THEORY OF COMPUTING, Volume 22 (1), 2026, pp. 1–4
www.theoryofcomputing.org

SPECIAL ISSUE: CCC 2021

Guest Editors' Foreword

Nutan Limaye Igor C. Oliveira

May 10, 2026

This collection comprises the expanded and fully refereed versions of selected papers presented at the 36th Computational Complexity Conference (CCC 2021), held July 20–23, 2021, online. These papers were selected by the Program Committee from among the 41 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 41 out of 116 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.

- "On the Power and Limitations of Branch and Cut" by Noah Fleming, Mika Göös, Russell Impagliazzo, Toniann Pitassi, Robert Robere, Li-Yang Tan, and Avi Wigderson.

  This paper provides a number of powerful analyses of branch-and-cut proof systems for inference, particularly proofs of unsatisfiability, that involve systems of integer linear inequalities over the reals. The main results give strong relationships between such proof systems—recently termed stabbing planes proofs—and cutting planes proofs provided that the coefficients of branching proofs have a somewhat loose upper bound. Indeed, the authors identify a natural semantic restriction on stabbing planes proofs, being 'facelike,' for which they can prove a direct correspondence with cutting planes proof size. In this latter identification, the authors generalize surprising recent results of Dadush and Tiwari

ACM Classification: F, F.2

AMS Classification: 68Qxx

Key words and phrases: foreword, special issue, CCC 2021

 DOI: 10.4086/toc.2026.v022a001

(CCC'20) on cutting planes proofs of Tseitin formulas. As a consequence, the authors obtain (the first) exponential size lower bounds on general branch-and-cut proofs, albeit subject to a size restriction on their coefficients.

The authors also provide general cutting planes proofs for systems of modular linear equations following the method of Dadush and Tiwari and identify an intriguing open question involving a potential supercritical tradeoff between proof depth and proof size: It is possible that to obtain somewhat small (e. g., quasipolynomial) size, one must use proof depth much larger than the number of variables even though depth equal to the number of variables always suffices for a (potentially inefficient) proof. Motivated by looking for new methods to prove depth lower bounds for cutting planes proofs, the authors develop a general method for obtaining lower bounds for proof depth in the semantic version of the Cutting Planes proof system.

- "A Lower Bound for Polynomial Calculus with Extension Rule" by Yaroslav Alekseev.

  This paper proves an unconditional lower bound for a very strong algebraic proof system: polynomial calculus augmented with extension variables (so that complex circuits can be named by single variables) and a natural additional rule permitting square roots of polynomials. The system is dynamic (line-by-line), unlike the static Ideal Proof System (IPS); whereas IPS can freely use polynomial identities, here identities must be derived step-by-step. The system can be viewed as an algebraic analogue of Extended Frege. The hard family is the Binary Value Principle (BVP)—the unsatisfiable linear equation $\sum_{i=0}^{n-1} 2^i x_{i+1} = -1$ asserting that a binary string $x_1, \ldots, x_n$ has value -1, with coefficients of polynomial bit-length. Crucially, proof size is measured by total bit-size rather than by line or symbol counts with unit-cost coefficients. Building on ideas from prior conditional results for IPS, the argument becomes fully unconditional by working in this Cook–Reckhow system and accounting for coefficient size.

  Conceptually, the result shows that by allowing non-Boolean hard instances such as BVP—i. e., instances that are not strictly propositional formulas—one can obtain proof-complexity lower bounds far beyond what is known in the propositional (Frege-style) regime. These non-Boolean instances are equally relevant to complexity, since the language of unsatisfiable systems of polynomial equations over 0-1 variables is natural and is coNP-complete. The bit-size complexity measure for algebraic proofs is new and natural, and it is precisely what enables the unconditional lower bound.

- "Pseudodistributions That Beat All Pseudorandom Generators" by Edward Pyne and Salil Vadhan.

  This paper presents new explicit constructions of weighted pseudorandom generators (WPRGs) that fool ordered branching programs. The constructions are based on graph algorithms due to Ahmadenijad, Kelner, Murtagh, Peebles, Sidford, and Vadhan (FOCS'20). The paper insightfully reinterprets these algorithms as WPRGs and then combines them with the classic Impagliazzo–Nisan–Wigderson pseudorandom generator (STOC'94) to improve the seed lengths.

This approach leads to two main results. First, the paper constructs a WPRG that fools unbounded-width single-accept-state ordered permutation branching programs with error $1/n$ and seed length $\tilde{O}(\log^{3/2} n)$. This result is especially notable because Hoza, Pyne, and Vadhan previously showed that every unweighted pseudorandom generator that fools this model with error $1/n$ has seed length $\Omega(\log^2 n)$ (ITCS'21). Thus, the paper demonstrates for the first time that WPRGs are intrinsically more powerful than unweighted pseudorandom generators. Second, the paper constructs a WPRG that fools polynomial-width ordered branching programs with error ϵ and seed length $\tilde{O}(\log^2 n + \log(1/\epsilon))$. This construction, which was independently discovered by Cohen, Doron, Renard, Sberlo, and Ta-Shma (CCC'21), simplifies a prior construction by Braverman, Cohen, and Garg (STOC'18, SICOMP 2020).

- "Hardness of KT Characterizes Parallel Cryptography" by Hanlin Ren and Rahul Santhanam.

  A recent breakthrough by Liu and Pass (FOCS'20) showed an equivalence between the existence of one-way functions and the *bounded-error average-case* hardness of computing the K^t complexity (the Kolmogorov complexity of a string with respect to a given polynomial time bound t) over the uniform distribution.

  This paper makes significant conceptual and technical contributions to this area.

  The paper strengthens the Liu–Pass result and extends it in several ways. First, the authors show that the KT complexity is bounded-error average-case hard if and only if there exist one-way functions in constant parallel time. This result crucially relies on the idea of *randomized encodings*. Inspired by the above result, the paper presents randomized average-case reductions among the log-depth versions and logspace versions of K^t complexity, and the KT complexity. The reductions preserve both bounded-error average-case hardness and zero-error average-case hardness.

  The paper further presents the first construction of one-way functions of near-optimal hardness based on a natural complexity assumption, namely a *Strong Perebor Hypothesis* postulating that brute-force search is close to optimal for computing the K^t complexity.

  The paper also establishes the first unconditional construction of one-way functions from the hardness of MCSP over a natural distribution. Specifically, it shows that a Weak Perebor Hypothesis for MCSP implies the existence of one-way functions, and also provides a partial converse. Finally, the work offers new insights about the average-case hardness of MKtP by proving that it characterizes cryptographic pseudorandomness and complexity-theoretic pseudorandomness in some natural regimes of parameters.

We thank the authors for their contributions; the CCC Program Committee for their initial reviews; Valentine Kabanets for his outstanding work as Program Committee Chair; László Babai and Nikhil Bansal for their advice on matters related to *Theory of Computing;* Iddo Tzameret and William Hoza for their help during the preparation of this foreword; and the anonymous referees for their careful and dedicated efforts. It was a pleasure to edit this Special Issue for Theory of Computing.

CCC 2021 Program Committee

Arkadev Chattopadhyay (Tata Institute of Fundamental Research Mumbai)

Irit Dinur (Weizmann Institute of Science)

Yuval Ishai (Technion)

Valentine Kabanets (Simon Fraser University) (Chair)

Swastik Kopparty (Rutgers University)

Nutan Limaye (Indian Institute of Technology Bombay)

Ryan O'Donnell (Carnegie Mellon University)

Igor C. Oliveira (University of Warwick)

Alexander Razborov (University of Chicago/Steklov Institute)

Barna Saha (University of California Berkeley)

Emanuele Viola (Northeastern University)

Henry Yuen (University of Toronto/Columbia University)

GUEST EDITORS

Nutan Limaye
IT University of Copenhagen
nuli@itu.dk
https://www.itu.dk/~nuli/

Igor C. Oliveira
University of Warwick
igor.oliveira@warwick.ac.uk
https://www.dcs.warwick.ac.uk/~igorcarb/