ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing Group

Gloriastr. 35
ETH Zurich
CH-8092 Zurich

Prof. Dr. Roger Wattenhofer
phone +41 44 632 6312
fax +41 44 632 1035
wattenhofer@ethz.ch
www.disco.ethz.ch

Zurich, March 7, 2025

Letter of Recommendation for Yahya Jabary

To whom it may concern:

It is our pleasure to recommend Yahya Jabary for your position.

Yahya began his master's thesis in July of 2024 and finished at the beginning of January 2025.

His project focused on assessing the adversarial robustness of image classification models when applying geometric masks to the images. Specifically, Yahya took a range of state-of-the-art image classification models and applied the geometric masks to images to asses how the performance dropped under different styles and intensities of the geometric masks. Additionally, Yahya evaluated how ResNet models with self-ensembling methods handle the geometric masks. He did this by designing an evaluation pipeline to test the models effectively.

Yahya demonstrated excellent research and learning skills during his thesis, jumping into a new research area, catching up, and quickly bringing novel ideas. Yahya researched the field of adversarial machine learning and got a much deeper understanding of the field than expected of a master's student. He also managed to draw connections to existing work in computational geometry, which was not seen in the existing literature. Besides this, Yahya also went beyond the machine learning community and found existing work in areas such as statistics that study concepts similar to adversarial machine learning. However, these works usually are not linked to adversarial machine learning.

Yahya was a diligent and driven student. During his thesis, he demonstrated this by working focused and independently towards the objective and solving loosely defined problems without much assistance.

During our meetings, he has been focused on using them effectively to show new results and proactively raise any questions that have come up.

Sincerely,

Roger Wattenhofer
Supervising Professor

Andreas Plesner
Supervising PhD student