FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA
Fakultät für Mathematik und Informatik

Institut für Mathematik

Seminar zur Stochastik

Mittwoch, 4. Mai 2022
12 Uhr s. t.
HS 3 Abbeanum, Fröbelstieg 1

Frau Prof. Dr. Julia Christine Hörrmann
(Friedrich-Schiller-Universität Jena)

"A new mathematical view on classification inspired by the desire to understand adversarial examples"

Abstract:
We take different mathematical view points on the task of classification namely a statistical, probabilistic, geometric and inverse problem theoretic
viewpoint with the goal to tackle the problem of understanding adversarial examples. We assume the domain to be a hypercube which is prototypical for image classification. Here we show that
the usual and robust classification tasks are never well-posed for the whole hypercube.
By introducing a don't know class we reformulate the classification task so that well-posedness can be achieved if the distance of the class supports is positive. Furthermore we complement the lower bound on the probability of adversarial examples in (Shafahi et al., 2019) by upper bounds under suitable geometric conditions on the class supports.

Alle Interessierte sind herzlich eingeladen

Kontakt:
Stefan Ankirchner
Stochastische Analysis
Institut für Mathematik
Ernst-Abbe-Platz 2
07743 Jena