World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:16, No:04, 2022

Private Coded Computation of Matrix Multiplication

Authors : Malihe Aliasgari, Yousef Nejatbakhsh

Abstract : The era of Big Data and the immensity of real-life datasets compels computation tasks to be performed in a distributed fashion, where the data is dispersed among many servers that operate in parallel. However, massive parallelization leads to computational bottlenecks due to faulty servers and stragglers. Stragglers refer to a few slow or delay-prone processors that can bottleneck the entire computation because one has to wait for all the parallel nodes to finish. The problem of straggling processors, has been well studied in the context of distributed computing. Recently, it has been pointed out that, for the important case of linear functions, it is possible to improve over repetition strategies in terms of the tradeoff between performance and latency by carrying out linear precoding of the data prior to processing. The key idea is that, by employing suitable linear codes operating over fractions of the original data, a function may be completed as soon as enough number of processors, depending on the minimum distance of the code, have completed their operations. The problem of matrix-matrix multiplication in the presence of practically big sized of data sets faced with computational and memory related difficulties, which makes such operations are carried out using distributed computing platforms. In this work, we study the problem of distributed matrix-matrix multiplication W = XY under storage constraints, i.e., when each server is allowed to store a fixed fraction of each of the matrices X and Y, which is a fundamental building of many science and engineering fields such as machine learning, image and signal processing, wireless communication, optimization. Non-secure and secure matrix multiplication are studied. We want to study the setup, in which the identity of the matrix of interest should be kept private from the workers and then obtain the recovery threshold of the colluding model, that is, the number of workers that need to complete their task before the master server can recover the product W. The problem of secure and private distributed matrix multiplication W = XY which the matrix X is confidential, while matrix Y is selected in a private manner from a library of public matrices. We present the best currently known trade-off between communication load and recovery threshold. On the other words, we design an achievable PSGPD scheme for any arbitrary privacy level by trivially concatenating a robust PIR scheme for arbitrary colluding workers and private databases and the proposed SGPD code that provides a smaller computational complexity at the workers.

Keywords : coded distributed computation, private information retrieval, secret sharing, stragglers
Conference Title : ICNIT 2022 : International Conference on Neutrosophic Information Theory
Conference Location : New York, United States
Conference Dates : April 25-26, 2022