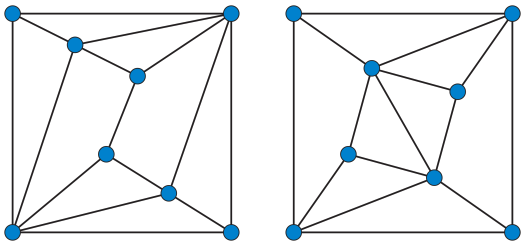
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

# Adversarial Perturbation of Graph Structure



Neural networks have been successful in handling various forms of data. Since some of the world's most interesting data is represented by graphs, Graph Neural Networks (GNNs) have achieved state-of-the-art performance in various fields such as quantum chemistry, physics, or social networks. However, it is still not clear what are the best graph manipulation operations that change the graph structure in the context of adversarial perturbations for machine learning. For images, adversarial perturbations such as cropping, masking, or rotation are used with great success for contrastive learning which reduces the need for labeled data, or adversarial learning which can improve model performance.

In this thesis, we will create new graph structure perturbation techniques based on spectral graph theory and use them for new adversarial attacks on GNNs as well as adversarial and contrastive learning.

**Requirements:** Strong motivation, knowledge in deep learning, or a solid background in machine learning. Experience with Python and TensorFlow or PyTorch is an advantage as well as knowledge in graph theory and graph neural networks. We will have weekly meetings to address questions, discuss progress and think about future ideas.

**Interested? Please contact us for more details!**

## Contact


- Karolis Martinkus: martinkus@ethz.ch, ETZ G60.1
- Zhao Meng: zhmeng@ethz.ch, ETZ G61.3