협업필터링을 위한 Variational 오토인코더의 연합학습 방법

김유준○ 홍충선*
경희대학교 컴퓨터공학과
{yj4889○, cshong*}@khu.ac.kr

A Federated Learning Method of Variational Autoencoders for Collaborative Filtering

Youjun Kim○, ChoongSeon Hong*
Department of Computer Science and Engineering, Kyung Hee University

요 약

Collaborative Filtering(CF)은 사용자들의 선호도 유사성을 분석하여 사용자의 선호도를 예측 및 추천하는 방법이다. Artificial Intelligent(AI) 이전에는 행렬분해(Matrix Factorization)기법을 사용하여 CF문제를 해결하는 연구가 많이 진행되었으나 최근 AI의 발전으로 CF문제를 딥 러닝으로 접근하려는 시도가 굉장히 많아졌다. 특히 Variational Autoencoders(VAE)는 CF문제에 효과적으로 접근하여 좋은 성능을 내고 있다. 하지만 VAE를 학습시키려면 사용자들의 해당 컨텐츠(Contents)에 대한 선호도 데이터가 있어야한다. 선호도 데이터는 사용자의 자발적인 참여로 생성되기 때문에 생산적이 측면에서 굉장히 비효율적이다. 또한 AI의 예측 및 알고리즘의 사용자 감정분석을 통한 선호도 예측 데이터는 프라이버시(privacy)에 굉장히 민감하게 된다. 이에 본 논문은 사용자의 프라이버시를 완벽히 보존하면서 VAEs를 학습시키는 연합학습(Federated Learning)방법을 설명한다. 또한 사용자, 엣지(edge), 중앙서버 모두가 학습에 참여하는 이 방법이 선호도 데이터 특성상 기존 연합학습 방법이 학습시키지 못하는 VAE를 효과적으로 학습시킬 수 있다는 것을 설명함과 동시에 효율적인 연합학습 방법을 추가로 제시한다.

1. 서 론

최근 딥 러닝을 주축으로 AI가 놀라운 성장을 이루어내고 있다. 특히 기존 추천 시스템에서 사용되던 행렬분해(Matrix Factorization)기법[1]을 VAE(Variational Autoencoders) 라는 딥 러닝 기법으로 대체한 결과 사용자의 선호도 예측 및 추천 성능이 월등히 높아졌다[2]. 이 딥 러닝을 학습하려면 기존에는 중앙 서버에서 사용자들이 직접 매긴 선호도(예를 들어 1 ~ 5점)를 수집하고 중앙에서 학습이 이루어지게 된다. 이러한 학습방법은 사용자가 아무런 대가 없이 자발적으로 소비한 컨텐츠(contents)에 대해 선호도를 매겨야 한다. 대부분의 사용자들은 컨텐츠를 소비만 할 뿐 선호도를 매기지 않는다. 이는 데이터 생산의 한계를 나타내며 동시에 가능성을 나타낸다. 만약 음성인식, 글자인식 및 영상 인식을 통해 사용자가 소비한 컨텐츠에 대한 사용자의 선호도를 예측할 수 있다면, 또한 프라이버시(privacy)에 굉장히 민감한 예측정보의 유출 없이 딥 러닝을 학습 시킬 수 있다면 사용자의 프라이버시를 보존하면서 무한한 데이터의 학습이 가능할 것이다.

이에 본 논문에서는 사용자의 프라이버시(privacy)를 보존하면서 UAV, Base station등 과 같은 엣지(edge)에서 딥 러닝 학습이 행해지고 중앙 서버에서 통합하는 연합학습(federated learning) 기반의 VAE를 제시한다. 이는 기존의 클라우드(cloud) 중심의 학습방법이 아닌 사용자, 엣지, 클라우드가 모두 참여하는 학습 방법이다.

사용자 선호도 예측을 위한 VAE의 input 데이터는 각 사용자의 컨텐츠 선호도로써 각사용자가 보유한 데이터 개수는 한 개이다. 사용자의 데이터가 한 개이기 때문에 기존의 연합학습 방법은 VAE를 제대로 학습 시킬 수 없다. 그래서 본 논문에서는 VAE 학습을 위한 연합학습 방법론에 대해 설명한다.

2. 관련 연구

2.1 연합학습

연합학습은 사용자 데이터 유출 없이 딥 러닝 모델을 학습시킬 수 있는 방법이다. 중앙 서버에서 딥 러닝 모델을 사용자 단말에 보내고 사용자 단말에서는 자신의 데이터로 모델을 학습시킨다. 이후 각 사용자 단말에서 학습된 모델은 중앙에서 통합된다. 다음 식은 통합모델에 대한 식이다[3].

$$w_{t+1} \leftarrow \sum_{n=1}^{N} \left(\frac{a_n}{a}\right) w_{t+1}^{n} \qquad ①$$

다음의 조건은 연합학습에 큰 영향을 미친다.

(1) **Non-IID** : 사용자들은 모집단을 대표하지 않기 때문에 자신만의 고유 데이터를 보유하고 있다.

(2) **데이터의 대량 분포** : 학습에 참여하는 모든 사용자들의 데이터는 각 사용자가 가지고 있는 데이터의 평균보다 훨씬 많다.

(3) **불균형** : 각 사용자가 보유한 데이터의 양 차이는 엄청나다.

(4) 제한된 통신 환경 : 학습 참여자들의 통신환경에 따라 통신이 끊기거나 느려질 수 있다.

[3]에서는 변수 $(0 \le C \le 1)$를 이용하여 연합학습 한번 실행 시 $\text{전체사용자} * C$ 만큼의 사용자만이 학습에 참여하도록 하였다. 예로 들어 전체 사용자는 5명이고 $C = 0.4$라면 연합학습에 한번에 2명의 사용자가 학습에 참여하게 된다. 그리고 ①에 의해 모든 사용자(파란 점)의 모델들이 통합되게 된다. 이는 전체사용자의 수가 참여사용자의 수보다 많을수록 학습이 느려진다.

[4]은 Non-IID와 데이터의 대량분포, 불균형을 고려하여 연합학습을 시행하였다. 그리고 모델 통합과정에서 최근에 학습된 모델일수록 더 큰 가중치를 더해줌으로써 (그림 1에 4번째 연합학습에 참여한 사용자 3, 5가 가장 큰 가중치를 가짐) 빠른 정확도 수렴이 가능하도록 하는 방식을 사용하였다. 하지만 이 방법은 모델의 과 적합(overfitting)위험이 굉장히 크다.

2.2 Variational Autoencoders

VAE는 최근 협업필터링에서 사용되는 딥러닝 기법중 하나이다. 이 딥 러닝은 인풋 데이터의 평균과 분산을 이용하고 노이즈를 더해줌으로써 사용자들의 연관성을 모델이 학습하고 모델의 아웃풋은 사용자의 컨텐츠 선호도가 된다. 다음의 식은 VAE의 손실함수로써 [2]은 B라는 어닐링(annealing) 변수를 추가하여 정확도를 높였다.

$$L(x_u;\theta,\Phi) \equiv E_{q_\phi(z_u|x_u)}[\log p_\theta(x_u|z_u)] - B \bullet KL(q_\phi(z_u|x_u)\|p(z_u) \qquad ②$$

2.3 연합학습기반 협업필터링

[5]은 하이브리드 필터링(hybrid filtering)을 위해 오토인코더를 연합학습 기반으로 학습시켜 컨텐츠 캐싱의 효율을 높이는 연구를 하였다. 하지만 이 논문은 연합학습 방법에 대한 정확한 설명이 없고 데이터가 중앙 서버에서도 학습되어 완벽한 프라이버시 보존이 불가능하다.

3. 제안사항

그림 1은 VAE 모델을 연합학습 기법으로 학습하는 과정을 보여준다. 중앙 서버, 에지, 사용자가 모두 참여하는 학습 과정으로써 사용자단말의 데이터는 유출되지 않는다. 에지는 컴퓨팅 능력을 가지고 사용자 근처에 존재하며 무인항공기, 기지국 등이 될 수 있다. VAE의 인풋 데이터이자 각 사용자의 데이터 개수는 1개이다.

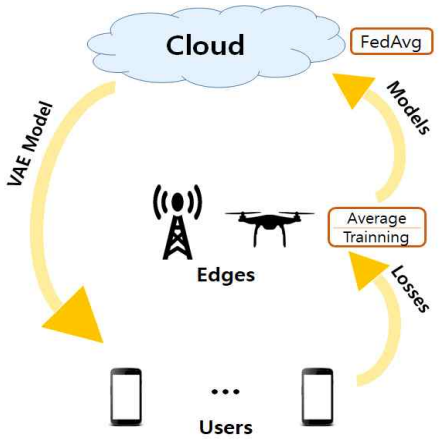

그림 1. System Model

그렇기 때문에 뉴럴 네트워크의 weights를 통합하는 일반적인 연합학습 방법으로는 VAE를 학습시킬 수 없다. 따라서 사용자 단말로 전송된 VAE 모델은 사용자 데이터를 통해 손실을 계산(식 ②)하고 각 사용자 단말에서 계산된 손실은 에지에서 평균이 계산된다. 계산된 평균은 중앙 서버에 전달되고 중앙에서 ①에 의해 통합된다. 이러한 과정을 통해 VAE 모델은 사용자 데이터 유출 없이 학습이 가능하여 사용자의 프라이버시를 보존할 수 있다. 본 논문은 제시된 VAE를 위한 연합학습 방법에 추가 전략을 더 제시한다.

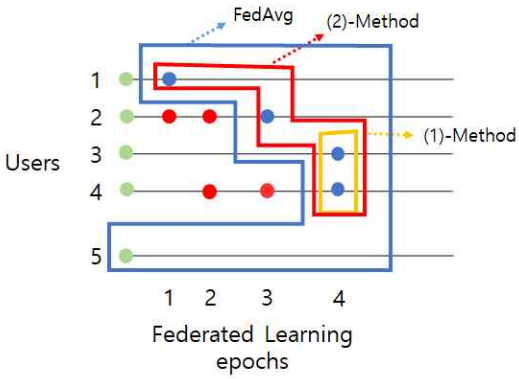

그림 2. 연합학습과 제시된 방법들의 학습과정

그림 2의 초록색 점은 에지들이 받은 초기 모델들이며 빨간 점은 과거 학습된 모델들이고 파란 점은 가장 최근에 학습된 모델들이다. 전통적인 연합학습은 모든 모델을 통합하며(FedAvg) (1), (2) 방법은 아래에 설명한다.

(1) 현재 학습에 참여한 에지의 모델만을 통합

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2015-0-00557, IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술 연구) 또한 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-01287, 분산 엣지를 위한 진화형 딥러닝 모델생성 플랫폼). *Dr. CS Hong is the corresponding author

$$w_{t+1} \leftarrow \sum_{n=1}^{N} P(\frac{a_n}{a}) w_{t+1}^{n} \quad ③$$

$$P = \begin{matrix} 1 & (n = current_{FL}) \\ 0 & (n \neq current_{FL}) \end{matrix}$$

(2) 과거에 학습에 참여를 한 이력이 있는 엣지의 모델과 현재 학습에 참여한 엣지의 모델을 통합

$$w_{t+1} \leftarrow \sum_{n=1}^{N} P(\frac{a_n}{a}) w_{t+1}^{n} \quad ④$$

$$P = \begin{matrix} 1 & (n \neq hasNeverParticipated) \\ 0 & (n = hasNeverParticipated) \end{matrix}$$

4. 성능평가

본 논문에서는 MovieLens 20M Dataset을 사용하였다. 엣지의 개수는 100개이다. 각 에지들은 서로 다른 수의 사용자들과 연결되어 있다. 그림 3은 각 에지에 연결된 사용자의 수를 나타낸다. 총 116677개의 학습 데이터(trainning data)를 100개의 엣지에 균등랜덤하게 분배하였다. 그림 3을 통해 우리는 2.1의 (1), (2), (3)의 조건을 만족시키고자 하였다.

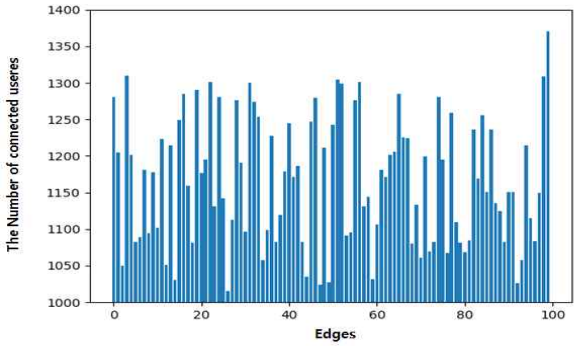

그림 3. 각 에지에 연결된 사용자 수

각 사용자들은 과거에 소비한 컨텐츠에 대한 자신만의 선호도 정보를 가지고 있다. 선호도는 3.5점 미만일 땐 0, 3.5점 이상일 땐 1로 하였다. 2.1에서 설명한 $C = 0.1$, 에지 내에서의 학습 반복수는 5번, 에지에서의 배치(batch) 사이즈는 100으로 하였다.

그림 4는 전통적인 연합학습과 3에서 제안된 (1), (2) 방법의 학습 속도를 비교한 그래프이며 표 1은 3가지 방법의 100번 연합학습 이후 모델의 성능이다. 3-(1)방법은 학습속도가 굉장히 빠르지만 18번의 학습과정 이후 과적합에 빠진 것을 알 수 있다. 3-(2)의 학습은 기존의 연합학습 방법보다 빠른 속도로 학습을 진행하며 과 적합은 일어나지 않았다. 2.1의 (4)에 따라 통신환경이 좋지 않아 빠른 수렴이 목표라면 3-(1) 방법을, 높은 성능이 목표라면 3-(2)방법을 사용할 수 있겠다.

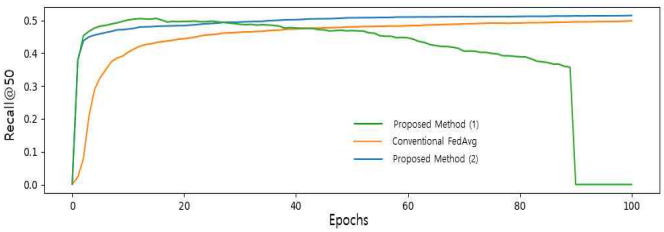

그림 4. 제시된 방법들과 전통적인 FedAvg 방법의 Recall@50

표 1. 100번의 연합학습 결과

	NDCG@100	Recall@20	Recall@50
Conventional FedAvg	0.3979	0.3636	0.4987
Proposed Method (1)	Over fitting		
Proposed Method (2)	0.4115	0.3810	0.5150

5. 결 론

협업필터링을 위한 연합학습은 기존에 제시된 연합학습 방법으로는 딥 러닝을 학습시킬 수 없다. 따라서 본 논문에서는 사용자, 엣지, 클라우드가 모두 참여하여 VAE를 학습시키는 연합학습 방법을 제시한다. 제시된 방법에 추가로 통합 전략 2가지를 설명한다. 이 2가지 방법 모두 전통적인 연합학습 통합방법보다 빠른 학습이 가능하다. 모델의 빠른 수렴이 중요한 상황이라면 3-(1) 방법을 모델의 높은 정확도가 중요한 상황에서는 3-(2) 방법을 적절히 사용하여 모델을 학습시킨다면 더욱 빠른 연합학습이 가능하다.

6. 참고문헌

[1] Ortega, F., Hernando, A., Bobadilla, J., & Kang, J. H. (2016). Recommending items to group of users using matrix factorization based collaborative filtering. Information Sciences, 345, 313-324.

[2] Liang, D., Krishnan, R. G., Hoffman, M. D., & Jebara, T. (2018, April). Variational autoencoders for collaborative filtering. In Proceedings of the 2018 World Wide Web Conference (pp. 689-698). International World Wide Web Conferences Steering Committee.

[3] McMahan, H. B., Moore, E., Ramage, D., & Hampson, S. (2016). Communication-efficient learning of deep networks from decentralized data. arXiv preprint arXiv:1602.05629.

[4] Chen, Y., Sun, X., & Jin, Y. (2019). Communication-Efficient Federated Deep Learning with Asynchronous Model Update and Temporally Weighted Aggregation. arXiv preprint arXiv:1903.07424.

[5] Yu, Z., Hu, J., Min, G., Lu, H., Zhao, Z., Wang, H., & Georgalas, N. (2018, December). Federated Learning Based Proactive Content Caching in Edge Computing. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.