Aprendizado Combinado

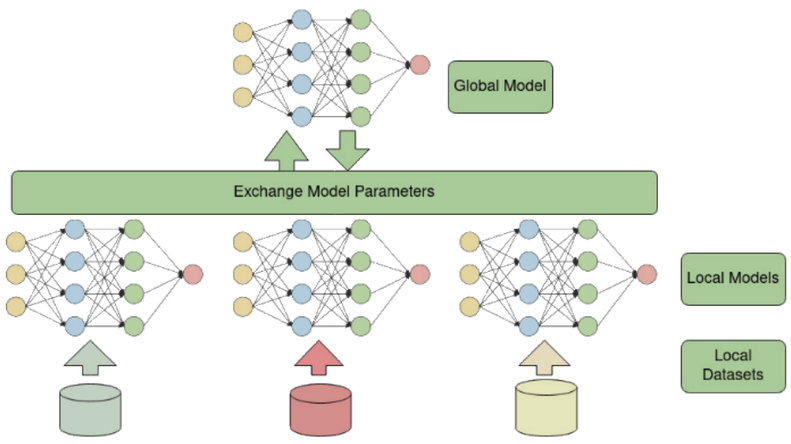
Miguel de Mello Carpi[1], Marcelo Finger[1], Aline Ioste[1]

[1]Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo

Introdução

O aprendizado combinado (coln - do inglês *Combined Learning*) é uma técnica de aprendizado de máquina similar ao aprendizado federado. Assim como no aprendizado federado, o aprendizado combinado busca encontrar um modelo robusto a partir da combinação de modelos de mesma arquitetura treinados em conjuntos de dados diferentes. Em ambos os casos, os clientes não podem compartilhar os dados entre si. Deste modo, uma forma de obter um modelo melhor é por meio da combinação dos parâmetros aprendidos por cada cliente em seu conjunto de dados particular. A Figura 1 ilustra uma arquitetura onde cada modelo aprende com seu conjunto de dados individual antes de se comunicarem com o coordenador.

Figura 1: Arquitetura distribuída.



Fonte: Ioste, A., R. [1]

Objetivos

O objetivo deste trabalho é levantar evidências empíricas de quais situações são favoráveis ao aprendizado combinado. Para isso, são realizados experimentos com redes neurais com arquiteturas convolucionais, recorrentes e multicamadas em três conjuntos de dados diferentes que são MNIST [1], CIFAR-10 [2] e Wisconsin Breast Cancer [3]. O desempenho do aprendizado combinado é também comparado com o desempenho do aprendizado federado nos mesmos cenários.

Uma visão de cima

As peças fundamentais das técnicas de aprendizado combinado e do aprendizado federado são os clientes e o coordenador. Os clientes são os responsáveis por treinarem um modelo de rede neural, decidido previamente, em seus dados locais por um determinado número de épocas e enviar os parâmetros obtidos para o coordenador. O coordenador tem como tarefa combinar os parâmetros recebidos para produzir novos parâmetros que são enviados para os clientes repetirem o treino local. Esse processo é repetido um certo número de vezes ou até o modelo gerado generalizar bem em todos os conjuntos de dados locais. A Figura 4 ilustra para 4 clientes uma iteração da técnica.

Metodologia

São realizados experimentos com redes neurais com arquiteturas convolucionais, recorrentes e multicamadas em três conjuntos de dados diferentes com variação no número de clientes - 2, 5, 10. Uma questão importante levantada em [1] é em relação a distribuição dos dados. Sabe-se que, por exemplo, a distribuição dos dados médicos de hospitais que atendem populações diferentes não é independente e identicamente distribuída (iid), e como os conjuntos de dados utilizados nos testes são balanceados, é necessário selecionar um critério para separar os dados de forma iid e não-iid. A divisão iid consiste em disponibilizar a cada cliente uma versão reduzida do conjunto original, de forma que as distribuições de cada classe a ser classificada seja a mesma em cada um. Já na versão não-iid cada cliente recebe apenas os dados de algumas classes, isto é, há casos que um determinado cliente não tem dados de uma determinada classe. A Figura 2 ilustra a divisão não-iid com o conjunto de dados MNIST e 5 clientes, neste caso cada cliente recebe imagens de apenas 2 dígitos.

Figura 2: Exemplo de Divisão não-iid

[1]http://yann.lecun.com/exdb/mnist/
[2]https://www.cs.toronto.edu/~kriz/cifar.html
[3]https://archive.ics.uci.edu/ml/datasets/breast+cancer+wisconsin+(diagnostic)

Figura 3: Esquema de Arquitetura de rede neural convolucional para classificação de dígitos

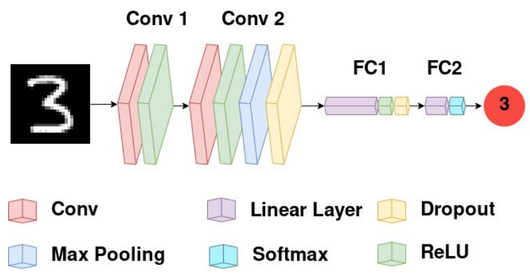
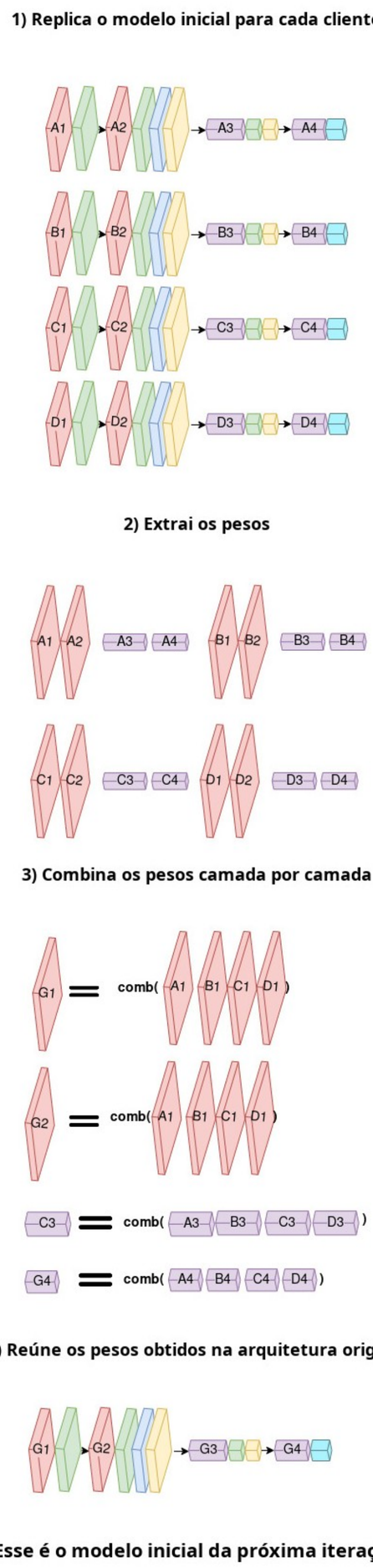


Figura 4: Esquema da combinação de pesos para 4 clientes



Resultados

Os resultados a seguir foram obtidos ao treinar uma rede convolucional com 1.199.882 parâmetros com arquitetura similar a da apresentada na 3. Neles, as linhas tracejadas correspondem a acurácia dos modelos treinados pelos clientes no conjunto de dados completo, enquanto que a linha contínua representa a acurácia do modelo gerado pelo coordenador.

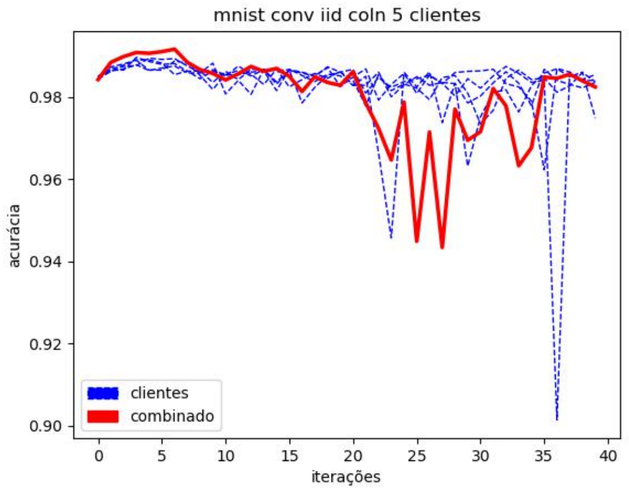


Figura 5: Aprendizado combinado 5 clientes iid

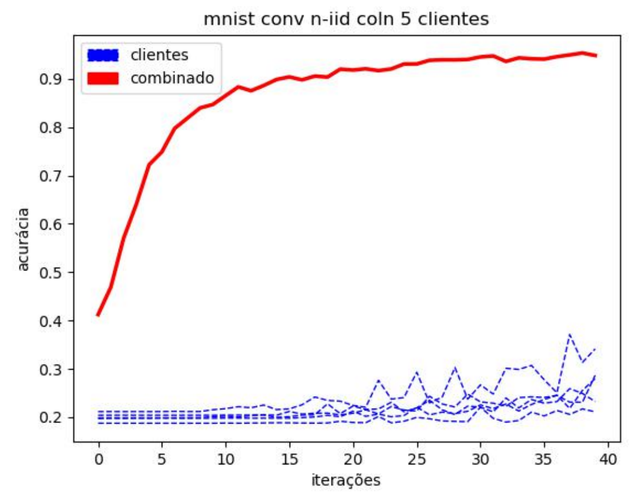


Figura 6: Aprendizado combinado 5 clientes niid

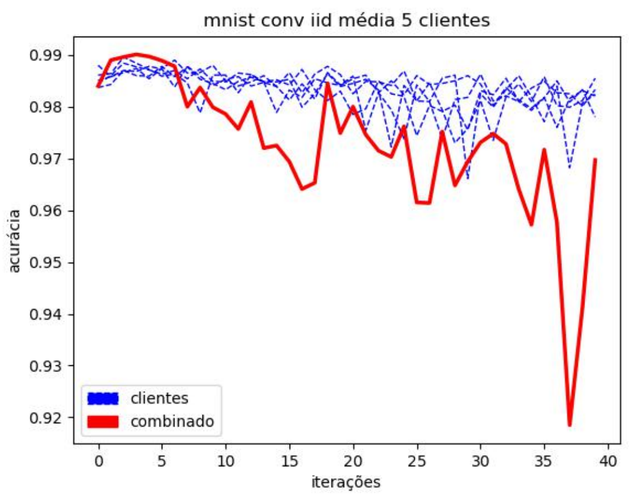


Figura 7: Aprendizado federado 5 clientes iid

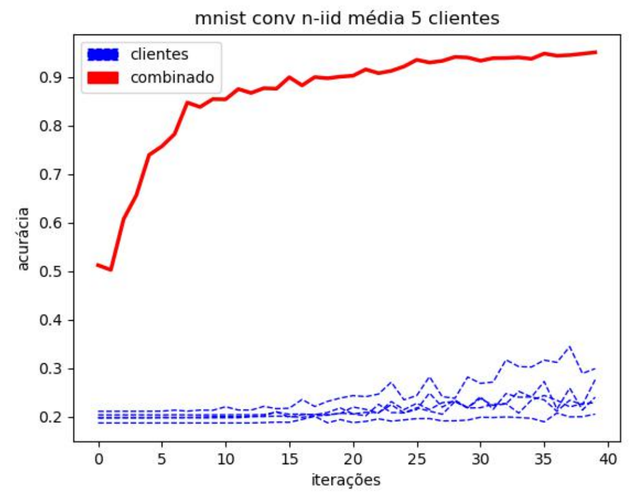


Figura 8: Aprendizado federado 5 clientes niid

Conclusão

Ao comparar os gráficos de acurácia do modelo obtido gerado pelo coordenador, nota-se que a técnica de aprendizado combinado proposta em [1] produz resultados melhores no caso não-iid em relação a técnica mais comum no aprendizado federado (média). Esse resultado não é exclusivo desse tipo de arquitetura e o trabalho final traz resultados para redes recorrentes e multicamadas que fortalecem a hipótese de que essa nova técnica é promissora.

Referências

[1] Ioste, A. R., Finger, M., Establishing the Parameters of a Decentralized Neural Machine Learning Model, 2022, in prep.