Junbo Zhao

☎ (86) 18343087267 | ✉ zhaojunbo2012@sina.cn

Personal Website: https://a-lincui.github.io

EDUCATION

Tsinghua University, Beijing, China 09/2021-06/2024
Master's degree in Electronic and Information Engineering
Thesis Title: Automatic Design Method of Efficient Neural Network Based on Performance Prediction and Weight sharing

Tsinghua University, Beijing, China 09/2017-06/2021
Bachelor's degree in Engineering Physics

PUBLICATION

- **Junbo Zhao***, Xuefei Ning*, Enshu Liu, Binxin Ru, Zixuan Zhou, Tianchen Zhao, Chen Chen, Jiajin Zhang, Qingmin Liao, Yu Wang, "**Dynamic Ensemble of Low-fidelity Experts: Mitigating NAS 'Cold-Start'**," AAAI 2023, Vol. 37 No. 9: AAAI-23 Technical Tracks, pp. 11316-11326. (Oral)
- Ning X*, Zhou Z*, **Zhao J**, et al. **TA-GATES: An Encoding Scheme for Neural Network Architectures**[J]. Advances in Neural Information Processing Systems, 2022, 35: 32325-32339. (Spotlight)
- Ning X*, **Zhao J***, Li W, et al. **Discovering Robust Convolutional Architecture at Targeted Capacity: A Multi-Shot Approach**[J]. 2020.DOI:10.48550/arXiv.2012.11835.
- Gao Z, Liu S, **Zhao J**, et al. **Ensemble-based Reliability Enhancement for Edge-Deployed CNNs in Few-shot Scenarios**, in IEEE Transactions on Machine Learning in Communications and Networking, doi: 10.1109/TMLCN.2024.3435168.
- Yu Wang, Xuefei Ning, **Junbo Zhao**, **Method, Device, Equipment, Storage Medium, and Program Product for Generating Text Adversarial Examples**. (Chinese Patent, Student First Inventor, Application Publication Number: CN118839786A)

RESEARCH EXPERIENCES

Dynamic Ensemble of Low-fidelity Experts: Mitigating NAS "Cold-Start" 04/2022-08/2022
Researcher Advisor: Yu Wang, Xuefei Ning

- **Literature Review**: Reviewed existing research on predictor-based neural architecture search, highlighting the challenge of limited architecture-performance data.
- **Cold-Start Solution**: Proposed using low-fidelity information (e.g., one-shot estimation, zero-shot estimation) to mitigate the "cold-start" problem in predictor-based NAS. Developed a dynamic ensemble prediction framework to fuse beneficial information from different low-fidelity data types.
- **Paper Writing**: Authored a comprehensive research paper detailing the proposed methods and results.

TA-GATES: An Encoding Scheme for Neural Network Architectures 11/2021-01/2022
Researcher Advisor: Yu Wang, Xuefei Ning

- **Strategy Exploration**: Investigated existing strategies for encoding neural network architectures, with a focus on graph-based schemes like GATES.
- **Encoding Scheme Development**: Created TA-GATES, a novel graph-based architecture encoding scheme designed to simulate the training process of neural networks, improving the ranking of candidate

architectures using limited data.

- **Validation**: Validated the efficacy of the proposed scheme in enhancing predictor performance and contributed to writing the research report.

Discovering Robust Convolutional Architecture at Targeted Capacity: A Multi-Shot Approach

09/2020-03/2021

Researcher Advisor: Yu Wang, Xuefei Ning

- **Robustness and Capacity Analysis**: Investigated the relationship between adversarial robustness in neural networks and model capacity.
- **NAS Methodology Improvement**: Identified limitations of the one-shot NAS method in discovering robust architectures and proposed training multiple super-networks with varying capacities to mitigate these issues.
- **Feasibility Validation**: Conducted experiments to validate the proposed strategy, exploring its main application scenarios.

Method, Device, Equipment, Storage Medium and Program Product for Generating Text Adversarial Examples

10/2023-12/2023

Researcher Advisor: Yu Wang, Xuefei Ning

- **Adversarial Text Generation**: Developed a black-box adversarial text example generation scheme leveraging a fine-tuned large language model, improving generation capability and control.
- **Prompt Paradigm Design**: Designed a comprehensive prompt paradigm encompassing attack background, purpose, control, and input. Created a dataset of "prompt-effective adversarial examples" and fine-tuned a pre-trained large language model to enhance adversarial text generation.
- **Experimental Validation**: Conducted experiments on the SST-2 binary text sentiment classification dataset using the ChatGLM-6B model, demonstrating the effectiveness of the proposed method.

Verification Study of Low-Bit Neural Networks in Compute-in-Memory Inference Chips

09/2022-10/2023

Researcher Advisor: Yu Wang, Xuefei Ning

- **Fault-Tolerant Model Design**: Led research in designing efficient fault-tolerant neural network models for tasks such as super-resolution and object detection, incorporating joint quantization.
- **Predictor Development**: Developed an architecture performance predictor for fault-tolerant neural architecture search and introduced a dynamic inference method to enhance fault tolerance.

AI Quantization Compression and AI Software-Hardware Architecture Design 09/2022-02/2023

Researcher Advisor: Yu Wang, Xuefei Ning

- **NAS for Super-Resolution**: Developed software for neural architecture search (NAS) tailored for super-resolution tasks, designing and validating the search space for UNET models.
- **Search Strategy Exploration**: Explored various search strategies, including differentiable search, reinforcement learning, and evolutionary algorithms, and wrote comprehensive feasibility reports.

PROFESSIONAL EXPERIENCES

Infinigence Technology Co., Ltd. 08/2023-12/2023

Algorithm Researcher

- **Model Efficiency Evaluation**: Evaluated the efficiency of large language models (e.g., GLM-6B, OPT-6.7B) on domestically produced chips (e.g., Tianyue, Haifeike) in China, providing crucial data for lightweight large language model design.

- **Chip Testing Solution**: Contributed to the design and development of a unified chip testing solution.

Novauto Technology Co., Ltd. 03/2023-07/2023

Algorithm Researcher

- **Hardware-Aware NAS Toolchain Development**: Developed a hardware-aware toolchain for neural network architecture optimization, enhancing computational efficiency and performance.
- **Toolchain Validation**: Validated the toolchain's effectiveness through practical applications in visual tasks (e.g., image denoising, object detection), analyzing its advantages and limitations for further improvement.

EXTRACURRICULAR ACTIVITIES

- 2023 AAAI Conference on Artificial Intelligence.
- The International Conference on Automated Machine Learning 2023.

LANGUAGE& SKILLS

- IELTS: Overall: 7.5 (Reading: 9.0, Listening: 8.0, Speaking: 5.5, Writing: 6.5)
- Software: Microsoft Office, Git, Vim, Linux, Python, C/C++

赵俊博（Junbo Zhao)

☎ (86) 18343087267 | ✉ zhaojunbo2012@sina.cn

个人主页: https://a-lincui.github.io

教育背景

清华大学 09/2021-06/2024
电子信息 硕士
论文题目: 基于性能预测和权重共享的高效神经网络自动设计方法

清华大学 09/2017-06/2021
工程物理 学士

发表论文或专利

- **Junbo Zhao***, Xuefei Ning*, Enshu Liu, Binxin Ru, Zixuan Zhou, Tianchen Zhao, Chen, Jiajin Zhang, Qingmin Liao, Yu Wang, "**Dynamic Ensemble of Low-fidelity Experts: Mitigating NAS 'Cold-Start'**," AAAI 2023, Vol. 37 No. 9: AAAI-23 Technical Tracks, pp. 11316-11326. (Oral)
- Ning X*, Zhou Z*, **Zhao J**, et al. **TA-GATES: An Encoding Scheme for Neural Network Architectures**[J]. Advances in Neural Information Processing Systems, 2022, 35: 32325-32339. (Spotlight)
- Ning X*, **Zhao J***, Li W, et al. **Discovering Robust Convolutional Architecture at Targeted Capacity: A Multi-Shot Approach**[J]. 2020.DOI:10.48550/arXiv.2012.11835.
- Gao Z, Liu S, **Zhao J**, et al. **Ensemble-based Reliability Enhancement for Edge-Deployed CNNs in Few-shot Scenarios**, in IEEE Transactions on Machine Learning in Communications and Networking, doi: 10.1109/TMLCN.2024.3435168.
- 汪玉, 宁雪妃, **赵俊博**, **文本对抗样本生成方法、装置、设备、存储介质及程序产品**（学生第一发明人，申请公布号：CN118839786A)

研究经历

Dynamic Ensemble of Low-fidelity Experts: Mitigating NAS "Cold-Start" 04/2022-08/2022

研究者（校内研究） 指导人: 汪玉, 宁雪妃

- **文献调研**: 调研既有基于预测器的神经架构搜索文献，明确指出架构性能数据量的不足是这类方法的首要挑战。
- **冷启动解决方案**: 提出使用低保真度信息（例如，单次评估指标，零次评估指标)以缓解基于预测器的神经架构搜索的“冷启动”问题。设计了动态集成的预测器框架以融合来自不同低保真度信息的有效知识。
- **论文撰写**: 撰写全文，详细描述了所提方法、实验设计与实验结果等内容。

TA-GATES: An Encoding Scheme for Neural Network Architectures 11/2021-01/2022

研究者（校内研究） 指导人：汪玉，宁雪妃

- **策略探索**: 详细调研神经网络架构的编码策略，特别关注 GATES 等图编码方案。
- **编码方案研发**: 与合作者共同提出一种新颖的基于图的编码方案 TA-GATES。该方案通过模拟神经网络的前向传播推理与反向传播训练过程，提高了有限训练数据量下的架构性能预测器的排序能力。
- **有效性验证**: 在 NAS-Bench-201 等搜索空间中验证所提方法的有效性；开发 anytime 预测器并进行实验；参与了文章的撰写。

Discovering Robust Convolutional Architecture at Targeted Capacity: A Multi-Shot Approach

09/2020-03/2021

研究者（校内研究） 指导人：汪玉，宁雪妃

- **模型鲁棒性与容量的关系分析**：探索神经网络的对抗鲁棒性与模型容量间的关联性。
- **神经架构搜索方法改进**：指出单次评估（one-shot）方法在该任务中的局限性，并提出使用容量不同的多个超网络来评估模型在指定容量下的性能。
- **可行性验证**：基于图像分类任务对所提方法的有效性进行验证。

文本对抗样本生成方法、装置、设备、存储介质及程序产品 10/2023-12/2023

学生第一发明人（在审专利） 指导人：汪玉，宁雪妃

- **对抗文本生成**：开发了一种利用微调大语言模型的黑盒对抗样本生成方案，提升了生成的能力与可控性。
- **提示范式设计**：设计了一种包含攻击背景、目的、控制和输入的提示词范式。基于该范式，创建了“有效提示词-对抗样本”数据集，并利用该数据集对预训练的大语言模型进行了微调，从而提升其生成对抗文本的能力。
- **实验验证**：在 SST-2 二元文本分类数据集以及 ChatGLM-6B 模型上进行了技术验证。

低比特神经网络在存内计算芯片上的验证研究 09/2022-10/2023

研究者（校企合作项目，华为-清华） 指导人：汪玉，宁雪妃

- **容错模型设计**：面向超分辨率与目标检测等任务，联合量化方法，研究设计高效的容错网络模型。
- **架构容错性能预测器开发**：开发了一种用于容错架构搜索的架构性能预测器。此外，设计了一种增强模型容错能力的动态推理方法。

AI 量化压缩与 AI 软硬件架构设计 09/2022-02/2023

研究者（校企合作项目，哲库-清华） 指导人：汪玉，宁雪妃

- **面向超分辨率的神经架构搜索**：开发了用于超分辨率任务的神经架构搜索软件，设计并在基于 UNET 构建的搜索空间上进行了验证。
- **搜索策略设计:** 探索了可微分搜索、基于强化学习的搜索以及进化搜索等多种策略，撰写详尽的报告与使用文档。

实习经历

无问芯穹科技有限公司 08/2023-12/2023

算法研究员

- **国产芯片大模型推理高效性测试:** 参与评测国产芯片（天数、海飞科等）的大模型推理性能，为公司进行的轻量化大模型设计提供关键数据。
- **芯片测试解决方案**: 参与设计与开发国产芯片大模型推理效率的统一测试方案。

北京超星未来科技有限公司 03/2023-07/2023

算法研究员

- **考虑硬件的神经架构搜索工具开发:** 开发考虑硬件的神经网络架构优化工具，从而提升公司模型的计算效率及任务性能。
- **工具链验证:** 基于去噪、目标检测等视觉任务验证上述工具链，分析其优势与局限性。

课外活动

- 2023 AAAI Conference on Artificial Intelligence.
- The International Conference on Automated Machine Learning 2023.

其他技能

- 英语（雅思）：总分 7.5 (阅读: 9.0，听力: 8.0，口语: 5.5，写作: 6.5)
- 开发相关: Microsoft Office, Git, Vim, Linux, Python, C/C++