



An Introduction of the Toolchain for Academic Researches

余阳

2022-10-12



Outline

2

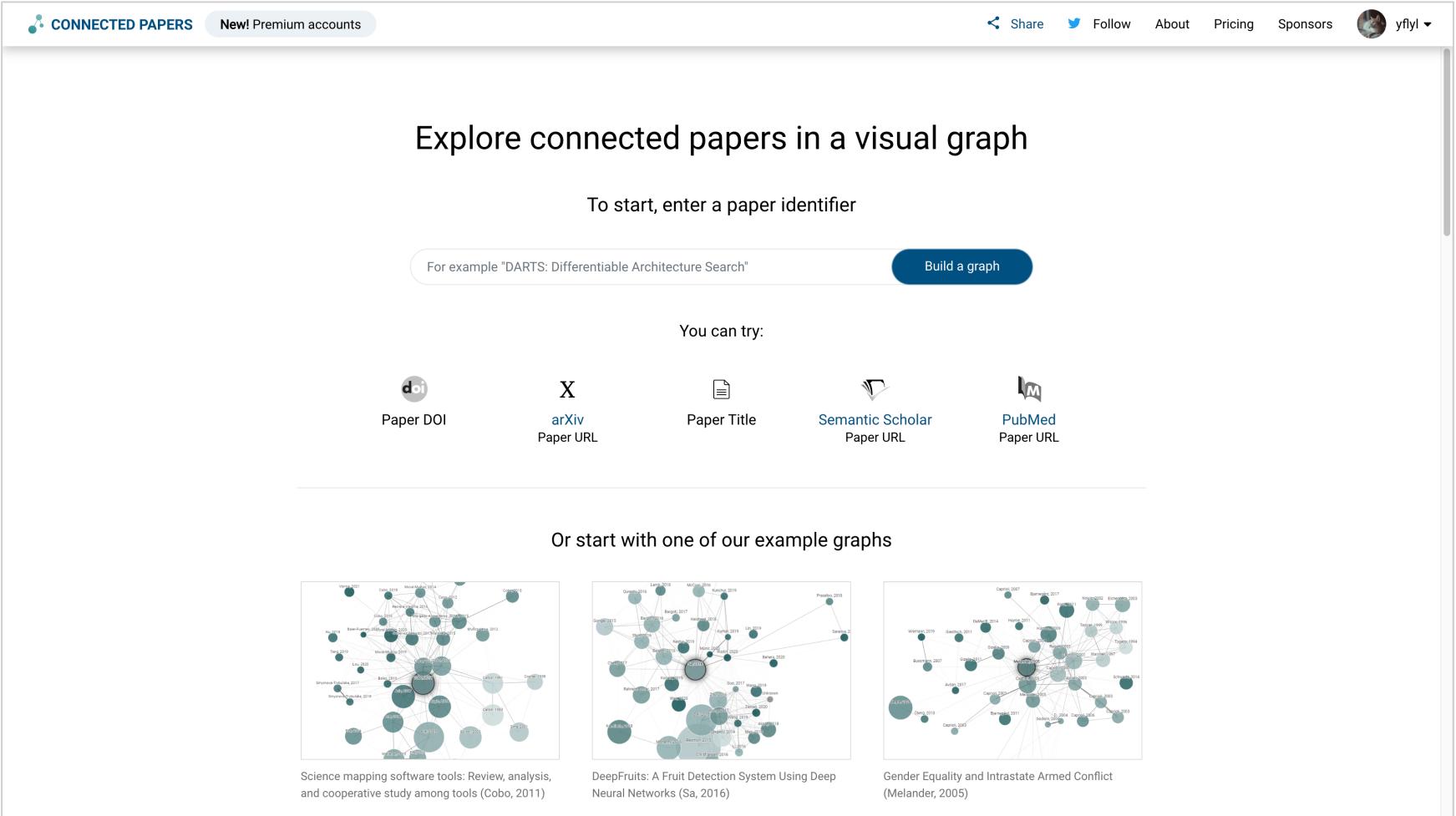
- Introduction & Related Work
- Methodology
- Experiments
- Conclusions

Introduction & Related Work

3

■ Investigate & Survey

□  CONNECTED PAPERS 



The screenshot shows the Connected Papers website interface. At the top, there is a navigation bar with links for Share, Follow, About, Pricing, Sponsors, and a user profile. Below the navigation bar, a large heading says "Explore connected papers in a visual graph". A search input field contains the placeholder text "To start, enter a paper identifier" and a "Build a graph" button. Below the search field, there is a section titled "You can try:" with icons for Paper DOI, arXiv Paper URL, Paper Title, Semantic Scholar Paper URL, and PubMed Paper URL. At the bottom, there is a section titled "Or start with one of our example graphs" featuring three visual graphs: "Science mapping software tools: Review, analysis, and cooperative study among tools (Cobo, 2011)", "DeepFruits: A Fruit Detection System Using Deep Neural Networks (Sa, 2016)", and "Gender Equality and Intrastate Armed Conflict (Melander, 2005)".

Explore connected papers in a visual graph

To start, enter a paper identifier

For example "DARTS: Differentiable Architecture Search"

Build a graph

You can try:

Paper DOI

arXiv Paper URL

Paper Title

Semantic Scholar Paper URL

PubMed Paper URL

Or start with one of our example graphs

Science mapping software tools: Review, analysis, and cooperative study among tools (Cobo, 2011)

DeepFruits: A Fruit Detection System Using Deep Neural Networks (Sa, 2016)

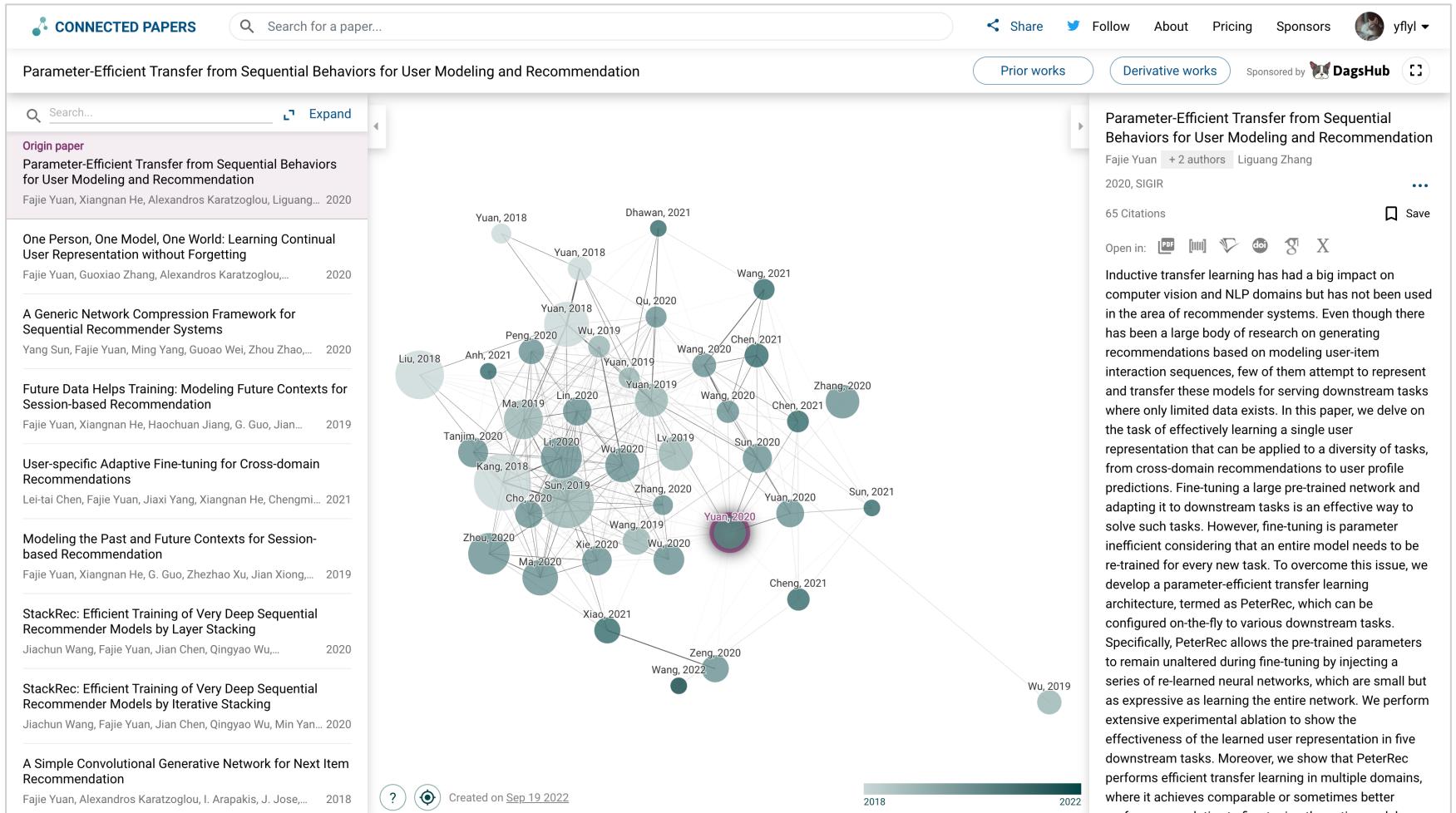
Gender Equality and Intrastate Armed Conflict (Melander, 2005)

Introduction & Related Work

4

■ Investigate & Survey

□ CONNECTED PAPERS





Introduction & Related Work

5

■ Investigate & Survey

□ CONNECTED PAPERS

- *To create each graph, we analyze an order of ~50,000 papers and select the few dozen with the strongest connections to the origin paper.*
- ***Connected Papers is not a citation tree.***
- **Similarity metric:** Co-citation and bibliographic coupling.
- **Algorithm:** Force directed graph.
- **Database:** Semantic Scholar Paper Corpus.
- **Pricing:** 5 free graphs per month, \$3 per month for unlimited graphs.



Introduction & Related Work

6

■ Investigate & Survey

- ❑ AI-Paper-Search (by MLNLP), Google Scholar, etc.

AI-Paper-Search

Input your keywords

Advanced setting Search GitHub

Tips!

You can get more precise results by using advanced setting.
If this project is helpful to you, please give us a ⭐ star!

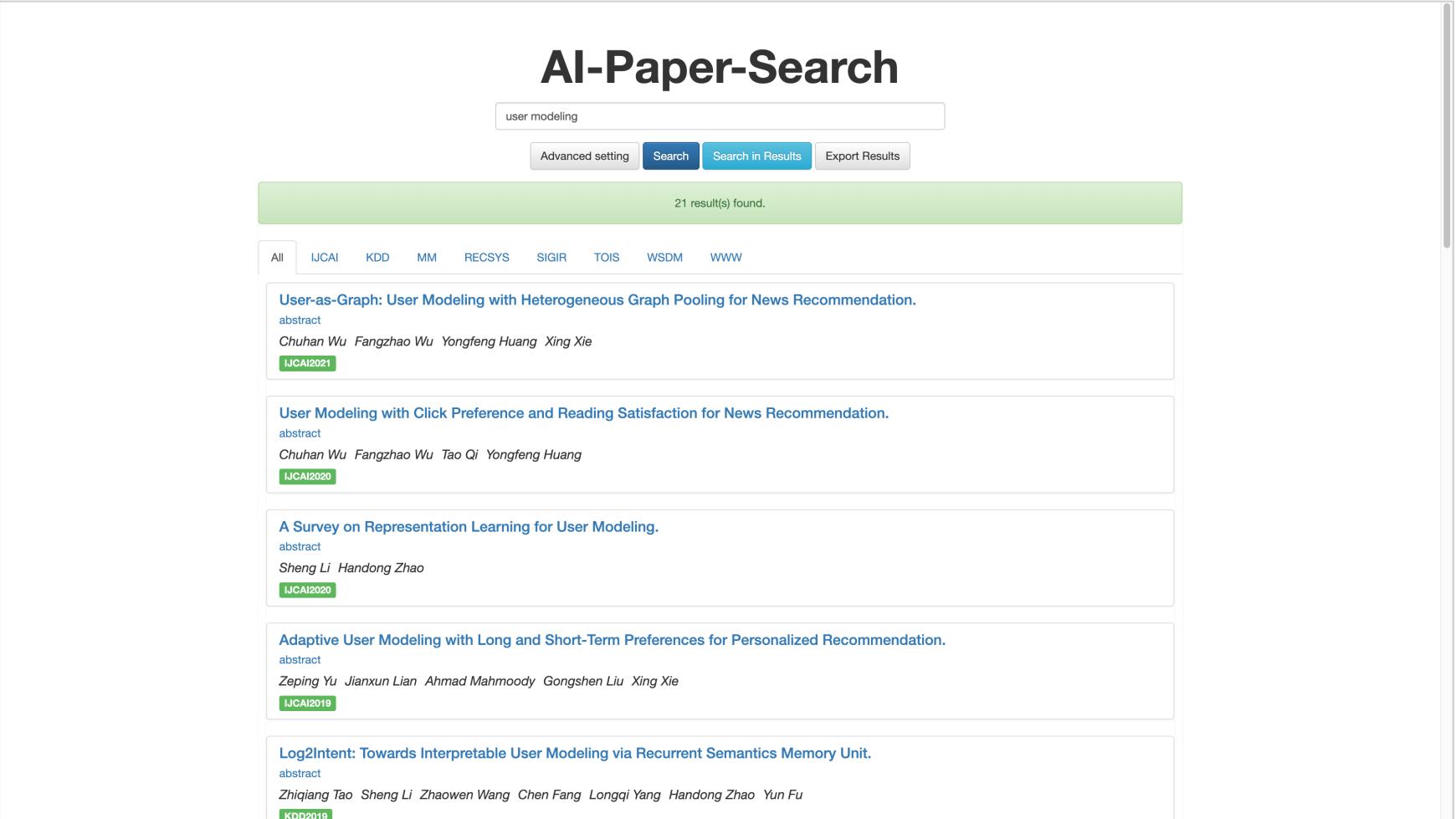
Introduction & Related Work

7

■ Investigate & Survey



AI-Paper-Search (by MLNLP), Google Scholar, etc.

A screenshot of the AI-Paper-Search web interface. The title "AI-Paper-Search" is at the top. A search bar contains the query "user modeling". Below the search bar are buttons for "Advanced setting", "Search", "Search in Results", and "Export Results". A green banner indicates "21 result(s) found." A navigation bar below shows categories: All, IJCAI, KDD, MM, RECSYS, SIGIR, TOIS, WSDM, and WWW. The first result is a paper titled "User-as-Graph: User Modeling with Heterogeneous Graph Pooling for News Recommendation." by Chuhan Wu, Fangzhao Wu, Yongfeng Huang, and Xing Xie, from IJCAI2021. The second result is "User Modeling with Click Preference and Reading Satisfaction for News Recommendation." by Chuhan Wu, Fangzhao Wu, Tao Qi, Yongfeng Huang, from IJCAI2020. The third result is "A Survey on Representation Learning for User Modeling." by Sheng Li and Handong Zhao, from IJCAI2020. The fourth result is "Adaptive User Modeling with Long and Short-Term Preferences for Personalized Recommendation." by Zeping Yu, Jianxun Lian, Ahmad Mahmood, Gongshen Liu, and Xing Xie, from IJCAI2019. The fifth result is "Log2Intent: Towards Interpretable User Modeling via Recurrent Semantics Memory Unit." by Zhiqiang Tao, Sheng Li, Zhaowen Wang, Chen Fang, Longqi Yang, Handong Zhao, and Yun Fu, from KDD2019.

Introduction & Related Work

8

■ Investigate & Survey



AI-Paper-Search (by MLNLP), Google Scholar, etc.

AI-Paper-Search

user modeling

Advanced setting

Years

Specific Year

Confs

<input checked="" type="checkbox"/> AAAI	<input checked="" type="checkbox"/> ACL
<input checked="" type="checkbox"/> AISTATS	<input checked="" type="checkbox"/> BMVC
<input checked="" type="checkbox"/> CIKM	<input checked="" type="checkbox"/> COLING
<input checked="" type="checkbox"/> COLT	<input checked="" type="checkbox"/> CVPR
<input checked="" type="checkbox"/> ECCV	<input checked="" type="checkbox"/> ECIR
<input checked="" type="checkbox"/> EMNLP	<input checked="" type="checkbox"/> ICASSP
<input checked="" type="checkbox"/> ICCV	<input checked="" type="checkbox"/> ICDM
<input checked="" type="checkbox"/> ICLR	<input checked="" type="checkbox"/> ICME
<input checked="" type="checkbox"/> ICML	<input checked="" type="checkbox"/> IJCAI
<input checked="" type="checkbox"/> INTERSPEECH	<input checked="" type="checkbox"/> ISWC
<input checked="" type="checkbox"/> JMLR	<input checked="" type="checkbox"/> KDD
<input checked="" type="checkbox"/> MICCAI	<input checked="" type="checkbox"/> MLSYS
<input checked="" type="checkbox"/> MM	<input checked="" type="checkbox"/> NAACL
<input checked="" type="checkbox"/> NIPS	<input checked="" type="checkbox"/> RECSYS
<input checked="" type="checkbox"/> SIGIR	<input checked="" type="checkbox"/> TASLP
<input checked="" type="checkbox"/> TIP	<input checked="" type="checkbox"/> TKDE
<input checked="" type="checkbox"/> TOIS	<input checked="" type="checkbox"/> TPAMI
<input checked="" type="checkbox"/> VLDB	<input checked="" type="checkbox"/> WACV
<input checked="" type="checkbox"/> WSDM	<input checked="" type="checkbox"/> WWW

21 result(s) found.

All

User-as-Graph: User Modeling with Heterogeneous Graph Pooling for News Recommendation.

Introduction & Related Work

9

■ Reference Management & Paper Reading

- **Zotero**: reference management
- **Zotero Connector**: browser plugin
- **Zotfile**: automatically rename and move PDF files
- **Nutstore**: synchronize across devices
- **PDF Expert**: access the synchronized files via WebDAV on Pad
- **Notion**: take notes



Zotero



Nutstore



PDF Expert

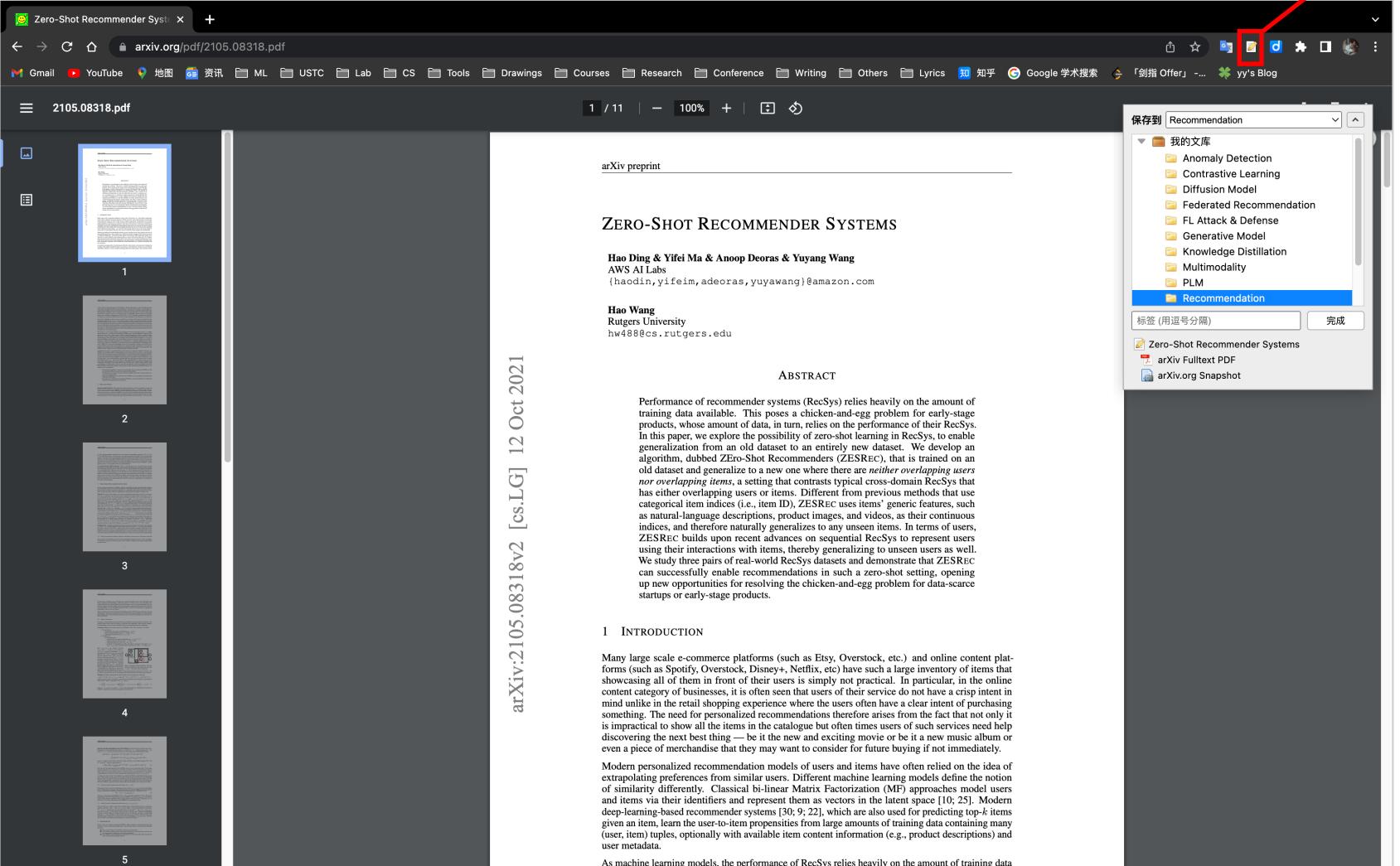


Notion

Introduction & Related Work

10

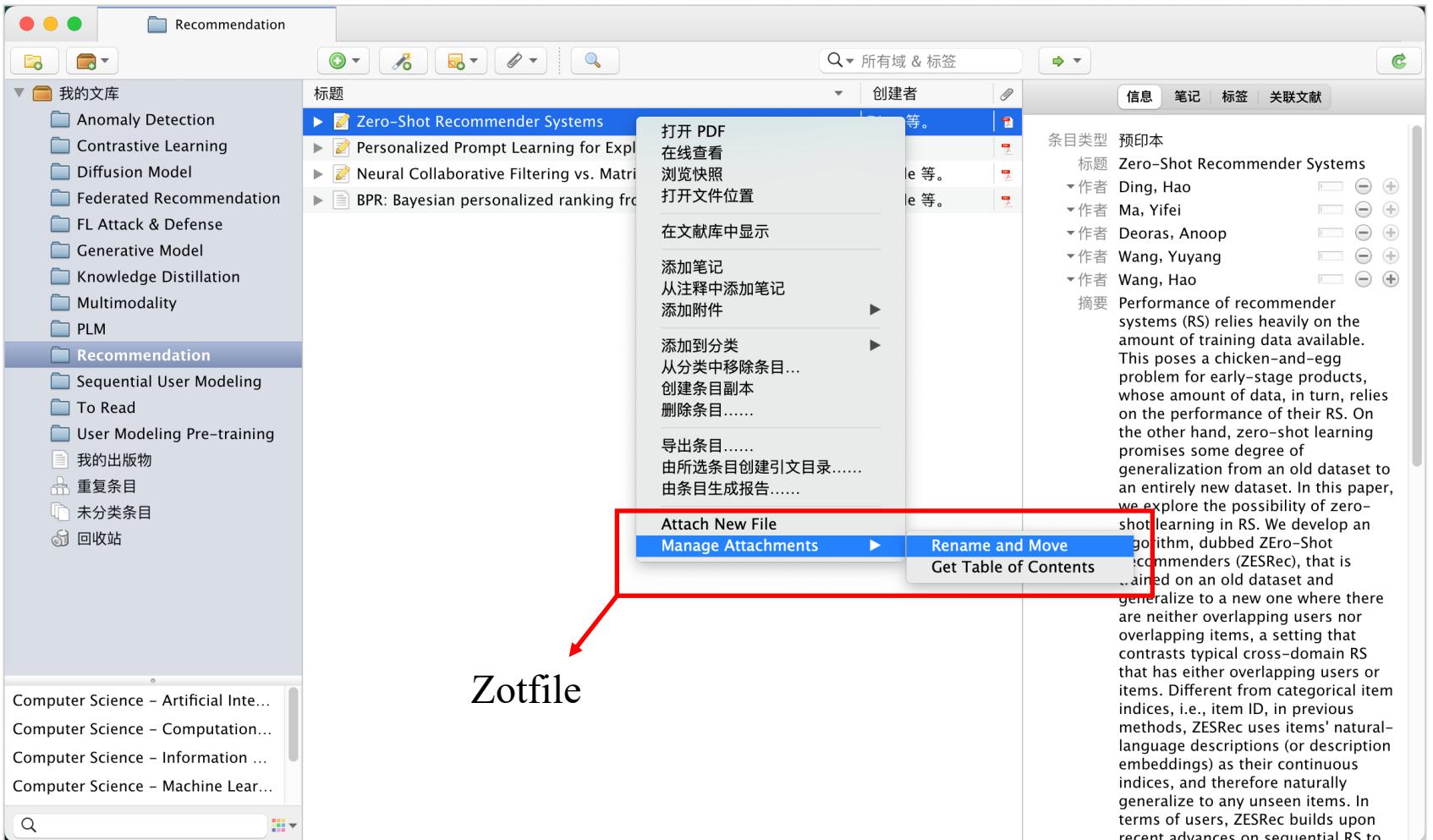
■ Reference Management & Paper Reading



Introduction & Related Work

11

■ Reference Management & Paper Reading

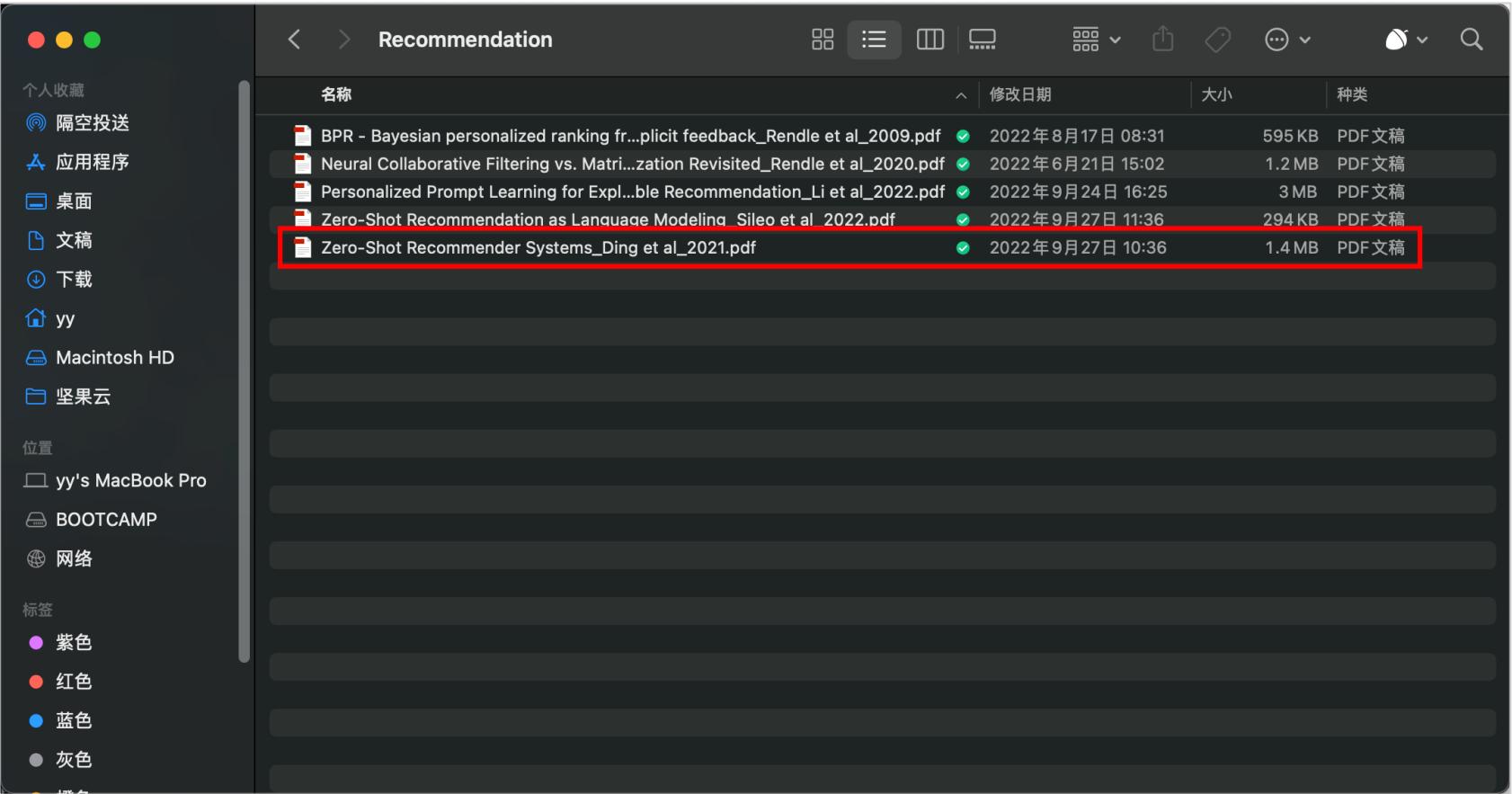


In Zotero

Introduction & Related Work

12

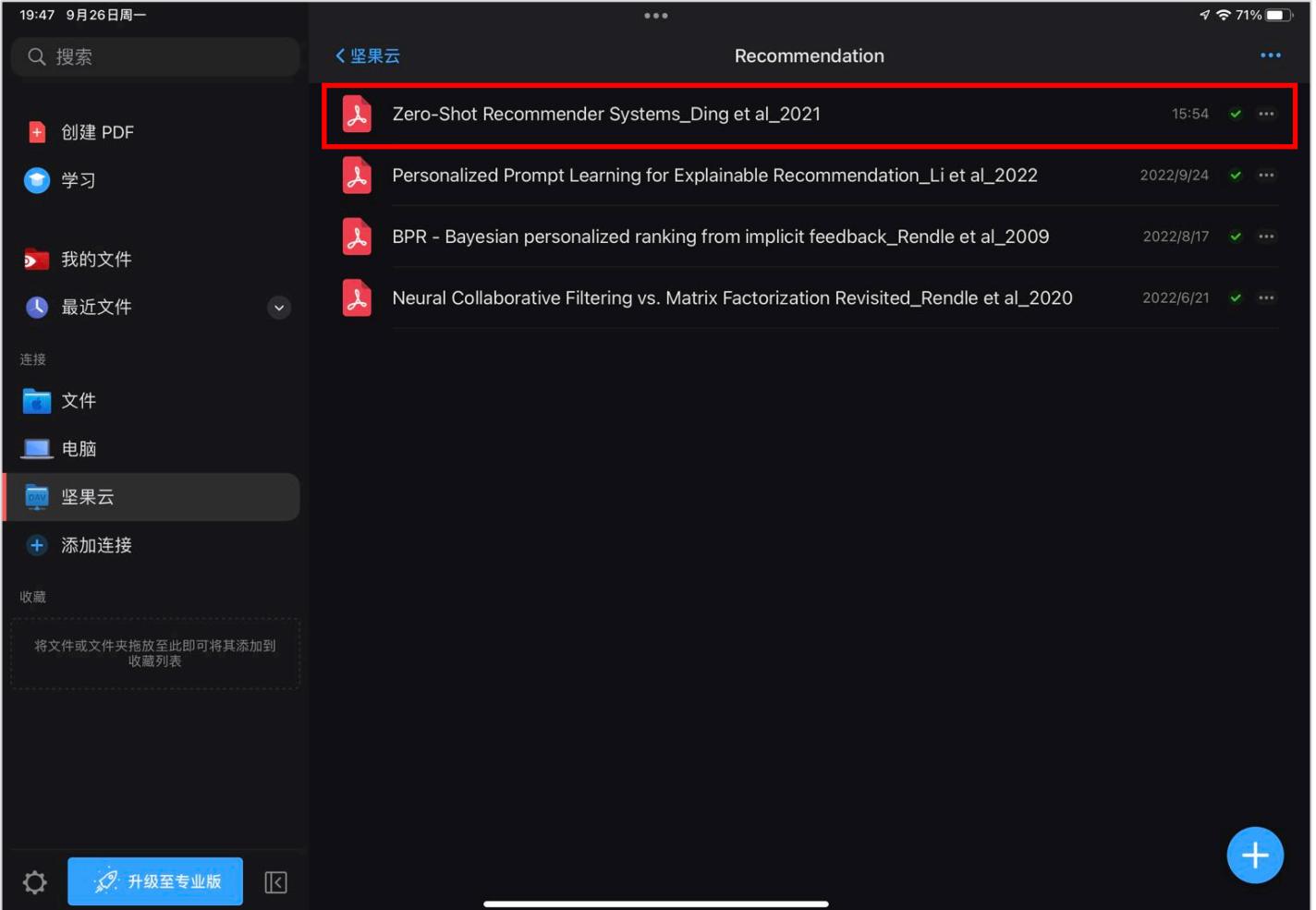
■ Reference Management & Paper Reading



Introduction & Related Work

13

■ Reference Management & Paper Reading



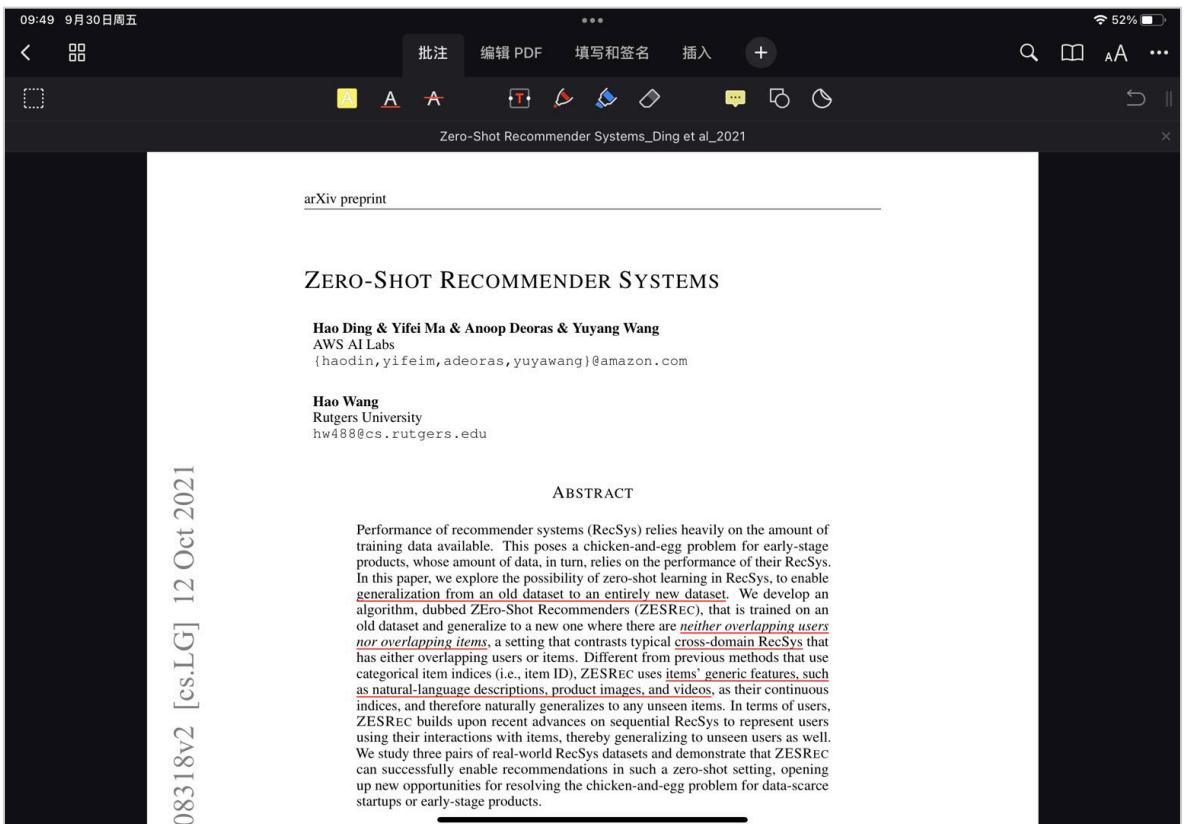
In PDF Expert
on iPad



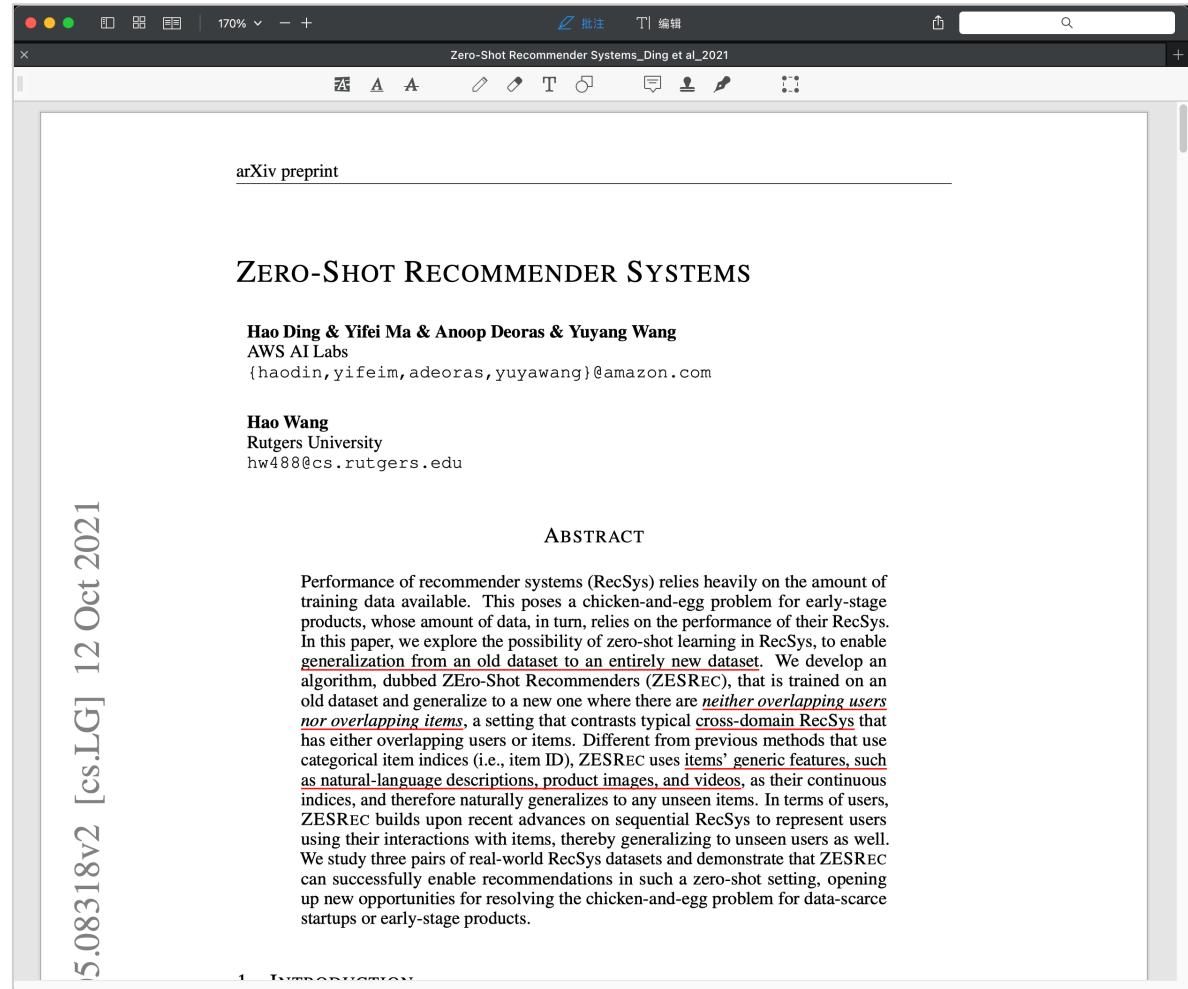
Introduction & Related Work

14

■ Reference Management & Paper Reading



On iPad



On PC



Outline

15

- Introduction & Related Work
- Methodology
- Experiments
- Conclusions

Methodology

16

■ Drawing

□ Illustrations



PPT



OmniGraffle (for Mac)



Visio (for Windows?)

□ Icons



Methodology

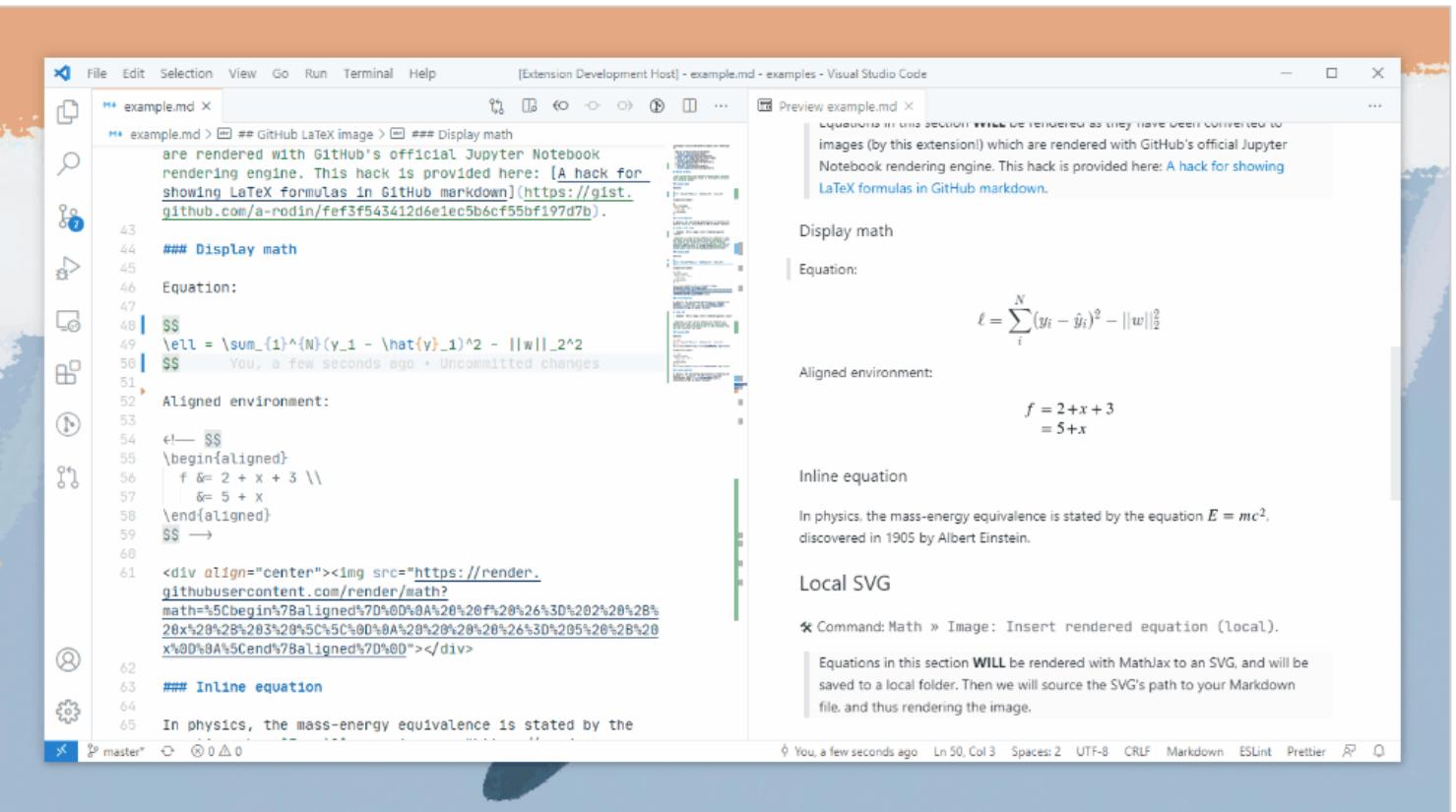


17

■ Drawing

□ Equations in Illustrations

➤ **Math to Image:** Convert LaTex equations into local SVGs. 



[2] <https://github.com/TeamMeow/vscode-math-to-image>



Outline

18

- Introduction & Related Work
- Methodology
- Experiments
- Conclusions



Experiments

19

■ Conducting Experiments

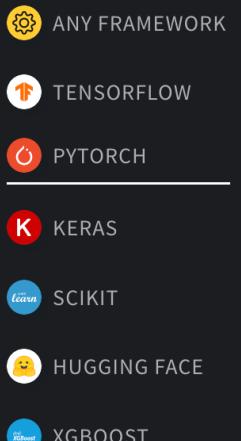
□ Weights & Biases

- Installation: `pip install wandb; wandb login;`
- Usage:

Track, compare, and visualize your ML models with 5 lines of code

Quickly and easily implement experiment logging by adding just a few lines to your script and start logging results. Our lightweight integration works with any Python script.

TRY A LIVE NOTEBOOK →



```
import wandb

# 1. Start a new run
wandb.init(project="gpt-3")

# 2. Save model inputs and hyperparameters
config = wandb.config
config.learning_rate = 0.01

# 3. Log gradients and model parameters
wandb.watch(model)
for batch_idx, (data, target) in enumerate(train_loader):

    if batch_idx % args.log_interval == 0:
        # 4. Log metrics to visualize performance
        wandb.log({"loss": loss})
```

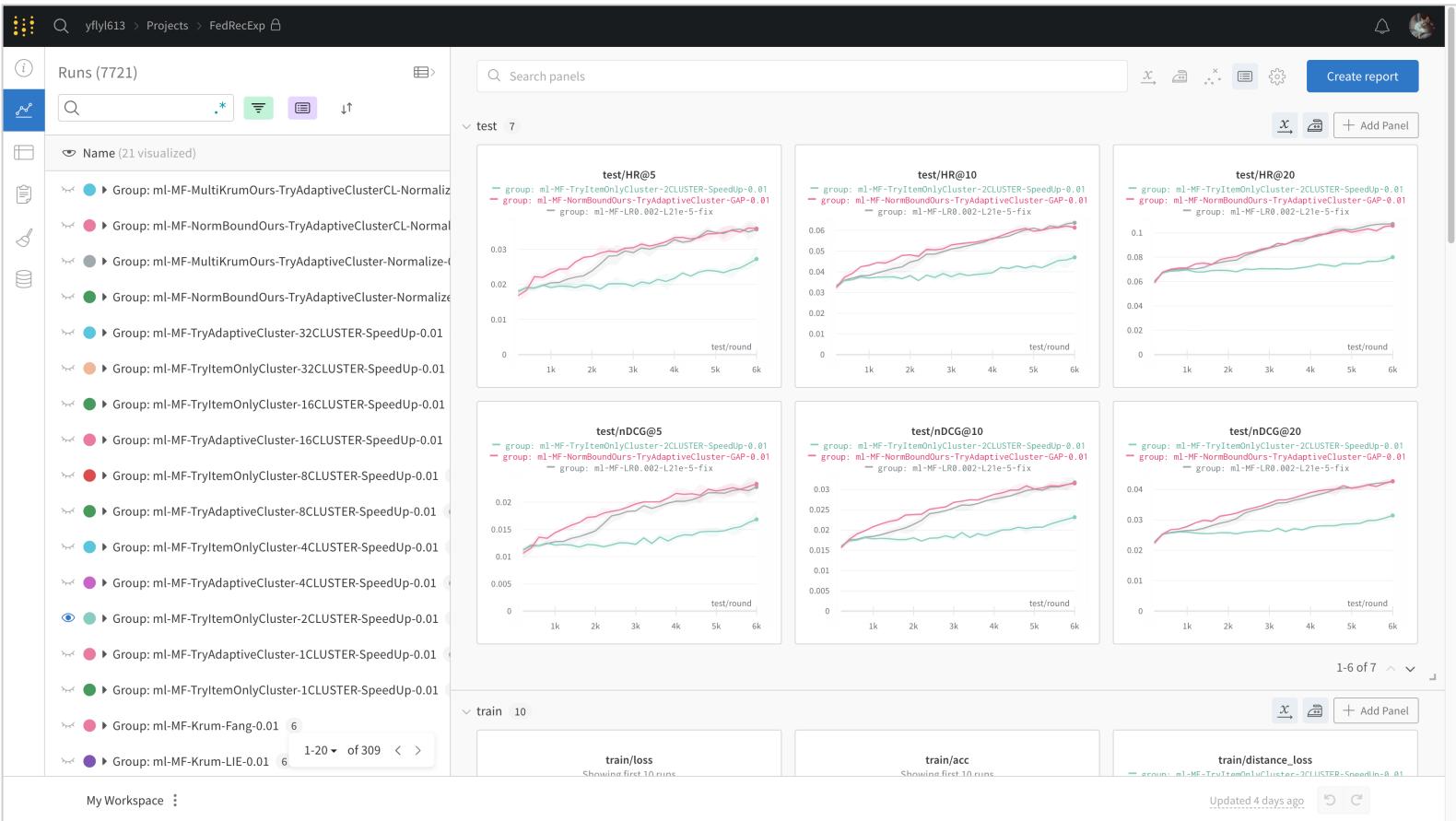
Experiments

20

■ Conducting Experiments

□ Weights & Biases

➤ Experiment tracking





Experiments

21

■ Conducting Experiments

□ Weights & Biases

- More than tracking ...

Explore the Weights & Biases platform

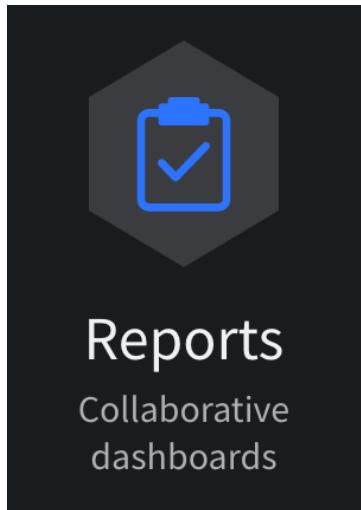
Experiments	Reports	Artifacts	Tables	Sweeps
Experiment tracking	Collaborative dashboards	Dataset and model versioning	Interactive data visualization	Hyperparameter optimization

Experiments

22

■ Conducting Experiments

- Weights & Biases
- Reports

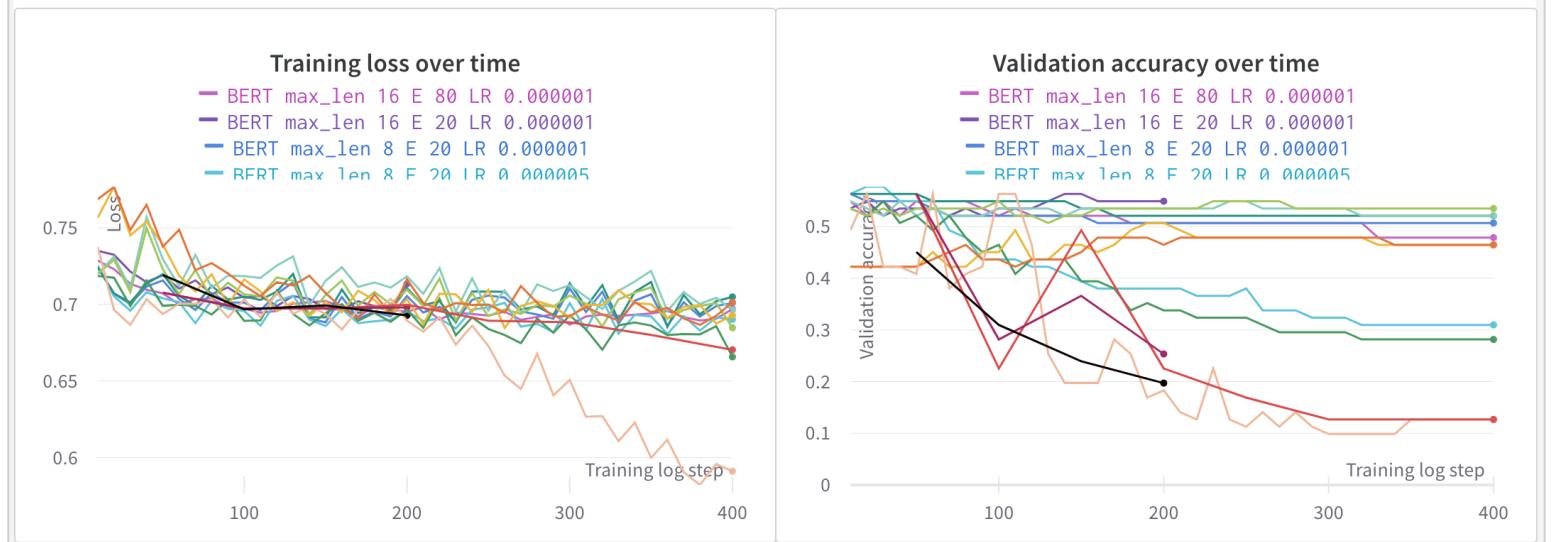


▼ First pass: Fine-tuning BERT baseline

▼ Short manual hyperparameter exploration

I started with the hyperparameter settings in the [example provided with Transformers](#). Based on the loss and validation accuracy (`eval_acc`) curves plotted in W&B after each run, I adjusted my model to improve performance from a **baseline eval_acc of 0.127 to 0.535 in fewer than 20 experiments**.

Below, you can see the training loss and validation accuracy curves plotted over time. The starting baseline is in black, and the rest of the runs are colored in rainbow order from red to purple based on their creation order: my earlier experiments are reds/oranges, and the later experiments are blues/purples. The legend shows the maximum sequence length (`max_len`), training epochs (E), and learning rate (LR) for each run. You can also expand the "BERT variants" run set at the end of this section to see more details about each run.

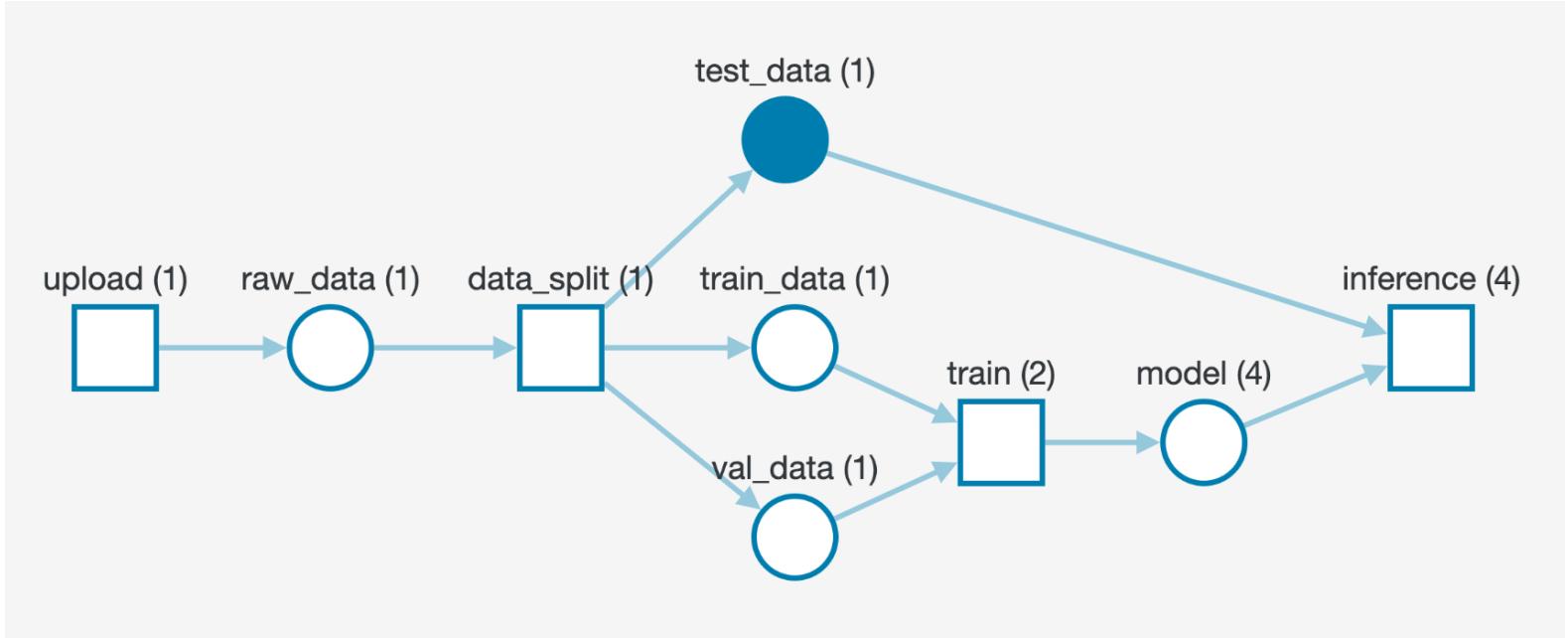


Experiments

23

■ Conducting Experiments

- Weights & Biases
 - Artifacts

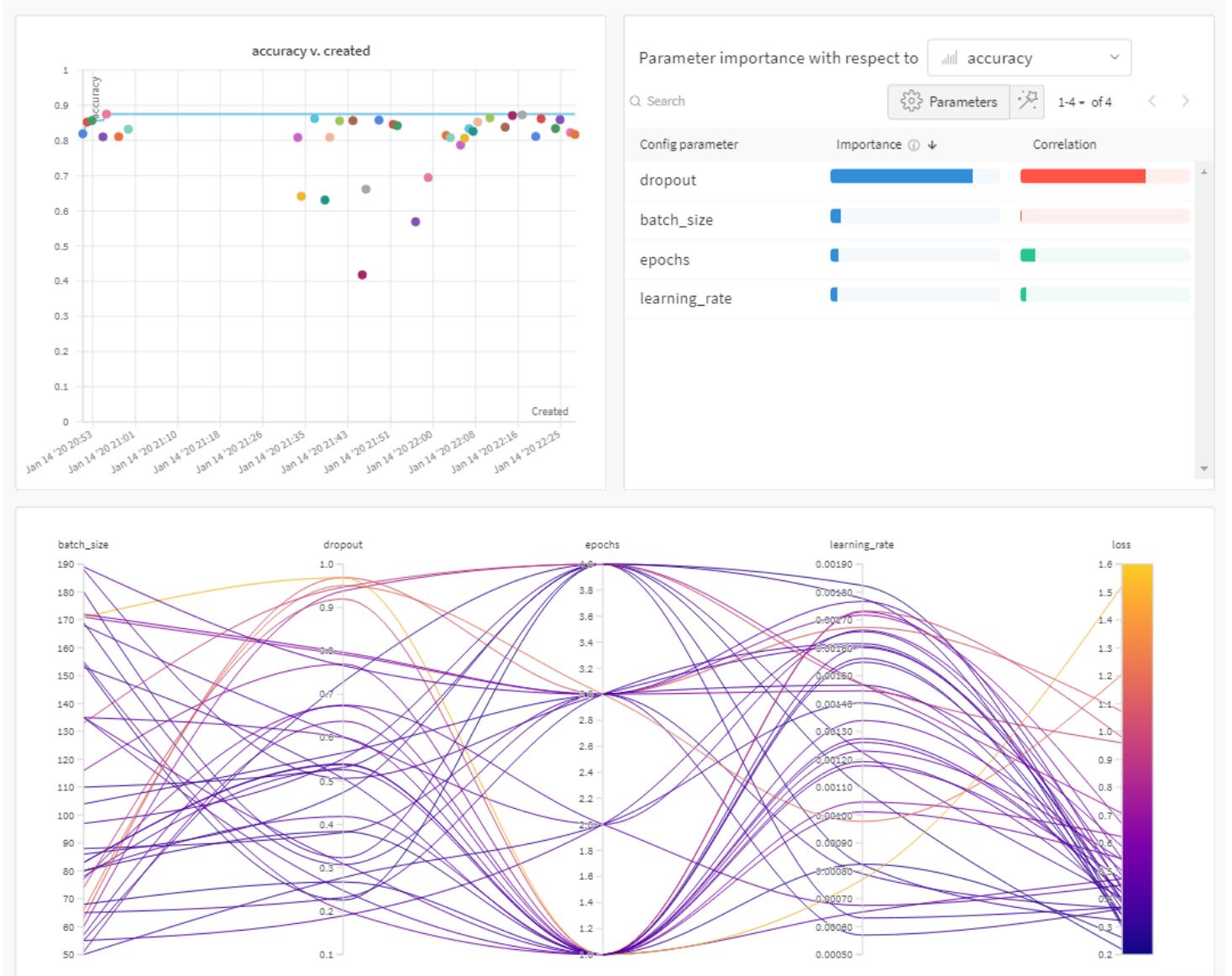


Experiments

24

■ Conducting Experiments

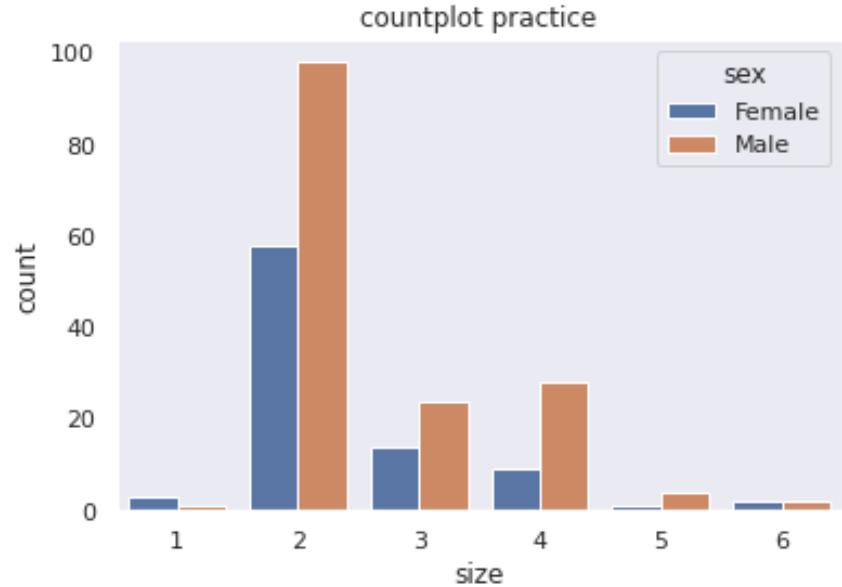
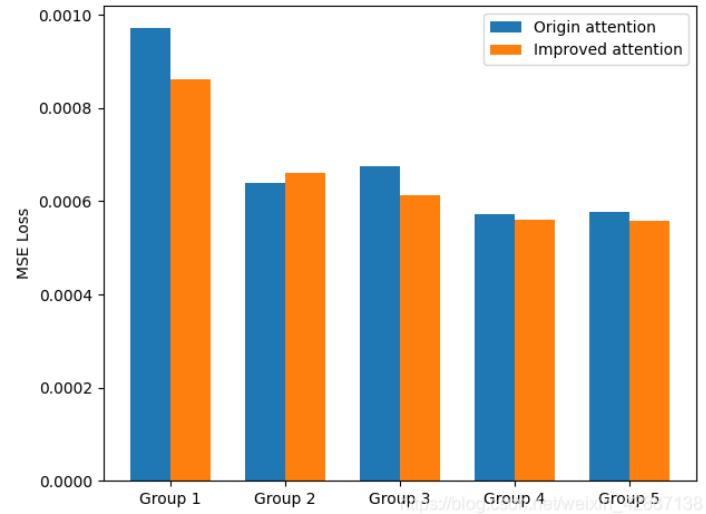
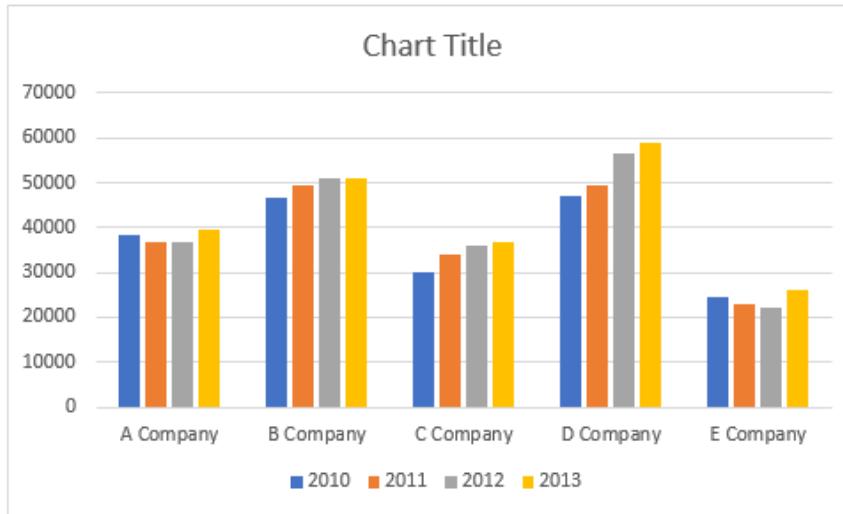
- Weights & Biases
 - Sweeps



Experiments

25

Experiment Results





Outline

26

- Introduction & Related Work
- Methodology
- Experiments
- Conclusions



Conclusions

27

■ Paper Writing with LaTeX

□ Online LaTeX Editor (Overleaf)

➤ Pros

- ✓ Easy to use (the environment is already installed).
- ✓ Easy for collaboration and synchronization.
- ✓ Track the document history automatically.

➤ Cons

- ✓ Sometimes slow and unstable, especially near the DDL.



Conclusions

28

■ Paper Writing with LaTeX

- Local LaTeX Editor (MacTeX/TeX Live/MiKTeX + vscode LaTeX Workshop)

- Pros

- ✓ Fast and stable.

- Cons

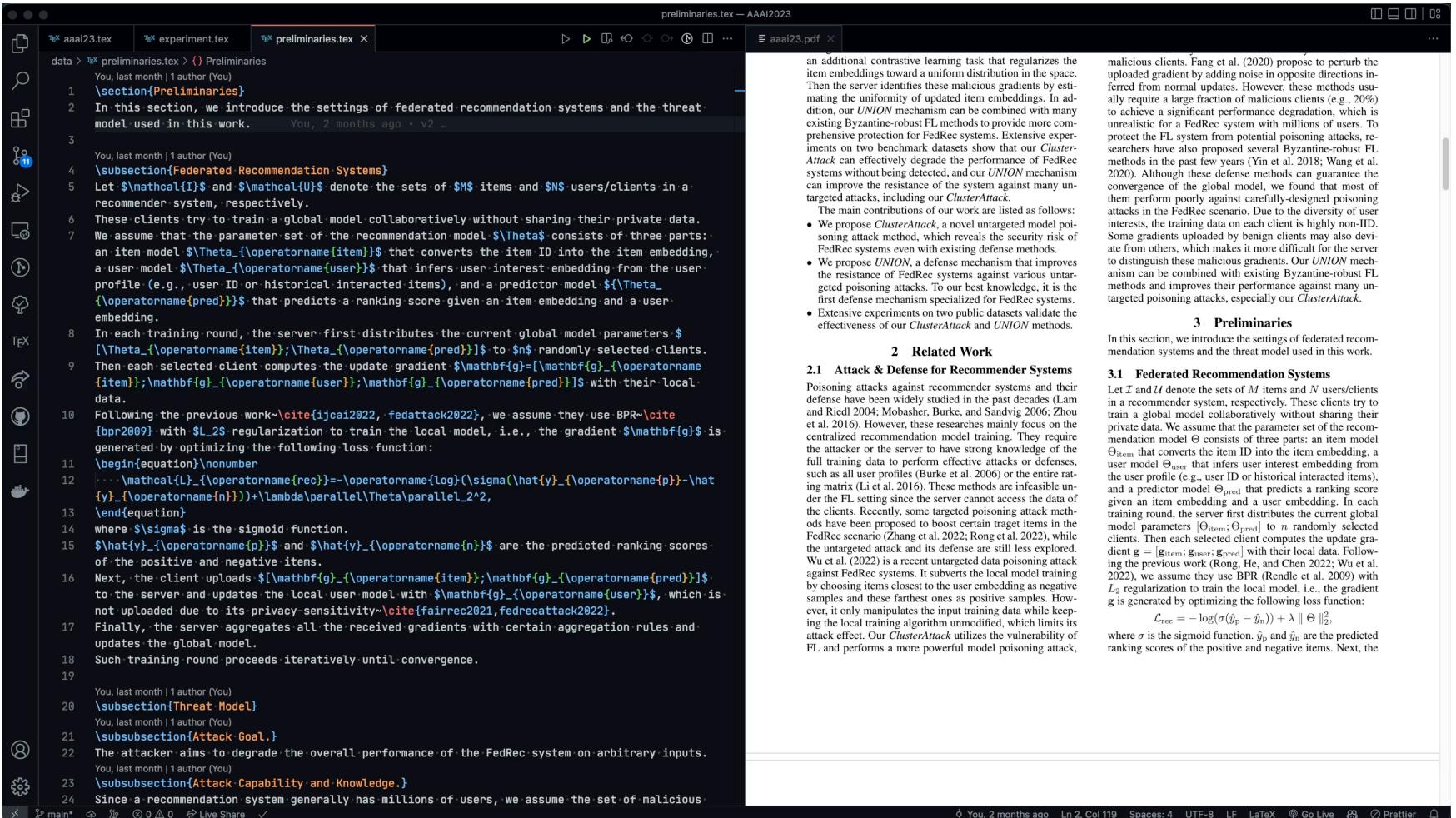
- ✓ Setting up the environment for the first time may take some time.

Conclusions

29

■ Paper Writing with LaTeX

□ Local LaTeX Editor (MacTeX/TeX Live/MiKTeX + vscode LaTeX Workshop)



preliminaries.tex – AAAI2023

```

data > \section{Preliminaries}
      You, last month | 1 author (You)
      1 \subsection{Federated Recommendation Systems}
      2 In this section, we introduce the settings of federated recommendation systems and the threat
         model used in this work.      You, 2 months ago • V2 ...
      3
      4 You, last month | 1 author (You)
      5 Let  $\mathcal{I}$  and  $\mathcal{U}$  denote the sets of  $M$  items and  $N$  users/clients in a
         recommender system, respectively.
      6 These clients try to train a global model collaboratively without sharing their private data.
      7 We assume that the parameter set of the recommendation model  $\Theta$  consists of three parts:
         an item model  $\Theta_{item}$  that converts the item ID into the item embedding,
         a user model  $\Theta_{user}$  that infers user interest embedding from the user
         profile (e.g., user ID or historical interacted items), and a predictor model  $\Theta_{pred}$ 
         that predicts a ranking score given an item embedding and a user
         embedding.
      8 In each training round, the server first distributes the current global model parameters  $\Theta$  to  $n$  randomly selected clients.
      9 Then each selected client computes the update gradient  $\nabla \Theta = \nabla \mathbf{L}(\Theta)$  with their local
         data.
      10 Following the previous work~\cite{ijcai2022, fedattack2022}, we assume they use BPR~\cite{bpr2009}
         with  $L_2$  regularization to train the local model, i.e., the gradient  $\nabla \Theta$  is generated by optimizing the following loss function:
      11 \begin{equation}\nonumber
      12 
$$\nabla \Theta = \frac{1}{n} \sum_{i=1}^n \left( \hat{y}_i - \hat{y}_{-i} \right) \nabla \log \sigma(\hat{y}_i - \hat{y}_{-i}) + \lambda \nabla \parallel \Theta \parallel_2^2,$$

      13 \end{equation}
      14 where  $\sigma$  is the sigmoid function.
      15  $\hat{y}_i$  and  $\hat{y}_{-i}$  are the predicted ranking scores
         of the positive and negative items.
      16 Next, the client uploads  $\nabla \Theta$  to the server and updates the local user model with  $\nabla \Theta$ , which is
         not uploaded due to its privacy-sensitivity~\cite{fairrec2021, fedrecattack2022}.
      17 Finally, the server aggregates all the received gradients with certain aggregation rules and
         updates the global model.
      18 Such training round proceeds iteratively until convergence.
      19
      20 You, last month | 1 author (You)
      21 \subsection{Threat Model}
      22 You, last month | 1 author (You)
      23 \subsubsection{Attack Goal}
      24 The attacker aims to degrade the overall performance of the FedRec system on arbitrary inputs.
      25 \subsubsection{Attack Capability and Knowledge}
      26 Since a recommendation system generally has millions of users, we assume the set of malicious
         clients is small. Fang et al. (2020) propose to perturb the uploaded gradient by adding noise in opposite directions inferred from normal updates. However, these methods usually require a large fraction of malicious clients (e.g., 20%) to achieve a significant performance degradation, which is unrealistic for a FedRec system with millions of users. To protect the FL system from potential poisoning attacks, researchers have also proposed several Byzantine-robust FL methods in the past few years (Yin et al. 2018; Wang et al. 2020). Although these defense methods can guarantee the convergence of the global model, we found that most of them perform poorly against carefully-designed poisoning attacks in the FedRec scenario. Due to the diversity of user interests, the training data on each client is highly non-IID. Some gradients uploaded by benign clients may also deviate from others, which makes it more difficult for the server to distinguish these malicious gradients. Our UNION mechanism can be combined with existing Byzantine-robust FL methods and improves their performance against many untargeted poisoning attacks, especially our ClusterAttack.


The main contributions of our work are listed as follows:



- We propose ClusterAttack, a novel untargeted model poisoning attack method, which reveals the security risk of FedRec systems even with existing defense methods.
- We propose UNION, a defense mechanism that improves the resistance of FedRec systems against various untargeted poisoning attacks. To our best knowledge, it is the first defense mechanism specialized for FedRec systems.
- Extensive experiments on two public datasets validate the effectiveness of our ClusterAttack and UNION methods.



### 3 Preliminaries



In this section, we introduce the settings of federated recommendation systems and the threat model used in this work.



#### 3.1 Federated Recommendation Systems



Poisoning attacks against recommender systems and their defense have been widely studied in the past decades (Lam and Riedl 2004; Moshaver, Burke, and Sandvig 2006; Zhou et al. 2016). However, these researches mainly focus on the centralized recommendation model training. They require the attacker or the server to have strong knowledge of the full training data to perform effective attacks or defenses, such as all user profiles (Burke et al. 2006) or the entire rating matrix (Li et al. 2016). These methods are infeasible under the FL setting since the server cannot access the data of the clients. Recently, some targeted poisoning attack methods have been proposed to boost certain target items in the FedRec scenario (Zhang et al. 2022; Rong et al. 2022), while the untargeted attack and its defense are still less explored. Wu et al. (2022) is a recent untargeted data poisoning attack against FedRec systems. It subverts the local model training by choosing items closest to the user embedding as negative samples and these farthest ones as positive samples. However, it only manipulates the input training data while keeping the local training algorithm unmodified, which limits its attack effect. Our ClusterAttack utilizes the vulnerability of FL and performs a more powerful model poisoning attack:


$$L_{\text{res}} = -\log(\sigma(\hat{y}_p - \hat{y}_n)) + \lambda \parallel \Theta \parallel_2^2,$$


where  $\sigma$  is the sigmoid function,  $\hat{y}_p$  and  $\hat{y}_n$  are the predicted ranking scores of the positive and negative items. Next, the


```



Conclusions

30

■ English Writing

□ Grammarly

The screenshot shows a Grammarly document titled "Untitled document". The text discusses Federated recommendation (FedRec) and its susceptibility to poisoning attacks, specifically targeting and untargeted attacks. It also mentions the proposed ClusterAttack and UNION defense mechanism.

All suggestions

CONCISENESS

In fact, untargeted

It appears that ***In fact***, may be unnecessary in this sentence. Consider removing it.

Learn more

Overall score: 97

Goals: 3 of 4 set

Correctness: Looking good

Clarity: Clear

Engagement: Engaging

Delivery: Just right

Premium: Advanced suggestions (3)

Get Expert Writing Help

Plagiarism

221 words



Conclusions

31

■ English Writing

□ QuillBot

The screenshot shows the QuillBot interface with two main sections. On the left, the original text is displayed:

Modes: Standard Fluency Formal Simple Creative Expand Shorten

Federated recommendation (FedRec) can train personalized recommenders without collecting user data, but the decentralized nature makes it susceptible to poisoning attacks. Most previous studies focus on the targeted attack to promote certain items, while the untargeted attack that aims to degrade the overall performance of the FedRec system remains less explored. In fact, untargeted attacks can disrupt the user experience and bring severe financial loss to the service provider. However, existing untargeted attack methods are either inapplicable or ineffective against FedRec systems.

On the right, the AI-generated paraphrased text is shown with various words highlighted in orange, indicating changes made by the AI:

Synonyms: Rephrase

Without user data, Federated Recommendation (FedRec) can train individualized recommenders, but because it is decentralized, it is vulnerable to poisoning attempts. The majority of earlier research has concentrated on targeted attacks meant to promote certain products, but untargeted attacks meant to harm the FedRec system's overall performance have received less attention. Untargeted attacks can actually ruin the user experience and cost the service provider a lot of money. On the other hand, FedRec systems are inaccessible to or ineffectual against current untargeted attack techniques.

82 Words Rephrase 1/4 Sentences • 84 Words ⓘ ⓘ ⓘ

● Changed Words ○ Structural Changes ● Longest Unchanged Words ⓘ

Conclusions

32

■ English Writing

□ DeepL, Academic Phrasebank, etc.



GENERAL LANGUAGE FUNCTIONS

- Being cautious
- Being critical**
- Classifying and listing
- Compare and contrast
- Defining terms
- Describing trends
- Describing quantities
- Explaining causality
- Giving examples
- Signalling transition
- Writing about the past

An enhanced and expanded version of PHRASEBANK is available in PDF or Kindle format:

 PDF
 Kindle

[ABOUT PHRASEBANK](#)

Being critical

As an academic writer, you are expected to be critical of the sources that you use. This essentially means questioning what you read and not necessarily agreeing with it just because the information has been published. Being critical can also mean looking for reasons why we should not just accept something as being correct or true. This can require you to identify problems with a writer's arguments or methods, or perhaps to refer to other people's criticisms of these. Constructive criticism goes beyond this by suggesting ways in which a piece of research or writing could be improved.

... being against is not enough. We also need to develop habits of constructive thinking.

Edward de Bono

— Highlighting inadequacies of previous studies

Previous studies of X have not dealt with ...
 Researchers have not treated X in much detail.
 Such expositions are unsatisfactory because they ...
 Most studies in the field of X have only focused on ...
 Such approaches, however, have failed to address ...
 Previous published studies are limited to local surveys.
 Half of the studies evaluated failed to specify whether ...
 The research to date has tended to focus on X rather than Y.
 Previously published studies on the effect of X are not consistent.
 Smith's analysis does not take account of ..., nor does she examine ...
 The existing accounts fail to resolve the contradiction between X and Y.
 Most studies of X have only been carried out in a small number of areas.
 However, much of the research up to now has been descriptive in nature ...
 The generalisability of much published research on this issue is problematic.
 Research on the subject has been mostly restricted to limited comparisons of ...
 However, few writers have been able to draw on any systematic research into ...
 Short-term studies such as these do not necessarily show subtle changes over time ...
 Although extensive research has been carried out on X, no single study exists which ...
 However, these results were based upon data from over 30 years ago and it is unclear if ...
 The experimental data are rather controversial, and there is no general agreement about ...

+ Identifying a weakness in a single study or paper



Thanks!

Q&A