数学与系统科学研究院

计算数学所网络学术报告

报告人： 凌青 教授

（ 中山大学 ）

报告题目：

Federated Variance-Reduced Stochastic Gradient Descent With Robustness to Byzantine Attacks

邀请人： 刘歆 研究员

报告时间：2020 年 11 月 20 日（周五）晚上 20:10-20:45

报告工具：腾讯会议（ID：521 3538 2330）

会议密码：311311

Abstract:

This talk deals with distributed finite-sum optimization for learning

over multiple workers in the presence of malicious Byzantine attacks. Most resilient approaches so far combine stochastic gradient descent (SGD) with different robust aggregation rules. However, the sizeable SGD-induced stochastic gradient noise challenges discerning malicious messages sent by the Byzantine attackers from noisy stochastic gradients sent by the 'honest' workers. This motivates reducing the variance of stochastic gradients as a means of robustifying SGD. To this end, a novel Byzantine attack resilient distributed (Byrd-) SAGA approach is introduced for federated learning tasks involving multiple workers. Rather than the mean employed by distributed SAGA, the novel Byrd-SAGA relies on the geometric median to aggregate the corrected stochastic gradients sent by the workers. When less than half of the workers are Byzantine attackers, Byrd-SAGA attains provably linear convergence to a neighborhood of the optimal solution, with the asymptotic learning error determined by the number of Byzantine workers. Numerical tests corroborate the robustness to various Byzantine attacks, as well as the merits of Byrd-SAGA over Byzantine attack resilient distributed SGD.

Bio:

Qing Ling received the B.E. degree in automation and Ph.D. degree in control theory and control engineering from the University of Science and Technology of China, Hefei, China, in 2001 and 2006, respectively. He was a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI, USA, from 2006 to 2009 and an Associate Professor with the Department of Automation, University of Science and Technology of China, from 2009 to 2017. He is currently a Professor with the School of Data and Computer Science, Sun Yat-Sen University, Guangzhou, China. His current research interest includes distributed and decentralized optimization and its application in machine learning. He received the 2017 IEEE Signal Processing Society Young Author Best Paper Award as a Supervisor. He is an Associate Editor of IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, and a Senior Area Editor of IEEE SIGNAL PROCESSING LETTERS.

欢迎大家参加！