Machine Learning Seminar

Preliminary Meeting (IN2107, IN4872)

Lecturer: Prof. Dr. Stephan Günnemann

Summer Term 2021

Team

- Prof. Dr. Stephan Günnemann
- Anna Kopetzki, Simon Geisler, Aleksei Kuvshinov, Daniel Zügner

This is a seminar for **Master** students!
Main prerequisite: Machine Learning (IN2064)

Website

`https://www.in.tum.de/daml/lehre/sommersemester-2021/seminar/`

Why attend this Seminar?

1. Learn about and explore **state-of-the-art** research in ML
2. **Analyze and criticize** recent publications
3. Improve your **scientific writing**
4. Participate in a **review process** akin to international conferences
5. Improve your **presentation skills**

Topics I: Properties of ML models

- Adversarial robustness
  - Attacks beyond Lp-setting (rotations, translations, . . .)
  - Robustness of graph neural networks
  - Robustness of CNNs
  - Adversarial training
- Robustness
  - Randomized smoothing & verification
  - Robustness verification against Lp-perturbations
  - Robustness to non-Lp-bounded perturbations (lighting changes, . . .)
- Uncertainty estimation
- Transfer learning

Topics II: Modern Architectures

- Sparse neural networks
- Transformers for perception (or non-sequential data)
- Neural network ensembles (focus on rank-1 (Bayesian) ensembles)
- Object-centric deep learning
- Scalable attention models

Requirements

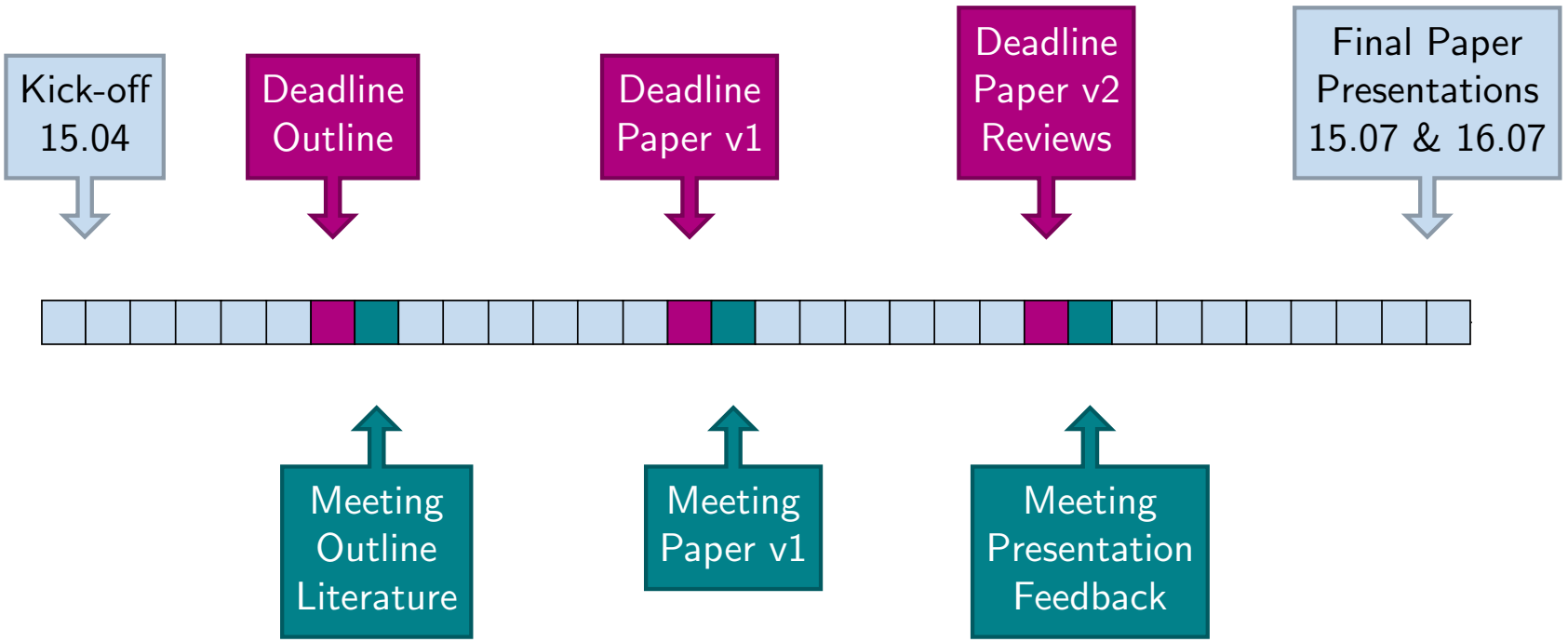
- Strong knowledge of machine learning and mathematics
- Passed relevant courses (the more, the better)
  - Machine Learning (hard requirement)
  - Machine Learning for Graphs and Sequential Data (formerly Mining Massive Datasets)
  - Machine Learning Lab
- Motivation
- Additional selection criteria
  - relevant experience (projects in companies, experience as a HiWi)
    $\Rightarrow$ you can send an overview of your experience to us (see end of slides)

Tasks

1. Read **seed research papers** (provided by us)
2. Start your **snowball research** from there (references to, from these papers, relevant keywords)
3. Summarize your findings, criticism, and research ideas in a **short paper** (4 pages, double column)
4. Write **reviews** of other students work
5. **Present** your work in 25-minute talks

Grade will be based on **all** parts: Paper, reviews, talk and overall participation

Schedule


Kick-off
15.04
Deadline
Outline
Deadline
Paper v1
Deadline
Paper v2
Reviews
Final Paper
Presentations
15.07 & 16.07
Meeting
Outline
Literature
Meeting
Paper v1
Meeting
Presentation
Feedback

Registration

Registration via the matching system!
Selected Topics in Machine Learning Research
(IN2107, IN4872)

+ Fill out the application form!
`https://docs.google.com/forms/d/e/1FAIpQLSecqkNH3n_B6ZkHRWUVgakLXtRQgvuNoqu2fUKWgNKv9FPrkg/viewform`

- provide us with your list of experience in ML (courses, projects, etc.)
- please send us a **concise** overview (bullet list, not a complete CV)