

Modelling the LLL Algorithm by Sandpiles

Manfred Madritsch and Brigitte Vallée

GREYC, CNRS and University of Caen, 14032 Caen Cedex (France)

Abstract. The LLL algorithm aims at finding a “reduced” basis of a Euclidean lattice and plays a primary role in many areas of mathematics and computer science. However, its general behaviour is far from being well understood. There are already many experimental observations about the number of iterations or the geometry of the output, that raise challenging questions which remain unanswered and lead to natural conjectures which are yet to be proved. However, until now, there exist few experimental observations about the precise execution of the algorithm. Here, we provide experimental results which precisely describe an essential parameter of the execution, namely the “logarithm of the decreasing ratio”. These experiments give arguments towards a “regularity” hypothesis (R). Then, we propose a simplified model for the LLL algorithm based on the hypothesis (R), which leads us to discrete dynamical systems, namely sandpiles models. It is then possible to obtain a precise quantification of the main parameters of the LLL algorithm. These results fit the experimental results performed on general input bases, which indirectly substantiates the validity of such a regularity hypothesis and underlines the usefulness of such a simplified model.

Introduction

Lenstra, Lenstra, and Lovász designed the LLL algorithm [10] in 1982 for solving integer programming problems and factoring polynomials. This algorithm belongs to the general framework of lattice basis reduction algorithms and solves a general problem: Given a basis for a lattice, how to find a basis for the same lattice, which enjoys good euclidean properties? Nowadays, this algorithm has a wide area of applications and plays a central algorithmic role in many areas of mathematics and computer science, like cryptology, computer algebra, integer linear programming, and number theory. However, even if its overall structure is simple (see Figure 1), its general probabilistic behaviour is far from being well understood. A precise quantification of the main parameters which are characteristic of the algorithms —principally, the number of iterations and the geometry of reduced bases— is yet unknown. The works of Gama, Nguyen and Stehlé [6,11] provide interesting experiments, which indicate that the geometry of the output seems to be largely independent of the input distribution, whereas the number of iterations is highly dependent on it. The article of Daudé and Vallée [5] provides a precise description of the probabilistic behaviour of these parameters (number of iterations, geometry of the output), but only in the particular case in which the vectors of the input basis are independently chosen in the unit ball. This

input distribution does not arise naturally in applications. In summary, the first works [6,11] study general inputs, but do not provide proofs, whereas the second one [5] provides proofs, but for non realistic inputs. Furthermore, none of these studies is dedicated to the fine understanding of the internal structure of the algorithm.

The LLL algorithm is a multidimensional extension, in dimension n , of the Euclid algorithm (obtained for $n = 1$) or the Gauss algorithm (obtained for $n = 2$). In these small dimensions, the dynamics of the algorithms is now well understood and there exist precise results on the probabilistic behaviour of these algorithms [12,13,14] which are obtained by using the dynamical systems theory, as well as its related tools. However, even in these small dimensions, the dynamics is rather complex and it does not seem possible to directly describe the fine probabilistic properties of the internal structure of the LLL algorithm in an exact way.

This is why we introduce here a simplified model of the LLL algorithm, which is based on a regularity hypothesis: Whereas the classical version deals with a decreasing factor which may vary during the algorithm, the simplified version assumes *this decreasing factor to be constant*. Of course, this appears to be a strong assumption, but we provide arguments towards this simplification. This assumption leads us to a classical model, the *sandpile model*, and this provides another argument for such a simplification.

Sandpile models are instances of dynamical systems which originate from observations in Nature [9]. They were first introduced by Bak, Tang and Wiesenfeld [3] for modelling sandpile formations, snow avalanches, river flows, etc.. By contrast, the sandpiles that arise in a natural way from the LLL algorithm are not of the same type as the usual instances, and the application of sandpiles to the LLL algorithm thus needs an extension of classical results.

Plan of the paper. Section 1 presents the LLL algorithm, describes a natural class of probabilistic models, and introduces the simplified models, based on the regularity assumption. Section 2 provides arguments for the regularity assumption. Then, Section 3 studies the main parameters of interest inside the simplified models, namely the number of iterations, the geometry of reduced bases, and the independence between blocks. Section 4 then returns to the actual LLL algorithm, within the probabilistic models of Section 1, and exhibits an excellent fitting between two classes of results : the proven results in the simplified model, and the experimental results that hold for the actual LLL algorithm. This explains why these “regularized” results can be viewed as a first step for a probabilistic analysis of the LLL algorithm.

1 The LLL Algorithm and Its Simplified Version

1.1 Description of the Algorithm

The LLL algorithm considers a Euclidean lattice \mathcal{L} given by a system B of n linearly independent vectors in the ambient space \mathbb{R}^p ($n \leq p$). It aims at finding