FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, edificio norte, Piso 7
Santiago, Chile
CP 837 0456

Tel. +56-2 2978 4870

Seminar AGCO

Speaker: Cristóbal Guzmán, University of Twente, Países Bajos.

***Title*:** Non-Euclidean Differentially Private Stochastic Convex Optimization.

Abstract: Differentially private (DP) stochastic convex optimization (SCO) is a fundamental problem, where the goal is to approximately minimize the population risk with respect to a convex loss function, given a dataset of i.i.d. samples from a distribution, while satisfying differential privacy with respect to the dataset. Most of the existing works in the literature of private convex optimization focus on the Euclidean (i.e., ℓ_2) setting, where the loss is assumed to be Lipschitz (and possibly smooth) w.r.t.~the ℓ_2 norm over a constraint set with bounded ℓ_2 diameter. Algorithms based on noisy stochastic gradient descent (SGD) are known to attain the optimal excess risk in this setting.

In this talk I will provide a brief overview of differential privacy and its applications in stochastic convex optimization, together with new upper and lower bounds on the population risk for DP-SCO in non-Euclidean setups, in particular where the reference norm is the ℓ_p-norm, $1\leq p\leq \infty$. Our algorithms include DP versions of variance-reduced stochastic Frank-Wolfe and mirror-descent methods, together with a novel privacy mechanism, which generalizes the Gaussian mechanism. Our work draws upon concepts from the geometry of normed spaces, such as the notions of regularity, uniform convexity, and uniform smoothness.

Based on joint work with Raef Bassily and Anupama Nandi, and available at arXiv:2103.01278

Wednesday, May 05, 14:30 hrs (Chilean time).

Dónde: https://zoom.us/j/98855281600?pwd=Z3A4bGMvSGFwQnl5OXhOWE41UVNIQT09