Enhance Robustness of Machine Learning with Improved Efficiency

Yan Yan

EECS, Washington State University
355 NE Spokane St, Pullman, WA 99163, USA
yan.yan1@wsu.edu

Abstract

Robustness of machine learning, often referring to securing performance on different data, is always an active field due to the ubiquitous variety and diversity of data in practice. Many studies have been investigated to enhance the learning process robust in recent years. To this end, there is usually a trade-off that results in somewhat extra cost, e.g., more data samples, more complicated objective functions, more iterations to converge in optimization, etc. Then this problem boils down to finding a better trade-off under some conditions. My recent research focuses on robust machine learning with improved efficiency. Particularly, the efficiency here represents learning speed to find a model, and the number of data required to secure the robustness. In the talk, I will survey three pieces of my recent research by elaborating the algorithmic idea and theoretical analysis as technical contributions — (i) epoch stochastic gradient descent ascent for min-max problems, (ii) stochastic optimization algorithm for non-convex inf-projection problems, and (iii) neighborhood conformal prediction. In the first two pieces of work, the proposed optimization algorithms are general and cover objective functions for robust machine learning. In the third one, I will elaborate an efficient conformal prediction algorithm that guarantee the robustness of prediction after model is trained. Particularly, the efficiency of conformal prediction is measured by its bandwidth.

Machine learning roughly involves three major steps: (i) build the model/objective, (ii) learn the model by optimizing the objective, (iii) perform prediction using the learned model (for validation or testing). Due to their sequential nature, it is inevitable to enhance the robustness of all three steps, which I will elaborated in the following three papers.

The first two papers focus on optimization for two family of problems. In the first paper (Yan et al. 2020b), a min-max problem is considered, which covers machine learning objectives, such as distributionally robust optimization (DRO), AUC maximization. The proposed algorithm works for both strongly-convex-strongly-concave (SCSC) with a fast rate $O(1/T)$ for the duality gap, and weakly-convex-strongly-concave (WCSC) problems with $\tilde{O}(1/\epsilon^4)$ iteration complexity for nearly stationary point. The fast rate for duality gap under SCSC matches the lower bound and is therefore the best possible convergence rate without adding more assumptions. In the second paper (Yan et al. 2020a), a novel objective is proposed to improve generalization, inspired by variance-based regularization. Under several conditions, optimization algorithms are proposed and their convergence are analyzed, leading to $O(1/\epsilon^{4/v})$ where v is a parameter in condition. Empirical results verify the improved generalization performance. The third paper (Ghosh et al. 2023) focuses on the robust inference via conformal prediction that provides statistically valid coverage on true label. This paper considers the concentrated distribution condition for data samples' neighborhood and incorporates this condition into the conformal prediction framework. In this way, the bandwidth of conformalized prediction would be further reduced.

Speaker Bio

Yan Yan is an assistant professor at School of Electrical Engineering And Computer Science, Washington State University. Yan was a postdoctoral research associate working with Professor Tianbao Yang at the Computer Science Department, University of Iowa. Yan received Ph.D in 2018 from Centre for Artificial Intelligence (CAI), University of Technology Sydney (UTS), Australia, under the supervision of Professor Yi Yang. In 2013, Yan received B.E. from Tianjin University, China, in Computer Science. His research interests include machine learning and its applications to computer vision, particularly, optimization for robust machine learning, uncertainty-aware learning and prediction via conformal prediction .

References

Ghosh, S.; Belkhouja, T.; Yan, Y.; and Doppa, J. R. 2023. Improving Uncertainty Quantification of Deep Classifiers via Neighborhood Conformal Prediction: Novel Algorithm and Theoretical Analysis. In *Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI)*.

Yan, Y.; Xu, Y.; Lin, Q.; Liu, W.; and Yang, T. 2020a. Optimal epoch stochastic gradient descent ascent methods for min-max optimization. *Advances in Neural Information Processing Systems*, 33: 5789–5800.

Yan, Y.; Xu, Y.; Zhang, L.; Xiaoyu, W.; and Yang, T. 2020b. Stochastic optimization for non-convex inf-projection problems. In *International Conference on Machine Learning*, 10660–10669. PMLR.