Communication-Efficient Learning of Deep Networks from Decentralized Data

竹本志恩

May 23, 2025

INIAD

書誌情報

- **題名**: Communication-Efficient Learning of Deep Networks from Decentralized Data
- **発表会議/論文誌名**: 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017
- **著者**: H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, Blaise Agüera y Arcas

目次

1. **はじめに** (Introduction)

2. **関連研究** (Related Work)

3. **提案手法**: FederatedAveraging (FedAvg) **アルゴリズム**

4. **実験結果** (Experimental Results)

5. **議論・結論** (Discussion, Conclusions)

1. はじめに (Introduction)

- 論文が解決しようとする問題:
  - 電話やタブレットは主要なコンピューティングデバイスとなりつつある
  - これらのデバイス上のプライベートデータから学習したモデルは大きな可能性を秘める
  - しかし，プライベートデータを中央に集約・保存することは望ましくない
  - 更新内容からも漏洩の可能性
  - 従来とデータの分布が大きく異なる（非 IID、不均衡）
- 提案手法の概要:
  - **Federated Learning (FL)** を提案
  - 各端末がローカルで学習し，モデルの更新や差分を統合サーバが平均化してグローバルモデルを更新
  - 特に，**FedAvg** アルゴリズムは、SGD とモデル平均化を組み合わせた手法

目次

1. はじめに (Introduction)

2. 関連研究 (Related Work)

3. 提案手法: FederatedAveraging (FedAvg) アルゴリズム

4. 実験結果 (Experimental Results)

5. 議論・結論 (Discussion, Conclusions)

2. 関連研究 (Related Work)

- 先行研究との差異:
  - 従来手法は以下が前提
    - IID データ
    - データ数 $>$ クライアント数
    - 高速ネットワーク
  - FL の最適化は前提が異なる:
    - 非 IID かつ不均衡なデータ
    - クライアント数$\gg$データ数
    - 通信リソースが限定的
  - FedAvg は，これら課題（非 IID，不均衡，通信制約）に対応

目次

1. はじめに (Introduction)

2. 関連研究 (Related Work)

3. **提案手法**: FederatedAveraging (FedAvg) **アルゴリズム**

4. 実験結果 (Experimental Results)

5. 議論・結論 (Discussion, Conclusions)

3. 提案手法: FederatedAveraging (FedAvg) アルゴリズム

- **FedAvg の考え方**:
  - 各ラウンドごとにクライアントを選択 (割合 C) し，ローカルで学習
    - 各クライアントが，ミニバッチサイズ B で SGD を E 回実行
  - サーバはモデルの更新 | モデルパラメータを平均化
  - 平均化は，クライアントのデータ量 (n_k) で重み付け
- **アルゴリズムの主要パラメータ (C, E, B)**:
  - **C**: 各ラウンドで選択されるクライアントの割合
  - **E**: 各クライアントがローカルデータを何回学習するか
  - **B**: ローカル学習におけるミニバッチのサイズ
  - これらは通信コストや収束に影響
  - ローカル計算量を増やし（E を大きく、B を小さく），必要な通信ラウンド数を削減

提案手法: FedAvg アルゴリズム (続き)

- **FedSGD との違い**:
  - **FedSGD は** E=1，B=∞ **の** FedAvg **に相当**
    - ローカルでの SGD を一回だけ実行
    - ローカルデータを全て使用 $>$ ミニバッチサイズが無限大
  - **FedAvg は，ローカルで複数回** SGD **を実行可能（**$E > 1$）
  - FedSGD は勾配を、FedAvg はモデルパラメータを平均化するという記述も見かけたが、本論文の FedAvg はデータ量で重み付けしたモデルパラメータの平均化を行っている...?

目次

1. はじめに (Introduction)

2. 関連研究 (Related Work)

3. 提案手法: FederatedAveraging (FedAvg) アルゴリズム

4. 実験結果 (Experimental Results)

5. 議論・結論 (Discussion, Conclusions)

4. 実験結果 (Experimental Results)

- 実験設定
  - 複数のデータセットとモデルで検証
    - MNIST (手書き数字認識): シンプルな 2 層 NN、CNN
    - Shakespeare (言語モデリング): LSTM
    - CIFAR-10 (画像認識): CNN
  - データ分割方法を検証
    - IID (独立同分布)
    - 非 IID (非独立同分布): 病的な分割（例: MNIST で各クライアントが 2 種類のみの数字を持つ），自然な分割（Shakespeare の役割ごと）
    - 不均衡データ（FedAvg にとっては少し容易だったとの記述あり）
- 主要な評価指標
  - 目標精度に達するまでの通信ラウンド数
  - FedAvg のパラメータ (C, E, B) が通信コストに与える影響

実験結果 (Experimental Results) (続き)

- 主要な結果:
  - パラメータ (C, E, B) の影響:
    - ローカル計算量 ($E\times$ データサイズ $/B$) の増加で，通信ラウンド数を削減
    - 特に E の効果が大きい．例: MNIST 2NN (IID) で E=1 から E=20, B=10 にすることで、ラウンド数は 45.9 倍削減
    - クライアント選択率 C を増やすと、各ラウンドの通信量は増えるが、ラウンド数は減少傾向にある
  - 非 IID データでの性能:
    - 病的な非 IID データに対しても、FedAvg は収束し、FedSGD と比較して通信ラウンド数を大幅に削減した

目次

1. はじめに (Introduction)

2. 関連研究 (Related Work)

3. 提案手法: FederatedAveraging (FedAvg) アルゴリズム

4. 実験結果 (Experimental Results)

5. 議論・結論 (Discussion, Conclusions)

5. 議論・結論 (Discussion, Conclusions)

- 論文の貢献:
  - FL の実用的な枠組みと FedAvg アルゴリズムを提案
  - FedAvg が深層学習モデルや非 IID/不均衡データに機能すると示した
  - ローカルでの計算量増加が，通信ラウンド数を劇的に削減すると示した
  - FedAvg は学習損失の最適化にも有効である?
- 今後の課題:
  - 更なるプライバシー強化 (差分プライバシー，セキュアマルチパーティ計算)
  - クライアントデータの動的な変化やクライアントの可用性といった実環境での課題への対応．同期型 FedAvg では応答のないクライアントへの対処が必要
  - ローカル計算量の過剰な増加による収束への悪影響．収束状況に応じたパラメータ調整が有効?

今後の展望

- 自身の研究テーマとの関連:
  - IoT デバイスへの適用に興味がある
    - しかし本論文の初期想定はスマホ寄り
    - IoT 特有のリソース制約（計算能力，バッテリー，通信帯域）を考慮した FedAvg の変形や他手法の検討が必要?
  - プライバシー・セキュリティ（悪意ある参加者への対策など）は重要な課題
    - DP，MCP などの組み合わせを深掘りしたい
    - 特に集約方法によって適切な施策が変わる可能性に関心がある
  - 最適化について
    - FedAvg は通信回数について通信効率化に寄与
    - しかし他はあまり気にしていなさそう
    - エネルギー消費や帯域利用など低レイヤやネットワークも気にしたい

今後の展望

- 今後は以下をサーベイ，追試
  - IoT 環境での FL アルゴリズム
  - セキュリティ・プライバシー担保: DP や MCP の適用
  - エネルギー消費や帯域利用などの最適化
  - 音による行動認識と関連する社会課題
- 自身の研究テーマを具体化する