Using Functional Analysis in Average Case Analysis: the Example of the Gauss Reduction Algorithm

Brigitte Vallée
Université de Caen

May 15, 1995

[summary by Pierre Nicodème]

Abstract

The Gaussian algorithm may be viewed as a formal generalization of the Euclidean algorithm: it uses an extension of the real shift operator U used for continued fractions. We study the random variable "number of iterations" L, when the input data are distributed along an initial density, and we describe the evolution of the data while processing the algorithm. The results use spectral properties of a family of Ruelle-Mayer operators $\mathcal{H}_s$ "inverting" the shift operator U. The operator family $\mathcal{H}_s$ defines a unifying framework allowing a common analysis of both Euclid and Gauss algorithms. This work is a generalization of a common work with Hervé Daudé and Philippe Flajolet [2].

1. The Euclidean and Gaussian algorithms

Starting from a lattice in dimension 2, $\mathcal{L} = \mathbb{Z}u \bigoplus \mathbb{Z}v$, with $u, v \in \mathbb{C}$ not collinear, the Gaussian algorithm finds a minimal basis (m, n) in the sense that the triangle built on (m, n) has no obtuse angle. The problem is invariant by similitude $u \mapsto \lambda u$, with $\lambda \in \mathbb{C}$, and therefore the problem on (u, v) is equivalent to the problem on $(1, v/u)$. The triangle built on $(1, z)$ has no obtuse angles iff $z \in \mathcal{B} - \mathcal{D}$, where $\mathcal{B} = \{z, 0 \leq \Re z \leq 1\}$, and $\mathcal{D}$ is the disk of diameter $[0, 1]$.

FIGURE 1. A lattice and two of its bases represented by the parallelogram they span. The first basis is skew, the second one is minimal (reduced).

The Gaussian algorithm is the composition of a succession of transforms of two types: *(i)* inversion S with $S(z) = 1/z$, *(ii)* translation T^{-m} with $T(z) = z + 1$. With $U(z) = 1/z - \lfloor \Re(1/z) \rfloor$, the Gaussian algorithm terminates whenever $U^k(z) \in \mathcal{B} - \mathcal{D}$. Applying a suitable transform T^{-m} with acute basis, so that $\Re(z) \geq 0$, it is readily seen that it suffices to consider cases where $z \in \mathcal{D}$.

The Gaussian algorithm for lattice reduction is a generalization of the Euclidean algorithm for finding the gcd of two integers in the following way:

	Euclid Continued Fractions	Gauss Lattice Reduction
Algorithm	Input: $x \in [0,1[$	input $z \in \mathcal{D}$ = disc of diameter $[0,1[$
	while $x \neq 0$ do $x = 1/x - \lfloor 1/x \rfloor$	while $z \in \mathcal{D}$ do $z = 1/z - \lfloor \Re(1/z) \rfloor$
Termination	terminates on $\mathbb{Q}$ when the input is in $\mathbb{R}$	terminates on $\mathbb{C} \setminus \{\mathbb{R} \setminus \mathbb{Q}\}$ when the input is in $\mathbb{C}$

We are investigating a generalization of a problem set by Gauss around 1800 for the Euclidean algorithm: starting with a density f on $[0,1]$, what is the density $F_k[f]$ after k iterations of U, with $U(x) = 1/x - \lfloor 1/x \rfloor$. The possible antecedents of x are of the form $1/(m+x)$, with $m \geq 1$, and F_k and F_{k+1} are connected by

$$F_{k+1}[f](x) = \sum_{m \geq 1} \frac{1}{(m+x)^2} F_k[f]\left(\frac{1}{m+x}\right). \tag{1}$$

Introducing the operator $\mathcal{G}$, defined by

$$\mathcal{G}_s[f](x) = \sum_{m \geq 1} \frac{1}{(m+x)^s} f\left(\frac{1}{m+x}\right), \tag{2}$$

many properties of the Euclidean algorithm can be expressed in terms of spectral quantities related to the operator $\mathcal{G}_s$ (with s close to 2): the existence of a limit density $F_\infty[f](x) = \frac{1}{\log 2}\frac{1}{1+x}$ corresponds to the dominant eigenvector of $\mathcal{G}_2$ (with eigenvalue $\lambda = 1$); the expectation of the number K_n of iterations of Euclid on p/q verifying $1 \leq p < q \leq N$ is given by $\mathrm{E}[K_N] = \frac{12 \log 2}{\pi^2} \log N + \mathcal{O}(1)$, in tight relationship with $\lambda'(2)$ (with $\lambda(s)$ dominant eigenvalue of $\mathcal{G}_s$).

We will derive from the properties of the $\mathcal{G}$ operators the "stationary" distribution $F_\infty[f]$, and the distribution of the number L of iterations of the Gaussian algorithm along any initial distribution f.

Like the continued fraction expansion of a number under the Euclidean algorithm, with $z_j \in \mathcal{D}$, which implies $\Re(1/z_j) > 1$, we have $z_{j+1} = 1/z_j - m_j$, with $m_j \geq 1$, which is equivalent to $z_j = 1/(m_j + z_{j+1})$, and gives the expansion

$$z_0 = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots \cfrac{}{m_k + z_k}}}}. \tag{3}$$

This expansion terminates as soon as $z_k \in \mathcal{B} - \mathcal{D}$. Then $L(z_0) = k$, $z_0 = h_m(z_k)$ and $h_m(z)$ may be expressed in terms of the continuants $Q_k(m_1, m_2, \ldots, m_k)$ and $P_k(m_1, m_2, \ldots, m_k) = Q_{k-1}(m_2, \ldots, m_k)$ as

$$h_m(z) = \frac{P_k + zP_{k-1}}{Q_k + zQ_{k-1}} \tag{4}$$

for $|h| = k$; the continuants are defined by the recurrence equations

$$Q_n(x_1, x_2, \ldots, x_n) = x_n Q_{n-1}(x_1, \ldots, x_{n-1}) + Q_{n-2}(x_1, \ldots, x_n),$$

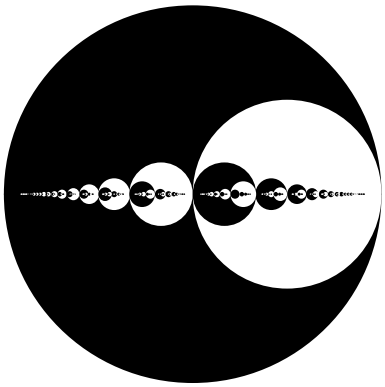

FIGURE 2. The domains $\mathcal{D}_0 \setminus \mathcal{D}_1$, $\mathcal{D}_1 \setminus \mathcal{D}_2$, $\mathcal{D}_2 \setminus \mathcal{D}_3$, $\mathcal{D}_3 \setminus \mathcal{D}_4$, $\mathcal{D}_4 \setminus \mathcal{D}_5$ represented alternatively in black and white. (The largest disk is $\mathcal{D}_0 \equiv \mathcal{D}$ which is the disk of diameter $[0,1]$.)

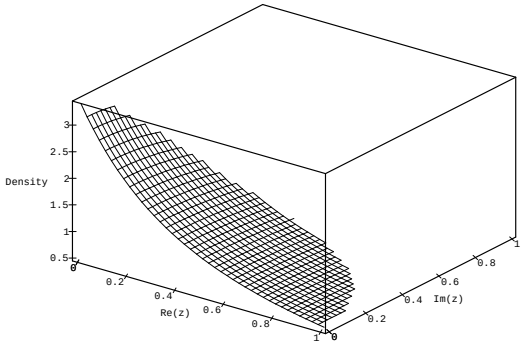

FIGURE 3. The conditional invariant density F_∞.

with $Q_0 = 1$, $Q_1(x_1) = x_1$. Then, the set of points giving more than k iterations is $[L(z) \geq k+1] = \bigcup_{|h|=k} h(\mathcal{D})$ with $h(\mathcal{D})$ the fundamental disk of diameter $h(\mathcal{I}) = [P_k/Q_k, (P_k + P_{k-1})/(Q_k + Q_{k-1})]$.

We have $\mu[h(\mathcal{D})] = \iint_{h(\mathcal{D})} f(z)dxdy = \iint_{\mathcal{D}} |h'(z)|^2 f \circ h(z)\, dxdy$, the measure μ being associated with the density f, and, remarking that the disks $h(\mathcal{D})$ are disjoint, after exchanging the sum and integral signs,

$$\varpi_k = \Pr[L \geq k+1] = \frac{1}{\mu(\mathcal{D})} \sum_{|h|=k} \mu[h(\mathcal{D})] = \iint_{\mathcal{D}} \Big(\sum_{|h|=k} |h'(z)|^2 f \circ h(z) \Big)\, dxdy. \tag{5}$$

Introducing the operator $\mathcal{H}^k_{2s}[f][z] = \sum_{|h|=k} |h'(z)|^s f \circ h(z)$, we have

THEOREM 1. *For a density f, the probability of making more than k iterations of the Gaussian algorithm is*

$$\varpi_k[f] = \frac{\iint_{\mathcal{D}} \mathcal{H}^k_4[f](z)\, dxdy}{\iint_{\mathcal{D}} f(z)\, dxdy};$$

if the density f is uniform, the probability is

$$\varpi_k[f] = \sum_{m_1,\ldots,m_k} \frac{1}{Q_k^2 (Q_k + Q_{k-1})^2},$$

and the expectation of the number of iterations is

$$\mathrm{E}[L] = \frac{5}{4} + \frac{180}{\pi^4} \sum_{d \geq 1} \frac{1}{d^2} \sum_{d < c < 2d} \frac{1}{c^2}.$$

Therefore all the objects we are studying may be expressed with $\mathcal{H}_s[f](z) = \sum_{m \geq 1} \frac{1}{|m+z|^s} f(\frac{1}{m+z})$ and its holomorphic version $\mathcal{G}_s[f](z) = \sum_{m \geq 1} \frac{1}{(m+z)^s} f(\frac{1}{m+z})$, the classical Ruelle-Mayer operator $\mathcal{G}_s$. While in the uniform case, the study of $\mathcal{G}_4$ is sufficient, in general it is necessary to study the complete family of the $\mathcal{H}_s$.

2. Properties of the Ruelle-Mayer operators and application to the analysis of the Gaussian algorithm

The Ruelle-Mayer operators $\mathcal{G}_s$ are defined on the set $A_\infty(V)$ of holomorphic functions on V, continuous on $\overline{V}$, with $V = \{|z-1| < \frac{3}{2}\}$, for s with $\Re(s) > 1$. They are nuclear operators of order 0 (very similar to infinite matrices); after transfer in another Hilbert space, they are diagonalisable with a discrete spectrum; moreover, they are Perron-Frobenius operators for $s > 1$, having a unique dominant eigenvalue $\lambda(s)$.

As a consequence, turning back to the uniform case, we have the theorem.

THEOREM 2. *The probability ϖ_k has a geometric behaviour, $\varpi_k \simeq c\lambda_4^k$, with $\lambda_4 \approx 0.1994$ and $c \approx 1.3$.*

The dynamic density $F_k(z)$ converges to a (conditional) invariant density $F_\infty(z)$ proportional to $\int_{-1}^{+1}(1-w^2)c_4(x+iyw)\,dw$, where c_4 is the dominating eigenvector of $\mathcal{G}_4$.

In the general case, we have to study generalized Ruelle-Mayer operators [3]

The spectral properties of the operator $\mathcal{H}_s$ are essentially the same as those of $\mathcal{G}_s$; there is a dominant eigenvalue $\lambda(s)$ and a dominant eigenvector which may be expressed easily in terms of $\mathcal{G}_s$. However, an interesting improvement is possible in case of functions with valuations.

THEOREM 3. *For an initial density of valuation t—$f(x,y) = |y|^t g(x,y)$, with $g \not\equiv 0$ on the real axis—the asymptotical behaviours of $\varpi_k[f]$ and $F_k[f]$ depend on the dominant spectral objects of $\mathcal{G}_{4+2t}$:*

$$\varpi_k[f] \simeq c\lambda_{4+2t}^k \tag{6}$$

and $F_\infty[f](z)$ is proportional to $|y|^t \int_{-1}^{+1}(1-w^2)^{1+t} g_{4+2t}(x+iyw)\,dw$.

3. Conclusion

These results lead to two main applications:

from Gauss to Euclid: then, we have $t \to 1$, $\lambda_{4+2t} \to \lambda_2 = 1$, and $g_{4+2t} \to g_2 = \frac{1}{\log 2}\frac{1}{1+t}$;

from Gauss to LLL: considering n vectors $b_1, \ldots, b_n$ uniformly distributed in $\mathcal{B}_n$, the unit ball of $\mathbb{R}^n$, with l_i the length of the i-th orthogonalized, the initial density has valuation $n-i-1$, and we can apply our results with use of $\mathcal{G}_{2(1+n-i)}$ [1].

We showed how to "inverse" the operator U of the Gaussian algorithm by use of a functional operator $\mathcal{G}_s$. An open question is the generalization of such a method to other algorithms.

Bibliography

[1] Daudé (H.) and Vallée (B.). – An upper bound on the average number of iterations of the LLL algorithm. *Theoretical Computer Science*, vol. 123, n° 1, 1994, pp. 95–115.

[2] Daudé (Hervé), Flajolet (Philippe), and Vallée (Brigitte). – An analysis of the Gaussian algorithm for lattice reduction. In Adleman (L.) (editor), *Algorithmic Number Theory Symposium*, *Lecture Notes in Computer Science*, pp. 144–158. – 1994. Proceedings of *ANTS'94*.

[3] Vallée (B.). – Le rôle des opérateurs de Ruelle-Mayer généralisés dans l'analyse en moyenne des algorithmes d'Euclide et de Gauss. – GREYC, Département d'Informatique, Université de Caen, 14032 Caen Cedex, France.