Information Security and Cryptography
Texts and Monographs

Phong Q. Nguyen • Brigitte Vallée
Editors

The LLL Algorithm

Survey and Applications

Springer

Editors
Dr. Phong Q. Nguyen
INRIA Research Director
École Normale Supérieure
Département d'Informatique
Paris, France
phong.nguyen@ens.fr

Dr. Brigitte Vallée
CNRS Research Director
and Research Director
Département d'Informatique
Université de Caen, France
brigitte.vallee@info.unicaen.fr

ISSN 1619-7100
ISBN 978-3-642-02294-4 e-ISBN 978-3-642-02295-1
DOI 10.1007/978-3-642-02295-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2009934498

ACM Computing Classification (1998): F.2, F.1, E.3, G.1

Cover design: KuenkelLopka GmbH

Printed on acid-free paper

Springer is a part of Springer Science+Business Media (www.springer.com)

Preface

Computational aspects of geometry of numbers have been revolutionized by the Lenstra–Lenstra–Lovász lattice reduction algorithm (LLL), which has led to breakthroughs in fields as diverse as computer algebra, cryptology, and algorithmic number theory. After its publication in 1982, LLL was immediately recognized as one of the most important algorithmic achievements of the twentieth century, because of its broad applicability and apparent simplicity. Its popularity has kept growing since, as testified by the hundreds of citations of the original article, and the ever more frequent use of LLL as a synonym to lattice reduction.

As an unfortunate consequence of the pervasiveness of the LLL algorithm, researchers studying and applying it belong to diverse scientific communities, and seldom meet. While discussing that particular issue with Damien Stehlé at the 7th Algorithmic Number Theory Symposium (ANTS VII) held in Berlin in July 2006, John Cremona accurately remarked that 2007 would be the 25th anniversary of LLL and this deserved a meeting to celebrate that event. The year 2007 was also involved in another arithmetical story. In 2003 and 2005, Ali Akhavi, Fabien Laguillaumie, and Brigitte Vallée with other colleagues organized two workshops on cryptology and algorithms with a strong emphasis on lattice reduction: CAEN '03 and CAEN '05, CAEN denoting both the location and the content (*Cryptologie et Algorithmique En Normandie*). Very quickly after the ANTS conference, Ali Akhavi, Fabien Laguillaumie, and Brigitte Vallée were thus readily contacted and reacted very enthusiastically about organizing the LLL birthday conference. The organization committee was formed.

Within a couple of months, the three L's, Arjen and Hendrik Lenstra, and László Lovász, kindly accepted to participate, which provided confidence to the organizing team. At the same time, a program committee was created. Its members – Karen Aardal, Shafi Goldwasser, Phong Nguyen, Claus Schnorr, Denis Simon, and Brigitte Vallée – come from diverse fields, so as to represent as many LLL-practitioners as possible. They invited speakers to give overview talks at the conference.

The anniversary conference eventually took place between 29th June and 1st July 2007, at the University of Caen. During these three days, 14 invited talks were given on topics closely related to the LLL algorithm. A poster session gathered 12 presentations on ongoing research projects. Overall, 120 researchers from 16 countries and very diverse scientific backgrounds attended the event. And naturally,

a birthday party was set and the three L's blew out the candles of their algorithm's birthday cake!

Unlike many other domains, the community misses a reference book dealing with almost all aspects of lattice reduction. One important goal of the conference was to provide such material, which may be used by both junior and senior researchers, and hopefully even useful for undergraduate students. The contributors were selected to make such a collective book possible. This book is a brief (and inevitably incomplete) snapshot of the research, which was sparked by the publication of the LLL algorithm in 1982. The survey articles were written to be accessible by a large audience, with detailed motivations, explanations, and examples. We hope they will help pursuing further research on this very rich topic. Each article of the present book can be read independently and provides an introductory overview of the results obtained in each particular area in the past 25 years.

The first contribution of this book, by Ionica Smeets and in collaboration with Arjen Lenstra, Hendrik Lenstra, László Lovász, and Peter van Emde Boas, describes the genesis of the LLL algorithm. The rest of the book may be informally divided into five chapters, each one essentially matching a session of the anniversary conference.

The first chapter deals with algorithmic aspects of lattice reduction, independently of applications. The first article of that chapter, by Phong Nguyen, introduces lattices, and surveys the main provable algorithms for finding the shortest vector in a lattice, either exactly or approximately. It emphasizes a somewhat overlooked connection between lattice algorithms and Hermite's constant, that is, between computational and mathematical aspects of the geometry of numbers. For instance, LLL is presented as an (efficient) algorithmic version of Hermite's inequality on Hermite's constant. The second article, by Brigitte Vallée and Antonio Vera, surveys the probabilistic analysis of several lattice reduction algorithms, in particular LLL and Gauss' algorithm. Different random models for the input bases are considered and the result introduces sophisticated analytic tools as complex and functional analysis. The third article, by Claus Schnorr, surveys provable and heuristic algorithmic variations around LLL, to make the algorithm more efficient or with better outputs. For example, the fruitful notion of blockwise reduction is a natural generalization of LLL. The fourth article, by Damien Stehlé, surveys all aspects of floating-point lattice reduction. The different analyses exhibit the parameters that play an important role when relating the execution time of the floating-point versions of LLL to the quality of the output. Both provable and heuristic versions of the algorithm are considered.

The second chapter is concerned with the applications of lattice reduction in the vast field of algorithmic number theory. Guillaume Hanrot's article describes several efficient algorithms to solve diverse Diophantine approximation problems. For example, these algorithms relying on lattice reduction tackle the problems of approximating real numbers by rational and algebraic numbers, of disclosing linear relations and of solving several Diophantine equations. Denis Simon's paper contains a collection of examples of problems in number theory that are solved efficiently via lattice reduction. Among others, it introduces a generalization of the

LLL algorithm to reduce indefinite quadratic forms. Finally, the article by Jürgen Klüners surveys the original application of the LLL, namely factoring polynomials with rational coefficients. It compares the original LLL factoring method and the recent one developed by Mark von Hoeij, which relies on the knapsack problem.

The third chapter contains a single article, by Karen Aardal and Friedrich Eisenbrand. It surveys the application of the LLL algorithm to integer programming, recalling Hendrik Lenstra's method – an ancestor of the LLL algorithm, and describing recent advances.

The fourth chapter is devoted to an important area where lattices have been applied with much success, both in theory and practice: cryptology. Historically, LLL and lattices were first used in cryptology for "destructive" purposes: one of the very first applications of LLL was a practical attack on the Merkle–Hellman knapsack public-key cryptosystem. The success of reduction algorithms at breaking various cryptographic schemes since the discovery of LLL have arguably established lattice reduction techniques as the most popular tool in public-key cryptanalysis. Alexander May's article surveys one of the major applications of lattices to cryptanalysis: lattice attacks on the RSA cryptosystem, which started in the late eighties with Håstad's work, and has attracted much interest since the mid-nineties with Coppersmith's method to find small roots of polynomials. The other two articles of the chapter deal instead with "positive" applications of lattices to cryptography. The NTRU paper by Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, and William Whyte gives an excellent example of an efficient cryptosystem whose security relies on the concrete hardness of lattice problems. The paper by Craig Gentry surveys security proofs of non-lattice cryptographic schemes in which lattices make a surprising appearance. It is perhaps worth noting that lattices are used both to attack RSA in certain settings, and to prove the security of industrial uses of RSA.

The final chapter of the book focuses on the complexity of lattice problems. This area has attracted much interest since 1996, when Miklós Ajtai discovered a fascinating connection between the worst-case and average-case complexity of certain lattice problems. The contribution of Daniele Micciancio deals with (lattice-based) cryptography from worst-case complexity assumptions. It presents recent cryptographic primitives whose security can be proven under worst-case assumptions: any instance of some well-known hard problem can be solved efficiently with access to an oracle breaking random instances of the cryptosystem. Daniele Micciancio's article contains an insightful discussion on the concrete security of lattice-based cryptography. The last two articles of the book, by respectively Subhash Khot and Oded Regev, are complementary. The article by Subhash Khot surveys inapproximability results for lattice problems. And the article by Oded Regev surveys the so-called limits to inapproximability results for lattice problems, such as the proofs that some approximation lattice problems belong to the complexity class coNP. It also shows how one can deduce zero-knowledge proof systems from the previous proofs.

Acknowledgements We, the editors, express our deep gratitude to the organizing committee comprised of Ali Akhavi, Fabien Laguillaumie, and Damien Stehlé. We also acknowledge with gratitude the various forms of support received from our sponsors; namely, CNRS, INRIA, Université de Caen, Mairie de Caen, Pôle TES, as well as several laboratories and research groups (LIP, GREYC, LIAFA, Laboratoire Elie Cartan, LIENS, GDR IM, ECRYPT, Orange Labs). Together with all participants, we were naturally extremely happy to benefit from the presence of the three **L**'s and our thanks are extended to Peter van Emde Boas for providing invaluable historical material. We also wish to thank all the speakers and participants of the conference LLL+25. Finally, we are indebted to Loick Lhote for his extensive help in the material preparation of this book.

Paris, August 2009

Phong Nguyen and Brigitte Vallée
Caen

Foreword

I have been asked by my two co-L's to write a few words by way of introduction, and consented on the condition of being allowed to offer a personal perspective.

On 1 September 2006, the three of us received an e-mail from Brigitte Vallée. John Cremona, she wrote, had suggested the idea of celebrating the 25th anniversary of the publication of "the LLL paper," and together with Ali Akhavi, Fabien Laguillaumie, and Damien Stehlé, she had decided to follow up on his suggestion. As it was "not possible to celebrate this anniversary without (...) the three L's of LLL," she was consulting us about suitable dates. I was one of the two L's who were sufficiently flattered to respond immediately, and the dates chosen turned out to be convenient for number three as well.

In her very first e-mail, Brigitte had announced the intention of including a historical session in the meeting, so that we would have something to do other than cutting cakes and posing for photographers. Hints that some of my own current work relates to lattices were first politely disregarded, and next, when I showed some insistence, I was referred to the Program Committee, consisting of Karen Aardal, Shafi Goldwasser, Phong Nguyen, Claus Schnorr, Denis Simon, and Brigitte herself. This made me realize which role I was expected to play, and I resolved to wait another 25 years with the new material.

As the meeting came nearer, it transpired that historical expertise was not represented on the Program Committee, and with a quick maneuver I seized unrestricted responsibility for organizing the historical session. I did have the wisdom of first securing the full cooperation of LLL's court archivist Peter van Emde Boas. How successful the historical session was, reported on by Ionica Smeets in the present volume, is not for me to say. I did myself learn a few things I was not aware of, and do not feel ashamed of the way I played my role.

All three L's extended their stay beyond the historical session. Because of the exemplary way in which the Program Committee had acquitted themselves in this job, we can now continue to regard ourselves as universal experts on all aspects of lattice basis reduction and its applications.

John Cremona, apparently mortified at the way his practical joke had run out of hand, did not show up, and he was wrong. John, it is my pleasure to thank you most cordially on behalf of all three L's. Likewise, our thanks are extended not only to everybody mentioned above, but also to all others who contributed to the success of the meeting, as speakers, as participants, as sponsors, or invisibly behind the scenes.

Leiden,
August 2008 *Hendrik Lenstra*

Contents

List of Contributors

Karen Aardal Delft Institute of Applied Mathematics, TU Delft, Mekelweg 4, 2628 CD Delft, The Netherlands and CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands, k.i.aardal@tudelft.nl

Friedrich Eisenbrand EPFL, MA C1 573 (Bâtiment MA), Station 8, CH-1015 Lausanne, Switzerland, friedrich.eisenbrand@epfl.ch

Peter van Emde Boas ILLC, Depts. of Mathematics and Computer Science, Faculty of Sciences, University of Amsterdam, The Netherlands, peter@bronstee.com

Craig Gentry Stanford University, USA, cgentry@cs.stanford.edu

Guillaume Hanrot INRIA/LORIA, Projet CACAO - Bâtiment A, 615 rue du jardin botanique, F-54602 Villers-lès-Nancy Cedex, France, hanrot@loria.fr

Jeff Hoffstein NTRU Cryptosystems, 35 Nagog Park, Acton, MA 01720, USA, jhoffstein@ntru.com

Nick Howgrave-Graham NTRU Cryptosystems, 35 Nagog Park, Acton, MA 01720, USA, nhowgravegraham@ntru.com

Subhash Khot New York University, New York, NY-10012, USA, khot@cs.nyu.edu

Jürgen Klüners Mathematisches Institut, Universität Paderborn, Warburger Str. 100, 30098 Paderborn, Germany. klueners@math.uni-paderborn.de

Arjen K. Lenstra EPFL IC LACAL, Station 14, Lausanne, Switzerland, arjen.lenstra@epfl.ch

Hendrik W. Lenstra Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands, hwl@math.leidenuniv.nl

László Lovász Eötvös Loránd Tudományegyetem, Számitógéptudományi Tanszék, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary, lovasz@cs.elte.hu

Alexander May Horst Görtz Institute for IT-Security, Faculty of Mathematics, Ruhr-University Bochum, Germany, alex.may@ruhr-uni-bochum.de

Daniele Micciancio Department of Computer Science and Engineering, University of California at San Diego, La Jolla CA 92093, USA, daniele@cs.ucsd.edu

Phong Nguyen Department of Computer Science, Ecole Normale Supérieure de Paris, 45 rue d'Ulm, 75230 Paris Cedex 05, France, Phong.Nguyen@ens.fr

Jill Pipher NTRU Cryptosystems, 35 Nagog Park, Acton, MA 01720, USA, jpipher@ntru.com

Oded Regev School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel, odedr@post.tau.ac.il

Claus Peter Schnorr Fachbereich Informatik und Mathematik, Universität Frankfurt, PSF 111932, D-60054 Frankfurt am Main, Germany, schnorr@cs.uni-frankfurt.de

Ionica Smeets Mathematisch Institut, Universiteit Leiden, Niels Bohrweg 1, 2333 CA Leiden, Netherlands, smeets@math.leidenuniv.nl

Denis Simon Université de Caen, LMNO, Bd Maréchal Juin BP 5186 – 14032 Caen Cedex, France, simon@math.unicaen.fr

Damien Stehlé CNRS/Universities of Macquarie, Sydney and Lyon/INRIA/ÉNS Lyon, Dept of Mathematics and Statistics, University of Sydney, NSW 2008, Australia, damien.stehle@gmail.com

Brigitte Vallée Laboratoire GREYC, CNRS UMR 6072, Université de Caen and ENSICAEN, F-14032 Caen, France, brigitte.vallee@info.unicaen.fr

Antonio Vera Laboratoire GREYC, CNRS UMR 6072, Université de Caen and ENSICAEN, F-14032 Caen, France, antonio.vera@info.unicaen.fr

William Whyte NTRU Cryptosystems, 35 Nagog Park, Acton, MA 01720, USA, wwhyte@ntru.com