Probabilistic analysis of Gauss' algorithm in a realistic model

Antonio Vera, joint work with Brigitte Vallée

October 15, 2007

A Euclidean lattice $\mathcal{L}$ is a discrete subgroup of $(\mathbb{R}^n, +)$, and it can be characterized as the set of integer linear combinations of some $d \leq n$ linearly independent vectors:

$$\mathcal{L} = \bigoplus_{i=1}^{d} \mathbb{Z}\mathbf{b}_i.$$

The set $\{\mathbf{b}_i\}_{i=1}^{d}$ is called *basis* of $\mathcal{L}$, and is represented by a matrix B having as columns the $\mathbf{b}_i$'s. Each matrix of the form BP, with $P \in GL_n(\mathbb{Z})$, represents a basis of $\mathcal{L}$. A lattice can have bases with arbitrarily long and skew vectors. See figure 1.

By *lattice basis reduction* we mean solving the following problem: given a lattice basis formed by long (and probably skew) vectors, compute a basis formed by short (and quite orthogonal) vectors. This problem plays a primary rôle in many areas of computational mathematics and computer science: for instance, modern cryptanalysis [10], computer algebra [16], integer linear programming [9] and number theory [3].

In the two-dimensional case, there exists an algorithm due to Lagrange and Gauss which computes a *minimal* basis (i.e., a basis formed by shortest possible vectors) in linear time: it is a generalization of the Euclidean algorithm. This

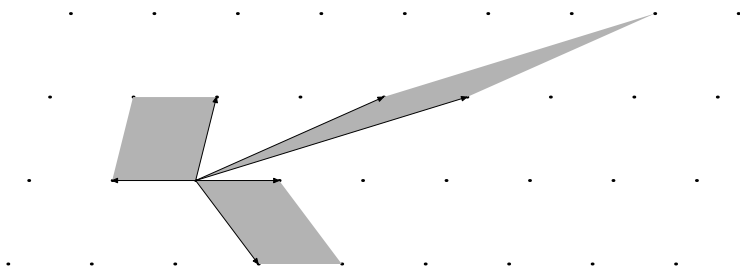

Figure 1: A lattice of $\mathbb{R}^2$, and three of its bases. The area of the parallelogram determined by each basis does not depend on the particular basis.

PGauss(u, v)

Input. A basis (u, v) with $|v| < |u|$, $|\frac{(u \cdot v)}{|u|^2}| \leq (1/2)$, $\det(u, v) > 0$.

Output. A minimal basis (u, v) with $|v| \geq |u|$, $\det(u, v) > 0$.

`While` $|v| < |u|$ `do`
$(u, v) := (v, -u)$;
$m := \left\lfloor \frac{(u \cdot v)}{|u|^2} \right\rceil$;
$v := v - mu$;

Figure 2: One of the variants of Gauss' Algorithm which is used in our analysis. This variant preserves the positive orientation of u and v, that is, it mantains the invariant $\det(u, v) > 0$.

algorithm is in a sense optimal, from the points of view of time-complexity and quality of the output. For a precise description of Gauss' algorithm, see figure 2.

For $n \geq 3$, the LLL algorithm [8] due to Lenstra, Lenstra and Lovász, computes a *reduced* basis of an n-dimensional lattice in polynomial time. When $n = 2$, reduced basis means minimal basis. When $n \geq 3$, even if we have guarantees of quality, we don't know the expected quality of a basis nor the exact complexity of the algorithm (even in the worst-case, and for small dimensions). The LLL algorithm uses Gauss' Algorithm as a main procedure.

Even if the understanding of Gauss' Algorithm is important in itself, the use that LLL makes of it boosts significantly its interest. The survey [14] develops this topic.

Previous results

Gauss' algorithm has been analyzed in the worst case by Lagarias, [6], then Vallée [12], who also describes the worst-case input. Then, Daudé, Flajolet and Vallée [4] completed the first work [5] and provided a detailed average-case analysis of the algorithm, in a natural probabilistic model which can be called a uniform model. They study the mean number of iterations, and prove that it is asymptotic to a constant, and thus essentially independent of the length of the input. Moreover, they show that the number of iterations follows an asymptotic geometric law, and determine the ratio of this law. On the other side, Laville and Vallée [7] study the geometry of the outputs, and describe the law of some output parameters, when the input model is the previous uniform model.

The previous analyses only deal with uniform-distributed inputs and it is not possible to apply these results "inside" the LLL algorithm, because the distribution of "local bases" which occur along the execution of the LLL algorithm is far from uniform. Akhavi, Marckert and Rouault [2] showed that, even in the uniform model where all the vectors of the input bases are independently and

uniformly drawn in the unit ball, the skewness of "local bases" may vary a lot. It is then important to analyse the Gauss algorithm in a model where the skewness of the input bases may vary. Furthermore, it is natural from the works of Akhavi [1] to deal with a probabilistic model where, with a high probability, the modulus of the determinant $\det(u, v)$ of a basis (u, v) is much smaller than the product of the lengths $|u| \cdot |v|$. More precisely, a natural model is the so–called model of valuation r, where

$$\mathbb{P}\left[(u, v); \quad \frac{|\det(u, v)|}{\max(|u|, |v|)^2} \leq y\right] = \Theta(y^{r+1}), \qquad \text{with} \quad (r > -1).$$

Remark that, when r tends to -1, this model tends to the "one dimensional model", where u and v are collinear. In this case, Gauss' Algorithm "tends" to the Euclidean Algorithm, and it is important to precisely describe this transition. This model "with valuation" was already presented in [13] in a slightly different context, but not actually studied.

As for the Euclidean algorithm, Gauss' algorithm is better understood when viewed as a dynamical system. The gaussian dynamical system is specified by a triple $(\mathcal{B}, \mathcal{F}, U)$, where $\mathcal{F} \subset \mathcal{B} \subset \mathbb{C}$ and $U : \mathcal{B} \to \mathcal{B}$ is a function to be iterated starting from a point of $\mathcal{B} \setminus \mathcal{F}$ and stopping when the current point falls into $\mathcal{F}$. The domains $\mathcal{B} \setminus \mathcal{F}$ and $\mathcal{F}$ are called input and output domain, respectively. In figure 3 we give two examples of gaussian systems.

Our results

A natural question is: given a probability density on the input domain $\mathcal{B} \setminus \mathcal{F}$, what is the induced density on the output domain $\mathcal{F}$? This is the first question we answer: this density is related to a classical object of the theory of modular forms, namely the Eisenstein series.

The second question is related to the properties of the output basis provided by the algorithm. Suppose we are given a basis (u, v) as input and a basis $(\hat{u}, \hat{v})$ as output. We are interested in the probabilistic description of the following parameters:

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

The first one coincides with the length of a shortest nonzero vector of $\mathcal{L}(u, v)$ and it is typically called first minimum. The second stands for the length of the orthogonal projection of a vector realizing the second minimum, on $(\mathrm{span}\{\hat{u}\})^\perp$. The third parameter is called Hermite's defect, and it is invariant by scaling of the lattice. They all play a fundamental rôle in a detailed analysis of the LLL algorithm. We describe the level sets for parameter μ (for λ and γ they were described in [7]), and we provide sharp estimates for the distribution of λ, μ and γ.

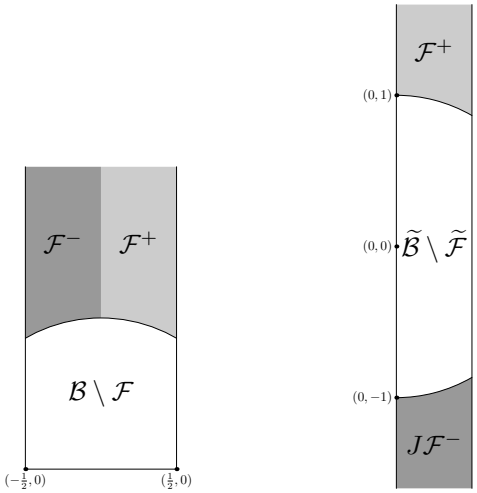

Figure 3: Fundamental domains for two gaussian dynamical systems. The associated transformations are $U(z) := -\frac{1}{z} - \lfloor -\Re(\frac{1}{z}) \rceil$ and $\widetilde{U}(z) := \text{sign}(\Re(\frac{1}{z}) - \lfloor \Re(\frac{1}{z}) \rceil)(\frac{1}{z} - \lfloor \Re(\frac{1}{z}) \rceil)$.

We finally consider various parameters which describe the execution of the algorithm (in a more precise way than the number of iterations), namely the so–called additive costs, the bit-complexity, the length decreases, and we analyze their probabilistic behaviour.

Along the papers [14] and [15], we explain the rôle of the valuation r, and the transition phenomena between the Gauss Algorithm and the Euclidean algorithms which occur when $r \to -1$.

References

[1] A. Akhavi. Random lattices, threshold phenomena and efficient reduction algorithms, *Theoretical Computer Science*, 287 (2002) 359–385

[2] A. Akhavi, J.-F. Marckert et A. Rouault. On the Reduction of a Random Basis, *Proceedings of SIAM-ALENEX/ANALCO'07.* New-Orleans, january 07

[3] H. Cohen. A course in Computational Algebraic Number Theory, GTM 138, Springer Verlag, 4th Edition (2000).

[4] H. Daudé, P. Flajolet, B. Vallée. An average-case analysis of the Gaussian algorithm for lattice Reduction, *Combinatorics, Probability and Computing* (1997) 6, pp 397–433.

[5] P. Flajolet, B. Vallée. *Gauss'reduction Algorithm : an average case analysis*, *Proceedings of IEEE-FOCS 90*, St-Louis, Missouri, volume 2, pp 830-39.

[6] J. C. Lagarias. Worst–case complexity bounds for algorithms in the theory of integral quadratic forms. *Journal of Algorithms 1*, 2 (1980), 142–186.

[7] H. Laville, B. Vallée. Distribution de la constante d'Hermite et du plus court vecteur dans les réseaux de dimension 2, *Journal de Théorie des nombres de Bordeaux* 6 (1994) pp 135-159

[8] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen 261* (1982), 513–534.

[9] H. W. Lenstra. Integer programming with a fixed number of variables, *Mathematics of Operations Research*, vol. 8, 4, (1983), 538–548

[10] P. Nguyen, J. Stern. The Two Faces of Lattices in Cryptology, *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*, Springer, LNCS, volume 2146, (2001), 146–180.

[11] P. Nguyen, D. Stehlé. LLL on the average, *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)*, Springer, LNCS vol. 4076, (2006), 238–256

[12] B. Vallée. Gauss' algorithm revisited. *Journal of Algorithms 12* (1991), 556–572.

[13] B. Vallée. Algorithms for computing signs of 2×2 determinants: dynamics and average–case analysis, *Proceedings of ESA '97* (5th Annual European Symposium on Algorithms) (Graz, Septembre 97), LNCS 1284, pp 486–499.

[14] B. Vallée, A. Vera. Probabilistic analyses of Lattice Reduction Algorithms. *To appear in the proceedings of the LLL+25 conference, Caen, June 29-July 1, 2007, Springer.*

[15] B. Vallée, A. Vera. Lattice reduction in two dimensions: analyses under realistic probabilistic models. *To appear in the Proceedings of AofA'07, Discrete Mathematics and Theoretical Computer Science.*

[16] C.K. Yap. Fundamental Problems in Algorithmic Algebra, Princeton University Press (1996)