Einladung zum Oberseminar Mathematik des Maschinellen Lernens und Angewandte Analysis

Julius-Maximilians-Universität Würzburg
Professur für Mathematik des Maschinellen Lernens

MSc. Lucas Schmitt

Universität Würzburg
Mathematik des Maschinellen Lernens

Adversarial Training as a Primal-Dual Problem

An important topic in machine learning, particularly concerning security, is the robustness of models against adversarial attacks. This issue can be addressed through adversarial training, although this approach typically incurs high computational costs. In this work, we establish a characterization of the subdifferential of a nonlocal total variation functional, which is one-homogeneous and arises in a convex relaxation of the adversarial training problem for binary classification. To this end, we derive a dual representation of the nonlocal total variation involving a nonlocal divergence and gradient, and we ensure its consistency with their local counterparts. Based on this dual formulation, we develop a primal-dual algorithm for the relaxed adversarial training problem, providing an efficient algorithmic approach to solving the original problem.

Ort: Mathematik Ost, Seminarraum 40.01.003 Zeit: Dienstag, 28.10.2025 13:00

Zu diesem Vortrag laden wir Sie herzlich ein.

gez. Leon Bungert