Emergent Research:
The PIMS Postdoctoral Fellow Seminar

September 27, 2023 | 9:30am

Pacific Institute *for the* Mathematical Sciences

Understanding adversarial robustness via optimal transport perspective

ABSTRACT:
In this talk, I will present the recent progress of understanding adversarial multiclass classification problems, motivated by the empirical observation of the sensitivity of neural networks by small adversarial attacks. From the perspective of optimal transport theory, I will give equivalent reformulations of this problem in terms of 'generalized barycenter problems' and a family of multimarginal optimal transport problems. These new theoretical results reveal a rich geometric structure of adversarial learning problems in multiclass classification and extend recent results restricted to the binary classification setting. Furthermore, based on this optimal transport approach I will give the result of the existence of optimal robust classifiers which not only extends the binary setting to the general one but also provides shorter proof and an interpretation between adversarial training problems and related generalized barycenter problems.

For more information and registration:
https://www.pims.math.ca/seminars/PIMSPDF
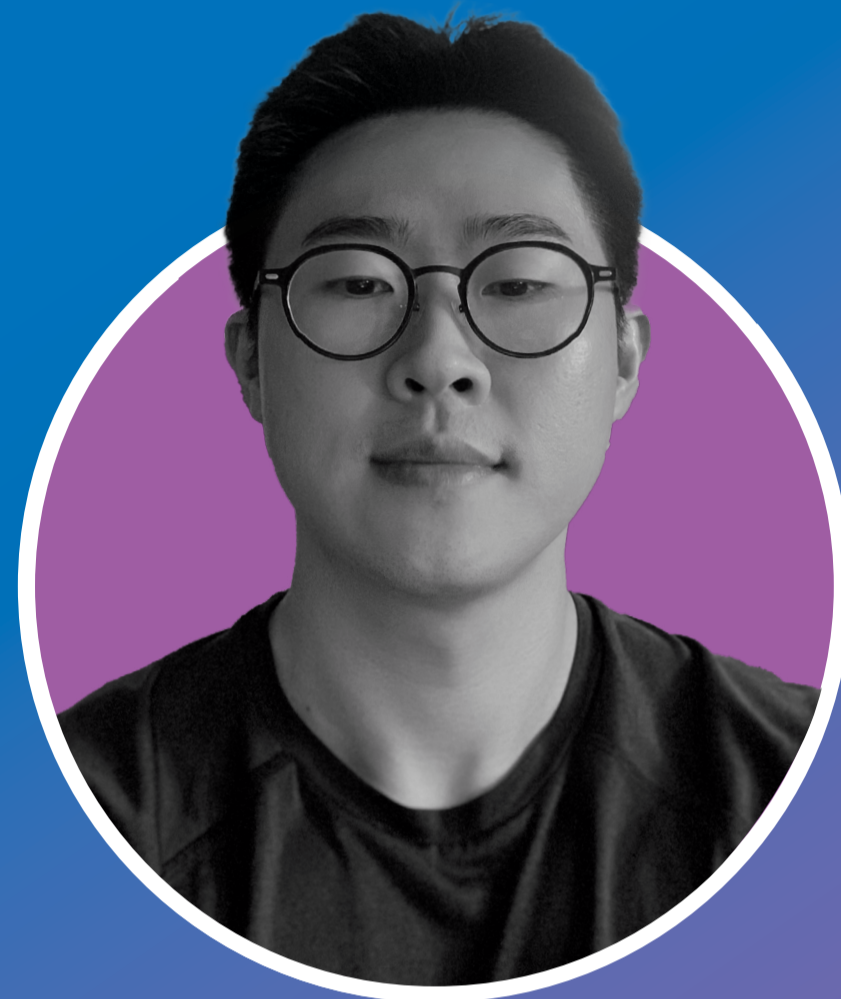
Jakwang Kim
PIMS PDF, UBC

SPEAKER BIO:
Jakwang Kim is a PIMS Postdoctoral fellow at the University of British Columbia, under the sponsorship of the PIMS Research Network - Kanotrovich Initiative. His area of research is in Optimal Transport, as well as high-dimensional inference problems like stochastic block models, planted clique problems, and graph matching problems. In particular, statistical-information phase transition will play an important role to understand not only these toy models of random optimization but also real-world problems, e.g. success of deep learning, LLM etc.

ABOUT PIMS PDF SEMINARS:
PIMS ongoing lecture series featuring our Postdoctoral Fellows every three weeks. You will have the opportunity to connect with emerging research in the mathematical sciences from a PIMS Postdoctoral Fellow. PIMS PDFs are amongst the top young researchers in Canada, and this is an excellent opportunity to learn about them, and their work.