

蒸留を用いた非同期型連合学習

Asynchronous Federated Learning Using Distillation

矢島大路[†] 小野翔多^{††} 三好 匠^{†,††} 山崎 託[†]
 Hiromichi YAJIMA Shota ONO Takumi MIYOSHI Taku YAMAZAKI

[†] 芝浦工業大学大学院理工学研究科
 Graduate School of Engineering and Science
 Shibaura Institute of Technology

^{††} 東京大学生産技術研究所
 Institute of Industrial Science
 The University of Tokyo

1. まえがき

機械学習におけるサーバへの集中的な負荷を軽減するため、複数のクライアントデバイスへ処理を分散させる連合学習が注目されている。連合学習において、従来サーバで行われていた高負荷な機械学習処理を性能の低いクライアントデバイスで効率的に行う手法として、機械学習モデルの圧縮技術である蒸留を用いる手法が提案されている [1]。本手法では、従来の連合学習よりもクライアントの処理負荷と学習時間を削減し、機械学習モデルの精度をより速く向上させることが可能であるが、サーバが蒸留処理を行う際にクライアントが待機状態に入ることによるタイムロスが発生する。本稿では、クライアントの学習処理とサーバの蒸留処理を独立させた非同期型連合学習を提案する。

2. 従来手法

文献 [1] では、蒸留を用いた連合学習が提案されている。まず、サーバはグローバルモデルを正蒸留を用いて小型化した蒸留グローバルモデルを作成し、クライアントへ送信する。次に、クライアントは送られてきた機械学習モデルを学習し、学習結果をサーバへ送信する。サーバはクライアントから送られてきたモデルを平均化することでサーバ内の蒸留グローバルモデルを更新し、逆蒸留を用いてグローバルモデルを更新する。

本手法では、クライアントは通常の連合学習よりも小さな機械学習モデルを用いて学習を行うため、処理負荷と学習時間が削減される。しかし、サーバで蒸留処理を行う間、クライアントは更新された機械学習モデルが返信されるまで待機する必要がある。また、クライアントが学習している間は逆にサーバが待機状態に入る。これらの待機時間をなくすことで、より速く機械学習モデルの精度を向上させることができると考えられる。

3. 提案手法

本稿では、蒸留を用いた非同期型連合学習を提案する。提案手法の概要を図 1 に示す。本手法では、グローバルモデルを所持し蒸留処理を担当する蒸留サーバと、クライアントから蒸留グローバルモデルの学習結果を収集し平均化する部分を担当する平均化サーバの 2 種類のサーバを用いる。蒸留サーバはまず、グローバルモデルを蒸留して蒸留グローバルモデルを作成し、平均化サーバを通じてクライアントへ送信する。次に、クライアントは送られてきた機械学習モデルを学習した後、学習結果を平均化サーバへ送信する。平均化サーバは、クライアントから送られてきた機械学習モデルを平均化し、平均化サーバ内の蒸留グローバルモデルを更新するとともに、更新後のモデルを蒸留サーバへ送信する。蒸留サーバは、送られてきた最新の蒸留グローバルモデルを用いて蒸留サーバ内のグローバルモデルへ逆蒸留を行う。なお、提案手法ではグローバルモデルの精度向上の高速化に焦点をあてるため、従来手法における正蒸留処理は行わない。

提案手法では、従来手法で行われていたクライアントの学習部分と蒸留処理を切り離して非同期で動作させることで、待機状態を回避することが可能となる。また、平均化サーバとクライアントの間では一般的な連合学習を実行すればよく、実装も比較的容易である。

4. 性能評価

機械学習モデルの精度と学習時間の観点から、提案手法と従来手法の性能評価を行う。実験では、CIFAR-10 を用いた画像認識学習を蒸留サーバ、平均化サーバ、及びクライアント 3 台で行っ

た。なお、今回は 1 台の PC 上に二つのサーバプログラムを動作させた。また、グローバルモデルには 12 層、蒸留グローバルモデルには 6 層の畳み込み深層学習 (CNN) モデルを使用した。正蒸留を行う従来手法と正蒸留を行わない従来手法を比較対象とし、平均化サーバのラウンドごとに逆蒸留を行う提案手法と平均化サーバの更新を待たずに継続的に逆蒸留を行う 2 種類の提案手法を設定した。

横軸を経過時間としたグローバルモデルの精度を図 2 に示す。結果より、提案手法は従来手法よりもグローバルモデルの精度がより速く向上していることが分かる。グローバルモデルの精度が 60% に到達するまでの時間は、従来手法 (正蒸留あり) が 436 秒、従来手法 (正蒸留なし) が 406 秒、提案手法 (ラウンドごと) が 308 秒、提案手法 (継続的) が 244 秒となった。これは、提案手法ではクライアントの学習部分とサーバでの蒸留部分を分離し非同期で動作することで、従来手法における待機状態によるタイムロスが削減されたためであると考えられる。しかし、提案手法では正蒸留処理を行わないため、蒸留グローバルモデルの精度が低下し、それに伴いグローバルモデルが最終的に到達できる精度が従来手法よりも低下してしまう問題がある。

5. むすび

本稿では、蒸留を用いた非同期型連合学習を提案した。今後は、グローバルモデルの精度を低下させずにより速く精度向上させる手法について検討する予定である。

謝辞 本研究成果は、国立研究開発法人情報通信研究機構 (NICT) の委託研究 (JPJ012368C05201) により得られた。

文献

[1] 矢島大路, 三好 匠, 山崎 託, 小野翔多, “連合学習における蒸留を用いた処理負荷と通信量の削減,” 信学技報, NS2022-87, Oct. 2022.

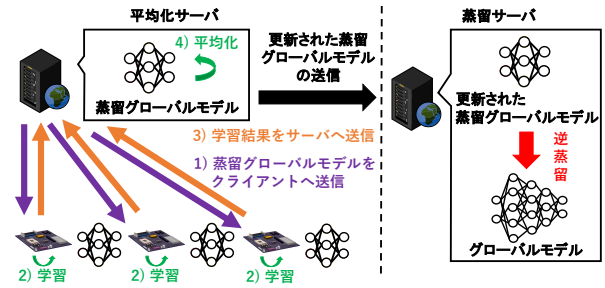


図 1 提案手法の概要

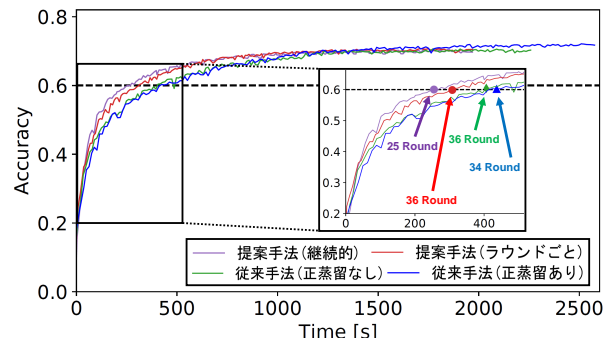


図 2 グローバルモデルの精度評価