Einladung zum Oberseminar Mathematik des Maschinellen Lernens und Angewandte Analysis, im Rahmen der AI Talks @ JMU

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

Dr. Muni Sreenivas Pydi

Université Paris Dauphine-PSL

Differentially Private Gradient Flow for Generative Modeling

Safeguarding privacy in sensitive training data is paramount, particularly in the context of generative modeling. This is done through either differentially private stochastic gradient descent, or with a differentially private metric for training models or generators. In this talk, I will introduce a novel differentially private generative modeling approach based on parameter-free gradient flows in the space of probability measures. The proposed algorithm is a new discretized flow which operates through a particle scheme, utilizing drift derived from the sliced Wasserstein distance and computed in a private manner. Our experiments show that compared to a generator-based model, our proposed model can generate higher-fidelity data at a low privacy budget, offering a viable alternative to generator-based approaches.

Ort: Gebäude Z6, Raum 0.002 Zeit: Dienstag, 30.04.2024 16:15

Zu diesem Vortrag laden wir Sie herzlich ein.

gez. Leon Bungert