Efficient Protocol for Collaborative Dictionary Learning in Decentralized Networks

T. Idé (井手 剛) 1, Raymond Rudy 2, and Dzung T. Phan 1
1 IBM Research, T.J. Watson Research Center
2 IBM Research - Tokyo

Problem setting
Decentralized multi-task density estimation with data privacy

Prior work
Multi-task learning
- Actively studied area but mostly for supervised learning
- Not many of them are fully probabilistic
- Little is known about how to decentralize it

Decentralized computation
- Byzantine protocols assume categorical values
- Multi-agent consensus methods are not in the context of multi-task learning
- Differential privacy is problematic in distributed environment
- Multi-agent consensus methods are not in the context of multi-task learning
- Secure multi-party computation typically needs a central server
- Homomorphic encryption is slow

Multi-task density estimation model
Employ a mixture model with agent-specific weights
\[ p^s(x | \Theta, \Pi^s) = \sum_{k=1}^{K} \pi_k^s f(x | \Theta_k^s) \] Shared by all the agents
Mixture weights are agent-specific

The density is assumed to be in the exponential family
\[ f(x | \theta_k) = G(\theta_k)H(x) \exp \{ \eta(\theta_k)^T T(x) \} \]

Decentralized aggregation with data privacy
Decentralized aggregation
- Finding stationary state of Markovian transition process

Given the incidence matrix A, an update equation
\[ c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} A_{s,j} (c^j - c^s) \quad \text{or} \quad c \leftarrow W_t c \]
converges to
\[ c = \sum_{s=1}^{S} c^s = 1^T c \]
S-dimensional vector of ones

Graph structure matters!
What kind of communication graph A should be chosen?

Cycle graph
- Most sparse and symmetric
- Slow convergence (quadratic in S)

“Cycle graph with inverse chord”
- Not regular/symmetric
- FAST convergence (log S)

Orders of magnitude faster than homomorphic encryption-based methods

Motivating application:
collaborative condition-based monitoring of industrial assets

Noisy sensor data
- IoT data is generally noisy
- Data privacy is a major concern but sample-wise encryption is not practical
- Need a new approach!