Séminaire de Probabilités et Statistique

Mardi 17 janvier à 14h00

Salle de conférences

Yassine Laguel

Rutgers

Robustness for models and algorithms in Machine Learning

Risk-averse optimization plays a major role in the design of safety for machine learning applications. In this talk, we will present a set of tools to enhance the robustness of models and algorithms to potentially harmful data shifts. First, we will expose some general results on the modeling of risk aversion and highlight the interest of superquantile-based risk measures to enforce robustness to worst-case events. We will then show how such a measure may be minimized in the centralized setting based on a smoothing à la Nesterov of the superquantile. We will then present applications of this framework in federated learning to handle statistical heterogeneity among the devices of a given network. Second, we will revisit the bias-variance trade-off of first-order stochastic algorithms from a robust perspective. Precisely, we study the convergence properties of accelerated methods on saddle-point problems for diverse robustness metrics. We present a tight convergence analysis in the strongly convex/strongly concave setting and an in-depth analysis for quadratics and discuss how this may lead us to novel parameter selection procedures.