Xutao Henry Mao

xutao.mao@vanderbilt.edu | +1 857-869-6559

EDUCATION

Vanderbilt University **Aug 2022 – Dec 2025**

- *Grade: 3.867/4.0*
- Key courses: AI, Foundation of Machine Learning, Data Mining and AI, Privacy & Security (PHD-Level)
- Dean's List for all semesters (Fall 2022-Spring 2025); Vanderbilt University Summer Research Scholarship (2025, $6000)

RESEARCH EXPERIENCE

Research on Fake Voice Generation and Fake Voice Detection **Sept 2023-May 2025**

Leader & First Author, Supervised by Dr. Dan (Linda) Lin, Vanderbilt University

- Investigated the evolving threat landscape targeting voice-based systems, identifying potential misuse scenarios of fake voice generation about advanced TTS and voice conversion technologies.
- Benchmarked the resilience of 20+ fake voice generators and 8 fake voice detectors to investigate the interaction and threats between fake voice generation and detection.

Research on Personalization Imputation on Textual Edge Graph **Oct 2024 – July 2025**

Key Contributor & Co-first Author, Supervised by Dr. Tyler Derr, Vanderbilt University

- Designed and implemented a graph-aware LLM aggregator that captures higher-order context through line-graph views, enabling the generation of coherent, personalized reviews that are more helpful, authentic, and specific.
- Conducted comprehensive evaluations on Amazon and Goodreads benchmarks, demonstrating superior performance over numeric, graph-based, and LLM baselines in both recommendation quality and review generation.

Research on Opinion Distribution Prediction in Social Media (MindVote) **April 2025-June 2025**

Leader & First Author

- Developed MindVote, a comprehensive benchmark for evaluating LLMs' ability to predict human opinions within naturalistic social discourse, addressing critical limitations of existing sanitized survey-based evaluation methods.
- Revealed substantial performance gaps and systematic biases invisible to traditional benchmarks, including domain-specific knowledge limitations, source of origin bias, and social media context dependencies, enabling authentic assessment of LLM social reasoning capabilities.

Research on Text-to-SQL Optimization via Graph-guided Reasoning **June 2025-Aug 2025**

Leader & Co-first Author

- Developed SteinerSQL, a novel three-stage framework that reformulates complex mathematical Text-to-SQL generation as a unified graph optimization problem.
- Addressed the dual challenge of multi-step computation decomposition and intricate database schema navigation, achieving state-of-the-art performance with 36.10% execution accuracy on LogicCat and 36.75% on Spider2.0-Lite.

PROFESSIONAL EXPERIENCE

Cloud Engineer Intern **May 2024-Aug 2024**

Pegasystems, Boston, MA

- Designed an automated security alert system for CI/CD pipelines using AWS CloudWatch, Lambda, and Elasticsearch, generating over 10 security reports and reducing vulnerability exposure by 40% and proactive early-stage issue detection.

PUBLICATIONS

[1] MindVote: When AI Meets the Wild West of Social Media Opinion. Pre-print in Arxiv.
[2] SoK: Benchmarking Fake Voice Detection in the Voice Arms Race. Under Review.
[3] Towards Bridging Review Sparsity in Recommendation with Textual Edge Graph Representation. Pre-print in Arxiv.
[4] Building Bridges Where Rivers Run: Graph-Guided Reasoning for Complex SQL Generation. Under Review.
[5] LogicCat: Text-to-SQL Benchmark for Multi-Domain Reasoning Challenges. Pre-print in Arxiv.

SKILLS

LLM & AI: Transformers, Instruction-tuning & alignment, Parameter-efficient finetuning, Chain-of-Thought Reasoning
ML/DL: Classical ML (regression, tree ensembles, clustering), Deep Learning, GNN, Hyper-parameter Tuning
Language/Technologies: Python, Go, Java, C++, SQL, Bash, PyTorch, AWS, Git, Linux