Vedant Bhasin

408-707-4441 — vedantbhasin@cmu.edu — vbhasin999 — vedant-bhasin — vbhasin999.github.io

EDUCATION

Carnegie Mellon University December 2024
Master of Science in Electrical & Computer Engineering *Pittsburgh, PA*
AI/ML Systems Concentration [CGPA: 3.81/4.00]
Coursework: LLM Systems, Distributed Systems, Multimodal Machine Learning, Advanced Natural Language Processing, Parallel Computer Architecture and Programming (Fall '24), On-Device Machine Learning (Fall '24)

Carnegie Mellon University May 2023
Bachelor of Science in Electrical & Computer Engineering *Pittsburgh, PA*
Software Systems Concentration [CGPA: 3.39/4.00]
Coursework: Deep Reinforcement Learning & Control, Introduction to Deep Learning, Introduction to Machine Learning

EXPERIENCE

Peraton Labs, Autonomous Systems Research June 2024 - present
Cyber Research Intern *Basking Ridge, NJ*

- Researching the detection of trojan backdoors in large language models under the TrojAI program, supported by the Intelligence Advanced Research Projects Activity (IARPA). Competing with research teams from companies such as ARM, SRI, and ICSI.
- Developed a novel black-box trojan detection algorithm that relies solely on model logits, improving ROC-AUC from 0.708 to 1.0 and reducing runtime by approximately 60%, achieving a top position on the leaderboard.
- Implemented and modified state-of-the-art discrete optimization-based jailbreaking techniques, including GBDA, GCG, and PEZ

Carnegie Mellon University, Language Technologies Institute January 2023 - May 2023
Teaching Assistant - Deep Learning *Pittsburgh, PA*

- Teaching Assistant for Carnegie Mellon University's flagship deep learning course with Professor Bhiksha Raj.
- Lead TA for two of the four major projects in the course; responsible for preparing data sets, developing starter notebooks, and conducting experiments to discover high-performing architectures and optimization specifications.
- Leading recitations and lectures on vision transformers, deep reinforcement learning, and project workflow fundamentals.

PROJECTS

MiniTorch January 2024
CUDA, C++, Python, Deep Learning Systems, Shared Memory Management, Kernel Fusion

- Developed a deep-learning framework with reverse mode auto differentiation, a custom CUDA backend, and accelerated transformer operations. Optimized performance using coalesced memory access, shared memory tiling, and kernel fusion.
- Achieved a 10% speedup on GPT-2 by optimizing softmax and layernorm operations with reduced synchronization.

Fine Grained Image Grounding for Visual Abductive Reasoning December 2023
PyTorch, Computer Vision, Multimodal Machine Learning, Contrastive Learning

- Collaborated with a team of two other researchers to address the task of Visual Abductive Reasoning (VAR) in vision-language models. VAR refers to the task of making the most plausible inference about an image region with incomplete information.
- Pioneered a method that incorporates scene graph information of the image with no modification to the model architecture.
- Led the development of a fine-tuning pipeline using PyTorch, enabling the enhancement of BLIP2 models with an InfoNCE contrastive loss for improved performance, Improving P@1 scores by 15.6% and 3.9% over scene graph and image-only models.

Attention-based Automatic Speech Recognition January 2023
PyTorch, Speech Recognition, Multi Head Self Attention, Autoregressive Generation

- Devised an end-to-end speech-to-text model based on Listen-Attend-Spell architecture to transcribe speech, using MFCC coefficients from the LibriSpeech dataset.
- Implemented scaled dot product attention from scratch. Incorporated data augmentation techniques such as time and frequency masking in addition to regularization techniques such as weight tying, locked dropout, and weight decay.
- Designed a custom teacher-forcing schedule to boost the performance of the auto-regressive decoder module.
- Achieved a promising Levenshtein distance of 9.54 on the test set.

Face Classification and Verification with CNNs December 2022
PyTorch, Computer Vision, Model Architecture, Regularization, Contrastive Learning

- Performed ablation studies with MobileNetV2, ResNet-50, and ConvNeXt for facial recognition on the VGG Face 2 dataset.
- Experimented with different deep metric learning approaches such as ArcFace loss, triplet margin loss, and circle loss to maximize verification accuracy. Independently implemented ArcFace loss using the research paper as a reference.
- Implemented data augmentation techniques, including Random Augment, Random Perspective, and Random Erasing to mitigate overfitting. Applied regularization methods, including label smoothing, stochastic depth, and weight decay.
- The model correctly classified a satisfactory 92.83% of faces during testing.

SKILLS

Programming Languages: Python, C/C++, CUDA, Java, JavaScript, HTML/CSS, SQL
Libraries and Frameworks: PyTorch, Tensorflow, Hugging Face, Scikit-Learn, Pandas, Seaborn, Django, Docker, AWS, GCP