COMPUTER SCIENCE COLLOQUIUM

Trimming Data Sets: a Verified Algorithm for Robust Mean Estimation

Alessandro Bruni
ITU

Friday, 24 June, 2022 at 15:00
IMADA's Methods Lab

Abstract:

The operation of trimming data sets is heavily used in AI systems. Trimming is useful to make AI systems more robust against adversarial or common perturbations. At the core of robust AI systems lies the concept that outliers in a data set occur with low probability, and therefore can be discarded with little loss of precision in the result. The statistical argument that formalizes this concept of robustness is based on an extension of the Chebyshev's inequality first proposed by Tukey in 1960.

In this paper we present a mechanized proof of robustness of the trimmed mean algorithm, which is a statistical method underlying many complex applications of deep learning. For this purpose we use the Coq proof assistant to formalize Tukey's extension to Chebyshev's inequality, which allows us to verify the robustness of the trimmed mean algorithm. Our contribution shows the viability of mechanized robustness arguments for algorithms that are at the foundation of complex AI systems.

Host: Jacopo Mauro