# The University of Chicago

# Department of Computer Science & Mathematics

# Combinatorics & Theory Seminar

**PRESENTS:**



**Scott Aaronson**

University of Texas, Austin

Title: “Gentle Measurement of Quantum State & Differential Privacy”

Abstract: In differential privacy (DP), we want to query a database about n  
users, in a way that "leaks at most eps about any individual user,"  
conditioned on any outcome of the query.  Meanwhile, in gentle  
measurement, we want to measure n quantum states, in a way that  
"damages the states by at most alpha," conditioned on any outcome of  
the measurement.  In both cases, we can achieve the goal by techniques  
like deliberately adding noise to the outcome before returning it.  We  
prove a new and general connection between the two subjects.  
Specifically, on products of n quantum states, any measurement that is  
alpha-gentle for small alpha is also O(alpha)-DP, and any product  
measurement that is eps-DP is also O(eps\*sqrt(n)) -gentle.  
  
Illustrating the power of this connection, we apply it to the recently  
studied problem of shadow tomography.  Given an unknown d-dimensional  
quantum state rho, as well as known two-outcome measurements  
E\_1,...,E\_m, shadow tomography asks us to estimate Pr[E\_i accepts  
rho], for every i in [m], by measuring few copies of rho.  Using our  
connection theorem, together with a quantum analog of the so-called  
private multiplicative weights algorithm of Hardt and Rothblum, we  
give a protocol to solve this problem using O((log m)^2 (log d)^2)  
copies of rho, compared to Aaronson's previous bound of ~O((log m)^4  
(log d)).  Our protocol has the advantages of being online (that is,  
the E\_i's are processed one at a time), gentle, and conceptually  
simple.

Joint work with Guy Rothblum (to appear in STOC'2019).

**Note: Non-Standard Day**

Thursday, February 28, 2018

Ry. 251 @ 3:30 pm

(Refreshments will be served prior to the talk in Ry. 255 @ 3:00pm)