

abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR I

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In recent joint work with Alex Arkhipov, we proposed a quantum optics experiment, which would sample from a probability distribution that we believe cannot be sampled (even approximately) by any efficient classical algorithm, unless the polynomial hierarchy collapses. Several optics groups are already working toward doing our experiment.

However, our computational hardness argument currently depends on two unproved conjectures, both concerning the permanent of an n -by- n matrix X of independent $N(0,1)$ complex Gaussians. The first conjecture says that that $\Pr[|\text{Per}(X)| < \sqrt{n!}/\text{poly}(n)]$ is upper-bounded by $1/\text{poly}(n)$, while the second conjecture says that approximating $\text{Per}(X)$, for most Gaussian matrices X , is a $\#P$ -complete problem. Both conjectures seem interesting even independently of our application. In this talk, I'll tell you about these conjectures, and the progress we were able to make toward proving them. Specifically, I'll show that our conjectured anti-concentration bound holds with the determinant in place of the permanent. If time permits, I'll also show that a weaker anti-concentration bound holds for the permanent; that *exactly* computing $\text{Per}(X)$ with high probability for a Gaussian matrix X is $\#P$ -hard; and that extending this $\#P$ -hardness to the approximate case will require going outside the LFKN/Lipton polynomial interpolation paradigm.