

## Threshold Phenomena in Random Lattices and Reduction Algorithms

*Ali Akhavi*

GREYC, Université de Caen

November 8, 1999

*Summary by Philippe Flajolet*

By a *lattice* is meant here the set of all linear combinations of a finite collection of vectors in  $\mathbb{R}^n$  taken with integer coefficients,

$$\mathcal{L} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_p.$$

One may think of a lattice as a regular arrangement of points in space, somewhat like atoms composing a crystal in  $\mathbb{R}^3$ . Given the generating family  $(e_j)$ , there is great interest in finding a “good” basis of the lattice. By this is meant a basis that is “almost” orthogonal and is formed with vectors of “small” length. The process of constructing a “good” basis from a skewed one is referred to as lattice [basis] reduction.

Lattice reduction is of structural interest in various branches of number theory. For instance, reduction in dimension 2 is completely solved by a method due to Gauß. This entails a complete classification of binary quadratic forms with integer coefficients, a fact that has numerous implications in the analysis of quadratic irrationals and in the representation of integers by quadratic forms (cf. for example Pell’s equation,  $x^2 - dy^2 = 1$ .)

The algorithmic and computational questions that stem from lattice reduction are of even greater applicability. In all generality, the *exact* optimization problem (i.e., finding the “best” basis, for instance, the one formed by vectors of strictly minimal lengths) is *NP*-complete, hence computationally intractable even in relatively low dimensions. However, as is usual in this range of optimization problems, *approximate* solutions may be found at a reasonable cost. In fact, a major advance in this area is due to Lenstra, Lenstra, and Lovász [4] who were the first to give a polynomial approximation algorithm (nicknamed the ‘LLL’ algorithm); this algorithm applies in all dimensions and is of polynomial time complexity. A spectacular consequence was to provide (for the first time) an algorithm that factorizes univariate polynomials over the rationals in polynomial time.<sup>1</sup> The LLL algorithm takes its inspiration from the classical Gram–Schmidt orthogonalization process, with the important modification that orthogonalization coefficients must be approximated by integers, while the algorithm strives to keep vectors of a “reasonable” length. This results both in a default of orthogonality and a default of minimality as regards the basis that is constructed.

Since 1982, the LLL algorithm has found innumerable consequences in various branches of computational number theory, computer algebra, cryptography, and combinatorial optimization.<sup>2</sup> The

---

<sup>1</sup>The authors of [4] proceed as follows. Let  $f$  be the initial polynomial (with integer coefficients) and  $h$  be an irreducible factor of  $f \pmod{p^n}$ . The set of polynomials of degree one which reduce modulo  $p^n$  to a multiple of  $h$  is a lattice, and this lattice contains a vector of (relatively) short length if and only if it contains a multiple of the irreducible factor of  $f$  corresponding to  $h$ .

<sup>2</sup>An example of application at the crossroads of combinatorial optimization and cryptography is the Knapsack Problem.

superb book of von zur Gathen and Gerhard [5] devotes Chapters 16 and 17 to the question and offers a very readable account.

The talk presents two new notions of reduction that are structurally weaker than LLL reduction. These are called Gram reduction and Schmidt reduction. Regarding the algorithms associated to these reductions, not much gain is perceptible in the worst case when compared to LLL reduction. However, interesting differences start appearing in the average case. In contrast, the relaxation of constraints afforded by Gram or Schmidt reduction brings measurable benefits in many cases to be encountered in practice. We refer to Akhavi’s Ph.D. thesis and especially to his paper [1] for a precise description of the algorithms involved. In what follows, we focus on modelling issues.

A simple and natural model of what a *random lattice* is can be described as follows: take a system of  $p$  vectors  $(e_1, \dots, e_p)$  chosen uniformly and independently inside the unit ball of  $\mathbb{R}^n$  (with  $n \geq p$ ). Let  $\ell_j$  denote the length of the  $j$ th element of the orthogonalized version according to the classical Gram–Schmidt procedure (in the real domain). Daudé and Vallée have shown that each  $\ell_j$  has a distribution that is asymptotically of the Beta type, with probability density proportional to  $u^{n-j}(1-u^2)^{(j-1)/2}$ ; see [3]. A consequence of the estimates of [3] is the following upper bound for the expected number  $E(K)$  of iterations of the LLL algorithm over inputs bounded from above by  $M$ ,

$$E(K) \leq \frac{n^2}{\log t} \left( \frac{\log n}{2} + 3 \right) + n + 3n^2 \frac{\log_t M}{M^{1/3}}.$$

(There  $t \in (1, 2)$  is a control parameter which influences the performance of the reduction algorithm.) This result implies an upper bound on the number of iterations of the order of  $n^2 \log n$ .

Akhavi improves the estimates of [3]. The noticeable fact here is the presence of *thresholds*. Consider a large dimension  $n$  together with the lengths of the  $a$ th and  $b$ th (standard Gram–Schmidt) orthogonalized vectors in  $\mathbb{R}^n$ . Then one has (Theorem 8 of [1]):

1. If  $a = \alpha n + i$  and  $b = \beta n + j$  with fixed  $0 < \alpha < \beta < 1$ , then the ratio  $\ell_b/\ell_a$  exhibits a sharp threshold: the random variable  $\ell_b/\ell_a$  is with high probability concentrated around its mean, namely  $\theta_0 := \sqrt{1-\alpha}/\sqrt{1-\beta}$ .
2. If  $a = n - i$  and  $b = n - j$ , then the ratio  $\ell_b/\ell_a$  is governed by a modified Beta distribution (that admits a continuous density).

These results quantify precisely the “evolution” of the lengths of vectors during the orthogonalization process. They describe in fact two regimes, one with sharp thresholds is relative to the “initial” steps of the process while the other with continuous transitions describes what happens at the end.

Technically, the geometry of the problem leads to multidimensional integrals that one needs to estimate asymptotically. The method of choice here is the Laplace method for integrals as described for instance in [2]. The general method needs to be amended for the case at hand and Akhavi offers in [1] a valuable discussion of the asymptotics of 2-dimensional Laplace integrals when taken over polygonal domains. Naturally, the discussion bases itself on whether the maximum of the integrand lies inside, on the boundary, or outside of the integration domain. The net result is the precise quantification summarized above.

Finally, the estimates are put to use in order to analyse three reduction methods, in the sense of Siegel, Gram, and Schmidt. It turns out that, by relaxing the LLL conditions, the new reduced bases are obtained faster (see Theorem 9 of [1] for precise statements). An experimental study is conducted that supports the theoretical results. First, under the uniform model, there is little loss in the quality of the bases produced. Next the reduction of lattices associated with the “Subset

Sum” problem are considered: these are of cryptographic relevance (in connection with the Schnorr–Euchner system) and Akhavi reports computational gains by a factor in the range 2–5, while the new reduced bases obtained prove to be of a quality comparable to what classical reduction algorithms provide.

### Bibliography

- [1] Akhavi (Ali). – Threshold phenomena in random lattices and efficient reduction algorithms. In Nešetřil (Jaroslav) (editor), *Algorithms, ESA'99. Lecture Notes in Computer Science*, vol. 1643, pp. 476–489. – Springer, Berlin, 1999. Proceedings of the 7th Annual European Symposium, Prague, Czech Republic, July 1999.
- [2] Bleistein (Norman) and Handelsman (Richard A.). – *Asymptotic expansions of integrals*. – Dover Publications Inc., New York, 1986, xvi+425p. A reprint of the second Holt, Rinehart and Winston edition, 1975.
- [3] Daudé (Hervé) and Vallée (Brigitte). – An upper bound on the average number of iterations of the LLL algorithm. *Theoretical Computer Science*, vol. 123, n° 1, 1994, pp. 95–115. – Number theory, combinatorics and applications to computer science (Marseille, 1991).
- [4] Lenstra (A. K.), Lenstra (H. W., Jr.), and Lovász (L.). – Factoring polynomials with rational coefficients. *Mathematische Annalen*, vol. 261, n° 4, 1982, pp. 515–534.
- [5] von zur Gathen (Joachim) and Gerhard (Jürgen). – *Modern computer algebra*. – Cambridge University Press, New York, 1999, xiv+753p.