algebraic complexity theory grundlehren der mathematischen wissenschaften

#algebraic complexity theory #computational complexity #theoretical computer science #mathematical foundations #grundlehren mathematischen wissenschaften

Explore the fundamental principles of algebraic complexity theory, a cornerstone discipline within the mathematical sciences. This comprehensive text, part of the esteemed 'Grundlehren der mathematischen Wissenschaften' series, delves into the intricate analysis of computational problems using algebraic methods. It offers an essential resource for researchers and students seeking a deep understanding of the inherent difficulty and efficiency of algorithms within a rigorous mathematical framework.

Algebraic Complexity Theory

The algorithmic solution of problems has always been one of the major concerns of mathematics. For a long time such solutions were based on an intuitive notion of algorithm. It is only in this century that metamathematical problems have led to the intensive search for a precise and sufficiently general formalization of the notions of computability and algorithm. In the 1930s, a number of quite different concepts for this purpose were pro posed, such as Turing machines, WHILE-programs, recursive functions, Markov algorithms, and Thue systems. All these concepts turned out to be equivalent, a fact summarized in Church's thesis, which says that the resulting definitions form an adequate formalization of the intuitive notion of computability. This had and continues to have an enormous effect. First of all, with these notions it has been possible to prove that various problems are algorithmically unsolvable. Among of group these undecidable problems are the halting problem, the word problem theory, the Post correspondence problem, and Hilbert's tenth problem. Secondly, concepts like Turing machines and WHILE-programs had a strong influence on the development of the first computers and programming languages. In the era of digital computers, the question of finding efficient solutions to algorithmically solvable problems has become increasingly important. In addition, the fact that some problems can be solved very efficiently, while others seem to defy all attempts to find an efficient solution, has called for a deeper under standing of the intrinsic computational difficulty of problems.

Completeness and Reduction in Algebraic Complexity Theory

Two central problems in computer science are P vs NP and the complexity of matrix multiplication. The first is also a leading candidate for the greatest unsolved problem in mathematics. The second is of

enormous practical and theoretical importance. Algebraic geometry and representation theory provide fertile ground for advancing work on these problems and others in complexity. This introduction to algebraic complexity theory for graduate students and researchers in computer science and mathematics features concrete examples that demonstrate the application of geometric techniques to real world problems. Written by a noted expert in the field, it offers numerous open questions to motivate future research. Complexity theory has rejuvenated classical geometric questions and brought different areas of mathematics together in new ways. This book will show the beautiful, interesting, and important questions that have arisen as a result.

Geometry and Complexity Theory

The algorithmic solution of problems has always been one of the major concerns of mathematics. For a long time such solutions were based on an intuitive notion of algorithm. It is only in this century that metamathematical problems have led to the intensive search for a precise and sufficiently general formalization of the notions of computability and algorithm. In the 1930s, a number of quite different concepts for this purpose were pro posed, such as Turing machines, WHILE-programs, recursive functions, Markov algorithms, and Thue systems. All these concepts turned out to be equivalent, a fact summarized in Church's thesis, which says that the resulting definitions form an adequate formalization of the intuitive notion of computability. This had and continues to have an enormous effect. First of all, with these notions it has been possible to prove that various problems are algorithmically unsolvable. Among of group these undecidable problems are the halting problem, the word problem theory, the Post correspondence problem, and Hilbert's tenth problem. Secondly, concepts like Turing machines and WHILE-programs had a strong influence on the development of the first computers and programming languages. In the era of digital computers, the question of finding efficient solutions to algorithmically solvable problems has become increasingly important. In addition, the fact that some problems can be solved very efficiently, while others seem to defy all attempts to find an efficient solution, has called for a deeper under standing of the intrinsic computational difficulty of problems.

Algebraic Systems of Equations and Computational Complexity Theory

This comprehensive introduction to algebraic complexity theory presents new techniques for analyzing P vs NP and matrix multiplication.

Algebraic Complexity Theory

This book constitutes the refereed proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science, STACS 2007, held in Aachen, Germany in February 2007. The 56 revised full papers presented together with 3 invited papers address the whole range of theoretical computer science as well as current challenges like biological computing, quantum computing, and mobile and net computing.

Geometry and Complexity Theory

This book constitutes the refereed proceedings of the Third International Computer Science Symposium in Russia, CSR 2008, held in Moscow, Russia, June 7-12, 2008. The 33 revised papers presented together with 5 invited papers and one opening lecture were carefully reviewed and selected from 103 submissions. All major areas in computer science are addressed. The theory track deals with algorithms, protocols, and data structures; complexity and cryptography; formal languages, automata and their applications to computer science; computational models and concepts; proof theory and applications of logic to computer science. The application part comprises programming and languages; computer architecture and hardware design; symbolic computing and numerical applications; application software; artificial intelligence and robotics.

STACS 2007

This book constitutes the proceedings of the 16th International Computer Science Symposium in Russia, CSR 2021, held in Sochi, Russia, in June/July 2021. The 28 full papers were carefully reviewed and selected from 68 submissions. The papers cover a broad range of topics, such as formal languages and automata theory, geometry and discrete structures; theory and algorithms for application domains and much more.

Computer Science - Theory and Applications

Now in its third edition, this highly successful textbook is widely regarded as the 'bible of computer algebra'.

Computer Science – Theory and Applications

This volume is composed of six contributions derived from the lectures given during the UIMP-RSME Lluis Santalo Summer School on ``Recent Advances in Real Complexity and Computation'', held July 16-20, 2012, in Santander, Spain. The goal of this Summer School was to present some of the recent advances on Smale's 17th Problem: ``Can a zero of n complex polynomial equations in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?'' These papers cover several aspects of this problem: from numerical to symbolic methods in polynomial equation solving, computational complexity aspects (both worse and average cases and both upper and lower complexity bounds) as well as aspects of the underlying geometry of the problem. Some of the contributions also deal with either real or multiple solutions solving.

Modern Computer Algebra

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.

Recent Advances in Real Complexity and Computation

The book contains 8 detailed expositions of the lectures given at the Kaikoura 2000 Workshop on Computability, Complexity, and Computational Algebra. Topics covered include basic models and questions of complexity theory, the Blum-Shub-Smale model of computation, probability theory applied to algorithmics (randomized alogrithms), parametric complexity, Kolmogorov complexity of finite strings, computational group theory, counting problems, and canonical models of ZFC providing a solution to continuum hypothesis. The text addresses students in computer science or mathematics, and professionals in these areas who seek a complete, but gentle introduction to a wide range of techniques, concepts, and research horizons in the area of computational complexity in a broad sense.

Completeness and Reduction in Algebraic Complexity Theory

This book constitutes the refereed proceedings of the 26th International Symposium on Mathematical Foundations of Computer Science, MFCS 2001, held in Marianske Lazne, Czech Republic in August 2001. The 51 revised full papers presented together with 10 invited contributions were carefully reviewed and selected from a total of 118 submissions. All current aspects of theoretical computer science are addressed ranging from mathematical logic and programming theory to algorithms, discrete mathematics, and complexity theory. Besides classical issues, modern topics like quantum computing are discussed as well.

Aspects of Complexity

This book constitutes the refereed proceedings of the 26th International Symposium on Mathematical Foundations of Computer Science, MFCS 2001, held in Marianske Lazne, Czech Republic in August 2001. The 51 revised full papers presented together with 10 invited contributions were carefully reviewed and selected from a total of 118 submissions. All current aspects of theoretical computer science are addressed ranging from mathematical logic and programming theory to algorithms, discrete mathematics, and complexity theory. Besides classical issues, modern topics like quantum computing are discussed as well.

Mathematical Foundations of Computer Science 2001

Algorithmic and quantitative aspects in real algebraic geometry are becoming increasingly important areas of research because of their roles in other areas of mathematics and computer science. The papers in this volume collectively span several different areas of current research. The articles are based on talks given at the DIMACS Workshop on "Algorithmic and Quantitative Aspects of Real

Algebraic Geometry". Topics include deciding basic algebraic properties of real semi-algebraic sets, application of quantitative results in real algebraic geometry towards investigating the computational complexity of various problems, algorithmic and quantitative questions in real enumerative geometry, new approaches towards solving decision problems in semi-algebraic geometry, as well as computing algebraic certificates, and applications of real algebraic geometry to concrete problems arising in robotics and computer graphics. The book is intended for researchers interested in computational methods in algebra.

Mathematical Foundations of Computer Science 2001

Algebraic geometry and geometric modeling both deal with curves and surfaces generated by polynomial equations. Algebraic geometry investigates the theoretical properties of polynomial curves and surfaces; geometric modeling uses polynomial, piecewise polynomial, and rational curves and surfaces to build computer models of mechanical components and assemblies for industrial design and manufacture. The NSF sponsored the four-day "Vilnius Workshop on Algebraic Geometry and Geometric Modeling", which brought together some of the top experts in the two research communities to examine a wide range of topics of interest to both fields. This volume is an outgrowth of that workshop. Included are surveys, tutorials, and research papers. In addition, the editors have included a translation of Minding's 1841 paper, "On the determination of the degree of an equations obtained by elimination", which foreshadows the modern application of mixed volumes in algebraic geometry. The volume is suitable for mathematicians, computer scientists, and engineers interested in applications of algebraic geometry to geometric modeling.

Algorithmic and Quantitative Real Algebraic Geometry

This volume contains the proceedings of the 17th International Conference on Arithmetic, Geometry, Cryptography and Coding Theory (AGC2T-17), held from June 10–14, 2019, at the Centre International de Rencontres Mathématiques in Marseille, France. The conference was dedicated to the memory of Gilles Lachaud, one of the founding fathers of the AGC2T series. Since the first meeting in 1987 the biennial AGC2T meetings have brought together the leading experts on arithmetic and algebraic geometry, and the connections to coding theory, cryptography, and algorithmic complexity. This volume highlights important new developments in the field.

Topics in Algebraic Geometry and Geometric Modeling

With a substantial amount of new material, the Handbook of Linear Algebra, Second Edition provides comprehensive coverage of linear algebra concepts, applications, and computational software packages in an easy-to-use format. It guides you from the very elementary aspects of the subject to the frontiers of current research. Along with revisions and updates throughout, the second edition of this bestseller includes 20 new chapters. New to the Second Edition Separate chapters on Schur complements, additional types of canonical forms, tensors, matrix polynomials, matrix equations, special types of matrices, generalized inverses, matrices over finite fields, invariant subspaces, representations of quivers, and spectral sets New chapters on combinatorial matrix theory topics, such as tournaments, the minimum rank problem, and spectral graph theory, as well as numerical linear algebra topics, including algorithms for structured matrix computations, stability of structured matrix computations, and nonlinear eigenvalue problems More chapters on applications of linear algebra, including epidemiology and quantum error correction New chapter on using the free and open source software system Sage for linear algebra Additional sections in the chapters on sign pattern matrices and applications to geometry Conjectures and open problems in most chapters on advanced topics Highly praised as a valuable resource for anyone who uses linear algebra, the first edition covered virtually all aspects of linear algebra and its applications. This edition continues to encompass the fundamentals of linear algebra, combinatorial and numerical linear algebra, and applications of linear algebra to various disciplines while also covering up-to-date software packages for linear algebra computations.

Arithmetic, Geometry, Cryptography and Coding Theory

Graduate-level introduction to error-correcting codes, which are used to protect digital data and applied in public key cryptosystems.

Handbook of Linear Algebra

This book constitutes the strictly refereed proceedings of the 15th Annual Symposium on Theoretical Aspects of Computer Science, STACS 98, held in Paris, France, in February 1998. The volume presents three invited surveys together with 52 revised full papers selected from a total of 155 submissions. The papers are organized in topical sections on algorithms and data structures, logic, complexity, and automata and formal languages.

Codes, Cryptology and Curves with Computer Algebra

TAMC 2006 was the third conference in the series. The previous two meetings were held May 17–19, 2004 in Beijing, and May 17–20, 2005 in Kunming

STACS 98

This Handbook gives a comprehensive snapshot of a field at the intersection of mathematics and computer science with applications in physics, engineering and education. Reviews 67 software systems and offers 100 pages on applications in physics, mathematics, computer science, engineering chemistry and education.

Theory and Applications of Models of Computation

This book constitutes the refereed proceedings of the 21st International Symposium on Fundamentals of Computation Theory, FCT 2017, held in Bordeaux, France, in September 2017. The 29 revised full papers and 5 invited papers presented were carefully reviewed and selected from 99 submissions. The papers cover topics of all aspects of theoretical computer science, in particular algorithms, complexity, formal and logical methods.

Computer Algebra Handbook

This volume contains the proceedings of the 18th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory, held (online) from May 31 to June 4, 2021. For over thirty years, the biennial international conference AGC^{2}T (Arithmetic, Geometry, Cryptography, and Coding Theory) has brought researchers together to forge connections between arithmetic geometry and its applications to coding theory and to cryptography. The papers illustrate the fruitful interaction between abstract theory and explicit computations, covering a large range of topics, including Belyi maps, Galois representations attached to elliptic curves, reconstruction of curves from their Jacobians, isogeny graphs of abelian varieties, hypergeometric equations, and Drinfeld modules.

Fundamentals of Computation Theory

Proceedings of a high-level conference on discrete mathematics, focusing on group actions in the areas of pure mathematics, applied mathematics, computer science, physics, and chemistry. A useful tool for researchers and graduate students in discrete mathematics and theoretical computer science.

Arithmetic, Geometry, Cryptography, and Coding Theory 2021

This second volume in a two-volume series provides an extensive collection of conjectures and open problems in graph theory. It is designed for both graduate students and established researchers in discrete mathematics who are searching for research ideas and references. Each chapter provides more than a simple collection of results on a particular topic; it captures the reader’s interest with techniques that worked and failed in attempting to solve particular conjectures. The history and origins of specific conjectures and the methods of researching them are also included throughout this volume. Students and researchers can discover how the conjectures have evolved and the various approaches that have been used in an attempt to solve them. An annotated glossary of nearly 300 graph theory parameters, 70 conjectures, and over 600 references is also included in this volume. This glossary provides an understanding of parameters beyond their definitions and enables readers to discover new ideas and new definitions in graph theory. The editors were inspired to create this series of volumes by the popular and well-attended special sessions entitled “My Favorite Graph Theory Conjectures,” which they organized at past AMS meetings. These sessions were held at the winter AMS/MAA Joint Meeting in Boston, January 2012, the SIAM Conference on Discrete Mathematics in Halifax in June 2012, as well as the winter AMS/MAA Joint Meeting in Baltimore in January 2014, at which many of the best-known graph theorists spoke. In an effort to aid in the creation and dissemination of conjectures

and open problems, which is crucial to the growth and development of this field, the editors invited these speakers, as well as other experts in graph theory, to contribute to this series.

Algebraic Combinatorics and Applications

These are the proceedings of the Conference on Coding Theory, Cryptography, and Number Theory held at the U. S. Naval Academy during October 25-26, 1998. This book concerns elementary and advanced aspects of coding theory and cryptography. The coding theory contributions deal mostly with algebraic coding theory. Some of these papers are expository, whereas others are the result of original research. The emphasis is on geometric Goppa codes (Shokrollahi, Shokranian-Joyner), but there is also a paper on codes arising from combinatorial constructions (Michael). There are both, historical and mathematical papers on cryptography. Several of the contributions on cryptography describe the work done by the British and their allies during World War II to crack the German and Japanese ciphers (Hamer, Hilton, Tutte, Weierud, Urling). Some mathematical aspects of the Enigma rotor machine (Sherman) and more recent research on quantum cryptography (Lomonoco) are described. There are two papers concerned with the RSA cryptosystem and related number-theoretic issues (Wardlaw, Cosgrave).

Graph Theory

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.

Coding Theory and Cryptography

This book constitutes the refereed proceedings of the 19th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, held in Honolulu, Hawaii, USA in November 1999. The 42 revised full papers presented together with six invited survey papers were carefully reviewed and selected from a total of 86 submissions. The papers are organized in sections on codes and iterative decoding, arithmetic, graphs and matrices, block codes, rings and fields, decoding methods, code construction, algebraic curves, cryptography, codes and decoding, convolutional codes, designs, decoding of block codes, modulation and codes, Gröbner bases and AG codes, and polynomials.

Independence in Algebraic Complexity Theory

This book constitutes the refereed proceedings of the 6th International Conference on Geometric Modeling and Processing, GMP 2010, held in Castro Urdiales, Spain, in June 2010. The 20 revised full papers presented were carefully reviewed and selected from a total of 30 submissions. The papers cover a wide spectrum in the area of geometric modeling and processing and address topics such as solutions of transcendental equations; volume parameterization; smooth curves and surfaces; isogeometric analysis; implicit surfaces; and computational geometry.

Combinatorics and Complexity of Partition Functions

This book provides comprehensive summaries of theoretical (algebraic) and computational aspects of tensor ranks, maximal ranks, and typical ranks, over the real number field. Although tensor ranks have been often argued in the complex number field, it should be emphasized that this book treats real tensor ranks, which have direct applications in statistics. The book provides several interesting ideas, including determinant polynomials, determinantal ideals, absolutely nonsingular tensors, absolutely full column rank tensors, and their connection to bilinear maps and Hurwitz-Radon numbers. In addition to reviews of methods to determine real tensor ranks in details, global theories such as the Jacobian method are also reviewed in details. The book includes as well an accessible and comprehensive introduction of

mathematical backgrounds, with basics of positive polynomials and calculations by using the Groebner basis. Furthermore, this book provides insights into numerical methods of finding tensor ranks through simultaneous singular value decompositions.

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

Tensors are ubiquitous in the sciences. The geometry of tensors is both a powerful tool for extracting information from data sets, and a beautiful subject in its own right. This book has three intended uses: a classroom textbook, a reference work for researchers in the sciences, and an account of classical and modern results in (aspects of) the theory that will be of interest to researchers in geometry. For classroom use, there is a modern introduction to multilinear algebra and to the geometry and representation theory needed to study tensors, including a large number of exercises. For researchers in the sciences, there is information on tensors in table format for easy reference and a summary of the state of the art in elementary language. This is the first book containing many classical results regarding tensors. Particular applications treated in the book include the complexity of matrix multiplication, P versus NP, signal processing, phylogenetics, and algebraic statistics. For geometers, there is material on secant varieties, G-varieties, spaces with finitely many orbits and how these objects arise in applications, discussions of numerous open questions in geometry arising in applications, and expositions of advanced topics such as the proof of the Alexander-Hirschowitz theorem and of the Weyman-Kempf method for computing syzygies.

Advances in Geometric Modeling and Processing

The notion of complexity is an important contribution of logic to theoretical computer science and mathematics. This volume attempts to approach complexity in a holistic way, investigating mathematical properties of complexity hierarchies at the same time as discussing algorithms and computational properties. A main focus of the volume is on some of the new paradigms of computation, among them Quantum Computing and Infinitary Computation. The papers in the volume are tied together by an introductory article describing abstract properties of complexity hierarchies. This volume will be of great interest to both mathematical logicians and theoretical computer scientists, providing them with new insights into the various views of complexity and thus shedding new light on their own research.

Algebraic and Computational Aspects of Real Tensor Ranks

This book gathers threads that have evolved across different mathematical disciplines into seamless narrative. It deals with condition as a main aspect in the understanding of the performance ---regarding both stability and complexity--- of numerical algorithms. While the role of condition was shaped in the last half-century, so far there has not been a monograph treating this subject in a uniform and systematic way. The book puts special emphasis on the probabilistic analysis of numerical algorithms via the analysis of the corresponding condition. The exposition's level increases along the book, starting in the context of linear algebra at an undergraduate level and reaching in its third part the recent developments and partial solutions for Smale's 17th problem which can be explained within a graduate course. Its middle part contains a condition-based course on linear programming that fills a gap between the current elementary expositions of the subject based on the simplex method and those focusing on convex programming.

Tensors: Geometry and Applications

This book constitutes the proceedings of the 14th International Workshop on Computer Algebra in Scientific Computing, CASC 2013, held in Berlin, Germany, in September 2013. The 33 full papers presented were carefully reviewed and selected for inclusion in this book. The papers address issues such as polynomial algebra; the solution of tropical linear systems and tropical polynomial systems; the theory of matrices; the use of computer algebra for the investigation of various mathematical and applied topics related to ordinary differential equations (ODEs); applications of symbolic computations for solving partial differential equations (PDEs) in mathematical physics; problems arising at the application of computer algebra methods for finding infinitesimal symmetries; applications of symbolic and symbolic-numeric algorithms in mechanics and physics; automatic differentiation; the application of the CAS Mathematica for the simulation of quantum error correction in quantum computing; the application of the CAS GAP for the enumeration of Schur rings over the group A5; constructive computation of zero separation bounds for arithmetic expressions; the parallel implementation of fast Fourier transforms with the aid of the Spiral library generation system; the use of object-oriented

languages such as Java or Scala for implementation of categories as type classes; a survey of industrial applications of approximate computer algebra.

Classical and New Paradigms of Computation and their Complexity Hierarchies

Recent Advances in RSA Cryptography surveys the most important achievements of the last 22 years of research in RSA cryptography. Special emphasis is laid on the description and analysis of proposed attacks against the RSA cryptosystem. The first chapters introduce the necessary background information on number theory, complexity and public key cryptography. Subsequent chapters review factorization algorithms and specific properties that make RSA attractive for cryptographers. Most recent attacks against RSA are discussed in the third part of the book (among them attacks against low-exponent RSA, Hastad's broadcast attack, and Franklin-Reiter attacks). Finally, the last chapter reviews the use of the RSA function in signature schemes. Recent Advances in RSA Cryptography is of interest to graduate level students and researchers who will gain an insight into current research topics in the field and an overview of recent results in a unified way. Recent Advances in RSA Cryptography is suitable as a secondary text for a graduate level course, and as a reference for researchers and practitioners in industry.

Condition

This book constitutes the refereed proceedings of the First Mediterranean Conference on Algorithms, MedAlg 2012, held in Kibbutz Ein Gedi, Israel, in December 2012. The 18 papers presented were carefully reviewed and selected from 44 submissions. The conference papers focus on the design, engineering, theoretical and experimental performance analysis of algorithms for problems arising in different areas of computation. Topics covered include: communications networks, combinatorial optimization and approximation, parallel and distributed computing, computer systems and architecture, economics, game theory, social networks and the World Wide Web.

Computer Algebra in Scientific Computing

This book constitutes the refereed proceedings of the 17th Annual European Symposium on Algorithms, ESA 2009, held in Copenhagen, Denmark, in September 2009 in the context of the combined conference ALGO 2009. The 67 revised full papers presented together with 3 invited lectures were carefully reviewed and selected: 56 papers out of 222 submissions for the design and analysis track and 10 out of 36 submissions in the engineering and applications track. The papers are organized in topical sections on trees, geometry, mathematical programming, algorithmic game theory, navigation and routing, graphs and point sets, bioinformatics, wireless communiations, flows, matrices, compression, scheduling, streaming, online algorithms, bluetooth and dial a ride, decomposition and covering, algorithm engineering, parameterized algorithms, data structures, and hashing and lowest common ancestor.

Recent Advances in RSA Cryptography

Design and Analysis of Algorithms