Review of the book

"The LLL Algorithm"

Nguyen and Vallée (editors)

Springer, 2010

ISBN: 978-3-642-02294-4

Steven Galbraith
Department of Mathematics, The University of Auckland, New Zealand

July 1, 2011

1 Summary of the review

Lattices, lattice reduction and the Lenstra-Lenstra-Lovász (LLL) algorithm are fundamental tools in computational number theory. They have a long tradition in cryptanalysis: starting with attacks on knapsack cryptosystems (by Shamir, Odlyzko, Lagarias and others) and, later, attacks on variants of RSA (via Coppersmith's method). Lattices (again, using Coppersmith's method) have also been used as components of security proofs (e.g. RSA-OAEP) and as a tool for bit security results (e.g., the hidden number problem). Recently, the hottest research area in public key cryptography has been the study of cryptosystems whose security relies on computational problems in lattices.
There has long been a need for a comprehensive and advanced text on lattices, the LLL algorithm, and applications. This book, comprising independent chapters written by a number of different people, authoritatively fills the gap in the literature. It is required reading for all researchers in the field, and will become a standard reference for many results about lattices and LLL.
There are previous books that deal with some of these topics, starting with Lovász's book from 1986, and going up to more recent volumes such as the proceedings of the CaLC conference (2001) and the book by Micciancio and Goldwasser (2002). But they are all mostly superseded by the book under review.
The editors have made an outstanding selection of contributing authors. Every important topic in the field is addressed in the book, and the chapters have been written by leading researchers. All the papers have an extensive bibliography.

2 Summary of the book

The LLL algorithm is truly one of the beautiful algorithms of nature. In two dimensions it is closely related to Euclid's algorithm and the continued fraction algorithm, so it can be considered as a high-dimensional generalisation of those algorithms. As with those famous algorithms, it has found numerous applications in branches of mathematics as diverse as integer programming, polynomial factorisation and cryptography. Another close similarity with the Euclidean and continued fraction algorithms is that LLL is rather simple to write down, yet the theoretical analysis is deep and subtle.
We now briefly discuss the individual chapters.

- Chapter 1 describes the history of the development of the algorithm and its early applications in optimisation and polynomial factorisation. Both Hendrik Lenstra and Laszlo Lovász give candid descriptions of their contribution and motivations. There are some wonderful photographs, and the reproduction of Lenstra's "excited postcard" to Lovász serves as both a valuable historial artifact, and also a reminder of how email has changed the way we do research.

- Chapter 2 sets the scene. Nguyen introduces the LLL algorithm and Hermite-Korkine-Zolotarev (HKZ) reduction, as well as the Lagrange algorithm (the two-dimensional version of LLL). One fascinating feature of this chapter is that it connects these algorithms with (older) theoretical investigations of Hermite's constant.

- In Chapter 3, Vallée describes the subtleties in analysing precisely the "average case" performance of lattice reduction algorithms, even in only two-dimensions. The chapter gives an extensive discussion of techniques used in the probabilistic analysis of such algorithms. This chapter is long and quite technical, but would serve as a springboard to the literature for a dedicated reader.

- Chapters 4 and 5 are both about implementing LLL using floating point arithmetic. The issue is that the LLL algorithm keeps track of the Gram-Schmidt orthogonalisation (GSO) of the current lattice basis. If the GSO vectors are represented using exact arithmetic (assuming that the original basis is given by exact integers or rational numbers) then the numbers involved become enormous and the algorithm becomes very slow. Instead, it is better to represent the GSO using floating point arithmetic, but then the usual problems of rounding errors and accuracy arise. Indeed, it is no longer clear that the algorithm has the desired properties. Schnorr and Stehlé discuss a number of techniques and variants of LLL that have evolved to deal with these issues. These chapters (I recommend they be read in parallel) are quite technical, but will be required reading for anyone serious about implementing LLL or trying to understand the performance of LLL for large dimension lattices.

- Chapters 6 to 8 sketch a number of applications of lattices in "mainstream" computational number theory. Chapter 6 (by Hanrot) is a delightful tour through diophantine approximation, with particular emphasis on how LLL can be used to provide negative results. Details are given of the famous disproof by Odlyzko and te Riele of the Mertens' conjecture. The chapter also contains a very good discussion of finding small solutions to inhomogenous linear equations. Chapter 7 (by Simon) is somewhat sketchy, but indicates (with examples) a number of applications of LLL in number theory. Chapter 8 (by Klüners) discusses polynomial factorisation, especially a recent algorithm due to van Hoeij.

- Chapter 9 is about integer programming, which was the historical starting-point of the LLL algorithm. Aardal and Eisenbrand give a very readable survey of this subject, with an excellent bibliography.

- In Chapter 10, May presents Coppersmith's method (mainly the univariate method, but there is also some discussion of the multivariate method) and gives a large number of applications to cryptanalysis of variants of RSA. This topic has been one of the major aspects of lattices in cryptanalysis since the mid 1990s. There is a very nice table that summarises these methods (page 340) and an extensive bibliography.

- Hoffstein, in Chapter 11, discusses the NTRU encryption and signature schemes. These schemes have excellent performance, but only heuristic security (based on computational problems in lattices). Since this book was written, Stehlé and Steinfeld have shown how to modify NTRU so that it fits into the framework of cryptosystems based on learning with errors (see Chapter 13).

- Chapter 12 presents a number of situations where lattices (usually Coppersmith's method) are used as a tool in security reductions for cryptosystems. Gentry discusses the RSA-OAEP saga in detail, and the various "fixes" for RSA-OAEP are sketched. The chapter also presents Rabin-SAEP, some elegant methods to compress Rabin signatures, some results about the Paillier cryptosystem, and a short discussion of the hidden number problem and bit security of Diffie-Hellman.

- Chapter 13 concerns modern lattice-based cryptosystems. Micciancio is one of the pioneers of this field, and the chapter gives a thorough discussion of several schemes with excellent theoretical properties. This research area is extremely fast-moving and, nowadays, the learning with errors (LWE) cryptosystem has become dominant. So this chapter does not represent the current state-of-the-art.

- Chapters 14 and 15 discuss complexity results about computational problems in lattices. Khot is mainly concerned with NP-hardness results for the standard computational problems in lattices (such as the shortest vector problem). Regev considers the more subtle problem of showing the hardness of approximate versions of these computational problems (e.g., where the goal is not to produce a non-zero lattice vector of minimal length, but one whose length is within a polynomial factor of the minimal length).

3 What is the book like (style)?

Despite the fact that the chapters are all written by different authors, the style is relatively consistent (though, as always seems to be the case, the community cannot agree on whether vectors should be written as columns or rows). Most of the chapters do not contain complete and detailed proofs; rather the emphasis is on sketches of arguments, and examples. All the authors have made a serious and successful attempt to write for a relatively general audience.
The strengths of the book are its breadth and authority. It covers all the main applications of the LLL algorithm in number theory, optimisation, cryptography and cryptanalysis. The chapters are written by leaders in the field.
Two unfortunate features of the book are that it does not have an index and that sections are not numbered. The lack of section numbers inconveniences authors who wish to refer to precise parts of the book (and indeed, this has inconvenienced the contributors to the book itself). As far as I can see, there is currently no errata for the book on the web, which is a pity as there are inevitably a few minor typographical errors.

4 Would you recommend this book?

This book is strongly recommended for students and researchers in lattices or lattice-cryptography. The book is not written for novices, and most chapters assume a solid background in mathematics. But I believe that, with a small amount of additional background reading, it will be valuable even for Masters or beginning PhD students.

The reviewer is an Associate Professor at the Department of Mathematics at the University of Auckland, New Zealand.