

**Twenty-First Annual IEEE  
Conference on  
Computational Complexity  
(CCC 2006)**

**Prague, Czech Republic  
16-20 July 2006**



**IEEE Catalog Number:**  
**ISBN:**

**PR2596**  
**0-7695-2596-2**

# Contents

## Proceedings of the Twenty-First Annual IEEE Conference on Computational Complexity

---

**CCC 2006**

<b>Preface</b> .....	viii
<b>Committees</b> .....	ix
<b>Reviewers</b> .....	x
<b>Ronald V. Book Prize for Best Student Paper Award and 2006 Best Paper Award</b> .....	xi

---

### Session 1

*Chair:* Manindra Agrawal

Invited Talk: Gödel and Computations .....	3
<i>Pavel Pudlák</i>	

### Session 2

*Chair:* Manindra Agrawal

Polynomial Identity Testing for Depth 3 Circuits .....	9
<i>Neeraj Kayal and Nitin Saxena</i>	
Every Linear Threshold Function Has a Low-Weight Approximator .....	18
<i>Rocco A. Servedio</i>	

### Session 3

*Chair:* Valentine Kabanets

Constructions of Low-Degree and Error-Correcting $\epsilon$ -Biased Generators .....	33
<i>Amir Shpilka</i>	
How to Get More Mileage from Randomness Extractors .....	46
<i>Ronen Shaltiel</i>	
Exposure-Resilient Extractors .....	61
<i>Marius Zimand</i>	

### Session 4

*Chair:* Valentine Kabanets

Making Hard Problems Harder .....	73
<i>Joshua Buresh-Oppenheim and Rahul Santhanam</i>	

Distinguishing SAT from Polynomial-Size Circuits, through Black-Box Queries ..... 88  
*Albert Atserias*

Parallel Repetition of Zero-Knowledge Proofs and the Possibility of Basing Cryptography on  
NP-Hardness ..... 96  
*Rafael Pass*

## Session 5

*Chair:* Madhu Sudan

Invited Talk: Applications of the Sum-Product Theorem in Finite Fields ..... 111  
*Avi Wigderson*

## Session 6

*Chair:* Madhu Sudan

Constructing Ramsey Graphs from Boolean Function Representations ..... 115  
*Parikshit Gopalan*

A Generic Time Hierarchy for Semantic Models with One Bit of Advice ..... 129  
*Dieter van Melkebeek and Konstantin Pervyshev*

## Session 7

*Chair:* John Hitchcock

Hardness of the Covering Radius Problem on Lattices ..... 145  
*Ishay Haviv and Oded Regev*

A 3-Query Non-Adaptive PCP with Perfect Completeness ..... 159  
*Subhash Khot and Rishi Saket*

New Lower Bounds for Vertex Cover in the Lovász-Schrijver Hierarchy ..... 170  
*Iannis Tourlakis*

## Session 8

*Chair:* Pierre McKenzie

FO[<]-Uniformity ..... 183  
*Christoph Behle and Klaus-Jörn Lange*

Circuit Lower Bounds via Ehrenfeucht-Fraïssé Games ..... 190  
*Michal Koucký, Clemens Lautemann, Sebastian Poloczek, and Denis Thérien*

On Modular Counting with Polynomials ..... 202  
*Kristoffer Arnsfelt Hansen*

## Session 9

*Chair:* Jacobo Toran

Learning Monotone Decision Trees in Polynomial Time ..... 213  
*Ryan O'Donnell and Rocco A. Servedio*

Optimal Hardness Results for Maximizing Agreements with Monomials ..... 226  
*Vitaly Feldman*

## Session 10

*Chair:* Pierre McKenzie

Minimizing DNF Formulas and $AC^0_d$ Circuits Given a Truth Table .....	237
<i>Eric Allender, Lisa Hellerstein, Paul McCabe, Toniann Pitassi, and Michael Saks</i>	
A Duality between Clause Width and Clause Density for SAT .....	252
<i>Chris Calabro, Russell Impagliazzo, and Ramamohan Paturi</i>	

## Session 11

*Chair:* John Hitchcock

QMA/qpoly $\subseteq$ PSPACE/poly: De-Merlinizing Quantum Protocols .....	261
<i>Scott Aaronson</i>	
Random Measurement Bases, Quantum State Distinction and Applications to the Hidden Subgroup Problem .....	274
<i>Pranab Sen</i>	
Strengths and Weaknesses of Quantum Fingerprinting .....	288
<i>Dmitry Gavinsky, Julia Kempe, and Ronald de Wolf</i>	

## Session 12

*Chair:* Jacobo Toran

Grid Graph Reachability Problems .....	299
<i>Eric Allender, David A. Mix Barrington, Tanmoy Chakraborty, Samir Datta, and Sambuddha Roy</i>	
An Isomorphism between Subexponential and Parameterized Complexity Theory .....	314
<i>Yijia Chen and Martin Grohe</i>	

## Session 13

*Chair:* Manindra Agrawal

On the Complexity of Numerical Analysis .....	331
<i>Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen</i>	
Oracles Are Subtle But Not Malicious .....	340
<i>Scott Aaronson</i>	
Derandomization of Probabilistic Auxiliary Pushdown Automata Classes .....	355
<i>H. Venkateswaran</i>	
<b>Author Index</b> .....	371