Mathematics, Statistics, and Computer Science **@ UIC**

Special Colloquium

Designing Fast and Robust Learning Algorithms Using Spectral Graph Theory

Yu Cheng (Duke)

Abstract: Most people interact with machine learning systems on a daily basis. Such interactions often happen in strategic environments where people have incentives to manipulate the learning algorithms. As machine learning plays a more prominent role in our society, it is important to understand whether existing algorithms are vulnerable to adversarial attacks and, if so, design new algorithms that are robust in these strategic environments.

In recent years, there have been exciting developments in algorithmic spectral graph theory, including faster algorithms for solving Laplacian linear systems, graph sparsification, and maximum flow. In this talk, I will focus on two lines of my work on leveraging the recent advancements in spectral graph theory to design fast and provably robust learning algorithms: making non-convex matrix completion approaches robust against semi-random adversaries, and designing robust high-dimensional statistical estimators that can be computed almost as efficiently as their non-robust counterparts.

Colloquium tea to follow at 4pm in SEO 300.

Thursday, February 21 at 3:00 PM in 636 SEO