FY2024/2024年度

Tensor Learning Team

Qibin Zhao

テンソル学習チーム　趙 啓斌

RIKEN Center for Advanced Intelligence Project

Outline

- **Tensor network (TN) algorithms and applications:** Our team has developed robust tensor decomposition algorithms and several methods for learning optimal tensor network structures as well as the extension to functional tensor completion that can address the combinatorial distribution shift challenges in multi-output regression task.
- **Adversarial robustness of deep models:** Our team has focused on advancing the generalization of adversarial robustness to unseen attacks as well as adversarial robustness in unsupervised learning, particularly for multi-view representation learning and clustering.

Tensor Method for Machine Learning

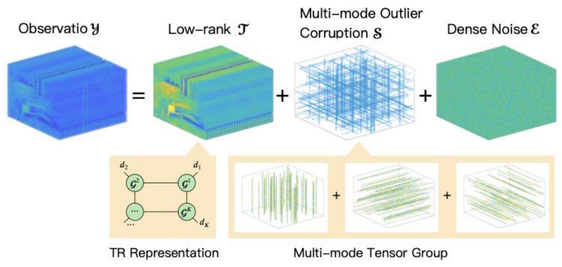
Motivation

- Low-rank tensor representation is ineffective when data is corrupted by multi-type of outliers.
- Finding optimal tensor network structure is challenging.
- Applying tensor methods to addressing key challenges in ML.

Robust tensor ring decomposition with multi-mode outliers

(Qiu et al. AAAI'24)

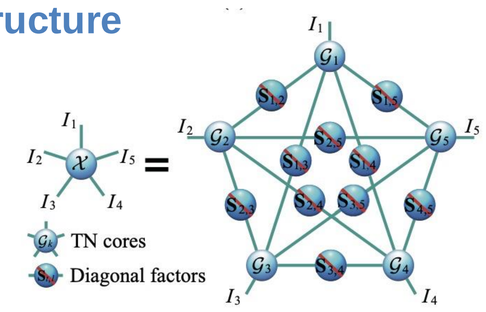
- Defining a novel norm to capture outliers with various structures
- Theoretical support on estimation error of recovery of low-rank tensor representations



Learning optimal tensor network structure

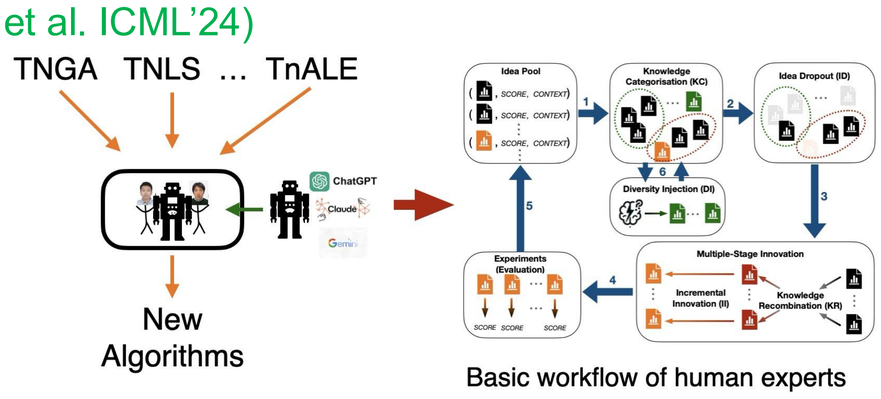
(Zheng et al. CVPR'24)

$$\min_{\mathcal{G},\mathbf{S}} \frac{1}{2}\|\mathcal{X} - \mathrm{STN}(\mathcal{G},\mathbf{S})\|_F^2 + \frac{\mu}{2}\sum_{k\in\mathbb{K}_N}\|\mathcal{G}_k\|_F^2 + \sum_{(t,l)\in\mathbb{TL}_N}\lambda_{t,l}\|\mathbf{S}_{t,l}\|_1,$$



- Learning from a fully connected TN to an optimal TN by imposing sparsity regularizer on diagonal factors associated with each TN edge

(Zeng et al. ICML'24)



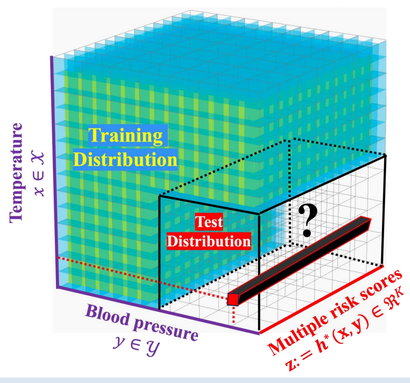
Basic workflow of human experts

- LLM to discover new effective algorithms by feeding existing algorithms
- Constructing a pipeline of prompts and evaluation with downstream tasks

Functional tensor for combinatorial distribution shift (CDS)

(Wang et al. NeurIPS'24)

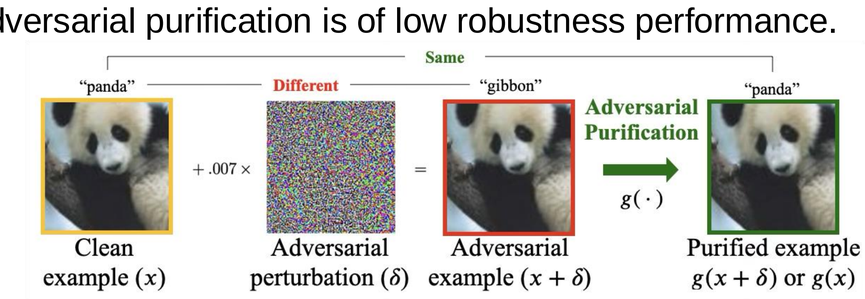
- Distribution of combinations of input features shifts between training and testing data.
- Development of functional tensor completion, an extension from discrete indices to continuous indices, aiming to achieve robust regression of new feature combinations.



Adversarial Robustness of Deep Models

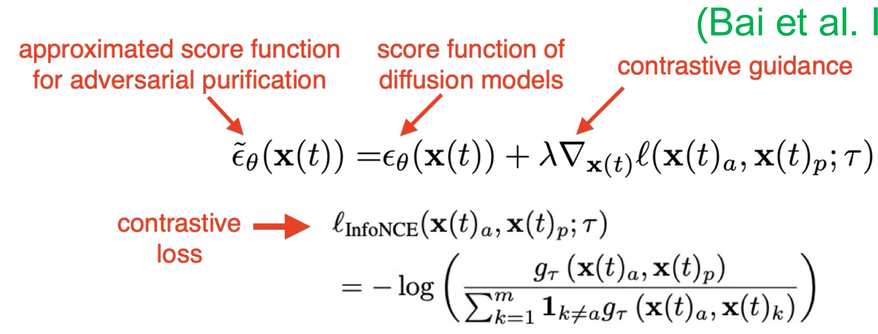
Motivation

- Adversarial training is of poor generalization to unseen attacks.
- Adversarial purification is of low robustness performance.



Guided diffusion model for adversarial purification

(Bai et al. ICML'24)

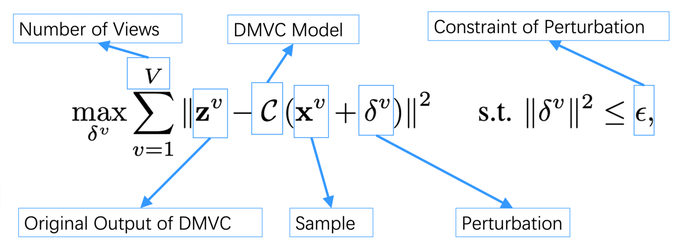


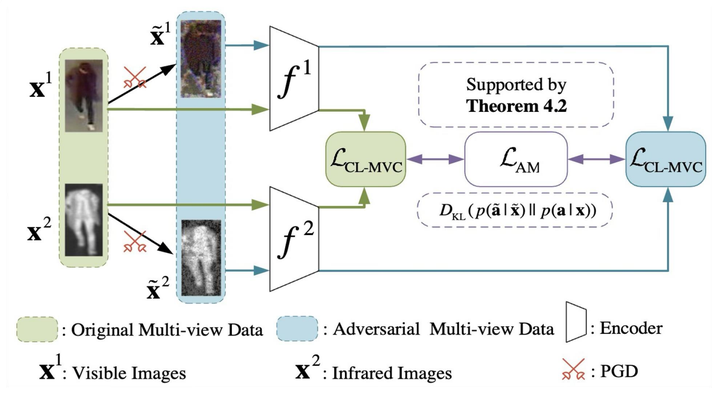
- Diffusion model with contrastive guidance can mitigate the tradeoff between keeping semantic information and removing adversarial perturbations.
- Contrasive loss is designed to ensure that purified examples at adjacent steps are similar, while remaining dissimilar to other purified examples.

Adversarially robust deep multi-view clustering (DMVC)

(Huang et al. ICML'24)

- Deep multi-view clustering, an unsupervised learning, is generally robust due to its robust representation learning.
- We found that it can be attacked by specially designed learning objectives.





- Robustifying multi-view representation learning by integrating adversarial training with both clustering loss and contrastive loss.
- The mutual information between adversarial inputs and predictive clusters is beneficial for robust multi-view learning.

Related Publications

- Y. Qiu, G. Zhou, A. Wang, Z. Huang, and Q. Zhao, "Towards multi-mode outlier robust tensor ring decomposition," AAAI 2024.
- M. Bai, W. Huang, T. Li, A. Wang, J. Gao, C. F. Caiafa, and Q. Zhao, "Diffusion models demand contrastive guidance for adversarial purification to advance," ICML 2024.
- H. Huang, G. Zhou, Y. Zheng, Y. Qiu, A. Wang, and Q. Zhao, "Adversarially robust deep multi-view clustering: A novel attack and defense framework," ICML 2024.
- J. Zeng, C. Li, Z. Sun, Q. Zhao, and G. Zhou, "tnGPS: Discovering unknown tensor network structure search algorithms via large language models (LLM)," ICML 2024.
- Y. Zheng, X. Zhao, J. Zeng, C. Li, Q. Zhao, et al., "SVDinsTN: A tensor network paradigm for efficient structure search from regularized modeling perspective," CVPR 2024.
- A. Wang, Y. Qiu, M. Bai, Z. Jin, G. Zhou, and Q. Zhao, "Generalized tensor decomposition for understanding multi-output regression under combinatorial shifts," NeurIPS 2024.