

2017 Theory Day in Taiwan

<http://theoryday.github.io>

Date: Friday, 6 January, 2017

Location: Auditorium 106 at IIS New Building,
Academia Sinica, Taipei



The Theory Day in Taiwan is an experimental one-day event that aims to stimulate interaction and discussion for TCS researchers in Taiwan and nearby countries. We invited 4 hour-long talks in general TCS area with long breaks for interaction and discussion. The meeting is free and open to everyone; in particular, students are encouraged to attend.

Program

9.00 – 10.00	Luca Trevisan (UC Berkeley) Known Your Place: Simple Distributed Graph-Partitioning Algorithms
10.00 - 10.30	Break and Discussion
10.30 - 11.30	Cedric Yen-Yu Lin (QuICS @ UMD & NIST) A Complete Characterization of Unitary Quantum Space
11.30 - 2.30	Break and Discussion
2.30 - 3.30	Vassilis Zikas (Rensselaer Polytechnic Institute) Fair and Robust Multi-Party Computation using a Global Transaction Ledger
3.30 - 4.00	Break and Discussion
4.00 - 5.00	Nai-Hui Chia (Penn State University) Quantum Worst-Case to Average-Case Reductions for QMA-Complete Problems

Talk Abstract

Known Your Place: Simple Distributed Graph-Partitioning Algorithms

Speaker: Luca Trevisan (UC Berkeley)

Abstract: We study network distributed processes of the following type: each node, independently, picks an initial state according to a certain distribution, then nodes repeatedly exchange information about their states with some or all of their neighbors. At each iteration, each node, based on its state, assigns itself to a cluster.

We show that a synchronous discrete-time algorithm of this sort (in which, at each time step, all nodes communicate their state to all neighbors) converges to the partition found by a centralized spectral partitioning algorithms, and we discuss preliminary results concerning an asynchronous continuous-time version of the algorithm (in which, at Poisson intervals, two adjacent nodes along a random edge exchange information about their states).

(Joint work with Luca Becchetti, Andrea Clementi, Francesco Pasquale, Prasad Raghavendra, and Emanuele Natale)

A Complete Characterization of Unitary Quantum Space

Speaker: Cedric Yen-Yu Lin (QuICS @ UMD & NIST)

Abstract: Motivated by understanding the power of quantum computation with restricted number of qubits, we give two complete characterizations of unitary quantum space bounded computation. First we show that approximating an element of the inverse of a well-conditioned efficiently encoded $2^k \times 2^k$ matrix is complete for the class of problems solvable by quantum circuits acting on $O(k)$ qubits with all measurements at the end of the computation. Similarly, estimating the minimum eigenvalue of an efficiently encoded Hermitian $2^k \times 2^k$ matrix is also complete for this class. In the logspace case, our results improve on previous results of Ta-Shma by giving new space-efficient quantum algorithms that avoid intermediate measurements, as well as showing matching hardness results.

Additionally, as a consequence we show that PreciseQMA, the version of QMA with

exponentially small completeness-soundness gap, is equal to PSPACE. Thus, the problem of estimating the minimum eigenvalue of a local Hamiltonian to inverse exponential precision is PSPACE-complete, which we show holds even in the frustration-free case. Finally, we can use this characterization to give a provable setting in which the ability to prepare the ground state of a local Hamiltonian is more powerful than the ability to prepare PEPS states. Interestingly, by suitably changing the parameterization of either of these problems we can completely characterize the power of quantum computation with simultaneously bounded time and space.

Fair and Robust Multi-Party Computation using a Global Transaction Ledger

Speaker: Vassilis Zikas (Rensselaer Polytechnic Institute)

Abstract: Classical results on secure multi-party computation (MPC) imply that fully secure computation, including fairness (either all parties get output or none) and robustness (output delivery is guaranteed), is impossible unless a majority of the parties is honest. Recently, cryptocurrencies like Bitcoin were utilized to leverage the fairness loss in MPC against a dishonest majority. The idea is that when the protocol aborts in an unfair manner (i.e., after the adversary receives output) then honest parties get compensated (in coins) by the adversarially controlled parties.

We describe the first robust MPC protocol with compensation, i.e., an MPC protocol where not only fairness is guaranteed (via compensation) but additionally the protocol is guaranteed to deliver output to the parties that get engaged. This means that the adversary, after an initial round of deposits, is not even able to mount a denial-of-service attack without having to suffer a monetary penalty. Our robust MPC protocol requires only a constant number of (coin-transfer and communication) rounds. To prove the security of our construction, we put forth a new formal model of secure MPC with compensation and show how the introduction of suitable ledger and synchronization functionalities makes it possible to describe such protocols using standard interactive Turing machines (ITM) circumventing the need for the use of extra features that are outside the standard model as in previous works. Our model is expressed in the universal composition setting with global setup and is equipped with a composition theorem that enables the design of protocols, which compose safely with each other and within larger environments alongside other protocols with compensation; such a composition theorem for MPC protocols with compensation was not known before.

This is joint work with Aggelos Kiayias and Hong-Sheng Zhou.

Quantum Worst-Case to Average-Case Reductions for QMA-Complete Problems

Speaker: Nai-Hui Chia (Penn State University)

Abstract: A fundamental question in the study of average-case complexity is whether there exist randomized reductions from worst-case NP-complete problems to average-case NP-complete problems. Feigenbaum and Fortnow first showed that the existence of nonadaptive random-self reduction for NP problems implies the polynomial hierarchy collapses to the third level. Then, Bogdanov and Trevisan showed that the existence of nonadaptive worst-case to average-case randomized reductions for NP problems also implies the polynomial hierarchy collapses to the third level.

In our work, we consider the quantum analogue of Bogdanov and Trevisan's theorem. To be more specific, we ask whether there exist quantum reductions which reduce worst-case QMA-complete problems to average-case QMA problems. We will first define the classical random-self reduction and the worst-case to average-case reduction and introduce the known results. Then, we will define the quantum analogue of these reductions and some quantum complexity classes and discuss if the classical approaches for Bogdanov and Trevisan's theorem and Feigenbaum and Fortnow's theorem also work in the quantum setting. In the last part of the talk, we will show our approach and partial results for quantum worst-case to average-case reductions for QMA-complete problems.

This is a joint work with Sean Hallgren.