Machine Learning Seminar

Preliminary Meeting (IN2107, IN4872)

Lecturer: Prof. Dr. Stephan Günnemann

Summer Term 2023

Team

- Prof. Dr. Stephan Günnemann
- Lukas Gosch, Tom Wollschläger, Nicholas Gao, Aleksei Kuvshinov

This is a seminar for **Master** students!
Main prerequisite: Machine Learning (IN2064)
Optional: Machine-Learning for Graphs and Sequential Data (IN2323)

Website

`https://www.cs.cit.tum.de/daml/lehre/sommersemester-2023/seminar/`

Topics I: (Preliminary)

- (Adversarial) Robustness
  - Adversarial Training of Deep Neural Networks
  - Randomized Smoothing: Limitations of the Standard Approach
  - Randomized Smoothing: Recent Advances
  - (Random) Lipschitz Neural Networks
- Modern Architectures & Training
  - Efficient Transformers
  - Learning-free Neural Architecture Search
  - Approximate Second-Order Optimization
  - Model-based Meta-Learning

Topics II: (Preliminary)

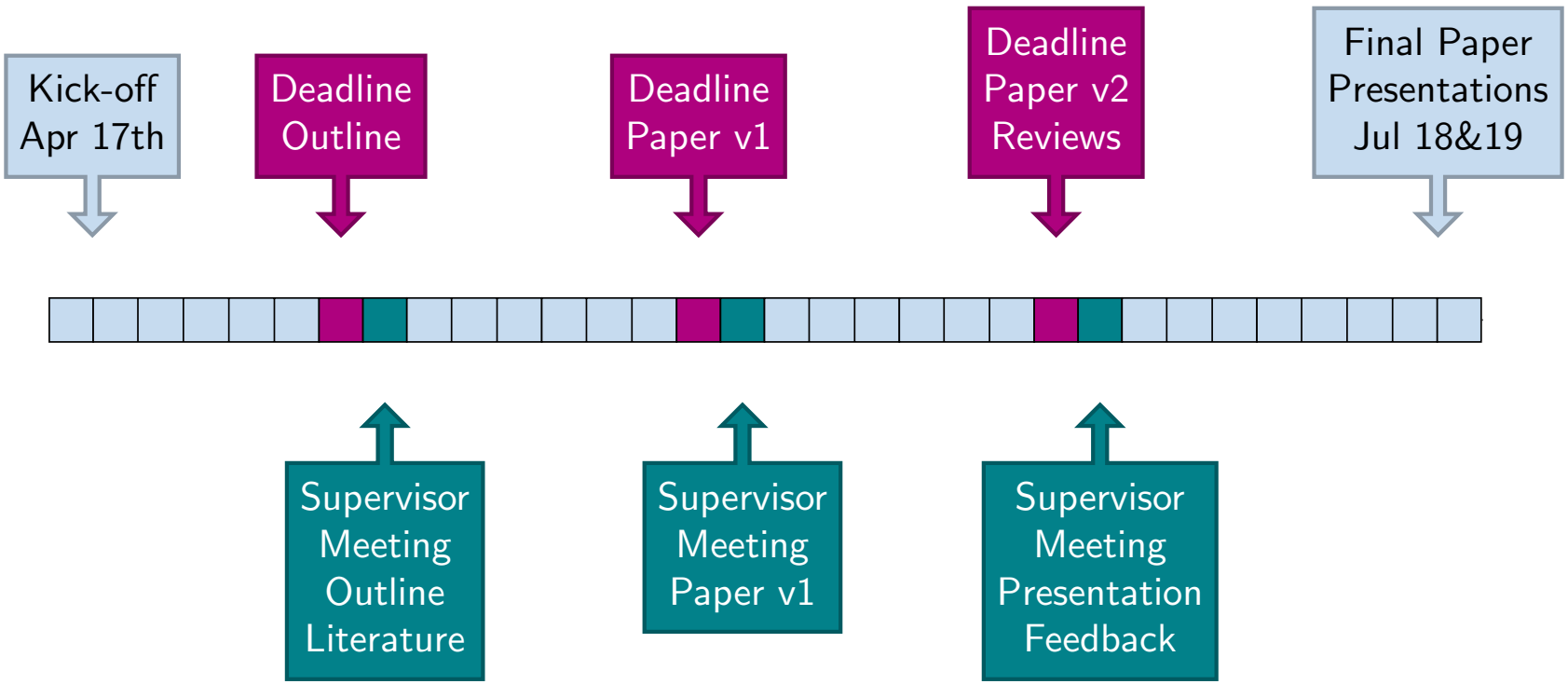
- ML & Graphs
  - Understanding Graph Neural Networks using Random Graph Models
  - Graph Neural PDEs
  - Semi-supervised Learning for Graph Classification
  - Active Learning on Node Level
- Robust ML & Graphs
  - Poisoning Attacks and Defenses for Graph Neural Networks
  - Robustness Certificates for Graph Neural Networks
  - Randomized Smoothing beyond Images (Graphs, etc.)
  - Distribution Shifts on Graphs

What will you do?

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 final talk + discussion round with your peers

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

Schedule


Kick-off
Apr 17th
Deadline
Outline
Deadline
Paper v1
Deadline
Paper v2
Reviews
Final Paper
Presentations
Jul 18&19
Supervisor
Meeting
Outline
Literature
Supervisor
Meeting
Paper v1
Supervisor
Meeting
Presentation
Feedback

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**

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)

Registration

Registration via the matching system!

`https://matching.in.tum.de/`

Selected Topics in Machine Learning Research (IN2107, IN4872)

+ Fill out the application form!

`https://forms.gle/ixqtcQxSpQ9An8mM6`

Deadline Feb 15th, 2023

Application

- Which course (lab/seminar) are you applying for?
- List of ML-related lectures you attended
- **Concise** overview of your resume (bullet list, not a complete CV)
- Brief motivation statement
- Any additional relevant experience (research, HiWi positions, etc.)