Friday 1 June 2018 – at 11.30 am
Room A108 – Polo Ferrari 1

Diego Fioravanti
(Max Planck Institute for Intelligent Systems)

Adversarial examples and optimal transport

Abstract:
Through state of the art methods, like convolution neural network, a number of breakthrough in classification problems were achieved. Despite their unquestionable success, many questions remain unanswered. In this talk I will focus on the problem of adversarial examples. An adversarial example is defined as a small alteration of a correctly classified input that leads to misclassification. While extensively studied empirically, there is still a lack of understanding on why adversarial examples happen and why they are so easily constructed for any given input. Recently, optimal transport emerged as the best way to model and analyse mathematically adversarial examples. After a short introduction, I will illustrate how the theory of optimal transport is currently used and how we hope to improve the state of the art.

Contact person: Claudio Agostinelli