Hot Topics Workshop

APRIL 10-11, 2021

Safety and Security of Deep Learning

Organizing Committee:
Ben Adcock, Simon Fraser University
Simone Brugiapaglia, Concordia University
Anders Hansen, University of Cambridge
Clayton Webster, University of Texas

Science
Adversarial attacks on medical machine learning

nature
NEWS FEATURE
Why deep-learning AIs are so easy to fool

physicsworld
AI-reconstructed medical images can't be trusted
04 Jun 2020

Deep learning is profoundly reshaping the research directions of entire scientific communities across mathematics, computer science, and statistics, as well as the physical, biological and medical sciences. Yet, despite their indisputable success, deep neural networks are known to be universally unstable. That is, small changes in the input that are almost undetectable produce significant changes in the output. This happens in applications such as image recognition and classification, speech and audio recognition, automatic diagnosis in medicine, image reconstruction and medical imaging as well as inverse problems in general. This phenomenon is now very well documented and yields non-human-like behaviour of neural networks in the cases where they replace humans, and unexpected and unreliable behaviour where they replace standard algorithms in the sciences.

The many examples produced over the last years demonstrate the intricacy of this complex problem and the questions of safety and security of deep learning become crucial. Moreover, the ubiquitous phenomenon of instability combined with the lack of interpretability of deep neural networks makes the reproducibility of scientific results based on deep learning at stake.

For these reasons, the development of mathematical foundations aimed at improving the safety and security of deep learning is of key importance. The goal of this workshop is to bring together experts from mathematics, computer science, and statistics in order to accelerate the exploration of breakthroughs and of emerging mathematical ideas in this area.

This workshop is fully funded by a Simons Foundation Targeted Grant to Institutes.

Confirmed Speakers:

Genevera Allen, Rice University
Emmanuel Candes, Stanford University
Rachel Cummings, Georgia Institute of Technology
Ronald DeVore, Texas A&M University

Gitta Kutyniok, TU Berlin
Aleksander Madry, Massachusetts Institute of Technology
Cynthia Rudin, Duke University

ICERM

Participation

ICERM anticipates that all scientific programming through 2021 will be made available virtually for those unable to travel to the institute, whether due to the pandemic or any other reason.

Most ICERM workshops are aimed at scientists and students who are actively involved in the topic of the workshop. To request an invitation to participate, complete an online application available on our website. Decisions are typically made several weeks before the workshop; late registrants who are accepted and plan to participate virtually may not receive Zoom credentials until the first day of the program.

ICERM encourages women and members of underrepresented minorities to apply.

About ICERM

The Institute for Computational and Experimental Research in Mathematics (ICERM) is a National Science Foundation Mathematics Institute at Brown University in Providence, RI. Its mission is to broaden the relationship between mathematics and computation: specifically, expand the use of computational and experimental methods in mathematics, support theoretical advances related to computation, and address problems posed by the existence and use of the computer through mathematical tools, research and innovation.

ICERM
121 South Main Street
Box E, 11th Floor
Providence, RI 02903
401-863-5030
info@icerm.brown.edu

BROWN
SIMONS FOUNDATION