Bocconi

23 OCTOBER 2023
12:00 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1, Milano (3° floor)

Classical simulation of one-query quantum distinguishers

Speaker

Andrej Bogdanov
Professor in the School of Electrical Engineering and Computer Sciencet
University of Ottawa

Abstract

A distinguisher is an algorithm that tells whether its input was sampled from one distribution or from another. The computational complexity of distinguishers is important for much of cryptography, pseudorandomness, and statistical inference.

We study the relative advantage of classical and quantum distinguishers of bounded query complexity over n-bit strings. Our focus is on a single quantum query, which is already quite powerful: Aaronson and Ambainis (STOC 2015) constructed a pair of distributions that is ε-distinguishable by a one-query quantum algorithm, but $O(\varepsilon k/\sqrt{n})$-indistinguishable by any non-adaptive k-query classical algorithm.

We show that every pair of distributions that is ε-distinguishable by a one-query quantum algorithm is distinguishable with k classical queries and (1) advantage $\min\{\Omega(\varepsilon\sqrt{(k/n)}), \Omega(\varepsilon^2 k^2/n)\}$ non-adaptively (i.e., in one round), and (2) advantage $\Omega(\varepsilon^2 k/\sqrt{(n \log n)})$ in two rounds. The second bound is tight in k and n up to a $(\log n)$ factor.

Based on joint work with Tsun Ming Cheung (McGill), Krishnamoorthy Dinesh (IIT Palakkad), and John C.S. Lui (CUHK)

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES