Workshop on Computational, Descriptive and Proof Complexity, and Algorithms

Independent University of Moscow, Russia, August 29–31, 2007

French–Russian Poncelet Laboratory, Moscow State University,
supported by **Russian Foundation for Basic Research**

Organizing committee:

Yuri Pritykin
Alexander Shen
Michael Tsfasman
Nikolai Vereshchagin

Invited speakers:

Farid Ablayev
Maxim Babenko
Lev Beklemishev
Harry Buhrman
Andrew Goldberg
Edward Hirsch
Dmitry Itsykson
Yury Lifshits
Yury Makarychev
Konstantin Pervyshev
Vladimir Podolskii
Alexander Razborov
Jayalal Sarma
Alexander Shen
Alexander Vasiliev

Titles

Farid Ablayev	*Classical Simulation Complexity of Bounded Error Quantum Branching Programs*
Maxim Babenko	*Generalized Path Structures in Graphs*
Lev Beklemishev	*Goedel Theorem for Very Weak Systems*
Harry Buhrman	*Quantum Computing*
Andrew Goldberg	*Point to Point Shortest Paths with Preprocessing*
Edward Hirsch	*What is the True Exponent for NP-hard Problems?*
Dmitry Itsykson	*One-way Function Based on an Average-Case Assumption*
Yury Lifshits	*Nearest Neighbors: Known Theoretical Results and Open Problems*
Yury Makarychev	*Embeddings of Finite Metric Spaces*
Yury Makarychev	*Semidefinite Programming*
Konstantin Pervyshev	*Recent Results on Time Hierarchies*
Vladimir Podolskii	*Perceptrons of Large Weight*
Alexander Razborov	*Grand Challenges of Proof Complexity*
Jayalal Sarma	*Complexity of Changing Matrix Rank*
Alexander Shen	*On-line Randomness*
Alexander Vasiliev	*On the Computational Power of Restricted k-OBDDs*

Information

The workshop consists of invited lectures of two types: tutorials and single talks. Topics include various fields of complexity theory, i. e., computational, Kolmogorov and proof complexity, combinatorial optimization, quantum computing, etc. Some other topics in theoretical computer science will be touched.

The workshop will be held in Independent University of Moscow (address: metro station Kropotkinskaya or Smolenskaya, 11 Bolshoi Vlasievskiy per.), room 310.

Do not hesitate to send any further questions and comments to `yura@mccme.ru`. Web page of the workshop: `http://www.mccme.ru/compl2007/`

Preliminary program

	August 29	August 30	August 31
9:30–10:30	Maxim Babenko	Lev Beklemishev	Lev Beklemishev
10:30–11:00	coffee break	coffee break	coffee break
11:00–12:00	Alexander Razborov	Alexander Razborov	Edward Hirsch
12:00–13:00	Harry Buhrman	Harry Buhrman	Harry Buhrman
13:00–14:30	lunch	lunch	lunch
14:30–15:30	Andrew Goldberg	Farid Ablayev	Yury Makarychev
15:30–16:30	Andrew Goldberg	Alexander Vasiliev	Yury Makarychev
16:30–17:00	coffee break	coffee break	coffee break
17:00–18:00	Yury Lifshits	Konstantin Pervyshev	Jayalal Sarma
18:00–18:30	Alexander Shen	Vladimir Podolskii	Dmitry Itsykson

Location

Abstracts

Farid Ablayev. *Classical Simulation Complexity of Bounded Error Quantum Branching Programs*
We present classical simulation techniques for measure once quantum branching programs.
For bounded error syntactic quantum branching program of width w that computes a function with error δ we present a classical deterministic branching program of the same length and width at most $(1 + 2/(1 - 2\delta))^{2w}$ that computes the same function.
Second technique is a classical stochastic simulation technique for bounded error and unbounded error quantum branching programs. Our result is that it is possible stochastically-classically simulate quantum branching programs with the same length and almost the same width, but we lost bounded error acceptance property.

Maxim Babenko. *Generalized Path Structures in Graphs*
The notion of a path plays a central role in graph theory. Two most prominent and widely used of its flavors are undirected and directed paths. Some combinatorial problems also employ the so-called "bidirected graphs" and "bidirected paths" (which provide a common generalization to directed and undirected ones).
Extending these ideas, one gets the general notion of a "fork environment". Under certain assumptions, this framework incorporates all of the above approaches while preserving good characterization and linear-time testing for reachability.

Lev Beklemishev. *Goedel Theorem for Very Weak Systems*
We shall present a beautiful extension, due to P. Pudlak, of Goedel's second incompleteness theorem to theories as weak as Robinson's arithmetic Q.

Harry Buhrman. *Quantum Computing*
We will introduce the mathematical framework of quantum mechanics and show how it can be used to define a quantum computer. We will then treat some of the known quantum algorithms including Shor's factorization algorithm, entanglement and the Einstein-Podolsky-Rozen paradox, quantum communication complexity, and quantum cryptography. If time permits we will mention some of the recent developments.

Andrew Goldberg. *Point to Point Shortest Paths with Preprocessing*
We study the point to point shortest path problem where one can preprocess the data and then answer queries quickly. This is a fundamental problem with many applications, including that of computing driving directions. We described two main techniques, A* search with landmark-based lower bounds and reach-based pruning, which are very effective in improving efficiency of the standard Dijkstra's algorithm for the problem. A combination of these techniques is especially effective. It allows answering queries on road networks with 20 to 30 million vertices (e.g., North America, Western Europe) while visiting a few thousand vertices in the worst case and less than a thousand on the average. We also state several open problems related to efficiency of our algorithms.

Edward Hirsch. *What is the True Exponent for NP-hard Problems?*
Preliminary list of topics:
1. Algorithms (upper bounds).
2. Lower bounds.
3. Structural questions.
4. Hardness as a resource.

Dmitry Itsykson. *One-way Function Based on an Average-Case Assumption*
We assume the existence of function f that is computable in polynomial time but its inverse function is not computable in randomized average polynomial time. The cryptographic setting is, however, different. Nevertheless, we show how to construct one way function based on f.

Yury Lifshits. *Nearest Neighbors: Known Theoretical Results and Open Problems*
Nearest neighbors problem is formulated as follows: Given a set S of points in some space V (equipped with similarity function), construct a data structure which given any query point q from V finds the closest point in S to q. This kind of search problems arise in many areas: pattern recognition, recommendation systems, text classification, data compression, coding theory, computational statistics.
In the first part we quickly survey known results for this problem. In particular, we discuss (1) black-box model: search space is represented by an oracle that returns a similarity value for any pair of points; and (2) vector model: all points belong to high-dimesional euclidian space. We consider the best known results for worst case complexity, average case complexity as well as known lower bounds. In the second part of the talk a list of open problems will be presented.

Yury Makarychev. *Embeddings of Finite Metric Spaces*
We will talk about low distortion embeddings of finite metric spaces into normed spaces and their applications to computer science. We will describe the connection between the Banach space l_1 and combinatorial optimization problems. Then we will prove Bourgain's theorem: Every metric space

of size n embeds into l_1 with distortion $\log n$. In the second part of the talk, we will discuss recent results in the area and open questions.

Yury Makarychev. *Semidefinite Programming*
I will talk about approximation algorithms based on Semidefinite Programming (SDP). I will present the general framework and describe the approximation algorithm by Goemans and Williamson for the MAX CUT problem. Then I will say a couple of words about the connection with the theory of low distortion metric embeddings. Finally, we will discuss the Unique Games Conjecture and whether SDP is "the best method" for solving combinatorial optimization problems.

Konstantin Pervyshev. *Recent Results on Time Hierarchies*
According to Time Hierarchy theorem, there are computational problems that have really odd time complexity. For example, there is a language recognizable by a deterministic algorithm in time $O(n^{100})$, and this upper time bound is close to optimal. Still, no time hierarchy theorem is known for probabilistic algorithms: are there languages recognizable by randomized algorithms in time $O(n^{100})$ but not in linear time? In this talk, we will overview recent results on time hierarchies for randomized heuristic algorithms and slightly non-uniform probabilistic algorithms.

Vladimir Podolskii. *Perceptrons of Large Weight*
A perceptron of order d is a depth-2 circuit having a threshold gate at the top level and ANDs of fanin d on the remaining level. We prove lower bounds for weights of perceptrons of constant order, which match the known upper bounds.

Alexander Razborov. *Grand Challenges of Proof Complexity*
These lectures will be centered around a set of questions that can be loosely described as follows: *Are major open problems in Complexity Theory like $NP \stackrel{?}{\subseteq} P/poly$ or $P \stackrel{?}{\subseteq} NC^1/poly$ independent from systems of Bounded Arithmetic? Do they possess efficient propositional proofs?*
For obvious reasons (and it should be noted that we are deliberately working with the systems that, to the best of our knowledge, do prove all known results in Circuit Complexity) these independence questions are of utmost importance for both areas, Computational Complexity and Proof Complexity. Nonetheless, despite numerous efforts, they are still widely open. We will try to put these questions in the historical context and survey ideas (sometimes even with complete proofs) that have so far lead to at least non-negligible progress toward their solution. Although we will try to make the lectures as self-contained as possible, some familiarity with Circuit Complexity and Propositional Logic might be helpful. Also, the Introduction to `http://www.mi.ras.ru/~razborov/res_k.ps` can give a rather good impression of the set of topics we will be discussing.

Jayalal Sarma. *Complexity of Changing Matrix Rank*
The number of entries in a matrix that needs to be changed to bring down the rank below a specified value is the rigidity of a matrix. Matrices with high rigidity have interesting applications in the theory of lowerbounds: mainly in arithmetic circuits and in communication complexity. The talk will briefly mention these results, and the attempts at proving lower bounds on rigidity. We will mainly look into the computational version of matrix rigidity: given a matrix M and numbers r, k, decide whether the rank of M can be brought to below r by changing at most k entries of M. This has close connections to the well-studied MINRANK problem. We will present some of our results and open ends concerning this problem and its close variants.

Alexander Shen. *On-line Randomness*
Consider a sequence of (presumably) fair coin tosses that are interleaved with other events (with no probability distribution), like coin tosses before the football games interleaved with the game results. How should we define random bit sequences in this case? Usually we require the sequence of bit to have maximal complexity, but here we should distinguish between two radically different cases: when the next bit is correlated with the previous game (bad) and the following game (allowed). This cannot be easily expressed in terms of standard Kolmogorov complexity. We discuss the appropriate notion of on-line complexity, on-line Martin-Löf randomness and on-line martingale, and the relation of these notions to tests of randomness (in the sense of Sandroni, Vovk a.o.)

Alexander Vasiliev. *On the Computational Power of Restricted k-OBDDs*
The well-known classical result of David M. Barrington (1986) shows that the class of functions, which can be computed by circuits of logarithmic depth (NC^1) is equal to the class of functions computable by branching programs of constant width and polynomial length ($BWBP$). Here we describe in more detail the structure of branching programs generated by the Barrington's method. In particular we prove that width-5 k-OBDDs of polynomial size can compute exactly those functions in NC^1. Formally it can be stated that $poly(n)$-OBDD$_5 = NC^1$.