7/12/2017

"Fast LLL basis reduction"

PhD research proposal

CSC - ENS de Lyon - École Doctorale InfoMaths

Laboratoire de l'Informatique du Parallélisme - LIP `http://www.ens-lyon.fr/LIP`
UDL, CNRS, Inria, ENS de Lyon, UCB Lyon 1

Project team: Arithmetic and Computing - AriC `http://www.ens-lyon.fr/LIP/AriC`

Supervisor: Gilles Villard gilles.villard@ens-lyon.fr `http://perso.ens-lyon.fr/gilles.villard`

Keywords: lattice, lattice basis reduction, algorithm design and implementation, computer algebra, numerical analysis, cryptography, algorithmic complexity, multicore programming.

Lattice basis reduction is a key tool in various domains of computer science, electrical engineering and mathematics, such as computer algebra and cryptography (see, e.g. [1]), and is a very active field on both theoretical and practical sides. Advances in the understanding of algorithmic aspects of the reduction impact many fields.

A lattice is a set of integer combinations of linearly independent vectors in a euclidean space, and admits infinitely many bases. For applications one looks for bases with "rather short" vectors. The LLL algorithm [2] allows to find reasonaly short bases in time polynomial in the bit-size of the input. The record complexity bounds for the LLL reduction have been recently improved by AriC members (see $[3-5]$), one may think however that it remains room for improvement. The long term goal is to obtain bounds as close as possible to those available for matrix multiplication.

The purpose of this PhD project is to improve our theoretical and practical understanding of LLL reduction. We may hope to lower the complexity bounds for the reduction, and provide faster implementations within the `fplll` software library (and the more experimental one `hplll`). Aspects considered should include the:

- study of the interplay between lattice reduction and numerical linear algebra;
- comparison of "iterative" and "dynamical system" based approaches;
- use of fast linear algebra kernels in implementations;
- use parallel API such as OpenMP for acceleration of high performance codes on multicores.

AriC in Lyon, one of the international leading teams on the topic, will host this project.

[1] P. Q. Nguyen and B. Vallée (editors). The LLL Algorithm: Survey and Applications. Information Security and Cryptography. Springer-Verlag, 2009.

[2] A.K. Lenstra, H.W. Lenstra,and L. Lovász. Factoring polynomials with rational coefficients. Mathematische Annalen, 261:515–534, 1982.

[3] G. Hanrot, X. Pujol, D. Stehlé. Analyzing Blockwise Lattice Algorithms using Dynamical Systems. Proceedings of the 31st International Cryptology Conference, Santa Barbara, California, USA, 2011.

[4] A. Neumaier, D. Stehlé. Faster LLL-type reduction of lattice bases. Proceedings of the 41st International Symposium on Symbolic and Algebraic Computation, Waterloo, Ontario, Canada, 2016.

[5] A. Novocin, D. Stehlé, G. Villard. An LLL-reduction algorithm with quasi-linear time complexity. Proceedings of the 43rd ACM Symposium on Theory of Computing, San Jose, California, USA, 2011.

`FPLLL`: a lattice reduction library. Available at `https://github.com/fplll/fplll`

`HPLLL`: `http://perso.ens-lyon.fr/gilles.villard/hplll`