CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, Edificio Norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

AGCO Seminar

Speaker: Ravi Sundaram, Northeastern U, USA.

***Title*:** Learning to cope with adversaries (in theory) and noise (in practice).

Abstract: Learning theory has burgeoned since 1971 (VC-dimension by Vapnik and Chervonenkis) when the framework was established and the fundamental theorem proved. We extend the framework to model a strategic setting that allows for adversarial behavior during the test phase. As an example consider a situation where students may manipulate their application materials knowing universities' admissions criteria. We define a new parameter, SVC (Strategic VC dimension) and use it to characterize the statistical and computational learnability of the strategic linear classification problem. The practice of learning exploded in 2012 (AlexNet by Krizhevsky, Sutskever and Hinton) leading to a profusion of deep neural network (DNN) architectures and training algorithms. We consider the problem of creating tags from a noisy scanning technology (e.g. optochemical inks, magnetic microwires etc.).

Formalizing it as a coding-theoretic problem. we develop a novel neural network architecture (DANNI) and training algorithm to solve it, with provable performance guarantees.

The theory part is joint work with Anil Vullikanti, Haifeng Xu and Fan Yao, and the practice part is joint with Akshar Varma.

***When*:** May 3, **3:00 pm hrs.**

***Where*:** Sala de Seminario John Von Neuman, CMM, Beauchef 851, Torre Norte.