CS584 Machine Learning (Spring 2022) (Tentative) Research Topics

Research topics	**Potential directions**
Deep learning theory	Information bottleneck, Neural Tangent Kernel, ReduNet, Causality
Unsupervised representation learning	Disentangled representation learning, Causal Representation Learning, Contrastive learning, self-supervised learning, variational methods
Semi-supervised learning	Graph neural networks, graph embedding, mixup, self-training, co-training
Trustworthy machine learning (DNN, graph learning, federated learning, etc.)	Security attacks (evasion, data/model poisoning, backdoor); Empirical defense (adversarial training, robust optimization); Provable defense (randomized smoothing, IBP)
Privacy-preserving machine learning (DNN, graph learning, federated learning, etc.)	Privacy attacks (model stealing/inversion, property/attribute inference) Privacy preserving (differential privacy, Crypto, information theory), …
Machine learning for security	Blockchain security, Network security, Software security, Hardware security, Cyber-Physical System security, …
Large-scale machine learning (High-dimensional/massive data)	Randomized algorithms, Streaming, sketching, compressive sampling, …
Federated learning	Communication efficient, computational-efficient, personalization, fairness, Robust & privacy-preserving federated learning
Meta learning	Model-agnostic meta learning, etc.
Fair machine learning	
Interpretable machine learning	
Machine unlearning	
(Deep) compressive sensing/sparse coding	
Other topics you may be interested in	