2026. 05. 15

연합학습 기반 군집형 개인화 추천 시스템

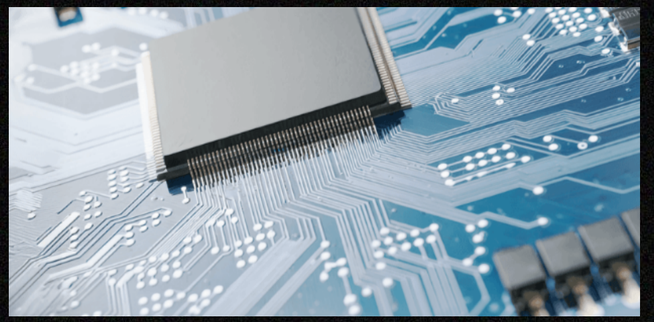
캡스톤디자인II | 2019270627 | 김상욱

목차

연구 배경 및 동기

프라이버시 문제

- 중앙 서버에 데이터 집중
- 대규모 개인정보 유출 사고 빈번
- 개인정보 보호 요구 증대



NPU 성능 향상

- 모바일 기기의 연산 능력 강화
- 온디바이스 학습 토대 마련

연합학습 필요성

- 분산, 협업 학습 패러다임
- 원시 데이터 전송 없는 학습
- 개인정보 침해 리스크 완화

개인화 중요성

- 취향의 다변화 및 파편화
- 콘텐츠 탐색 비용 증가
- 개별 특성에 대한 단일 모델 한계

문제 정의

Non-IID

- 통계적 이질성
: 독립 동일 분포(IID) 가정 위배

- 데이터 불균형성
: 사용자별 샘플 수 및 취향의 편차

- 수렴 불안정성
: 전역 모델 수렴 저해

개인화 한계

- 평균화된 파라미터 문제
: 대중적인 성향에 최적화

- 로컬 최적화 부족
: 개별 사용자 특성 미반영

- 일부 사용자 선호도 소외
: 소수 취향의 손실

성능 저하

- 추천 정확도 감소

- 수렴 속도 지연

- 학습 불안정성

- 사용자 만족도 저하

이질성 문제

- 클라이언트 간 데이터 차이

- 디바이스 성능 격차

- 통신 환경 불균등

제안 방법 개요

Model

PFedRec

- PFedRec
: 스코어 함수 & 아이템 임베딩 동시 최적화
- FedAvg
: 기울기 평균으로 전역 모델 집계

Method

Clustering

- Clustering
: 다중 전역 모델 사용
- Cosine Similarity
: 기울기 기반 유사도로 분리

핵심 기술 ① — PFedRec

이중 개인화 아키텍처

- 모델을 명시적으로 공유 파라미터(아이템 임베딩)와 개인 파라미터(스코어 함수)로 분리

- 공유 받은 아이템 임베딩을 기반으로 스코어 함수를 학습하고 이후 아이템 임베딩 미세조정

아이템 임베딩 공동 학습

- 매 라운드가 끝나면 FedAvg로 아이템 임베딩을 공동 학습

- 한 사용자가 보지 않은 아이템도 다른 사용자의 경험으로 학습되는 효과

프라이버시 보장

- 사용자별 선호를 결정하는 스코어 함수는 서버에 전송되지 않음

- 학습 데이터와 파라미터가 기기에만 존재하므로 프라이버시가 보장됨

경량화 모델

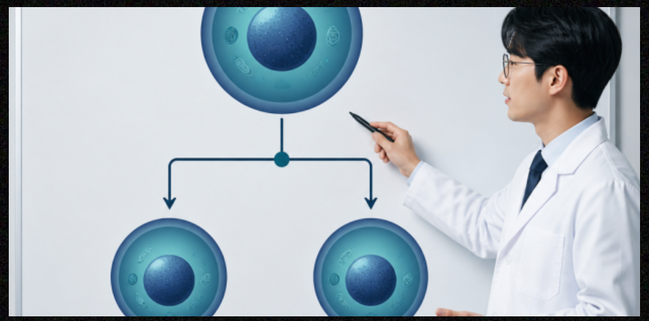
- 기존의 무거운 모델을 공유하는 대신 임베딩 변화량만 전송

- 스코어 함수 또한 가벼운 MLP 모델을 사용해 모바일 기기에서의 연산량 부담완화

핵심 기술 ② — Clustering

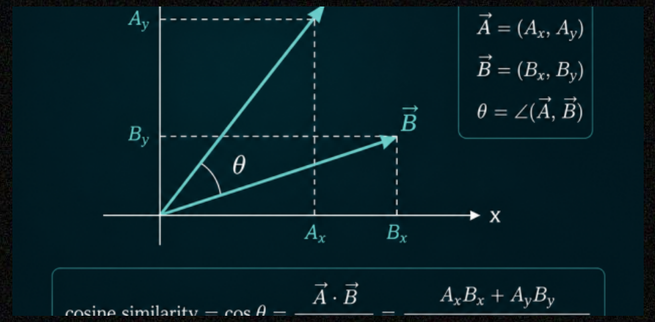
What?

- 아이템 임베딩의 변화량이 지표
- 이를 바탕으로 사용자를 분리



How?

- Bipartitioning Algorithm
- Ward 군집화로 최적 2분할
- 이후 군집마다 재귀적으로 반복



When?

- Cosine Similarity 사용
- 두 그룹간 평균 유사도 계산
- 임계값을 넘으면 분할 수락

Effect

- 부모 클러스터 가중치 계승
- 이후 클러스터별 FedAvg 수행
- 클러스터별 아이템 임베딩 보유

실험 설정

MovieLens 100K

- 영화 추천 표준 데이터셋
- 100,000개의 평점 데이터
- 1,682개의 영화 아이템
-943명의 사용자
- Non-IID 특성 반영

하이퍼 파라미터

- Item Embedding: 32 dim
- Score func: Linear(32→1)
- Optim: SGD
- lr (score): 0.1
- lr_eta(embedding): 80.0
- Local epochs: 1
- Fraction fit: 1
- Conflict threshold: 0.1

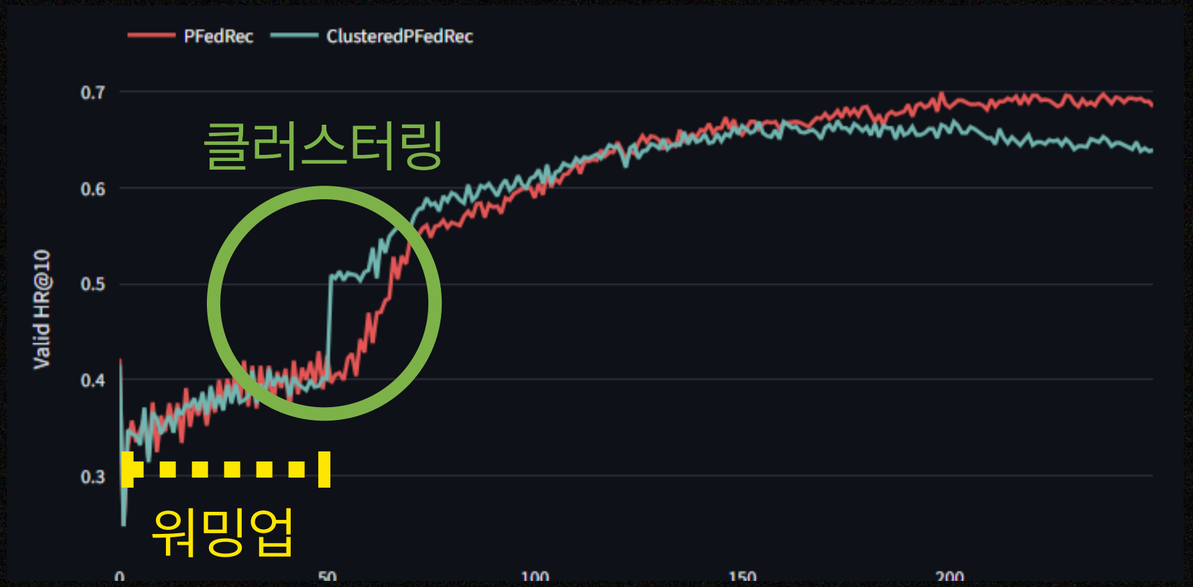
HR@10

- Hit Rate at 10
- 상위 10개 추천 정확도
- 추천 성공률 측정
- 표준 메트릭

NDCG@10

- Normalized Discounted Cumulative Gain
- 추천 순위 품질 평가
- 상위 랭킹 가중치 부여
- 정규화된 성능 측정
- 학술적 표준 메트릭

실험 결과



Validation HR@10 Graph

Validation NDCG@10 Graph

- 워밍업 구간은 클러스터링이 일어나지 않음
- 클러스터링 시점에 성능이 크게 향상됨
- 그러나 최종성능은 PFedRec이 우위
- 이 클러스터링 방식은 평균성능을 높이지는 못함

TestSet HR@10, NDCG@10
PFedRec(198r): 0.653, 0.377
Clustered PFedRec(173r): 0.617, 0.364

추가 분석

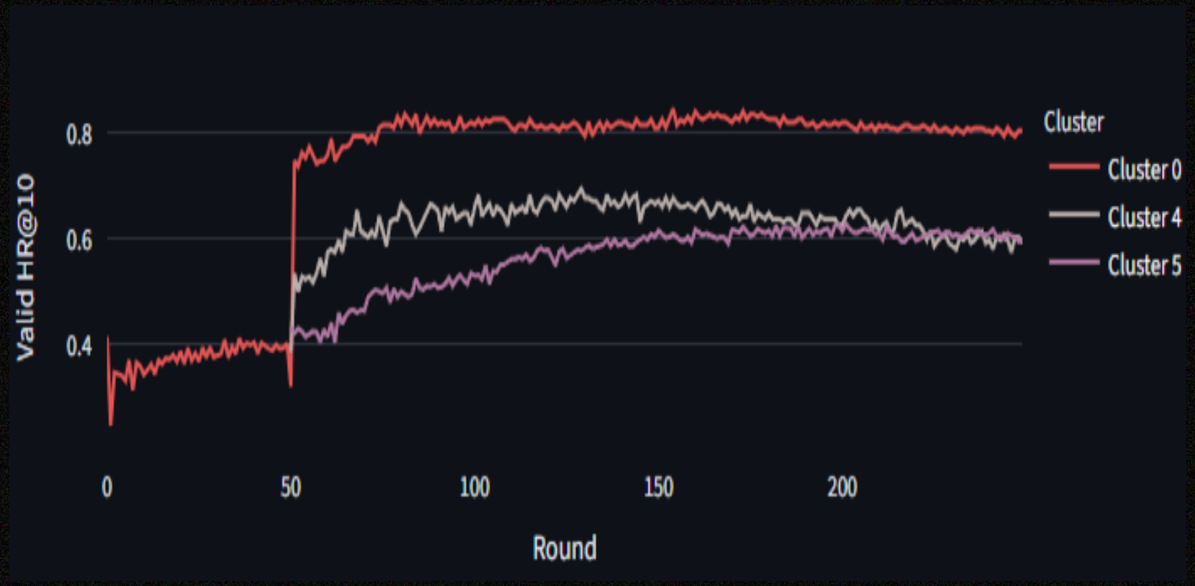
Strategy

ClusteredPFedRec

Round

173

Cluster	Valid HR@10	Valid NDCG@10	Valid Loss
0	0.8394	0.5460	0.0647
4	0.6420	0.3943	0.1090
5	0.6220	0.3588	0.1485



클러스터별 메트릭

클러스터별 Validation HR@10 Graph

- 그러나 특정 클러스터 성능이 크게 향상됨
- PFedRec의 0.653을 크게 웃도는 수치
- 따라서 클러스터링은 개인화에 기여할 수 있음

TestSet HR@10, NDCG@10
Cluster 0(173r): 0.746, 0.484
Cluster 4(173r): 0.665, 0.387
Cluster 5(173r): 0.559, 0.317

결론 및 기여

결론

- 코사인 유사도 기반의 명시적인 클러스터링은 아이템 임베딩 수준의 그룹 개인화를 실현할 수 있다.
- 또한, 유사한 학습 신호를 공유하는 그룹을 대상으로, PFedRec의 스코어 함수가 가진 개인화 한계를 극복하고 추가적인 성능 향상을 이끌어낼 수 있다.

기여

- PFedRec의 스코어 함수 개인화에 명시적 클러스터링을 결합하면 추가적인 성능 향상이 발생함을 실험적으로 확인함.
- 연합학습 환경 하에서 유사한 학습 신호를 공유하는 그룹에게 높은 수준의 추천성능을 제공할 수 있음을 보임.

연구 한계점

- Movielens 100K 단일 데이터셋으로 진행된 실험
- 클러스터링 혜택을 받지 못하는 그룹 문제를 해결하지 못함
- 워밍업 라운드 등 하이퍼 파라미터에 민감함
- 기울기 복원을 통한 프라이버시 등 간접적 정보 유출 가능성 존재

향후 연구 방향

- 다양한 데이터셋으로의 확장
- 코사인 유사도 분포를 통한 클러스터링 기준 마련
- 클러스터별 Early Stopping 적용
- Differential Privacy 적용 하에서 프라이버시 보장 및 품질 유지

2026. 5. 15

감사합니다.