2012 IEEE 27th Conference on Computational Complexity

(CCC 2012)

Porto, Portugal
26 – 29 June 2012
Preface .........................................................................................................................................................ix
Organizing Committee .................................................................................................................................x
Program Committee .....................................................................................................................................xi
Reviewers ....................................................................................................................................................xii
Awards ........................................................................................................................................................xiv

Session 1A
Amplifying Circuit Lower Bounds against Polynomial Time with Applications .................................1
Richard J. Lipton and Ryan Williams
Is Valiant-Vazirani's Isolation Probability Improvable? .................................................................10
Holger Dell, Valentine Kabanets, Dieter van Melkebeek, and Osamu Watanabe

Session 1B
Parallel Approximation of Min-max Problems with Applications to Classical
and Quantum Zero-Sum Games ..............................................................................................................21
Gus Gutoski and Xiaodi Wu
The Complexity of the Separable Hamiltonian Problem .................................................................32
André Chailloux and Or Sattath
Quantum Money with Classical Verification .........................................................................................42
Dmitry Gavinsky

Session 2A
On the Usefulness of Predicates ............................................................................................................53
Per Austrin and Johan Håstad
Reductions between Expansion Problems ...............................................................................................64
Prasad Raghavendra, David Steurer, and Madhur Tulsian
On Problems as Hard as CNF-SAT

Marek Cygan, Holger Dell, Daniel Lokshtanov, Dániel Marx, Jesper Nederlof,
Yoshio Okamoto, Ramamohan Paturi, Saket Saurabh, and Magnus Wahlström

Session 2B

Testing List H-homomorphisms

Yuichi Yoshida

A Dichotomy for Real Weighted Holant Problems

Sangxia Huang and Pinyan Lu

Session 3A

A Satisfiability Algorithm and Average-Case Hardness for Formulas over
the Full Binary Basis

Kazuhisa Seto and Suguru Tamaki

Approximating AC^0 by Small Height Decision Trees and a Deterministic
Algorithm for #AC^0SAT

Paul Beame, Russell Impagliazzo, and Srikanth Srinivasan

DNF Sparsification and a Faster Deterministic Counting Algorithm

Parikshit Gopalan, Raghu Meka, and Omer Reingold

Session 3B: Invited Talk I

Communication Complexity and Information Complexity: Foundations
and New Directions

Toniann Pitassi

Session 4A

Gaussian Noise Sensitivity and Fourier Tails

Guy Kindler and Ryan O'Donnell

Junto-Symmetric Functions, Hypergraph Isomorphism and Crunching

Sourav Chakraborty, Eldar Fischer, David Gacia–Soriano, and Arie Matsliah

Complexity Lower Bounds through Balanced Graph Properties

Guy Moshkovitz

Session 4B

Limitations of Lower-Bound Methods for the Wire Complexity of Boolean
Operators

Andrew Drucker

Limits on Alternation-Trading Proofs for Time-Space Lower Bounds

Samuel R. Buss and Ryan Williams
The Hardness of Being Private ................................................................. 192
Anil Ada, Arkadev Chattopadhyay, Stephen Cook, Lila Fontes, Michal Koucký,
and Toniann Pitassi

Session 5A
Matrix Isomorphism of Matrix Lie Algebras ..................................................... 203
Joshua A. Grochow
On Sunflowers and Matrix Multiplication .................................................. 214
Noga Alon, Amir Shpilka, and Christopher Umans
Algebras of Minimal Multiplicative Complexity ........................................ 224
Markus Bläser and Bekhan Chokaev

Session 5B: Invited Talk II
Prospects for Geometric Complexity Theory ............................................... 235
Peter Bürgisser

Session 6A
A Strong Direct Product Theorem for Quantum Query Complexity ............ 236
Troy Lee and Jérémie Roland
A Strong Parallel Repetition Theorem for Projection Games on Expanders .... 247
Ran Raz and Ricky Rosen
Share Conversion and Private Information Retrieval .................................... 258
Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Ilan Orlov

Session 6B
Nondeterministic Circuit Lower Bounds from Mildly De-randomizing
Arthur-Merlin Games .............................................................................. 269
Baris Aydintloglu and Dieter van Melkebeek
Hitting Set Generators for Sparse Polynomials over Any Finite Fields .......... 280
Chi-Jen Lu
Pseudorandom Generators for Read-Once ACC^0 ...................................... 287
Dmitry Gavinsky, Shachar Lovett, and Srikanth Srinivasan

Session 7A
Non-malleable Extractors with Short Seeds and Applications to Privacy
Amplification .......................................................................................... 298
Gil Cohen, Ran Raz, and Gil Segev
Better Condensers and New Extractors from Parvaresh-Vardy Codes .......... 309
Amnon Ta-Shma and Christopher Umans
List Decoding Barnes-Wall Lattices .............................................................................................................316
Elena Grigorescu and Chris Peikert

Session 7B
Space-Efficient Algorithms for Reachability in Surface-Embedded Graphs .................................................326
Derrick Stolee and N.V. Vinodchandran
Space Complexity in Polynomial Calculus ..................................................................................................334
Yuval Filmus, Massimo Lauria, Jakob Nordström, Neil Thapen, and Noga Ron-Zewi
Combinatorial PCPs with Short Proofs ........................................................................................................345
Or Meir

Author Index .............................................................................................................................................356