SPECIAL ISSUE “CONFERENCE ON COMPUTATIONAL COMPLEXITY 2014” GUEST EDITOR’S FOREWORD

MICHAEL E. SAKS

This special issue presents the full versions of five papers that were delivered at the 29th Annual IEEE Conference on Computational Complexity (CCC 2014) held in Vancouver, British Columbia, from June 11 to June 13, 2014. These outstanding papers were selected by the program committee from among the twenty-nine papers that appeared in the conference proceedings. They were invited for submission and evaluated through the standard refereeing process of the journal.

The study of parallel repetition of one-round interactive games arose naturally in the analysis of cryptographic protocols and the study of probabilistically checkable proofs. The key question is: When given many independent instances of a given task, how does the probability of succeeding on all tasks degrade as a function of the number of tasks? Parallel repetition theorems show that in a number of contexts, the success probability degrades exponentially in the number of tasks. In the paper “A parallel repetition theorem for entangled projection games,” Irit Dinur, David Steurer and Thomas Vidick prove the first such result in the quantum setting that applies to arbitrary projection games with entangled provers under an arbitrary input distribution.

The paper “Quantum algorithms for learning symmetric juntas via the adversary method” by Aleksandrs Belovs obtains efficient quantum algorithms for determining the set of relevant variables

when given oracle access to a boolean function whose behavior is given by a symmetric function h on a small set of variables. This model captures, in particular, the problem of combinatorial group testing. The author resolves the quantum complexity of combinatorial group testing and also gives an approach for arbitrary symmetric functions h . The algorithms are constructed by applying the connection between quantum algorithms and feasible solutions to an associated semi-definite program and using the representation theory of the symmetric group to construct a feasible solution that corresponds to an efficient algorithm. This paper received the best student paper award at the conference.

The polynomial identity testing problem (PIT) has been a major focus of research in algebraic complexity. The paper “Equivalence of polynomial identity testing and polynomial factorization” by Swastik Kopparty, Shubhangi Saraf and Amir Shpilka gives further impetus to the study of PIT, by showing that the problem of factoring a multivariate polynomial (given by a circuit) can be reduced to PIT.

The quest for circuit lower bounds, i.e., proving that explicit functions cannot be computed within a given circuit class $\mathcal{C}$, involves finding a “weakness” in the class $\mathcal{C}$ that limits its ability to compute hard functions. This viewpoint connects the problem of proving lower bounds to the problem of finding non-trivial algorithms that exploit the structure of the class $\mathcal{C}$. This connection is further explored in the paper “Mining circuit lower bound proofs for meta-algorithms” by Ruiwen Chen, Valentine Kabanets, Antonina Kolokolova, Ronen Shaltiel and David Zuckerman. In particular, the authors study the question of whether functions in a given circuit class can be non-trivially compressed. By exploiting insights derived from existing lower-bound results, they construct algorithms for achieving non-trivial compression of functions computable by AC^0 circuits, de Morgan formulas and read-once branching programs.

Over the past twenty years, geometric complexity theory (GCT) has been a conceptually promising, but technically formidable approach to obtaining complexity lower bounds. The paper “Unifying known lower bounds via geometric complexity theory” by Joshua

Grochow provides an introduction to GCT that is accessible to the broader theory community and shows how the GCT framework is broad enough to encompass most known lower bounds in algebraic complexity theory.

I'm grateful to the authors for submitting their papers to the special issue and the referees for their thorough and timely reviews. I very much appreciate the help of Lance Fortnow, Yuval Ishai, Shachar Lovett, Alexander Sherstov and Ryan Williams, who shared the editorial duties for this special issue. Finally, I thank Peter Bürgisser and the journal staff for producing the journal issue.

MICHAEL E. SAKS
Guest Editor

MICHAEL E. SAKS
Department of Mathematics,
Rutgers University,
Hill Center,
110 Frelinghuysen Road,
Piscataway, NJ 08854,
USA
`saks@math.rutgers.edu`