comput. complex. **22** (2013), 215 – 217

1016-3328/13/020215-3
published online May 7, 2013
DOI 10.1007/s00037-013–0070-z

SPECIAL ISSUE "CONFERENCE ON COMPUTATIONAL COMPLEXITY 2012" GUEST EDITORS' FOREWORD

Boaz Barak and Irit Dinur

This special issue contains the full versions of seven papers that were presented at the 27th Annual IEEE Conference on Computational Complexity (CCC 2012) held from June 26–29, 2012 at Universidade do Porto, Porto, Portugal. These papers were selected for invitation by the program committee from all the papers presented at the conference, and following submission underwent the standard refereeing process.

The papers are:

1. *On sunflowers and matrix multiplication* by Noga Alon, Amir Shpilka, and Christopher Umans.

2. *A satisfiability algorithm and average-case hardness for formulas over the full binary basis* by Kazuhisa Seto and Suguru Tamaki.

3. *DNF sparsification and a faster deterministic counting algorithm* by Parikshit Gopalan, Raghu Meka, and Omer Reingold.

4. *Amplifying circuit ower bounds against polynomial time, with applications* by Richard J. Lipton and Ryan Williams.

5. *Is Valiant–Vazirani's isolation probability improvable?* by Holger Dell, Valentine Kabanets, Dieter van Melkebeek, and Osamu Watanabe.

6. *Parallel approximation of min–max problems* by Gus Gutoski and Xiaodi Wu.

7. *A strong direct product theorem for quantum query complexity* by Troy Lee and Jérémie Roland.

Alon *et al.* show a very surprising connection between old conjectures in combinatorics such as the *sunflower conjecture* of Erdős and Rado and more recent questions that arise in the quest for an $n^{2+o(1)}$-time algorithm for multiplying $n \times n$ matrices. Specifically, they show that the sunflower conjecture and variants of it actually *contradict* conjectures that were proposed by Coppersmith and Winograd (1990) and Cohn *et al.* (2005) as approaches to achieve an $n^{2+o(1)}$-time matrix multiplication algorithm.

One of the hallmarks of computational complexity has been the interplay between algorithms and lower bounds. Underlying many lower bounds are *meta algorithms* that perform a task such as checking satisfiability or distinguishing from random for all functions from a certain complexity class. The next three papers are of that flavor. Seto and Tamaki give a faster-than-brute-force algorithm for satisfiability of Boolean formulas with arbitrary binary gates. This meta-algorithm yields a new average-case lower bound with respect to such formulas. Gopalan *et al.* give a faster algorithm to approximate the fraction of satisfying assignments of DNF formulas. This time, the complexity fruits from this algorithm (and the insights underlying it) are an improved pseudorandom generator and a derandomized version of Håstad's famous switching lemma. Lipton and Williams give a different kind of meta-algorithm—a self-reduction for the **P**-complete problem of evaluating Boolean circuits. Using this reduction, they show that an $n^{1+\epsilon}$ size lower bound for this problem (with respect to slightly shallow circuits) can be "amplified" into a lower bound for size n^k and also give some new unconditional lower bounds for the problem of recognizing valid quantified Boolean formulas.

Next, a paper by Dell *et al.* shows the essential impossibility of making the Valiant–Vazirani isolation lemma deterministic. This celebrated lemma gives a reduction from any SAT instance x into another SAT instance y such that: if x is not satisfiable, then neither is y, and if x is satisfiable, then with probability $\Omega(1/n)$ y

is satisfied by a unique assignment. This basic randomized reduction has quite a few applications in complexity theory including, for example, Toda's theorem. The current paper shows that the randomness is inherent. They show that the existence of a similar procedure with success probability above $2/3$ instead of just $1/n$ would imply $\mathbf{NP} = \mathbf{P/poly}$.

The final two papers address questions about quantum complexity. The first one, by Lee and Roland, proves a strong direct product theorem for quantum query complexity as well as a corresponding XOR lemma. They show that computing k copies of a function succeeds with exponentially small probability unless given k times more queries. The second paper, by Gutoski and Wu, presents a parallel algorithm for a particular class of optimization problems which includes a broad range of semi-definite programs. This class is motivated by certain classes in quantum complexity theory, capturing the model of "competing-prover quantum interactive proofs." The new algorithm herein shows that these classes are contained in **PSPACE**.

We wish to thank the authors of the papers for accepting the invitation and submitting and revising their manuscripts within a short time frame, and thank the referees for their thorough and timely reviews. Finally, we want to thank Venkatesan Guruswami and Joachim von zur Gathen for inviting us to edit this special issue.

Boaz Barak and Irit Dinur
Guest Editors

Manuscript received 17 April 2013

Boaz Barak
Microsoft Research New England,
Cambridge, MA, USA.
b@boazbarak.org
http://www.boazbarak.org

Irit Dinur
Weizmann Institute of Science,
Rehovot, Israel.
irit.dinur@weizmann.ac.il
http://www.wisdom.weizmann.ac.il/~dinuri/