南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

计算机科学与工程系学术报告

Time: August 12th (Friday) 2022, 15:00-16:30

Venue: Conference room 551, South Tower, Faculty of Engineering

Host: Xiao Yan

Robust deep learning with applications to computer vision and novel protein engineering

Speaker

Xinshao Wang

Biography：Xinshao Wang is a senior researcher of Zenith Ai. He was a postdoctoral researcher at the Department of Engineering Science, University of Oxford after finishing his PhD at the Queens University of Belfast, UK. Xinshao Wang is working on core deep learning techniques with applications to visual recognition, disease prediction based on electronic health records, and protein engineering. Concretely, he has been working on the following topics: (1) Deep metric learning: to learn discriminative and robust rep- resentations for downstream tasks, e.g., object retrieval and clustering; (2) Robust deep learning: robust learning and inference under adverse conditions, e.g., noisy labels, missing labels (semisupervised learning), out-of-distribution training examples, sample imbalance, etc; (3) Computer vision: video/set-based person re-identification; image/video classification/retrieval/clustering; (4) AI healthcare: electrocardiogram classification; (5) ML-assisted gene and protein engineering.

Abstract: To train robust deep neural networks (DNNs), we systematically study several target modification approaches, which include output regularisation, self and non-self label correction (LC). Three key issues are discovered: (1) Self LC is the most appealing as it exploits its own knowledge and requires no extra models. However, how to automatically decide the trust degree of a learner as training goes is not well answered inthe literature. (2) Some methods penalise while the others reward low-entropy predictions, prompting us to ask which one is better. (3) Using the standard training setting, a trained network is of low confidence when severe noise exists, making it hard to leverage its high-entropy self knowledge.

To resolve the issue (1), taking two well-accepted propositions--deep neural networks learn meaningful patterns before fitting noise and minimum entropy regularisation principle--we propose a novel end-to-end method named ProSelfLC, which is designed according to learning time and entropy. Specifically, given a data point, we progressively increase trust in its predicted label distribution versus its annotated one if a model has been trained for enough time and the prediction is of low entropy (high confidence). For the issue (2), according to ProSelfLC, we empirically prove that it is better to redefine a meaningful low-entropy status and optimise the learner toward it. This serves as a defence of entropy minimisation. To address the issue (3), we decrease the entropy of self knowledge using a low temperature before exploiting it to correct labels, so that the revised labels redefine a low-entropy target state.

ALL ARE WELCOME!