ε-局所差分プライバシを用いた連合サロゲート進化型多目的最適化フレームワークの検討

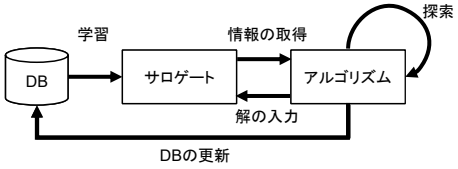
木下貴登

1. 背景

ビッグデータとサロゲート進化型多目的最適化

通信ネットワークや情報処理端末，IoT機器の普及により，大量かつ多種多様なデータが**ビッグデータ**として収集され，その**データ量は増加**している．

収集したデータから近似モデルであるサロゲートモデルを学習し，サロゲートから得られる情報に基づいて探索を行うサロゲート進化型多目的最適化アルゴリズムは，**データの利活用**を伴う実応用を実現する根幹技術として重要性を高めている．

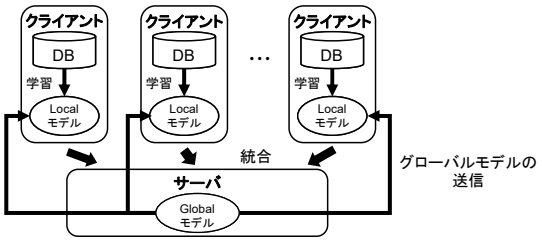


サロゲート進化型多目的最適化アルゴリズム

連合学習[1]

実世界タスクでは，データが複数のデバイスやクライアントに**分散**的に保持され，かつ個人や組織のプライバシや機密情報の**保護**が要求されることが想定される．

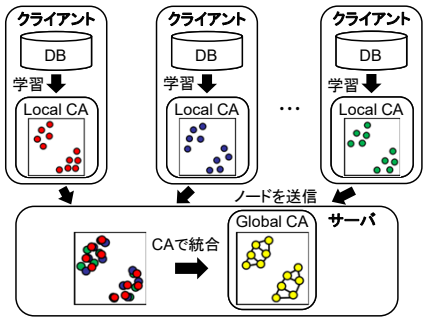
連合学習は，各クライアント上での並列分散的なモデルの学習とサーバ上でのモデルの統合による**高い学習効率**と，モデルパラメータ共有を通じたデータの間接的な公開によるセンシティブなデータの**プライバシ保護**の両方を達成する．



[1] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, *Federated Learning*. California: Morgan & Claypool Publishers, December, 2019.

2. Federated Clustering via ART- based Clustering (FCAC)[2]

FCACは適応共鳴理論 (ART) に基づくクラスタリング手法であるCIM-based ART (CA) を連合学習に適用した**連合クラスタリング手法**．Local CAのノードをデータセットとしてGlobal CAを学習することでモデルの統合を行う．



[2] N. Masuyama, Y. Nojima, Y. Toda, C. K. Loo, H. Ishibuchi, and N. Kubota, "Privacy-preserving continual federated clustering via adaptive resonance theory," arXiv. 2023, Under Review.

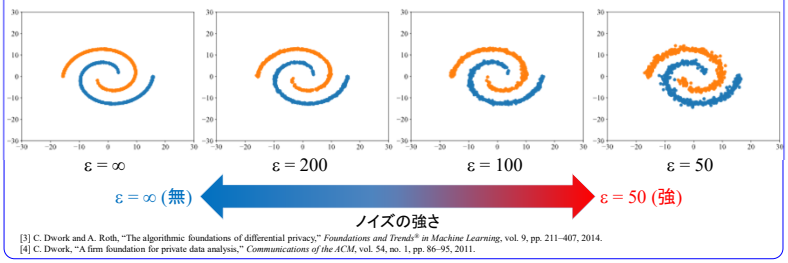
3. ε-局所差分プライバシ (DP)[3]

連合学習には共有したモデルから**データセットの情報が漏洩するリスク**がある．

ε-局所差分プライバシはデータにノイズを付加するのみで連合学習のプライバシ性を向上でき，**効率性とプライバシ保護の両立**が可能．

Laplace Mechanism[4]

Laplace Mechanismはε-局所差分プライバシの1種で，データに平均0，スケール $\Delta f / \varepsilon$ のLaplaceノイズを付与する．ここで Δf はデータの範囲．



[3] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Machine Learning*, vol. 9, pp. 211–407, 2014.
[4] C. Dwork, "A firm foundation for private data analysis," *Communications of the ACM*, vol. 54, no. 1, pp. 86–95, 2011.

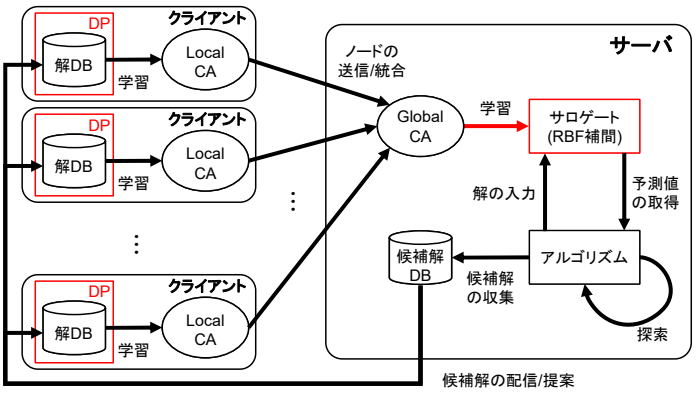
4. 提案手法

クライアント

1. 事前に幾つかの解を獲得，評価し，情報を解DBに保持している前提とする．
2. 解DBにノイズを付与したデータセットからLocal CAを学習する．
3. Local CAのノードをサーバに送信し，サーバからの応答を待機する．
4. 必要に応じて，新しい解を評価し，解DBに追加する．(本研究では行わない．)
5. サーバから配信/提案された候補解を，必要に応じて評価し解DBに追加する．2に戻る．
   (本研究では全て追加する．)

サーバ

1. 各クライアントから受信したノードをデータセットとしてGlobal CAを学習する．
2. Global CAのノードをデータセットとして回帰モデルを学習．(本研究ではRBF補間．)
3. 回帰モデルをサロゲートとして進化型多目的最適化アルゴリズムで候補解を探索する．
4. 探索終了後に，有望な解を候補解として各クライアントに配信/提案する．1に戻る．
   (本研究では最終世代個体群を候補解集合とする．)



5. 数値実験

実験設定

進化型多目的最適化アルゴリズムとして**NSGA-II**を用いて，3目的DTLZ1-7, WFG1, 2問題を探索し，全評価個体をIGD⁺で評価する．

その他パラメータ設定

パラメータ	値
試行回数	15
全評価回数	1,600
クライアント数	4
クライアント上の初期DBサイズ	100
サーバ上の探索終了世代数	20
サーバ上の個体群サイズ	100

実験結果

WMW検定 (有意水準5%) でDTLZ7を除く全ての問題で差分プライバシの有無による有意差は認められなかった．
→提案手法が一定のプライバシ強度のもとで**探索性能とプライバシ保護を両立する**ことが確認された．

Problem	差分プライバシ無 ($\varepsilon = \infty$)	差分プライバシ有 ($\varepsilon = 200$)	差分プライバシ有 ($\varepsilon = 100$)	差分プライバシ有 ($\varepsilon = 50$)
DTLZ1	3.3592e+1 (3.69e+0)	3.0785e+1 (4.66e+0) =	3.4156e+1 (6.28e+0) =	5.0224e+1 (1.65e+1) +
DTLZ2	3.1387e−2 (2.91e−3)	3.0420e−2 (2.65e−3) =	3.0421e−2 (2.80e−3) =	6.2205e−2 (6.41e−3) +
DTLZ3	2.5208e+2 (3.99e+1)	2.3772e+2 (5.25e+1) =	2.4665e+2 (3.23e+1) =	3.0552e+2 (7.75e+1) +
DTLZ4	1.4673e−1 (4.78e−2)	1.7039e−1 (6.66e−2) =	1.5981e−1 (6.17e−2) =	2.2997e−1 (5.86e−2) +
DTLZ5	1.5042e−2 (3.43e−3)	1.4493e−2 (3.41e−3) =	1.4252e−2 (3.04e−3) =	2.5651e−2 (4.39e−3) +
DTLZ6	2.6555e+0 (6.40e−1)	2.1732e+0 (5.36e−1) =	2.4076e+0 (5.86e−1) =	2.6486e+0 (6.62e−1) =
DTLZ7	5.1896e−2 (6.08e−3)	8.5681e−2 (1.23e−2) +	9.1836e−2 (1.20e−2) +	1.4142e−1 (1.76e−2) +
WFG1	1.7913e+0 (4.46e−2)	1.7699e+0 (6.40e−2) =	1.7996e+0 (5.68e−2) =	1.9863e+0 (8.53e−2) +
WFG2	6.8031e−1 (9.64e−2)	6.9704e−1 (7.62e−2) =	7.0576e−1 (6.17e−2) =	1.3561e+0 (1.83e−1) +
+/=/−		1/8/0	1/8/0	8/1/0