Alexandre Araujo

☎ +33 6 74752275 • ✉ aaraujo001@gmail.com

Summary

Accomplished machine learning researcher with over 6 years of experience designing, training, and evaluating large-scale neural networks. My research primarily focused on designing neural network architectures that are stable, scalable and robust. Below are relevant tasks from my research projects and experience:

- *Published 11 research papers at top machine learning conferences: NeurIPS, ICML, ICLR*
- *Supervised and mentored 3 graduate students and 3 undergraduate interns*
- *Trained large-scale networks (> 1B parameters) on a Slurm cluster on hundreds of GPUs*
- *Designed large-scale dataset of 150M images for distillation of DINOv2 architecture*
- *Designed a new stable neural network that allows scaling depth to 1000 layers without batch normalization*
- *Deployed tree-based machine learning model in production for a mortgage broker company*

Education

PhD, Computer Science, PSL Research University, Paris, France 2017 – 2021
MS, Business Administration, SKEMA Business School, Lille, France 2013 – 2016
BS, Mathematics, University of Versailles, Versailles, France 2008 – 2011

Research & Industry Experience

Postdoctoral Researcher on Trustworthy Machine Learning Jan. 2023 – Feb. 2024
New York University, New York, NY, US

- Advisors: Siddharth Garg, Farshad Khorrami
- Established theoretical connections between mathematical concept and areas of Trustworthy ML. Trained large-scale neural networks using PyTorch in a distributed fashion on a Slurm cluster.

Postdoctoral Researcher on Computer Vision Oct. 2021 – Dec. 2022
INRIA / École Normale Supérieure, Paris, France

- Advisors: Jean Ponce, Julien Mairal
- Research on Focus Stacking from Handheld Raw Image Bursts. Designed a large-scale computer vision dataset to improve recent advancements on Focus Stacking with supervised learning.

Ph.D. Candidate Sep. 2017 – June 2021
PSL Research University, Paris, France

- Thesis: Building Compact and Robust Deep Neural Networks with Toeplitz Matrices
- Advisors: Jamal Atif, Yann Chevaleyre and Benjamin Negrevergne
- PhD in Deep Learning with a focus on compact and robust neural network with structured matrices.

Data Scientist Sep. 2015 – Aug. 2017
Wavestone, Paris, France

- Collected 5 years of historical data for a mortgage broker and applied machine learning algorithms to predict mortgage application acceptance. Deployed the model into production.
- Gathered 3 years of historic data for an energy company with Hadoop to construct a 1 billion rows dataset. Applied machine learning algorithms to predict churn.
- Gathered 20 years of historic data for a European Railway Company and applied machine learning algorithms to predict train breakdown.

Data Engineer Intern dec. 2014 – may 2015
Amazon, Luxembourg

- Automated data pipelines to feed real-time dashboards that display transportation and financial statistics.

Publications

Conference Papers

Fine-grained Local Sensitivity Analysis of Standard Dot-Product Self-Attention
A. Havens, A. Araujo, H. Zhang, B. Hu – ICML (2024)

LipSim: A Provably Robust Perceptual Similarity Metric
S. Ghazanfari, A. Araujo, P. Krishnamurthy, F. Khorrami, S. Garg – ICLR (2024)

The Lipschitz-Variance-Margin Tradeoff for Enhanced Randomized Smoothing
B. Delattre, A. Araujo, Q. Barthélemy, A. Allauzen – ICLR (2024)

Novel Quadratic Constraints for Extending LipSDP beyond Slope-Restricted Activations
P. Pauli, A. Havens, A. Araujo, S. Garg, F. Khorrami, F. Allgöwer, B. Hu – ICLR (2024)

On the Scalability and Memory Efficiency of Semidefinite Programs for Lipschitz Constant Estimation of Neural Networks
Z. Wang, A. Havens, A. Araujo, Y. Zheng, B. Hu, Y. Chen, S. Jha – ICLR (2024)

Exploiting Connections between Lipschitz Structures for Certifiably Robust DEQ models
A. Havens*, *A. Araujo**, *S. Garg, F. Khorrami, B. Hu* – NeurIPS (2023)

Diffusion-Based Adversarial Sample Generation for Improved Stealthiness and Controllability
H. Xue, A. Araujo, B. Hu, Y. Chen – NeurIPS (2023)

Certification of Deep Learning Models for Medical Image Segmentation
O. Laousy. A. Araujo, G. Chassagnon, M. Revel, M. Vakalopoulou – MICCAI (2023)

Towards Better Certified Segmentation via Diffusion Models
O. Laousy. A. Araujo, G. Chassagnon, M. Revel, S. Garg, F. Khorrami, M. Vakalopoulou – UAI (2023)

Efficient Bound of Lipschitz Constant for Convolutional Layers by Gram Iteration
B. Delattre, Q. Barthélemy, A. Araujo, A. Allauzen – ICML (2023)

A Unified Algebraic Perspective on Lipschitz Neural Networks
A. Araujo*, *A. Havens**, *B. Delattre, A. Allauzen, B. Hu* – ICLR – Spotlight (2023)

A Dynamical System Perspective for Lipschitz Neural Networks
L. Meunier*, *B. Delattre**, *A. Araujo**, *A. Allauzen* – ICML – Oral (2022)

On Lipschitz Regularization of Convolutional Layers using Toeplitz Matrix Theory
A. Araujo, B. Negrevergne, Y. Chevaleyre, J. Atif – AAAI (2020)

Understanding and Training Deep Diagonal Circulant Neural Networks
A. Araujo, B. Negrevergne, Y. Chevaleyre, J. Atif – ECAI 2020 (2020)

Theoretical Evidence for Adversarial Robustness through Randomization
R. Pinot, L. Meunier, A. Araujo, H. Kashima, F. Yger, C. Gouy-Pailler, J. Atif – NeurIPS (2019)

Workshop Papers

R-LPIPS: An Adversarially Robust Perceptual Similarity Metric
S. Ghazanfari, S. Garg, P. Krishnamurthy, F. Khorrami, A. Araujo – ICML – Workshop (2023)

Advocating for Multiple Defense Strategies against Adversarial Examples
A. Araujo, L. Meunier, R. Pinot, and B. Negrevergne – ECML – Workshop (2020)

Compact Deep Learning Models for Video Classification using Circulant Matrices
A. Araujo, B. Negrevergne, Y. Chevaleyre, J. Atif – ECCV – Workshops (2018)

Preprints

PAL: Proxy-Guided Black-Box Attack on Large Language Models
C. Sitawarin, N. Mu, D. Wagner, A. Araujo – Preprint (2024)

Towards Real-World Focus Stacking with Deep Learning
A. Araujo, J. Ponce, J. Mairal – Preprint (2023)

Activities and Services

Teaching

New York University, New York, NY, US

Graduate Course: Adversarial Machine Learning	2023

PSL Research University, Paris, France

Executive Master: Adversarial Machine Learning	2020, 2021
Master IASD: Data Mining & Machine Learning	2019
Master ID: Data Mining & Machine Learning	2019

École Polytechnique, Paris, France

Data Science & Machine Learning	2016, 2017, 2018, 2019, 2020

Reviewer

Artificial Intelligence and Statistics (AISTATS)	2022, 2023
Association for the Advancement of Artificial Intelligence (AAAI)	2022, 2023
Computer Vision and Pattern Recognition Conference (CVPR)	2023
European Conference on Computer Vision (ECCV)	2024
International Conference on Computer Vision (ICCV)	2023
International Conference on Learning Representations (ICLR)	2023
International Conference on Machine Learning (ICML)	2023, 2024
Neural Information Processing Systems (NeurIPS)	2023, 2024

Invited Talks

University of Illinois Urbana-Champaign	October 2023
NYU – Center for Data Science	April 2022
INRIA / École Normale Supérieure de Paris	July 2021
École Normale Supérieure de Lyon	July 2021
INSIS – French National Center for Scientific Research	January 2021
PFIA – French AI conference	June 2019, 2020, 2021
International Cybersecurity Forum	January 2020
Limits of AI – BPI Conference	June 2019

Technical Skills

Programming Languages : Python, C++, SQL
HPC Job Schedulers : Slurm, IBM Spectrum LSF
Deep Learning Frameworks : TensorFlow, PyTorch
ML Libraries: XGBoost, LightGBM, Scikit-Learn
Data Science Framework : OpenCV, SciPy, NumPy, Pandas