Federated Learning

Nguồn tham khảo

* Sahoo J. Federated Learning. Principles, Paradigms, and Applications 2025
* Krishnan S. Handbook on Federated Learning. Advances, App and Opportunities 2024
* Jin Y. Federated Learning. Fundamentals and Advances 2022

I. Tổng quan

1.Giới thiệu

Federated Learning là phương pháp khắc phục những hạn chế của cách học truyền thống. Khác với phương pháp cũ, các máy khách (client) không cần chia sẻ dữ liệu với máy chủ (server). Thay vào đó, họ giữ lại dữ liệu của mình để huấn luyện. Một số tiêu chí để lựa chọn tham gia bao gồm thiết bị thông minh, băng thông, v.v. Thông thường, tất cả máy khách đều có thể tham gia, nhưng cũng có một số ngoại lệ.

Trong kỹ thuật này, các máy khách tham gia vào quá trình học để phát triển mô hình cục bộ (local model), sau đó gửi mô hình này đến máy chủ trung tâm. Máy chủ nhận tất cả các mô hình cục bộ và tổng hợp chúng thành một mô hình chung (global model). Mô hình chung này được gửi lại cho tất cả các máy khách tham gia. Các máy khách cập nhật mô hình của họ dựa trên mô hình chung và gửi lại cho máy chủ để tiếp tục tổng hợp. Quá trình này lặp đi lặp lại cho đến khi thu được một mô hình tốt nhất phù hợp với tất cả dữ liệu.

2.Ví dụ chi tiết

Gọi là vòng lặp cục bộ của máy khách và là vòng lặp tổng hợp mô hình của máy chủ. là tập hợp các mô hình cục bộ do các máy khách phát triển. Cụ thể:

-

-

-

- ...

-

Giả sử có máy khách tham gia. Sau mỗi vòng lặp , máy chủ tổng hợp mô hình bằng công thức:

Mô hình tổng hợp này được sử dụng cho các vòng lặp tiếp theo. Quá trình này tiếp tục cho đến khi đạt được vòng lặp thứ . Mô hình cuối cùng được dùng để cập nhật các mô hình cục bộ, đảm bảo phù hợp với tất cả dữ liệu.

3.Ưu điểm của Federated Learning

- Hỗ trợ ra quyết định với khả năng tái sử dụng rộng rãi – Mô hình học được có thể áp dụng cho nhiều tác vụ khác nhau.

- Bảo vệ dữ liệu người dùng – Thay vì chia sẻ toàn bộ dữ liệu, máy khách chỉ gửi mô hình đã huấn luyện đến máy chủ, giảm nguy cơ rò rỉ thông tin.

4.Nhược điểm của Federated Learning

- Sự khác biệt giữa các thiết bị – Các máy khách có thể có cấu hình phần cứng, hệ điều hành hoặc dữ liệu khác nhau, gây khó khăn trong việc đồng bộ hóa.

- Giới hạn băng thông mạng – Việc truyền tải mô hình giữa máy khách và máy chủ có thể gặp trở ngại nếu đường truyền không ổn định hoặc chậm.

5.Các bước chính trong Federated Learning

a) Huấn luyện mô hình cục bộ – Mỗi máy khách tự đào tạo mô hình bằng dữ liệu riêng của mình.

b) Mã hóa và gửi mô hình lên máy chủ – Máy khách mã hóa mô hình đã huấn luyện để đảm bảo an toàn trước khi gửi đi.

c) Tổng hợp mô hình toàn cục – Máy chủ nhận các mô hình từ máy khách và kết hợp chúng thành một mô hình chung (global model).

d) Phân phối mô hình toàn cục – Máy chủ gửi mô hình tổng hợp về các máy khách để tiếp tục cải thiện trong các vòng lặp tiếp theo.

II.Phân loại

Dựa trên cách lựa chọn mẫu từ tập dữ liệu, Federated Learning được chia thành 3 loại chính:

1. Federated Learning ngang (Horizontal Federated Learning)

2. Federated Learning dọc (Vertical Federated Learning)

3. Federated Learning chuyển giao (Federated Transfer Learning)

Quy ước thuật ngữ

- : Đại diện cho không gian đặc trưng (feature) và nhãn dữ liệu.

- : Không gian nhãn của các máy khách (client).

- : Tập dữ liệu của máy khách.

- : ID không gian mẫu (định danh các mẫu dữ liệu).

- Tập dữ liệu huấn luyện bao gồm:

+) : Các đặc trưng (features).

+) : Nhãn (labels).

+) : Định danh mẫu (sample IDs).

1.Horizontal Federated Learning

- Khái niệm

Trong Horizontal Federated Learning, các máy khách (client) sử dụng các mẫu dữ liệu khác nhau nhưng có cùng đặc trưng (features) để huấn luyện. Cách tiếp cận này còn được gọi là Federated Learning dựa trên mẫu (sample-based federated learning) hoặc Federated Learning đồng nhất (homogeneous federated learning).

- Công thức biểu diễn

* Các máy khách có cùng không gian đặc trưng (features giống nhau).
* : Nhãn dữ liệu (labels) giống nhau.
* : Các mẫu dữ liệu (samples) khác nhau giữa các máy khách.

- Ví dụ

A table with numbers and text

AI-generated content may be incorrect.

Dòng dữ liệu đại diện cho thông tin cá nhân của người dùng, bao gồm tuổi, giới tính, chiều cao, cân nặng và nhãn tương ứng. Tập dữ liệu cục bộ của máy khách 1 và máy khách 2 có cùng không gian đặc trưng, nhưng nhóm người dùng lại khác nhau.

2.Vertical Federated Learning

- Khái niệm

Federated Learning Dọc là phương pháp Federated Learning dựa trên đặc trưng (feature-based). Trong phương pháp này:

* Các máy khách (client) sử dụng cùng một tập mẫu dữ liệu (samples) nhưng với các đặc trưng (features) khác nhau.
* Còn được gọi là Federated Learning dị thể (heterogeneous federated learning).

- Công thức biểu diễn

* : Các máy khách có đặc trưng khác nhau.
* : Nhãn dữ liệu (labels) có thể khác nhau.
* : Cùng tập mẫu dữ liệu (ví dụ: cùng người dùng nhưng dữ liệu từ nhiều nguồn).

- Ví dụ: A table with numbers and text

AI-generated content may be incorrect.

Client 1 và Client 2 cùng có dữ liệu về các cá nhân (Person A, B, C,...) nhưng mỗi bên chỉ lưu trữ một phần thông tin khác nhau:

* Client 1: Giữ nhãn (label) và một số đặc trưng (tuổi, giới tính).
* Client 2: Chỉ giữ các đặc trưng khác (chiều cao, cân nặng) không có nhãn.

3.Federated Transfer Learning

- Khái niệm

Federated Learning Chuyển Giao là phương pháp áp dụng khi:

* Các mẫu dữ liệu có ID khác nhau (khác đối tượng)
* Đặc trưng dữ liệu khác nhau (khác thuộc tính)

Phương pháp này có một số điểm tương đồng với Federated Learning Dọc nhưng khác biệt trong cách tính toán gradient.

- Công thức biểu diễn

* : Các máy khách có đặc trưng hoàn toàn khác nhau.
* : Nhãn dữ liệu khác nhau.
* : Mẫu dữ liệu từ các đối tượng khác nhau.

- Ví dụ minh họa

Một ngân hàng ở Anh và một công ty chứng khoán ở Trung Quốc có dữ liệu khách hàng khác nhau về dịch vụ và đối tượng, nhưng muốn hợp tác xây dựng mô hình AI chung mà không chia sẻ dữ liệu gốc.

III.Các thành phần của Federated Learning

Có 5 thành phần chính trong Federated Learning:

* Máy khách (Client)
* Máy chủ trung tâm (Central server)
* Fetching global model
* Local model training
* Model aggregation

1. Máy khách (Client)

Trong Federated Learning (federated learning), máy khách là một thiết bị chứa tập dữ liệu đã được xử lý. Điểm đặc biệt là các máy khách không cần gửi tập dữ liệu thô lên máy chủ.

Thay vào đó, mỗi máy khách sẽ tự xây dựng một mô hình cục bộ (local model) từ chính tập dữ liệu của mình. Do đó, các mô hình này sẽ khác nhau giữa các máy khách.

2. Máy chủ trung tâm (Central Server)

Máy chủ trung tâm là một trong những thành phần chính của Federated Learning. Mô hình cục bộ do máy khách phát triển không thể áp dụng chung cho tất cả các tập dữ liệu, do có sự khác biệt về mẫu dữ liệu giữa các máy khách.

Nhiệm vụ của máy chủ trung tâm là tạo ra một mô hình thống nhất có thể áp dụng cho tất cả. Điều này được thực hiện bằng cách tổng hợp tất cả các mô hình cục bộ nhận được từ các máy khách, từ đó xây dựng nên một mô hình toàn cục (global model).

3. Thu nhận mô hình toàn cục (Fetching Global Model)

Các máy khách tham gia huấn luyện duy trì trạng thái hoạt động và lưu giữ mô hình cục bộ đã được đào tạo. Mô hình toàn cục là kết quả được máy chủ trung tâm tạo ra thông qua việc tổng hợp các mô hình cục bộ  từ các máy khách. Sau đó, mô hình toàn cục này sẽ được gửi ngược lại cho các máy khách để họ cập nhật mô hình của mình.

4. Huấn luyện mô hình cục bộ (Local Model Training)

Quá trình huấn luyện mô hình cục bộ diễn ra phía máy khách. Mỗi máy khách duy trì tập dữ liệu riêng để huấn luyện. Việc lựa chọn mẫu dữ liệu đã được thảo luận ở phần trước. Do các máy khách sử dụng tập dữ liệu khác nhau nên các mô hình họ phát triển cũng khác biệt. Những mô hình này không thể áp dụng chung cho mọi tập dữ liệu.

Để giải quyết vấn đề này, chúng tôi sử dụng mô hình toàn cục M = M - kết quả tổng hợp từ các mô hình cục bộ. Trong quá trình huấn luyện cục bộ, gradient được tính toán bằng công thức:

Trong đó:

* : số hiệu batch (batch number)
* : định danh máy khách

Sau khi huấn luyện, các mô hình  được gửi đến máy chủ để tổng hợp.

5. Tổng hợp mô hình (Model Aggregation)

Tổng hợp mô hình là một quy trình quan trọng được thực hiện bởi máy chủ trung tâm. Máy chủ sẽ tạo ra một mô hình tổng hợp (gọi là mô hình toàn cục) từ các mô hình cục bộ  nhận được từ các máy khách. Mô hình toàn cục này đóng vai trò là phiên bản cập nhật dùng chung cho tất cả các máy khách đã tham gia quá trình huấn luyện.

IV.Kỹ thuật tổng hợp mô hình (Model Aggregation)  
Kỹ thuật tổng hợp được thực hiện bằng cách tính trung bình các hệ số (coefficients) của mô hình mạng nơ-ron từ các máy khách. Trong Federated Learning, kỹ thuật này giúp:

* Cập nhật mô hình cục bộ trên từng thiết bị.
* Máy chủ trung tâm đóng vai trò tổng hợp và phân phối lại mô hình toàn cục.

**Thuật toán 1: Huấn luyện Cục bộ trong Federated Learning**

A screenshot of a computer

AI-generated content may be incorrect.

Thuật toán này mô tả quy trình huấn luyện mô hình mạng nơ-ron (Neural Network - NN) ở phía các máy khách (clients) trong một hệ thống Federated Learning. Mục tiêu là để mỗi máy khách tận dụng dữ liệu cục bộ của mình để cập nhật mô hình, sau đó gửi các cập nhật này về máy chủ trung tâm để tổng hợp.

Ký hiệu:

* : Tổng số lượng máy khách tham gia vào quá trình huấn luyện.
* : Chỉ số của một máy khách cụ thể ().
* : Kích thước của mini-batch, là kích thước của các phần nhỏ dữ liệu được sử dụng trong mỗi bước cập nhật gradient.
* : Số lượng local epochs, là số lần mỗi máy khách lặp lại việc huấn luyện trên toàn bộ dữ liệu cục bộ của mình.
* ​: Tập dữ liệu được phân bổ cho máy khách thứ .
* : Mô hình cục bộ của máy khách thứ . Tập hợp tất cả các mô hình cục bộ được ký hiệu là .
* : Tốc độ học (learning rate), một siêu tham số quyết định độ lớn của bước cập nhật trọng số trong quá trình tối ưu hóa.

Đầu vào:

* Mô hình toàn cầu hoặc mô hình cập nhật từ máy chủ trung tâm, ký hiệu là . Đây là mô hình ban đầu hoặc mô hình đã được tổng hợp từ các vòng huấn luyện trước đó, được phân phối cho các máy khách.

Đầu ra:

* Mô hình đã được huấn luyện cục bộ của máy khách thứ sau local epochs, ký hiệu là .

Các bước thực hiện:

1. Phân phối Mô hình (Bước 1-3):
   * Máy chủ trung tâm gửi mô hình hiện tại () đến máy khách thứ .
   * Máy khách thứ có thể thực hiện một bước cập nhật cục bộ ban đầu dựa trên mô hình nhận được ().
2. Chuẩn bị Dữ liệu (Bước 4):
   * Máy khách thứ chia tập dữ liệu cục bộ của mình (​) thành các mini-batch có kích thước . Ký hiệu đại diện cho một mini-batch.
3. Huấn luyện Cục bộ (Bước 5):
   * Máy khách thứ thực hiện một vòng lặp qua local epochs.
   * Trong mỗi local epoch (từ đến ):
     + Máy khách lặp qua tất cả các mini-batch trong ​.
     + Đối với mỗi mini-batch , máy khách cập nhật mô hình cục bộ của mình ( hoặc các trọng số ). Quá trình cập nhật thường sử dụng thuật toán gradient descent. Các công thức và biểu thị việc cập nhật mô hình dựa trên gradient của hàm mất mát tính trên mini-batch , nhân với tốc độ học . và đại diện cho gradient (đạo hàm) của hàm mất mát theo các tham số của mô hình.
4. Kết thúc Huấn luyện Cục bộ (Bước 6): Sau khi hoàn thành local epochs, quá trình huấn luyện cục bộ trên máy khách kết thúc.
5. Gửi Mô hình Đã Huấn luyện (Bước 7): Máy khách thứ gửi mô hình đã được huấn luyện cục bộ () trở lại máy chủ trung tâm.

1. ALL MODEL AVERAGING (AMA) - Trung bình Cộng Tất cả Mô hình

Kỹ thuật AMA là một phương pháp cơ bản và phổ biến trong Federated Learning để tổng hợp các mô hình được huấn luyện cục bộ từ nhiều máy khách. Ý tưởng cốt lõi của AMA là lấy trung bình các hệ số (trọng số) tương ứng của tất cả các mô hình cục bộ để tạo ra một mô hình toàn cầu duy nhất.

Quy trình thực hiện:

1. Huấn luyện Cục bộ: Trong giai đoạn huấn luyện, mỗi máy khách sử dụng Thuật toán 1 (đã được mô tả trước đó) để phát triển mô hình cục bộ của riêng mình dựa trên dữ liệu cục bộ của họ. Sau khi hoàn thành quá trình huấn luyện cục bộ, mỗi máy khách sẽ gửi mô hình đã được huấn luyện này đến máy chủ trung tâm.
2. Tổng hợp tại Máy chủ Trung tâm: Khi máy chủ trung tâm nhận được các mô hình cục bộ từ tất cả các máy khách tham gia, nó sẽ tiến hành quá trình tổng hợp bằng cách sử dụng Thuật toán 2 (cũng đã được mô tả). Thuật toán này thực hiện việc tính tổng và sau đó lấy trung bình các trọng số tương ứng của các nơ-ron trong các mô hình cục bộ.
3. Tạo Mô hình Tổng hợp: Kết quả của quá trình tổng hợp là một mô hình toàn cầu được gọi là mô hình tổng hợp (aggregate model). Mô hình này chứa các trọng số là giá trị trung bình của các trọng số tương ứng từ tất cả các mô hình cục bộ.
4. Phân phối Mô hình Tổng hợp: Mô hình tổng hợp này sau đó được gửi trả lại cho các máy khách đã tham gia vào quá trình huấn luyện.
5. Cập nhật Mô hình Cục bộ: Các máy khách sẽ sử dụng mô hình tổng hợp nhận được để cập nhật mô hình cục bộ của họ. Quá trình này thường là bước khởi đầu cho vòng huấn luyện liên kết tiếp theo, giúp các mô hình cục bộ tiếp tục học hỏi dựa trên kiến thức tổng hợp từ toàn bộ hệ thống.

Công thức toán học:

Giải thích công thức:

* : Đại diện cho mô hình tổng hợp cuối cùng được tạo ra.
* : Ký hiệu cho thao tác tổng hợp bằng phương pháp trung bình cộng tất cả mô hình.
* : Tổng số lượng mô hình cục bộ (từ n máy khách).
* : Số lượng nơ-ron trong mỗi lớp của mô hình.
* : Chỉ số của lớp trong mô hình.
* : Chỉ số của nơ-ron trong lớp i.
* ​: Trọng số của nơ-ron thứ ở lớp thứ trong mô hình cục bộ của máy khách thứ .
* Công thức này thực hiện việc tính tổng tất cả các trọng số tương ứng (cùng vị trí nơ-ron và lớp) từ tất cả mô hình cục bộ, và sau đó chia cho tổng số mô hình () để lấy giá trị trung bình. Giá trị trung bình này sẽ trở thành trọng số tương ứng trong mô hình tổng hợp .

**Thuật toán 2: Tổng hợp Mô hình (Average of Model Aggregation - AMA)**

A screenshot of a white sheet of paper

AI-generated content may be incorrect.

Thuật toán này mô tả quy trình tổng hợp các mô hình đã được huấn luyện cục bộ từ các máy khách để tạo ra một mô hình toàn cầu được cập nhật. Trong nghiên cứu này, máy chủ trung tâm nhận được mô hình đã huấn luyện từ bốn máy khách, ký hiệu là , trong đó ​ là mô hình đã được huấn luyện của máy khách thứ .

Ký hiệu:

* : Cấu trúc của mô hình toàn cầu, với đại diện cho các trọng số của mô hình.
* : Tập hợp các mô hình đã được huấn luyện từ máy khách.
* : Số lượng mô hình cục bộ được sử dụng để tổng hợp.
* ​: Trọng số thứ ở lớp thứ của mô hình ​ (mô hình thứ trong danh sách các mô hình cục bộ).
* : Số lượng lớp trong mô hình mạng nơ-ron.
* : Số lượng nơ-ron (hoặc tham số) trong mỗi lớp (chúng ta giả định rằng tất cả các mô hình cục bộ đều có cấu trúc giống nhau).
* : Giá trị trung bình của các trọng số tương ứng từ tất cả các mô hình cục bộ.
* : Mô hình toàn cầu đã được tổng hợp hoặc cập nhật.

Đầu vào:

* Các mô hình đã được huấn luyện từ các máy khách: .

Đầu ra:

* Mô hình toàn cầu đã được tổng hợp hoặc cập nhật: .

Các bước thực hiện:

1. Nhận Mô hình Cục bộ (Bước 1): Máy chủ trung tâm nhận được các mô hình đã được huấn luyện từ tất cả các máy khách tham gia.
2. Tạo Danh sách Mô hình (Bước 2): Máy chủ tạo một danh sách chứa tất cả các mô hình cục bộ đã nhận được: .
3. Xác định Số Lượng Mô hình (Bước 3): Máy chủ xác định tổng số mô hình cục bộ sẽ được sử dụng để tổng hợp.
4. Tiến hành Tổng hợp (Bước 4):
   * Máy chủ lặp qua tất cả các lớp của mô hình (với chỉ số từ đến ).
   * Đối với mỗi lớp, máy chủ lặp qua tất cả các nơ-ron (hoặc tham số) trong lớp đó (với chỉ số từ đến ).
   * Đối với mỗi vị trí trọng số (), máy chủ tính giá trị trung bình của các trọng số tương ứng từ tất cả các mô hình cục bộ:
   * Sau đó, máy chủ tính giá trị trung bình của các trọng số này bằng cách chia tổng cho số lượng mô hình ():

Giá trị trung bình này sẽ trở thành trọng số mới cho vị trí () trong mô hình toàn cầu được cập nhật.

1. Kết thúc Tổng hợp (Bước 5): Sau khi lặp qua tất cả các lớp và tất cả các trọng số trong mỗi lớp, mô hình toàn cầu đã được tổng hợp hoàn chỉnh.
2. Gửi Mô hình Toàn cầu (Bước 6): Máy chủ trung tâm gửi mô hình toàn cầu đã được tổng hợp trở lại cho các máy khách để họ sử dụng trong vòng huấn luyện tiếp theo.

2. ONE MODEL SELECTION (OMS) - Lựa chọn Một Mô hình

Kỹ thuật OMS là một phương pháp tổng hợp mô hình trong Federated Learning dựa trên hiệu suất của các mô hình cục bộ. Thay vì kết hợp thông tin từ tất cả các mô hình, OMS chọn ra duy nhất một mô hình có hiệu suất tốt nhất để làm mô hình toàn cầu hoặc để phân phối cho vòng huấn luyện tiếp theo.

Quy trình thực hiện:

1. Huấn luyện Cục bộ: Tương tự như AMA, trong giai đoạn huấn luyện, mỗi máy khách phát triển mô hình cục bộ của riêng mình.
2. Gửi Mô hình và Hiệu suất: Điểm khác biệt quan trọng của OMS là khi các máy khách gửi mô hình đã được huấn luyện đến máy chủ trung tâm, họ cũng gửi kèm theo thông tin về hiệu suất của mô hình đó. Hiệu suất này thường được đo bằng độ chính xác (accuracy) trên một tập dữ liệu cục bộ hoặc một tập dữ liệu kiểm tra chung nhỏ mà máy khách có thể truy cập.
3. Lựa chọn Mô hình Tốt nhất: Máy chủ trung tâm sẽ so sánh hiệu suất của tất cả các mô hình cục bộ nhận được. Dựa trên tiêu chí hiệu suất (thường là độ chính xác cao nhất), máy chủ sẽ chọn ra mô hình có hiệu suất tốt nhất trong số đó.
4. Sử dụng Mô hình Được Chọn: Mô hình được chọn sẽ được coi là mô hình toàn cầu (global model) cho vòng liên kết hiện tại.
5. Phân phối Mô hình Toàn cầu: Mô hình toàn cầu được chọn sẽ được gửi trở lại cho các máy khách để họ sử dụng làm điểm khởi đầu để huấn luyện mô hình cục bộ của mình trong vòng tiếp theo.

**Thuật toán 3: Tổng hợp Mô hình (Model Aggregation - OMS - One Model Selection)**

A screenshot of a computer

AI-generated content may be incorrect.

Thuật toán này mô tả quy trình tổng hợp các mô hình đã được huấn luyện cục bộ từ các máy khách bằng cách chọn ra một mô hình duy nhất được coi là tốt nhất dựa trên hiệu suất của nó. Trong nghiên cứu này, máy chủ trung tâm nhận được mô hình đã huấn luyện từ bốn máy khách, ký hiệu là .

Ký hiệu:

* : Cấu trúc của mô hình toàn cầu, với đại diện cho các trọng số của mô hình.
* : Tập hợp các mô hình đã được huấn luyện từ n máy khách.
* : Độ chính xác (accuracy) hoặc một số chỉ số đánh giá hiệu suất khác của mô hình ​ (mô hình của máy khách thứ ) trên một tập dữ liệu nào đó (có thể là tập kiểm tra cục bộ hoặc một tập kiểm tra chung nhỏ mà máy chủ có).
* : Danh sách chứa các giá trị hiệu suất của tất cả các mô hình cục bộ.
* : Hàm trả về giá trị lớn nhất trong danh sách , tức là độ chính xác cao nhất trong số các mô hình cục bộ.
* : Mô hình toàn cầu được chọn.

Đầu vào:

* Các mô hình đã được huấn luyện từ các máy khách: .

Đầu ra:

* Mô hình toàn cầu được chọn: , đây chính là mô hình cục bộ có hiệu suất tốt nhất.

Các bước thực hiện:

1. Nhận Mô hình Cục bộ (Implicit): Máy chủ trung tâm nhận được các mô hình đã được huấn luyện từ tất cả các máy khách tham gia.
2. Thu thập Hiệu suất Mô hình (Bước 2): Máy chủ thu thập hoặc tính toán hiệu suất của từng mô hình cục bộ. Các giá trị hiệu suất này được lưu trữ trong danh sách .
3. Lựa chọn Mô hình Tốt nhất (Bước 3): Máy chủ tìm ra mô hình có hiệu suất cao nhất bằng cách xác định giá trị lớn nhất trong danh sách . Giả sử ​ là giá trị lớn nhất trong , thì mô hình ​ sẽ được chọn làm mô hình toàn cầu.
4. Gửi Mô hình Toàn cầu (Bước 4): Máy chủ trung tâm gửi mô hình toàn cầu đã được chọn (chính là mô hình của một trong các máy khách) trở lại cho các máy khách để họ sử dụng trong vòng huấn luyện tiếp theo.

3. BEST MODEL AVERAGE (BMA) - Trung bình Cộng các Mô hình Tốt nhất

Kỹ thuật BMA tính toán trung bình của các mô hình được coi là "tốt nhất" trong số các mô hình cục bộ được huấn luyện bởi các máy khách.

Quy trình thực hiện:

1. Huấn luyện Cục bộ: Tương tự như AMA và OMS, mỗi máy khách huấn luyện mô hình cục bộ của riêng mình.
2. Gửi Mô hình và Hiệu suất: Các máy khách không chỉ gửi mô hình đã huấn luyện mà còn gửi kèm theo thông tin về hiệu suất mô hình (thường là độ chính xác) cho máy chủ trung tâm.
3. Lựa chọn Các Mô hình Tốt nhất: Máy chủ trung tâm sẽ sử dụng thông tin về hiệu suất để sắp xếp các mô hình cục bộ theo thứ tự hiệu suất (ví dụ: từ cao đến thấp). Sau đó, máy chủ sẽ chọn ra một số lượng nhất định các mô hình có hiệu suất cao nhất để tiến hành tổng hợp.
4. Tính Trung bình: Quá trình tính trung bình các trọng số của các mô hình tốt nhất được chọn tương tự như kỹ thuật AMA. Máy chủ sẽ lấy trung bình các trọng số tương ứng của các nơ-ron trong các mô hình tốt nhất này để tạo ra mô hình toàn cầu.
5. Phân phối Mô hình Toàn cầu: Mô hình toàn cầu được tạo ra bằng cách lấy trung bình các mô hình tốt nhất sẽ được gửi trở lại cho các máy khách để cập nhật mô hình cục bộ của họ.

Công thức toán học:

Giải thích công thức :

* : Mô hình tổng hợp được tạo ra bằng kỹ thuật BMA.
* : Ký hiệu cho thao tác tổng hợp bằng phương pháp trung bình cộng các mô hình tốt nhất.
* : Tổng số lượng mô hình cục bộ.
* : Số lượng nơ-ron trong mỗi lớp.
* : Chỉ số của lớp.
* : Chỉ số của nơ-ron trong lớp .
* ​: Trọng số của nơ-ron thứ ở lớp thứ trong một trong các mô hình được chọn là "tốt nhất".
* : Số lượng mô hình tốt nhất được chọn để tính trung bình.

**Thuật toán 4: Tổng hợp Mô hình BMA**

A white paper with black text

AI-generated content may be incorrect.

Thuật toán này mô tả một phương pháp tổng hợp các mô hình đã được huấn luyện cục bộ từ các máy khách bằng cách lấy trung bình của một phần các mô hình "tốt nhất" sau khi đã sắp xếp chúng. Trong nghiên cứu này, máy chủ trung tâm nhận được mô hình đã huấn luyện từ bốn máy khách, ký hiệu là .

Ký hiệu:

* : Cấu trúc của mô hình toàn cầu, với đại diện cho các trọng số của mô hình.
* : Tập hợp các mô hình đã được huấn luyện từ n máy khách.
* : Một danh sách chứa các mô hình cục bộ, được sắp xếp dựa trên hiệu suất của chúng (ví dụ: độ chính xác).
* : Số lượng mô hình cục bộ được sử dụng để tổng hợp.
* : Số lượng mô hình tốt nhất được chọn để tính trung bình.
* ​: Trọng số thứ ở lớp thứ của mô hình (Mô hình thứ trong danh sách đã sắp xếp ).
* : Số lượng lớp trong mô hình mạng nơ-ron.
* : Số lượng nơ-ron trong mỗi lớp (giả định rằng tất cả các mô hình cục bộ đều có cấu trúc giống nhau).
* : Trọng số thứ ở lớp thứcủa mô hình toàn cầu được cập nhật.
* : Mô hình toàn cầu đã được tổng hợp hoặc cập nhật.

Đầu vào:

* Các mô hình đã được huấn luyện từ các máy khách: .

Đầu ra:

* Mô hình toàn cầu đã được tổng hợp hoặc cập nhật: .

Các bước thực hiện:

1. Nhận Mô hình Cục bộ (Implicit): Máy chủ trung tâm nhận được các mô hình đã được huấn luyện từ tất cả các máy khách tham gia.
2. Sắp xếp Mô hình (Bước 2): Máy chủ sắp xếp các mô hình cục bộ trong danh sách A dựa trên hiệu suất của chúng (ví dụ: độ chính xác giảm dần).
3. Xác định Số Lượng Mô hình Tốt Nhất (Bước 3 & 4): Máy chủ xác định số lượng mô hình "tốt nhất" để lấy trung bình, . Điều này có nghĩa là nếu có n mô hình, thuật toán sẽ chọn lấy trung bình của mô hình có hiệu suất cao nhất.
4. Tiến hành Tổng hợp (Bước 5):
   * Máy chủ lặp qua tất cả các lớp của mô hình (với chỉ số từ đến ).
   * Đối với mỗi lớp, máy chủ lặp qua tất cả các nơ-ron trong lớp đó (với chỉ số từ đến ).
   * Đối với mỗi vị trí trọng số (i,j), máy chủ tính giá trị trung bình của các trọng số tương ứng từ k mô hình "tốt nhất" trong danh sách đã sắp xếp A:

Trong đó đến là mô hình đầu tiên (tốt nhất) trong danh sách đã sắp xếp .

1. Kết thúc Tổng hợp (Bước 6): Sau khi lặp qua tất cả các lớp và tất cả các trọng số trong mỗi lớp, mô hình toàn cầu đã được tổng hợp hoàn chỉnh.
2. Gửi Mô hình Toàn cầu (Bước 7): Máy chủ trung tâm gửi mô hình toàn cầu đã được tổng hợp trở lại cho các máy khách để họ sử dụng trong vòng huấn luyện tiếp theo.