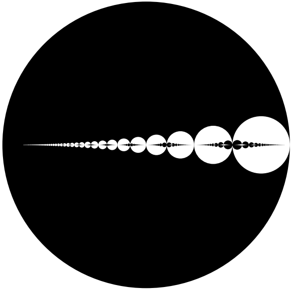
The domain $[R \geq k+1]$ is a union of disjoint disks,

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

Then: $$\mathbb{E}[R] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^\star} ||h(\mathcal{D})||$$

$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$)



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

Number of iterations of the Core-Gauss Algorithm

The `CoreGauss` Alg. is regular and has a nice structure.

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

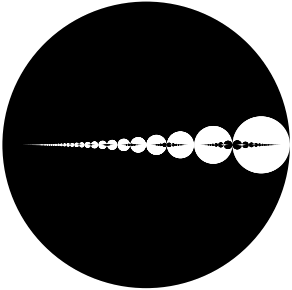
The domain $[R \geq k+1]$ is a union of disjoint disks,

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

Then: $$\mathbb{E}[R] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^\star} ||h(\mathcal{D})||$$

$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$)



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

A worst-case analysis.

For a given k,

– the largest disk $h(\mathcal{D})$ is obtained when all the quotients $(m, \epsilon) = (2, +1)$.

– In this case, the coefficients (c, d) of h are the terms (A_k, A_{k+1}) of the sequence

$$A_0 = 0, \quad A_1 = 1, \quad A_{k+1} = 2A_k + A_{k-1}, \quad (k \geq 1),$$

which satisfy $A_k \geq (1+\sqrt{2})^{k-2}$.

Then: $[R \geq k+1] \subset \left\{ z; \quad |\Im(z)| \leq \frac{1}{2} \left(\frac{1}{1+\sqrt{2}} \right)^{2k-2} \right\}$,

For any complex number z non real, the number of iterations of the Core-Gauss Algorithm on the input z satisfies

$$R(z) \leq 2 + \frac{1}{2} \log_{1+\sqrt{2}} \frac{1}{|\Im z|}.$$

A worst-case analysis.

For a given k,

– the largest disk $h(\mathcal{D})$ is obtained when all the quotients $(m, \epsilon) = (2, +1)$.

– In this case, the coefficients (c, d) of h are the terms (A_k, A_{k+1}) of the sequence

$$A_0 = 0, \quad A_1 = 1, \qquad A_{k+1} = 2A_k + A_{k-1}, \quad (k \geq 1),$$

which satisfy $A_k \geq (1 + \sqrt{2})^{k-2}$.

Then: $$[R \geq k+1] \subset \left\{ z; \quad |\Im(z)| \leq \frac{1}{2} \left(\frac{1}{1+\sqrt{2}} \right)^{2k-2} \right\},$$

For any complex number z non real, the number of iterations of the Core-Gauss Algorithm on the input z satisfies

$$R(z) \leq 2 + \frac{1}{2} \log_{1+\sqrt{2}} \frac{1}{|\Im z|}.$$

A worst-case analysis.

For a given k,

– the largest disk $h(\mathcal{D})$ is obtained when all the quotients $(m, \epsilon) = (2, +1)$.

– In this case, the coefficients (c, d) of h are the terms (A_k, A_{k+1}) of the sequence

$$A_0 = 0, \quad A_1 = 1, \qquad A_{k+1} = 2A_k + A_{k-1}, \quad (k \geq 1),$$

which satisfy $A_k \geq (1+\sqrt{2})^{k-2}$.

$$\text{Then: } [R \geq k+1] \subset \left\{ z; \quad |\Im(z)| \leq \frac{1}{2} \left(\frac{1}{1+\sqrt{2}} \right)^{2k-2} \right\},$$

For any complex number z non real, the number of iterations of the `Core-Gauss` Algorithm on the input z satisfies

$$R(z) \leq 2 + \frac{1}{2} \log_{1+\sqrt{2}} \frac{1}{|\Im z|}\,.$$

Now, a probabilistic study.

We first define an interesting class of probabilistic models
which takes into account the "geometry" of the events $[R \geq k+1]$

The model with valuation r is associated with a density f_r on the disk $\mathcal{D}$ proportional to $|y|^{r-1}$.

– The uniform density is obtained for $r = 1$

– The measure of a disk centered on the real axis with diameter d is proportional to d^{r+1}

When $r \to 0$,

– 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 $[\Im z = 0]$

Now, a probabilistic study.

We first define an interesting class of probabilistic models
which takes into account the "geometry" of the events $[R \geq k+1]$

The model with valuation r is associated with a density f_r on the disk $\mathcal{D}$ proportional to $|y|^{r-1}$.
– The uniform density is obtained for $r = 1$
– The measure of a disk centered on the real axis with diameter d is proportional to d^{r+1}

When $r \to 0$,

– 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 $[\Im z = 0]$

Now, a probabilistic study.

We first define an interesting class of probabilistic models
which takes into account the "geometry" of the events $[R \geq k+1]$

The model with valuation r is associated with a density f_r on the disk $\mathcal{D}$ proportional to $|y|^{r-1}$.
– The uniform density is obtained for $r = 1$
– The measure of a disk centered on the real axis with diameter d is proportional to d^{r+1}

When $r \to 0$,

– 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 $[\Im z = 0]$

Now, a probabilistic study.

We first define an interesting class of probabilistic models
which takes into account the "geometry" of the events $[R \geq k+1]$

The model with valuation r is associated with a density f_r on the disk $\mathcal{D}$ proportional to $|y|^{r-1}$.
– The uniform density is obtained for $r = 1$
– The measure of a disk centered on the real axis with diameter d is proportional to d^{r+1}

When $r \to 0$,

– 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 $[\Im z = 0]$

Now, a probabilistic study.

We first define an interesting class of probabilistic models
which takes into account the "geometry" of the events $[R \geq k+1]$

The model with valuation r is associated with a density f_r on the disk $\mathcal{D}$ proportional to $|y|^{r-1}$.
– The uniform density is obtained for $r = 1$
– The measure of a disk centered on the real axis with diameter d is proportional to d^{r+1}

When $r \to 0$,

– 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 $[\Im z = 0]$

Number of iterations of the Gauss Algorithm (II).

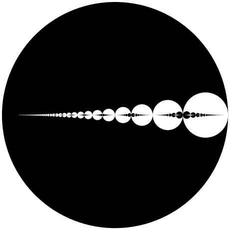
Strongly depends on the distribution near the real axis (described with the valuation)

$$\mathbb{E}[R] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^\star} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$).

For any valuation r, the mean value satisfies

$$\mathbb{E}_{(r)}[R] = \frac{2^{2r+2}}{\zeta(2r+2)} \sum_{\substack{c,d \geq 1 \\ d\phi < c < d\phi^2}} \frac{1}{(cd)^{1+r}}.$$



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

Number of iterations of the Gauss Algorithm (II).

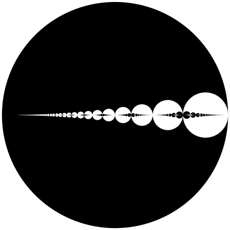
Strongly depends on the distribution near the real axis (described with the valuation)

$$\mathbb{E}[R] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^\star} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$).

For any valuation r, the mean value satisfies

$$\mathbb{E}_{(r)}[R] = \frac{2^{2r+2}}{\zeta(2r+2)} \sum_{\substack{c,d \geq 1 \\ d\phi < c < d\phi^2}} \frac{1}{(cd)^{1+r}}.$$



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

Number of iterations of the Gauss Algorithm (III).

Strongly depends on the distribution near the real axis (described with the valuation)

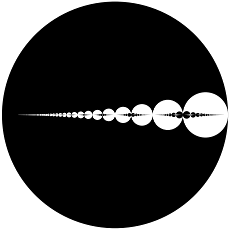
$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$).

For any valuation r,
R follows asymptotically a geometric law with a ratio $\lambda(1+r)$,
The map $s \mapsto \lambda(s)$ is an important mathematical object,
the dominant eigenvalue of the transfer operator $\mathbf{H}_s$

$$\mathbb{P}_{(r)}[R \geq k] \sim C_r \, \lambda(1+r)^k, \quad \lambda(2) \sim 0.07738$$

$$1 - \lambda(1+r) \sim \frac{\pi^2}{6 \log \phi} r \quad (r \to 0)$$



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

Number of iterations of the Gauss Algorithm (III).

Strongly depends on the distribution near the real axis (described with the valuation)

$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$).

For any valuation r,

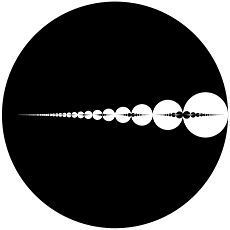
R follows asymptotically a geometric law with a ratio $\lambda(1+r)$,

The map $s \mapsto \lambda(s)$ is an important mathematical object,

the dominant eigenvalue of the transfer operator $\mathbf{H}_s$

$$\mathbb{P}_{(r)}[R \geq k] \sim C_r \, \lambda(1+r)^k, \quad \lambda(2) \sim 0.07738$$

$$1 - \lambda(1+r) \sim \frac{\pi^2}{6 \log \phi} r \quad (r \to 0)$$



The domains $[R = k]$

alternatively

in black and white

Number of iterations of the Gauss Algorithm (III).

Strongly depends on the distribution near the real axis (described with the valuation)

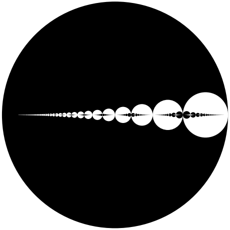
$$\mathbb{P}[R \geq k+1] = \frac{1}{||\mathcal{D}||} \sum_{h \in \mathcal{H}^k} ||h(\mathcal{D})||$$

(Remark: $||\mathcal{X}||$ is the measure of the domain $\mathcal{X}$).

For any valuation r,
R follows asymptotically a geometric law with a ratio $\lambda(1+r)$,
The map $s \mapsto \lambda(s)$ is an important mathematical object,
the dominant eigenvalue of the transfer operator $\mathbf{H}_s$

$$\mathbb{P}_{(r)}[R \geq k] \sim C_r \, \lambda(1+r)^k, \quad \lambda(2) \sim 0.07738$$

$$1 - \lambda(1+r) \sim \frac{\pi^2}{6 \log \phi} r \quad (r \to 0)$$



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 $\quad F_{1+r}(x, y) \cdot \eta(x, y)$,

– 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

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

via the relation $\quad F_s(x, y) = \dfrac{1}{\zeta(2s)} E_s(x, y) - y^s$

When $r \to 0$, the output distribution relative to the input distribution of valuation r tends to the distribution of random lattices.

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 $\quad F_{1+r}(x,y)\cdot\eta(x,y)$,

– 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

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

via the relation $\quad F_s(x,y) = \dfrac{1}{\zeta(2s)}E_s(x,y) - y^s$

When $r \to 0$, the output distribution relative to the input distribution of valuation r tends to the distribution of random lattices.

Instance of a Dynamical Analysis.

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

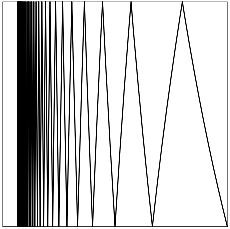
describes one step of the `C-Euclid` Alg. or the `CoreGauss` Alg.

For studying the Euclid Algorithm, a transfer operator is used,

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

For $s = 1$, 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 Dynamical 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

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

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

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

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

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

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

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