ADVERSARIAL ROBUSTNESS FOR MACHINE LEARNING

ADVERSARIAL ROBUSTNESS FOR MACHINE LEARNING

PIN-YU CHEN
IBM Research
Yorktown Heights, NY, United States

CHO-JUI HSIEH
University of California, Los Angeles
Los Angeles, CA, United States

ACADEMIC PRESS
An imprint of Elsevier