Sungyoon Lee

CONTACT Information Building 8 Room 8201

MATION Center for AI and Natural Sciences

Korea Institute for Advanced Study (KIAS)

Hoegiro 85, Dongdaemun-gu, Seoul 02455, Republic of Korea

 $\mathrm{TEL}: +82\ 2\ 958\ 2656$

Homepage / e-mail / GitHub / Google Scholar

RESEARCH EXPERIENCE Korea Institute for Advanced Study (KIAS), Seoul, Republic of Korea

AI Research Fellow in the Center for AI and Natural Sciences Sep. 2021 -

EDUCATION

Seoul National University, Seoul, Republic of Korea

Ph.D. in Mathematical Sciences Aug. 2021

Advisor: Jaewook Lee / Co-advisor: Seungyeal Ha

Thesis title: Robustness of Deep Neural Networks to Adversarial Attack: from

Feb. 2016

Heuristic Methods to Certified Methods

B.S. in Material Science and Engineering Feb. 2016

Major GPA: 3.98/4.3

B.S. in Mathematical Sciences (Double Major)

Major GPA: 4.10/4.3

RESEARCH INTERESTS Deep Learning / Robust, Reliable and Interpretable Machine Learning / Adversarial

Robustness / Certified Defense / Optimization and Generalization

Publications & Workshops

C: Conference, W: Workshop, J: Journal, *: Equal contribution

[C3] Towards Better Understanding of Training Certifiably Robust Models to Adversarial Examples

SL, Woojin Lee, Jinseong Park, Jaewook Lee

Advances in Neural Information Processing Systems (NeurIPS), 34, 2021.

To appear

[C2] Lipschitz-Certifiable Training with a Tight Outer Bound

SL, Jaewook Lee, Saerom Park

Advances in Neural Information Processing Systems (NeurIPS), 33, 2020.

[C1,W1] Defensive Denoising Methods against Adversarial Attack

SL, Saerom Park, Jaewook Lee

Preliminary version appeared at Knowledge Discovery and Data Mining (KDD) Deep

Learning Day, London, 2018

Korea Computer Congress (KCC), Jeju, 2018

Preprint& Under Review

[5] Implicit Jacobian Regularization Weighted with Impurity of Probability Output

SL, Jinseong Park, Jaewook Lee

Under review

[4] Bridged Adversarial Training: Towards a Smooth Classifier with a Large Margin

{Hoki Kim*, Woojin Lee*, **SL***}, Jaewook Lee

Under review, [arxiv]

[3] GradDiv: Adversarial Robustness of Randomized Neural Networks via

Gradient Diversity Regularization

SL, Hoki Kim, Jaewook Lee

Under review, [arxiv]

[2] Sliced Wasserstein Adversarial Training for Improving Adversarial Robustness

Woojin Lee, SL, Hoki Kim, Jaewook Lee

Under review

[1] Variational Cycle-consistent Imputation Adversarial Networks for General Missing Patterns

Woojin Lee, $\mathbf{SL},$ Junyoung Byun, Hoki Kim, Jaewook Lee

Under review

PATENTS

[1] Learning Method, Apparatus, Computer Readable Recording Medium for Imputating Missing Data and Electronic Device using the Method. Patent applied (1020200146311, Nov. 04, 2020)

Talks &

Presentations

AI center seminar, KIAS

Lipschitz-Certifiable Training with a Tight Outer Bound Sep. 15, 2021

CSE Special Seminar & Program, Sungshin Women's University

AI and Security Jul. 21, 2021

NeurIPS 2020 Social ML in Korea

Lipschitz-Certifiable Training with a Tight Outer Bound Dec. 10, 2020

Special Lecture, Dongguk University

Machine Learning with Python Feb. 2018

Programs

ATTENDED

Geometry and Learning from Data Tutorials, part of the long program Geometry and Learning from Data in 3D and Beyond, Institute for Pure and Applied Mathematics (IPAM) UCLA

Mar. 12-15, 2019

TEACHING EXPERIENCE

Teaching Assistant:

Seoul National University

Calculus for Life Science	Spring 21
Calculus for Life Science	Fall 20
Mathematics: The Basics and Applications	Spring 20
Mathematics in Civilization	Fall 19
Linear Algebra	Spring 19
Differential and Integral Calculus	Spring 19
Introduction to Numerical Analysis	Fall 18
Mathematics in Civilization	Fall 18
Mathematics in Civilization	Spring 18
Calculus	Spring 18
Introduction to Mathematical Analysis	Fall 17
Honor Calculus and Practice	Fall 17
Honor Calculus and Practice	Spring 17
Calculus	Fall 16

Academic Tutor:

SNU-HKUST Summer Research Program in Industrial and Applied Mathematics (SPIA) 2019

Jun.-Aug. 2019

Projects	Manufacturing Technology Center, Samsung Electronics	2018
Honors & Awards	BK21 Plus Research Scholarship, Seoul National University	2020
	Lecture & Research Scholarship, Seoul National University	2019-2020
	Scholarship for Next Generation of Researchers in Basic I tional University	Fields , Seoul Na- 2017-2019
	Outstanding TA Awards, Seoul National University	2018
	Outstanding TA Awards, Seoul National University	2017
	BK21 Plus Research Scholarship, Seoul National University	2016
	Merit Scholarship (Full-ride), Seoul National University	2013
OTHERS	Compulsory Military Service, Korean Augmentation To (KATUSA)	the U.S. Army 5. 2013 - Jul. 2015