1. Background: Learnware Paradigm

Building high-quality models:
- Complex, time-consuming and expensive: data, computing resources, expertise ...
- A heavy burden for ordinary users.

Difficult to reuse among different users: data privacy concerns, catastrophic forgetting.

Learnware paradigm [Zhou, 2016; Zhou and Tan, 2021]
- Construct a model market that manages numerous well-performing models.
- Solve future tasks by leveraging these models without having to build models from scratch.

LEARNWARE MARKET

1) Learnware components

let learnware = model + specification describe the functionality of the model

2) Procedure of learnware paradigm

Submitting stage: The learnware market assigns specifications to submitted models.
Deploying stage: The market helps the user identify & reuse helpful models according to the requirement.
Data privacy is preserved in both stages.

LEARNWARE MARKET

2. Motivation

Previous algorithms based on RKME specification [Xie et al., 2023][Zhang et al., 2021][Tan et al., 2022]:
- Require examining all learnwares in the market:
  - Computationally unaffordable in large markets.
- Impose strict restrictions on the market:
  - E.g., all learnwares share the same ground-truth labeling function.

This paper: a more efficient and flexible method
- A learnware scoring criterion with fewer restrictions.
- An anchor-based framework only examining only a small portion of the market.

3. Whether a learnware is helpful?

Question 1: How to judge whether a learnware is potentially helpful based on the limited labeled data of the user?

Case 1: There exists one learnware that can solve user’s task.
Solution: Calculate losses on user’s data, and choose the learnware with the smallest loss.

Case 2: No single learnware can tackle the user task as a whole, but multiple learnwares can each tackle a part of user’s task separately.

4. Anchor-based Learnware Identification Framework

Question 2: how to identify helpful learnwares efficiently?

- Examining the whole market: No!
- Uploading user’s data: No!

Our method: anchor-based scoring criterion:

1. Market sends anchor learnwares to user;
2. User tests anchor learnwares and returns scores to market;
3. Market identifies helpful learnwares based on scores.

5. Experiments

Market construction:
- 4 real-world datasets that can be naturally divided into several parts;
- Train 15 models on each part: different linear models, LightGBM, and neural networks.

Results:
1. Our learnware scoring criterion (Ours-traversal) achieves the best performance;
2. Our anchor method (Ours-anchor) greatly improves efficiency (examine 11.8%, 14.9%, 21.42%, 19.91% learnwares) with very little performance degradation.
3. Reduced Kernel Mean Embedding (RKME) specification [Zhou and Tan, 2022]

Key challenge: how to identify helpful models for a specific user task efficiently without leaking user data privacy?