35 Olden St, Computer Science 242
Princeton, NJ 08540
USA
yikai.wu@cs.princeton.edu

Yikai Wu

Education

Princeton University — **Princeton, NJ, USA**
Ph.D. student in Computer Science — *2022–present*

Yale University — **New Haven, CT, USA**
Ph.D. student in Computer Science — *2021–2022*

Duke University — **Durham, NC, USA**
Bachelor of Science (Summa Cum Laude) — *2017–2021*
Double major in Computer Science and Mathematics, Minor in Physics
Overall GPA: 3.97/4.00
Member of honor society Phi Beta Kappa

Research Experience

Differentially Private Optimization on Unitary Orbits — **Yale University**
Mentor: Prof. Nisheeth Vishnoi — *Jun 2021–Feb 2022*

- Consider the following optimization problem: Given $n \times n$ matrices A and Λ, maximize $\langle A, U\Lambda U \rangle$ where U varies over the unitary group $\mathrm{U}(\Lambda)$. The optimization can be used in multiple matrix approximation problems such as PCA and rank-k approximation. We designed an efficient differentially private algorithm for this optimization where A is constructed using users' private data. We also provided upper and lower bounds for the utility of the optimization.
- Paper [1] was presented at the Conference on Learning Theory (COLT) 2022.

Hessian in Neural Networks — **Duke University**
Mentor: Prof. Rong Ge — *May 2020–Aug 2021*

- The Hessian of the loss function captures important properties of neural networks. We observed that the Hessian has several interesting structures which appear commonly in different neural networks. We explained these structures using Kronecker factorization. Our new understanding of the Hessian can be used with PAC-Bayes techniques to get better generalization bounds.
- Manuscript [2] on arXiv. The paper is under review at Conference on Neural Information Processing Systems (NeurIPS) 2022.

Differential Privacy for Multiple Analysts **Duke University**
Mentor: Prof. Ashwin Machanavajjhala *Jan 2020–May 2021*

- Differential privacy is the gold standard of privacy protection. Existing differentially private algorithms are designed for a single analyst and are problematic for multiple analysts. We formulated three criteria to decide whether an algorithm is good for multiple analysts. We demonstrated how existing algorithms fail to satisfy them. We also designed new differentially private algorithms which satisfy these criteria provably.
- Paper [3] was presented at the International Conference on Very Large Data Bases (VLDB) 2021. The preliminary version was presented at the Theory and Practice of Differential Privacy Workshop (TPDP) 2020.

Differential Privacy for Summation Queries **Duke University**
Mentor: Prof. Ashwin Machanavajjhala *May 2018–Nov 2019*

- Answering summation queries under differential privacy is a little understood, non-trivial problem. Traditional differentially private algorithms for these queries are data-independent and often result in large errors for some types of data. We proposed a data-dependent algorithm using truncation to effectively reduce the errors in the results, while providing the same level of privacy protection.
- Paper [4] was presented at the Theory and Practice of Differential Privacy Workshop (TPDP) 2019.

Quantum Information and Algorithms **Duke University**
Mentor: Prof. Iman Marvian *May 2019–May 2020*

- Quantum information applies modern physics knowledge to develop a new type of computers and communication devices. We investigated a type of quantum operators useful for ion-trap quantum computers. We also designed and analyzed algorithms to purify quantum states, which is useful for quantum communication and quantum error correction.
- In addition, I studied several research papers on quantum algorithms, quantum learning theory, and quantum complexity theory.

Publications

[1] Oren Mangoubi, Yikai Wu, Satyen Kale, Abhradeep Thakurta, and Nisheeth K Vishnoi. Private matrix approximation and geometry of unitary orbits. In *Conference on Learning Theory*, pages 3547–3588. PMLR, 2022.
Presented at the Conference on Learning Theory (COLT) 2022.

[2] Yikai Wu, Xingyu Zhu, Chenwei Wu, Annie Wang, and Rong Ge. Dissecting Hessian: Understanding common structure of Hessian in neural networks. *arXiv:2010.04261 [cs.LG]*, 2020.
Plan to submit to the Annual Conference on Learning Theory (COLT) 2022.

[3] David Pujol, Yikai Wu, Brandon Fain, and Ashwin Machanavajjhala. Budget sharing for multi-analyst differential privacy. *Proceedings of the VLDB Endowment (PVLDB)*, 14(10): 1805–1817, 2021. doi: 10.14778/3467861.3467870.
Presented at the International Conference on Very Large Data Bases (VLDB) 2021.

[4] Yikai Wu, David Pujol, Ios Kotsogiannis, and Ashwin Machanavajjhala. Answering summation queries for numerical attributes under differential privacy. *arXiv:1908.10268 [cs.DB]*, 2019. Presented at the Theory and Practice of Differential Privacy Workshop (TPDP) 2019.

Teaching Assistant

COMPSCI 590.07: Computational Microeconomics (Graduate) — **Duke University**
Instructor: Prof. Vincent Conitzer — *Fall 2020*

COMPSCI 230: Discrete Mathematics for Computer Science — **Duke University**
Instructor: Prof. Kamesh Munagala — *Spring 2018*

Honors and Awards

Computing Research Association (CRA)
Outstanding Undergraduate Researcher Honorable Mention — *2020*

Duke University Faculty Scholar
Nomination (Top 2 in Computer Science department) — *2020*

Mathematical Contest in Modeling (MCM)
Meritorious Winner — *2019*

Duke University Mathematics Student Award
The Karl Menger Award — *2018*

The International Collegiate Programming Contest (ICPC)
Mid-Atlantic Regional Ranked 4th — *2017, 2018*

William Lowell Putnam Mathematical Competition
Ranked 142.5 (Top 4 at Duke Univeristy) — *2017*

Computer skills

Python, PyTorch, Tensorflow, C, C++, R, Mathematica