THEORY OF COMPUTING, Volume 15 (9), 2019, pp. 1–3
www.theoryofcomputing.org

SPECIAL ISSUE: CCC 2018

Guest Editors' Foreword

Srikanth Srinivasan

October 21, 2019

This collection comprises the expanded and fully refereed versions of selected papers presented at the 33rd Computational Complexity Conference (CCC 2018) held June 22-24, 2018 in San Diego, CA, USA. These papers were selected by the Program Committee from among the 28 papers that appeared in the conference proceedings. Preliminary versions of the papers were presented at the conference and the extended abstracts appeared in the proceedings of the conference published by Dagstuhl Publishing, LIPIcs. The CCC Program Committee selected 28 out of 74 submissions for presentation at the conference; of these, the four described below were invited to this Special Issue. These four papers were refereed in accordance with the rigorous standards of Theory of Computing.

- "Algebraic dependencies and PSPACE algorithms in approximative complexity" by Zeyu Guo, Nitin Saxena, and Amit Sinhababu.
  This paper makes contributions to two important problems in algebraic complexity.
  1. Algebraic independence. Given polynomials $f_1, ..., f_m \in \mathbb{F}[x_1, \ldots, x_n]$ as algebraic circuits, the question is to check if they are algebraically independent. This notion is a fundamental measure of the joint complexity of these polynomials. In characteristic zero, this can be checked by a simple polynomial-time (in terms of the sizes of the input circuits) randomized algorithm via the well-known Jacobian criterion. However, in positive characteristic, the best known result prior to this result was $\mathsf{NP}^{\#\mathsf{P}}$. In this paper, this problem is shown to lie in the polynomial hierarchy (specifically, inside $\mathsf{AM} \cap \mathsf{coAM}$) for all characteristics.
  2. Approximate polynomial satisfiability. This is a twist on the Hilbert Nullstellensatz problem, which asks to check if a given collection of multivariate polynomials $f_1, ..., f_m \in \mathbb{F}[x_1, \ldots, x_n]$ (given as algebraic circuits) has a common root over the algebraic closure. Here, we are

ACM Classification: F, F.2

AMS Classification: 68Qxx

Key words and phrases: foreword, special issue, CCC 2018

© 2019 Srikanth Srinivasan
Licensed under a Creative Commons Attribution License (CC-BY)
DOI: 10.4086/toc.2019.v015a009

required to check if the given collection of polynomials has an "approximate" root, or equivalently, if the image of the polynomial map defined by $(f_1, \ldots, f_m)$ contains 0 in its Zariski closure. The problem is motivated via connections to Geometric Complexity Theory, where we try to understand the complexity of "approximately" computing a given polynomial. In particular, the authors show that a solution to Approximate Polynomial Satisfiability implies the construction of explicit hitting sets for $\overline{\mathsf{VP}}$, which is the class of polynomials that can be approximated by polynomials in VP.

The best known bound for this problem was previously $\mathsf{EXPSPACE}$ via a Gröbner basis computation. This paper places this problem in PSPACE over arbitrary fields. As a corollary, this yields a PSPACE upper bound for constructing explicit hitting sets for $\overline{\mathsf{VP}}$ over arbitrary fields, improving on previous results which accomplished this in characteristic 0.

- "Pseudorandom Generators from Polarizing Random Walks" by Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett.

  This paper introduces a new paradigm for constructing pseudorandom generators (PRGs) for concrete computational models. This involves a weaker variant of PRGs called fractional PRGs (fPRGs, first defined in this paper) and it is shown that for Boolean function classes closed under restrictions, explicit fPRGs can be converted to explicit PRGs while only slightly weakening the parameters. In particular, this yields a unified and simpler construction for PRGs for various classes of functions that are either restricted in terms of their Fourier spectra or simplify considerably upon applying random restrictions. In some cases (e. g., Boolean functions with low sensitivity), this yields a significant quantitative improvement. In others, this idea significantly simplifies the proof (e. g., AC^0), since the construction works under quite general assumptions.
- "The Cayley Semigroup Membership Problem" by Lukas Fleischer.

  This paper concerns the semigroup membership problem: the input is a semigroup S, given as a multiplication table, a subset X of S, and an element $t \in S$, and the question is if t is generated by X. The problem is known to be NL-complete in general and even P-complete if the input is relaxed to be a general groupoid. Here, the author makes progress on the long-standing open problem on the complexity of the problem when S is a group. It is shown that in this case (and also the case when S is a commutative semigroup), the problem actually can be placed in the class qAC^0 (i. e., the problem has constant-depth quasipolynomial-size circuits made up of OR, AND, and NOT gates), and hence cannot be hard for any class of functions that contains the PARITY function. Previously, it was only known that if S is a commutative group, then the problem has polynomial-sized $\log\log n$-depth circuits.
- "On The Hardness of Approximate and Exact (Bichromatic) Maximum Inner Product" by Lijie Chen.

  This paper deals with fine-grained complexity, where a central theme is to understand why we have not been able to improve long-standing algorithms for some problems in P. The questions in this paper consider exact and approximation algorithms for the problem Max-IP, where the input is two lists, A and B, of n vectors each and the quantity to be computed (or approximated) is the maximum inner product between a vector in A and a vector in B. This problem generalizes the well-known Orthogonal Vectors problem, whose complexity is closely related to the Strong Exponential Time Hypothesis (SETH).

Under SETH (or the weaker Orthogonal Vectors Conjecture), the paper proves a range of improved hardness results for many variants of Max-IP, where the vectors are allowed to have entries that are Boolean (i. e., $0,1$), $\{-1,1\}$-valued, or arbitrary integers. These hardness results use many ideas including connections to MA-communication complexity (specifically a recently improved MA-communication protocol for Inner Product) and new connections to Quantum communication complexity. In the Boolean case, matching upper bounds are also proved. Finally, the paper also improves the parameters of the best known MA-communication protocol for the Inner Product problem.

I would like to thank the authors for their contributions, the CCC program committee for their initial reviews, Dieter van Melkebeek and Venkatesan Guruswami for their advice on matters related to CCC, László Babai for his advice on matters related to *Theory of Computing,* and the anonymous referees for their hard work. It was a pleasure to edit this Special Issue for Theory of Computing.

CCC 2018 Program Committee

Eric Allender (Rutgers University)
Paul Beame (University of Washington)
Eric Blais (University of Waterloo)
Mark Braverman (Princeton University)
Michael A. Forbes (University of Illinois at Urbana-Champaign)
Shafi Goldwasser (Massachusetts Institute of Technology and Weizmann Institute of Science)
Rocco Servedio (Columbia University) (Chair)
Srikanth Srinivasan (Indian Institute of Technology Bombay)
Thomas Thierauf (Aalen University)
Madhur Tulsiani (Toyota Technological Institute at Chicago)
Henry Yuen (University of California, Berkeley and University of Toronto)

GUEST EDITOR

Srikanth Srinivasan
Department of Mathematics
Indian Institute of Technology Bombay
Mumbai, India.
srikanth@math.iitb.ac.in
https://www.math.iitb.ac.in/~srikanth