
Computational Complexity
(Org: **Venkatesh Srinivasan** (University of Victoria))

PAUL BEAME, University of Washington

Making Branching Programs Oblivious Requires Superlogarithmic Overhead

An algorithm is oblivious if and only if its sequence of operations is determined independent of its input. Certain models of computation, such as circuits or straight-line programs are inherently oblivious. However, many computing models such as Turing machines and random access machines (RAMs) are not. Fairly efficient simulations of these general models by their more restricted oblivious variants are known.

We show that either a superlogarithmic increase in time or a large increase in space is necessary for any randomized oblivious simulation of general RAMs. In particular we show a $T = \Omega(n \log(n/S) \log \log(n/S))$ lower bound for any randomized oblivious RAM determining out-degree 1 graph reachability which has an easy linear time logspace non-oblivious algorithm. This is the largest time-space tradeoff lower bound known for any randomized non-uniform model. We show similar, though incomparable, results for Boolean branching programs.

Joint work with Widad Machmouchi

VALERIE KING, University of Victoria

Scalable Distributed Computing Using Averaging Samplers and Bit-fixing Random Sources

Averaging samplers and bit-fixing sources, used in the study of cryptography and pseudorandomness seem naturally applicable to distributed computing with a malicious adversary. We show how we can use these tools to reduce communication complexity for some fundamental problems in distributed computing with a malicious adversary.

(Joint work with Jared Saia and others)

DAVID KIRKPATRICK, University of British Columbia

Finding treasure in trees

We study a multi-goal variant of the classical *cow-path search problem*, when the search domain is modeled by a general rooted symmetric tree (as opposed to a star graph). We describe (near-optimal) competitive universal search strategies in this context that generalize our earlier results on the *multi-list traversal problem*.

[Based on joint work with Sandra Zilles, University of Regina]

ANUP RAO, University of Washington

Towards Coding for Maximum Errors in Interactive Communication

We show that it is possible to encode any communication protocol between two parties so that the protocol succeeds even if a $(1/4 - \epsilon)$ fraction of all symbols transmitted by the parties are corrupted adversarially, at a cost of increasing the communication in the protocol by a constant factor (the constant depends on ϵ). This encoding uses a constant sized alphabet. This improves on an earlier result of Schulman, who showed how to recover when the fraction of errors is bounded by $1/240$. We also show how to simulate an arbitrary protocol with a protocol using the binary alphabet, a constant factor increase in communication and tolerating a $1/8 - \epsilon$ fraction of errors.

Joint work with Mark Braverman.

VENKATESH SRINIVASAN, University of Victoria

Rewriting of Visibly Pushdown Languages for XML Data Integration

In this paper, we focus on XML data integration by studying rewritings of XML target schemas in terms of source schemas. Rewriting is very important in data integration systems where the system is asked to find and assemble XML documents from the data sources and produce documents which satisfy a target schema.

As schema representation, we consider Visibly Pushdown Automata (VPAs) which accept Visibly Pushdown Languages (VPLs). The latter have been shown to coincide with the family of (word-encoded) regular tree languages which are the basis of formalisms for specifying XML schemas. VPLs enjoy a "well-behavedness" which facilitates us in addressing rewriting problems for XML data integration.

Using VPAs, we show algorithmic and complexity results for many variants of rewriting problems for XML data integration.

(Joint work with Alex Thomo)