Enhancing Federated Learning Using Mathematical Theorems and Coding Technologies

Lu, Sarah (School: Centro Residencial de Oportunidades Educativas de Mayaguez)

Federated learning is a new and exciting field of topic that has arisen in the world of machine learning. This field is new and exciting because it offers innovative solutions that address many issues users have had. By enabling the sharing of model parameters without the need to share original data, federated learning offers solutions to data and privacy concerns. However, federated learning is still quite novel, and some issues have yet to be solved, particularly in the case of training complicated machine learning models on resource-limited devices as they are insufficient in speed and power (e.g. Raspberry Pi). This research investigates three coding techniques—One-hot encoding, Random Fourier Features, and Random Generator—which were used to not only solve said issues on resource-limited devices but also issues regarding privacy and security. Specifically, by using matrix calculus, two novel secure and privacy preserving schemes have been developed for gradient descent in federated learning. Extensive numerical experiments demonstrate promising outcomes such as input-output linearity, improved accuracy and privacy, and consistent high performance. The results and findings of this research indicate many promising features of federated learning and make contributions toward its enhancement.

Awards Won:
American Mathematical Society: Honorable Mention and One-Year Membership to AMS (for 5 projects with up to 3 team members per project)