Complexity Of Lattice Problems A Cryptographic Perspective The Springer International Series In Engineering And Computer Science

Second International Conference on Formal Concept Analysis, ICFCA 2004, Sydney, Australia, February 23-26, 2004, Proceedings
29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010, Proceedings
Concept Lattices
Handbook of Convex Geometry
26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings
Formal Concept Analysis
The Classical Decision Problem
6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings
21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I
Complexity of Lattice Problems
Completeness and Reduction in Algebraic Complexity Theory
Advances in Cryptology - EUROCRYPT 2010
Complexity of Infinite-Domain Constraint Satisfaction
23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings
Complexity of Lattice Problems
Public-Key Cryptography – PKC 2018
Algorithms for the Closest and Shortest Vector Problems on General Lattices
Advances in Cryptology – EUROCRYPT 2008
Covering Codes
Algorithmic Number Theory
Mathematics of Public Key Cryptography
An Algorithmic Theory of Numbers, Graphs and Convexity
International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers
Computational Complexity of Lattice Problems
Geometry and Complexity Theory
Mathematical Foundations
27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008, Proceedings
Post-Quantum Cryptography
Random Processes on Graphs and Lattices
Computational Complexity
Lattice Basis Reduction
The LLL Algorithm
Probability on Graphs
Foundations of Data Science
Mathematics and Computation

Introduction to the Theory of Complexity
Advances in Cryptology - ASIACRYPT 2008
Survey and Applications
A Theory Revolutionizing Technology and Science
Encyclopedia of Cryptography and Security

FRANCIS LI

Second International Conference on Formal Concept Analysis, ICFCA 2004, Sydney, Australia, February 23-26, 2004, Proceedings SIAM
This advanced graduate textbook gives an authoritative and insightful description of the major ideas and techniques of public key cryptography.
29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010, Proceedings Springer Science & Business Media
Surveys most of the major developments in lattice cryptography over the past ten years. The main focus is on the foundational short integer solution (SIS) and learning with errors (LWE) problems, their provable hardness assuming the worst-case intractability of standard lattice problems, and their many cryptographic applications.
Concept Lattices Prentice Hall PTR
This introduction to some of the principal models in the theory of disordered systems leads the reader through the basics, to the very edge of contemporary research, with the minimum of technical fuss. Topics covered include random walk, percolation, self-avoiding walk, interacting particle systems, uniform spanning tree, random graphs, as well as the Ising, Potts, and random-cluster models for ferromagnetism, and the Lorentz model for motion in a random medium. This new edition features accounts of major recent progress, including the exact value of the connective constant of the hexagonal lattice, and the critical point of the random-cluster model on the square lattice. The choice of topics is strongly motivated by modern applications, and focuses on areas that merit further research. Accessible to a wide audience of mathematicians and physicists, this book can be used as a graduate course text. Each chapter ends with a range of exercises.
Handbook of Convex Geometry CRC Press
Lattices are geometric objects that can be pictorially described as the set of intersection points of an infinite, regular n-dimensional grid. De spite their apparent simplicity, lattices hide a rich combinatorial struc ture, which has attracted the attention of great mathematicians over the last two centuries. Not surprisingly, lattices have found numerous ap plications in mathematics and computer science, ranging from number theory and Diophantine approximation, to combinatorial optimization and cryptography. The study of lattices, specifically from a computational point of view, was marked by two major breakthroughs: the development of the LLL lattice reduction algorithm by Lenstra, Lenstra and Lovasz in the early 80's, and Ajtai's discovery of a connection between the worst-case and average-case hardness of certain lattice problems in the late 90's. The LLL algorithm, despite the relatively poor quality of the solution it gives in the worst case, allowed to devise polynomial time solutions to many classical problems in computer science. These include, solving integer programs in a fixed number of variables, factoring polynomials over the rationals, breaking knapsack based cryptosystems, and finding solutions to many other Diophantine and cryptanalysis problems.
26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings Springer
The shortest vector problem (SVP) and closest vector problem (CVP) are the most widely known problems on point lattices. SVP and CVP have been extensively studied both as purely mathematical problems, being central in the study of the geometry of numbers and as algorithmic problems, having numerous applications in communication theory and computer science. There are two main algorithmic techniques for solving exact SVP and CVP: enumeration and sieving. The best enumeration algorithm was given by Kannan in 1983 and solves both problems in n^{O(n)} time, where n is the dimensionality of the lattice. Sieving was introduced by Ajtai, Kumar and Sivakumar in 2001 and lowered the time complexity of SVP to 2^{O(n)}, but required $2^{O(n)}$ space and randomness. This result posed a number of important questions: Could we get a \emph{deterministic} 2^{O(n)} algorithm for SVP? Is it possible to acquire a 2^{O(n)} algorithm for CVP?. In this dissertation we give new algorithms for SVP and CVP and resolve these questions in the affirmative. Our main result is a \emph{deterministic} Õ(2^{2n}) time and Õ(2^n) space that solves both SVP and CVP and by reductions of (Micciancio, 2008) most other lattice problems in NP considered in the literature. In the case of CVP the algorithm improves the time complexity from n^{O(n)} to 2^{O(n)}, while for SVP we achieve single exponential time as sieving, but without using randomization and improving the constant in the exponent from 2.465 (Pujol and Stehl\'e, 2010) to 2. The core of the algorithm is a new method to solve the closest vector problem with preprocessing (CVPP) that uses the Voronoi cell of the lattice (described as intersection of half-spaces) as the result of the preprocessing function. We also present our earlier results on sieving algorithms. Although the theoretical analysis of the proposed sieving algorithm gives worse complexity bounds than our new Voronoi based approach, we show that in practice sieving can be much more efficient. We propose a new heuristic sieving algorithm that performed quite well in practice, with estimated running time 2^{0.52n} and space complexity 2^{0.2n}.
Formal Concept Analysis Springer
This book constitutes the refereed proceedings of the 6th International Algorithmic Number Theory Symposium, ANTS 2004, held in Burlington, VT, USA, in June 2004. The 30 revised full papers presented together with 3 invited papers were carefully reviewed and selected for inclusion in the

book. Among the topics addressed are zeta functions, elliptic curves, hyperelliptic curves, GCD algorithms, number field computations, complexity, primality testing, Weil and Tate pairings, cryptographic algorithms, function field sieve, algebraic function field mapping, quartic fields, cubic number fields, lattices, discrete logarithms, and public key cryptosystems.

The Classical Decision Problem Springer

New and classical results in computational complexity, including interactive proofs, PCP, derandomization, and quantum computation. Ideal for graduate students.

6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings Springer Science & Business Media

Handbook of Convex Geometry, Volume B offers a survey of convex geometry and its many ramifications and connections with other fields of mathematics, including convexity, lattices, crystallography, and convex functions. The selection first offers information on the geometry of numbers, lattice points, and packing and covering with convex sets. Discussions focus on packing in non-Euclidean spaces, problems in the Euclidean plane, general convex bodies, computational complexity of lattice point problem, centrally symmetric convex bodies, reduction theory, and lattices and the space of lattices. The text then examines finite packing and covering and tilings, including plane tilings, monohedral tilings, bin packing, and sausage problems. The manuscript takes a look at valuations and dissections, geometric crystallography, convexity and differential geometry, and convex functions. Topics include differentiability, inequalities, uniqueness theorems for convex hypersurfaces, mixed discriminants and mixed volumes, differential geometric characterization of convexity, reduction of quadratic forms, and finite groups of symmetry operations. The selection is a dependable source of data for mathematicians and researchers interested in convex geometry.

21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I Springer Science & Business Media

This is a thorough and comprehensive treatment of the theory of NP-completeness in the framework of algebraic complexity theory. Coverage includes Valiant's algebraic theory of NP-completeness; interrelations with the classical theory as well as the Blum-Shub-Smale model of computation, questions of structural complexity; fast evaluation of representations of general linear groups; and complexity of immanants.

Complexity of Lattice Problems SIAM

This book constitutes the refereed proceedings of the 17th Annual International Cryptology Conference, CRYPTO'97, held in Santa Barbara, California, USA, in August 1997 under the sponsorship of the International Association for Cryptologic Research (IACR). The volume presents 35 revised full papers selected from 160 submissions received. Also included are two invited presentations. The papers are organized in sections on complexity theory, cryptographic primitives, lattice-based cryptography, digital signatures, cryptanalysis of public-key cryptosystems, information theory, elliptic curve implementation, number-theoretic systems, distributed cryptography, hash functions, cryptanalysis of secret-key cryptosystems.

Completeness and Reduction in Algebraic Complexity Theory Springer

This book constitutes the thoroughly refereed post-proceedings of the International Conference on Cryptography and Lattices, CaLC 2001, held in Providence, RI, USA in March 2001. The 14 revised full papers presented together with an overview paper were carefully reviewed and selected for inclusion in the book. All current aspects of lattices and lattice reduction in cryptography, both for cryptographic construction and cryptographic analysis, are addressed.

Advances in Cryptology - EUROCRYPT 2010 Springer

Introduces the universal-algebraic approach to classifying the computational complexity of constraint satisfaction problems.

Complexity of Infinite-Domain Constraint Satisfaction Springer

Expanded into two volumes, the Second Edition of Springer’s Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition’s base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition’s editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text’s practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings Springer Science & Business Media

The two-volume set LNCS 10769 and 10770 constitutes the refereed proceedings of the 21st IACR

International Conference on the Practice and Theory of Public-Key Cryptography, PKC 2018, held in Rio de Janeiro, Brazil, in March 2018. The 49 revised papers presented were carefully reviewed and selected from 186 submissions. They are organized in topical sections such as Key-Dependent-Message and Selective-Opening Security; Searchable and Fully Homomorphic Encryption; Public-Key Encryption; Encryption with Bad Randomness; Subversion Resistance; Cryptanalysis; Composable Security; Oblivious Transfer; Multiparty Computation; Signatures; Structure-Preserving Signatures; Functional Encryption; Foundations; Obfuscation-Based Cryptographic Constructions; Protocols; Blockchain; Zero-Knowledge; Lattices.

Complexity of Lattice Problems Springer Science & Business Media

This book constitutes the refereed proceedings of the Third International Workshop on Coding and Cryptology, IWCC 2011, held in Qingdao, China, May 30-June 3, 2011. The 19 revised full technical papers are contributed by the invited speakers of the workshop. The papers were carefully reviewed and cover a broad range of foundational and methodological as well as applicative issues in coding and cryptology, as well as related areas such as combinatorics.

Public-Key Cryptography – PKC 2018 Springer

This volume contains the Proceedings of ICFCA 2004, the 2nd International Conference on Formal Concept Analysis. The ICFCA conference series aims to be the premier forum for the publication of advances in applied lattice and order theory and in particular scienti?c advances related to formal concept analysis. Formal concept analysis emerged in the 1980s from e?orts to restructure lattice theory to promote better communication between lattice theorists and potentialusersoflatticetheory.Sincethen,the?eldhasdevelopedintoagrowing research area in its own right with a thriving theoretical community and an increasing number of applications in data and knowledge processing including data visualization, information retrieval, machine learning, data analysis and knowledge management. In terms of theory, formal concept analysis has been extended into attribute exploration, Boolean judgment, contextual logic and so on to create a powerful general framework for knowledge representation and reasoning. This conference aims to unify theoretical and applied practitioners who use formal concept an- ysis, drawing on the ?elds of mathematics, computer and library sciences and software engineering. The theme of the 2004 conference was ‘Concept Lattices” to acknowledge the colloquial term used for the line diagrams that appear in almost every paper in this volume. ICFCA 2004 included tutorial sessions, demonstrating the practical bene?ts of formal concept analysis, and highlighted developments in the foundational theory and standards. The conference showcased the increasing variety of formal concept analysis software and included eight invited lectures from distinguished speakersinthe?eld.Sevenoftheeightinvitedspeakerssubmittedaccompanying papers and these were reviewed and appear in this volume.

Algorithms for the Closest and Shortest Vector Problems on General Lattices Cambridge University Press

Partition functions arise in combinatorics and related problems of statistical physics as they encode in a succinct way the combinatorial structure of complicated systems. The main focus of the book is on efficient ways to compute (approximate) various partition functions, such as permanents, hafnians and their higher-dimensional versions, graph and hypergraph matching polynomials, the independence polynomial of a graph and partition functions enumerating 0-1 and integer points in polyhedra, which allows one to make algorithmic advances in otherwise intractable problems. The book unifies various, often quite recent, results scattered in the literature, concentrating on the three main approaches: scaling, interpolation and correlation decay. The prerequisites include moderate amounts of real and complex analysis and linear algebra, making the book accessible to advanced math and physics undergraduates.

Advances in Cryptology – EUROCRYPT 2008 Springer

This book offers a comprehensive treatment of the classical decision problem of mathematical logic and of the role of the classical decision problem in modern computer science. The text presents a revealing analysis of the natural order of decidable and undecidable cases and includes a number of simple proofs and exercises.

Covering Codes Elsevier

Lattices are geometric objects that can be pictorially described as the set of intersection points of an infinite, regular n-dimensional grid. De spite their apparent simplicity, lattices hide a rich combinatorial struc ture, which has attracted the attention of great mathematicians over the last two centuries. Not surprisingly, lattices have found numerous ap plications in mathematics and computer science, ranging from number theory and Diophantine approximation, to combinatorial optimization and cryptography. The study of lattices, specifically from a computational point of view, was marked by two major breakthroughs: the development of the LLL lattice reduction algorithm by Lenstra, Lenstra and Lovasz in the early 80's, and Ajtai's discovery of a connection between the worst-case and average-case hardness of certain lattice problems in the late 90's. The LLL algorithm, despite the relatively poor quality of the solution it gives in the worst case, allowed to devise polynomial time solutions to many classical problems in computer science. These include, solving integer programs in a fixed number of variables, factoring polynomials over the rationals, breaking knapsack based cryptosystems, and finding solutions to many other Diophantine and cryptanalysis problems.

Algorithmic Number Theory Cambridge University Press

Using a balanced approach that is partly algorithmic and partly structuralist, this book systematically reviews the most significant results obtained in the study of computational complexity theory. KEY TOPICS: Considers properties of complexity classes, inclusions between classes, implications between several hypotheses about complexity classes, and identification of structural properties of sets that affect their computational complexity. Features over 120 worked examples, over 200 problems, and 400 figures. For those interested in complexity and computability, algorithm design, operations research, and combinational mathematic.