RUTGERS

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

InstructAgent: Building User Controllable Recommender via LLM Agent

Wujiang Xu
Rutgers University
United States

Yunxiao Shi
University of Technology Sydney
Australia

Zujie Liang
Ant Group
China

Xuying Ning
University of Illinois
Urbana-Champaign
United States

Kai Mei
Rutgers University
United States

Kun Wang
Nanyang Technological University
Singapore

Xi Zhu
Rutgers University
United States

Min Xu
University of Technology Sydney
Australia

Yongfeng Zhang*
Rutgers University
United States

-- Present by Yunxiao Shi

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

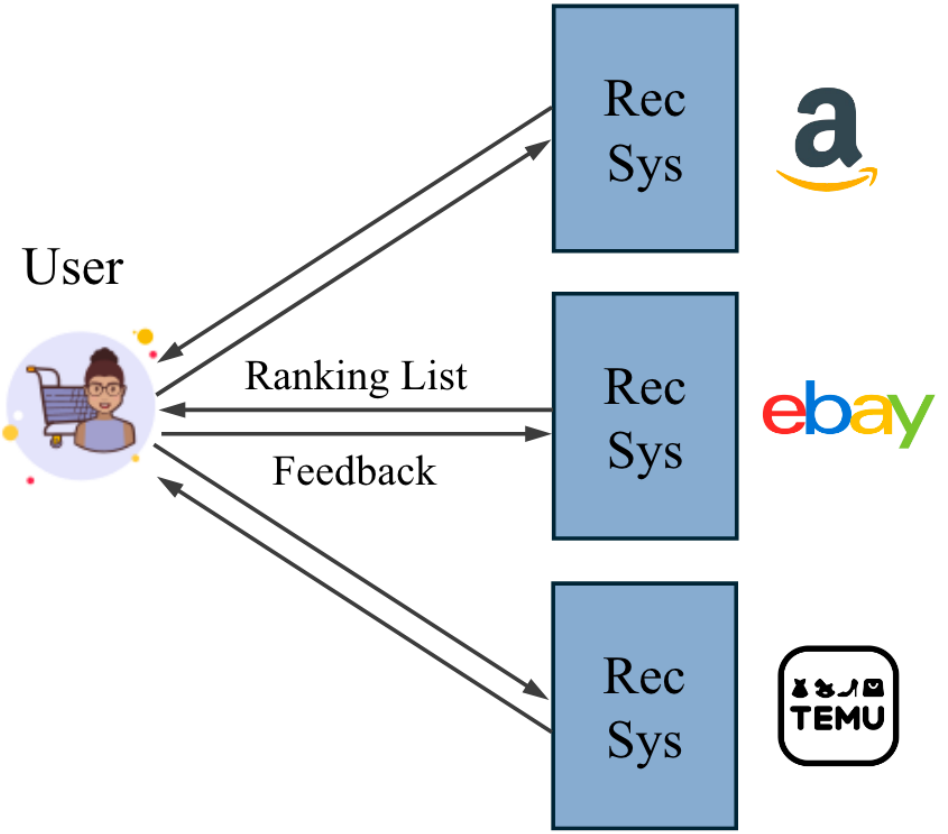
HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Rethink Recommenders

- Platform-centric by design.
  Sophisticated models maximise clicks & revenue rather than user intent.
- Zero user control, low transparency.
  Users cannot steer or inspect the algorithm's logic or objectives
- Echo-chamber & filter-bubble effects.
  Repeatedly reinforced interests → reduced diversity, potential manipulation.
- Bias toward *active* users.
  Collaborative learning skews toward heavy-interaction profiles, harming the long-tail (less-active) majority.
- Take-away → Need a *protective layer*.
  Insert an agent that *interprets free-text instructions* and re-ranks results on the user's behalf.



(a) Previous User-Platform Paradigm

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

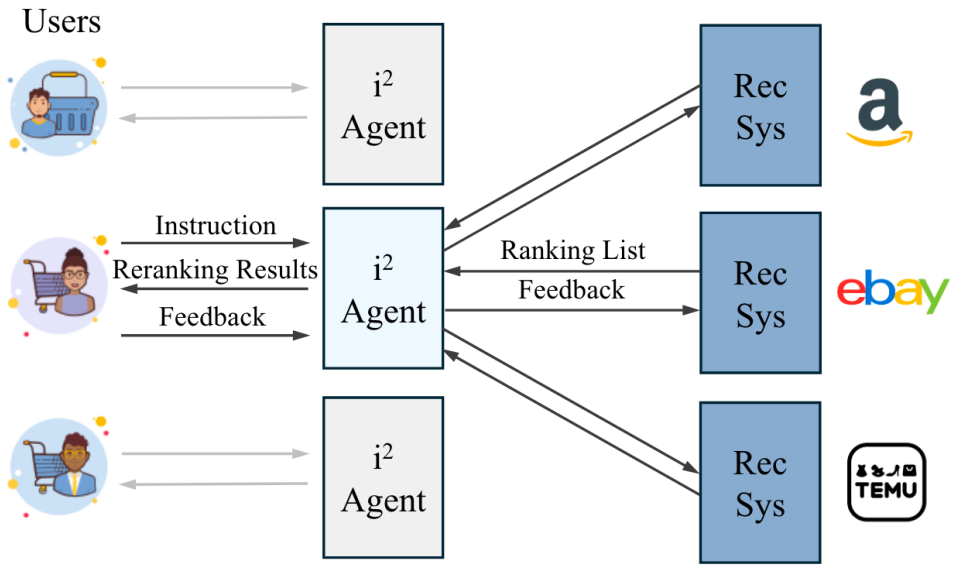
Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Paradigm Shift: User-Agent-Platform

- Previous Paradigm (User ↔ Platform).
  - Direct exposure: ranking list entirely determined by platform algorithms
  - User feedback **aggregated** with all users → individuality diluted
  - Vulnerable to commercial bias, echo chambers, manipulation

- Our Paradigm (User ↔ LLM Agent ↔ Platform)
  - Instruction parsing. Free-text commands express nuanced intent (e.g., *"I want non-violent sci-fi classics under $20"*)
  - Knowledge infusion. Agent retrieves internal & external knowledge to contextualise intent
  - Personal reranking. Agent reorders platform list, applies self-reflection to avoid hallucination
  - Individual memory (Instruct2Agent). Dynamic profile learned solely from this user's feedback



(b) Ours User-Agent-Platform Paradigm

> **Outcome**: Users regain control, diversity improves, less-active users protected.

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Our Key Contributions

❖ InstructRec Benchmark.
- 4 public datasets (Amazon-Book, Amazon-MovieTV, Goodreads, Yelp)
- Each interaction paired with *free-text* user instruction
- Enables instruction-aware evaluation in RS research

❖ InstructAgent (v1).
- Parser → Reranker → Self-Reflection pipeline
- Zero-shot LLM reranking guided by instruction + knowledge
- Hallucination rate ↓ > 20× with lightweight reflection

❖ InstructAgent (v2).
- Adds Dynamic Memory: profile generator + extractor
- Learns solely from individual feedback → protects less-active users
- Delivers +16.6 % average lift over SOTA baselines across 12 metrics

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

InstructRec Benchmark Construction

❖ Two-step pipeline (Figure 3)

- **(a) Instruction Generator.** Few-shot GPT-4o-mini with persona prompts ; Creates free-text instructions from user reviews.
- **(b) Instruction Cleaner.** LLM tries to guess the ground-truth item ; Keep only instructions where guessing fails (no leakage)

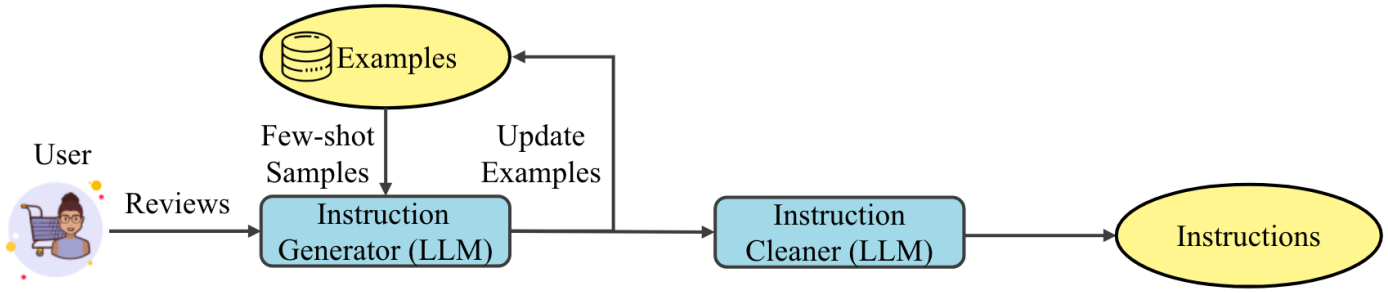


Figure 3: The overview of our InstructRec dataset construction.

❖ Four public domains (Table 2)

❖ Why it matters

- First benchmark pairing every interaction with flexible, free-text intent
- Enables evaluation of instruction parsing & user-side reranking in RS research

Table 2: Statistics of the InstructRec dataset: $|\mathcal{U}|$, $|\mathcal{V}|$, and $|\mathcal{E}|$ represent the number of users, items, and interactions, respectively. $\#|X_I|$ denotes the average token length of user instructions, while $\#|S_U|$ represents the average token length of the user's static memory.

Dataset	$\lvert\mathcal{U}\rvert$	$\lvert\mathcal{V}\rvert$	$\lvert\mathcal{E}\rvert$	Density	$\#\lvert X_I\rvert$	$\#\lvert S_U\rvert$
InstructRec - Amazon Book	7,377	120,925	207,759	0.023%	164	1276
InstructRec -Amazon Movietv	5,649	28,987	79,737	0.049%	40	726
InstructRec - Goodreads	11,734	57,364	618,330	0.092%	41	2827
InstructRec - Yelp	2,950	31,636	63,142	0.068%	40	1976

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Task Definition & Paradigm Comparison

❖ Task Definition

Consider a set of users $\mathcal{U}$ and items $\mathcal{I}$.

For each user $u \in \mathcal{U}$, past interactions are recorded as an ordered sequence

$$S_u = [s_1, s_2, \ldots, s_T], \qquad s_i \in \mathcal{I}.$$

Beyond purely sequential signals, we also leverage the user's free-text instructions Ω_u and real-time environmental context E.

Let ψ_u denote user-specific parameters.

The objective is

$$\hat{i} = \arg\max_{i \in \mathcal{I}} P(s_{T+1} = i \mid S_u, \Omega_u, E; \psi_u). \quad (3$$

Here:

- Ω_u — the set of current instructions issued by user u;
- E — the external environment supplying real-time signals to the agent;
- ψ_u — parameters personalised to user u.

❖ Paradigm Comparison

Table 1: Difference between previous recommendation models and our model.

Model	Instruction Awareness	Instruction Type	Dialogue Interaction	Dynamic Interest	Learning from Feedback	External Knowledge
SR	✗	N/A	N/A	✗	✗	✗
CRS	✓	Fixed	Multiple Turns	✓	✗	✗
RecAgent	✗	N/A	N/A	✗	✗	✓
Ours	✓	Flexible	0, 1, or Multiple Turns	✓	✓	✓

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

InstructAgent (V1 & V2) Architecture

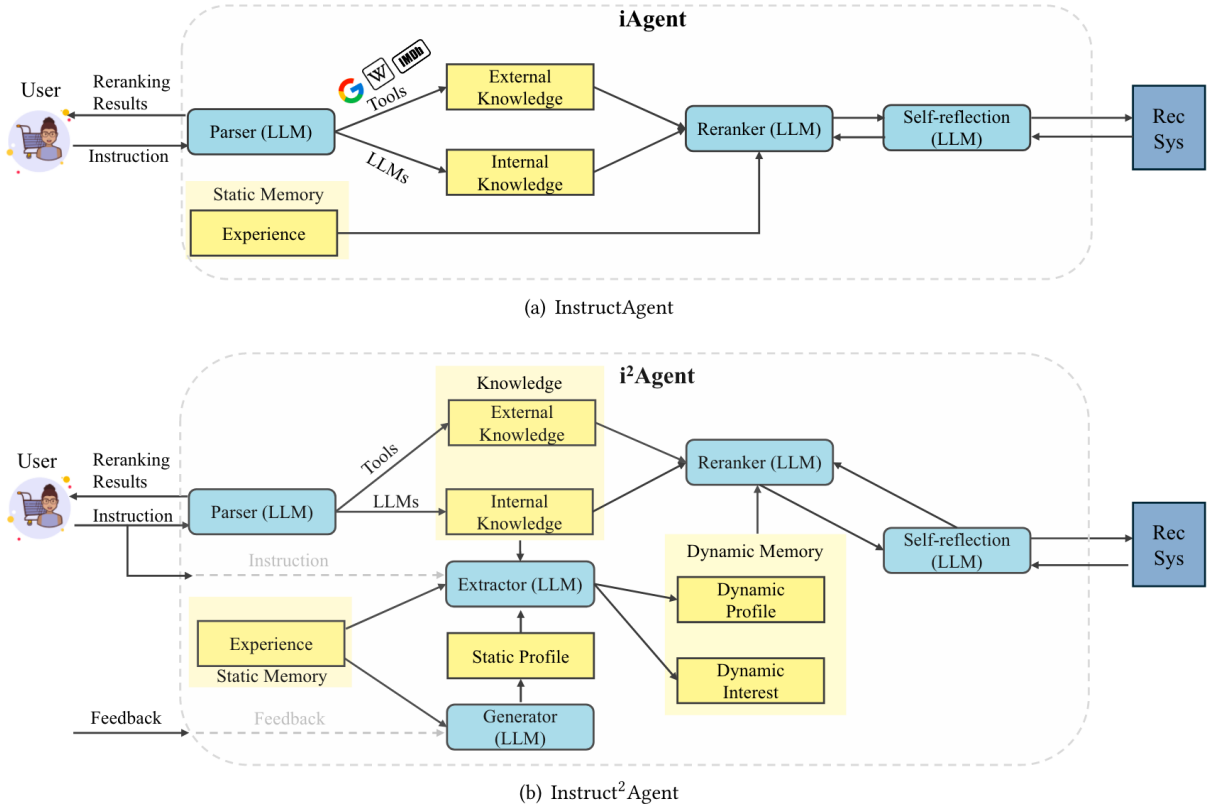


Figure 2: Workflow of our proposed agents. (a) InstructAgent explores the relative knowledge under the user's instruction and provides the reranking results refined by the self-reflection mechanism. (b) Instruct^{2}Agent designs the dynamic memory mechanism to improve the personalized ability of InstructAgent.

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Main Ranking Results (RQ1)

Table 3: Evaluation results (%) of the ranking metric (↑) on the InstructRec. We highlight the methods with the first, second and third best performances.

Model	InstructRec - Amazon Book				InstructRec - Amazon Movietv			
	HR@1	HR@3	NDCG@3	MRR	HR@1	HR@3	NDCG@3	MRR
GRU4Rec	11.00	31.41	22.53	30.10	15.80	36.85	27.63	34.36
BERT4Rec	11.48	30.90	22.32	30.31	14.74	35.13	26.36	33.43
SASRec	11.08	31.34	22.42	30.15	34.52	49.71	43.18	48.06
BM25	9.92	24.48	18.21	27.00	11.29	30.27	22.09	30.04
BGE-Rerank	25.36	45.90	37.11	42.84	25.44	47.48	38.02	43.28
EasyRec	**30.70**	**48.87**	**41.09**	**46.14**	**34.96**	**61.30**	**50.15**	**52.98**
ToolRec	10.56	30.60	21.88	29.77	13.84	35.67	26.20	33.21
AgentCF	14.24	34.16	25.55	32.77	25.90	49.82	39.64	44.23
InstructAgent	**31.89**	**48.99**	**41.69**	**47.23**	**38.19**	**56.87**	**48.93**	**53.04**
Instruct^{2}Agent	**35.11**	**53.51**	**45.64**	**50.28**	**46.43**	**65.77**	**57.67**	**60.43**

Table 4: Evaluation results (%) of the ranking metric (↑) on InstructRec.

Model	InstructRec - Goodreads				InstructRec - Yelp			
	HR@1	HR@3	NDCG@3	MRR	HR@1	HR@3	NDCG@3	MRR
GRU4Rec	15.36	39.52	29.08	35.41	10.94	30.67	21.88	29.70
BERT4Rec	12.70	34.69	25.02	32.32	10.99	31.02	22.32	30.05
SASRec	18.52	41.24	31.47	37.60	12.59	31.09	22.65	30.15
BM25	14.25	40.34	29.01	35.40	12.85	33.08	24.34	31.85
BGE-Rerank	17.26	40.82	30.60	36.97	**33.05**	55.29	45.70	**49.90**
EasyRec	13.94	35.38	26.11	33.27	32.41	**56.31**	**46.04**	49.86
ToolRec	19.06	42.79	32.61	38.44	12.07	30.92	22.83	30.21
AgentCF	**21.61**	**46.09**	**35.60**	**40.96**	13.36	34.83	25.66	32.61
InstructAgent	**23.56**	**47.01**	**36.98**	**42.19**	**37.40**	**56.33**	**48.28**	**52.42**
Instruct^{2}Agent	**30.97**	**56.69**	**45.76**	**49.14**	**39.22**	**57.92**	**49.96**	**53.78**

Echo Chamber Effect. (RQ2)

Key takeaways

- **Evaluation setup:**
  Ads from unrelated domains are randomly inserted into the candidate list to mimic real-world advertising while controlling for position bias.
- **Instruction awareness:**
  Instruct2Agent correctly interprets user instructions and filters out unwanted ads.
- **Profile construction:**
  Because it builds user profiles from explicit feedback rather than purely data-driven training, the model avoids over-fitting to popularity.
- **Diversity & performance:**
  It recommends a broader mix of active and less-active items, boosting both diversity and overall recommendation quality.
- **Echo-chamber mitigation:**
  These results show that Instruct2Agent acts as a "protective shield," reducing echo-chamber effects. (Full metrics are available in Appendix B.3.1.)

Table 5: Evaluation of the echo chamber effects (%) (↑) on InstructRec.

Model	InstructRec - Amazon Book				InstructRec - Yelp			
	FR@1	FR@3	P-HR@3	P-MRR	FR@1	FR@3	P-HR@3	P-MRR
EasyRec	**68.41**	**64.32**	**59.28**	**56.09**	**76.45**	**66.50**	**61.05**	**56.85**
ToolRec	70.13	66.61	36.74	35.80	72.64	63.64	32.50	32.73
AgentCF	58.02	50.04	41.10	39.42	71.30	64.15	38.46	36.44
InstructAgent	**71.98**	**67.82**	**59.51**	**57.32**	**78.24**	**69.71**	**62.74**	**58.76**
Instruct^{2}Agent	**77.15**	**70.15**	**64.70**	**60.87**	**87.69**	**84.20**	**64.48**	**60.20**

Protect Less-Active Users. (RQ3)

- **Segmentation rule:**
  Top 20 % of users → **"active"**; remaining *80 %* → **"less-active"**.
- **Data characteristic:**
  10-core sampling yields rich behavior logs; longer histories hurt baseline LLMs ⇒ active users start with lower accuracy.
- **Core finding (Table 6):**
  Instruct2Agent boosts performance for *both* segments despite length issues.

Table 6: The performance (%) of active and less-active users on InstructRec - Amazon book.

Model	Less-Active Users				Active Users			
	HR@1	HR@3	NDCG@3	MRR	HR@1	HR@3	NDCG@3	MRR
EasyRec	**32.93**	**51.07**	**43.32**	**48.04**	**28.71**	**47.64**	**39.53**	**44.61**
ToolRec	10.57	30.86	22.01	29.88	10.04	31.73	22.32	29.54
AgentCF	14.79	35.00	26.26	33.35	14.87	34.37	25.93	33.24
InstructAgent	34.07	50.79	43.67	49.00	29.96	47.73	40.14	45.71
Instruct^{2}Agent	37.92	55.75	47.84	52.11	33.27	51.74	43.81	48.67

InstructAgent: Building User Controllable Recommender via LLM Agent

- by Wujiang Xu, Yunxiao Shi et al.

HCRS '25

Proceedings of the The 1st Workshop on Human-Centered Recommender Systems at The 2025 ACM Web Conference

28 April - 2 May 2025 | Sydney, Australia

Model Study. (RQ4)

- **Objective**

  Test whether a *self-reflection* prompt can curb LLM hallucinations in recommendation reranking.

- **Method**

  - Added the mechanism to **ToolRec [75]** and **AgentCF [71]**:

    LLM first returns an initial ranking, then "reflects" to generate a revised list.

- **Key result (Fig. 4)**

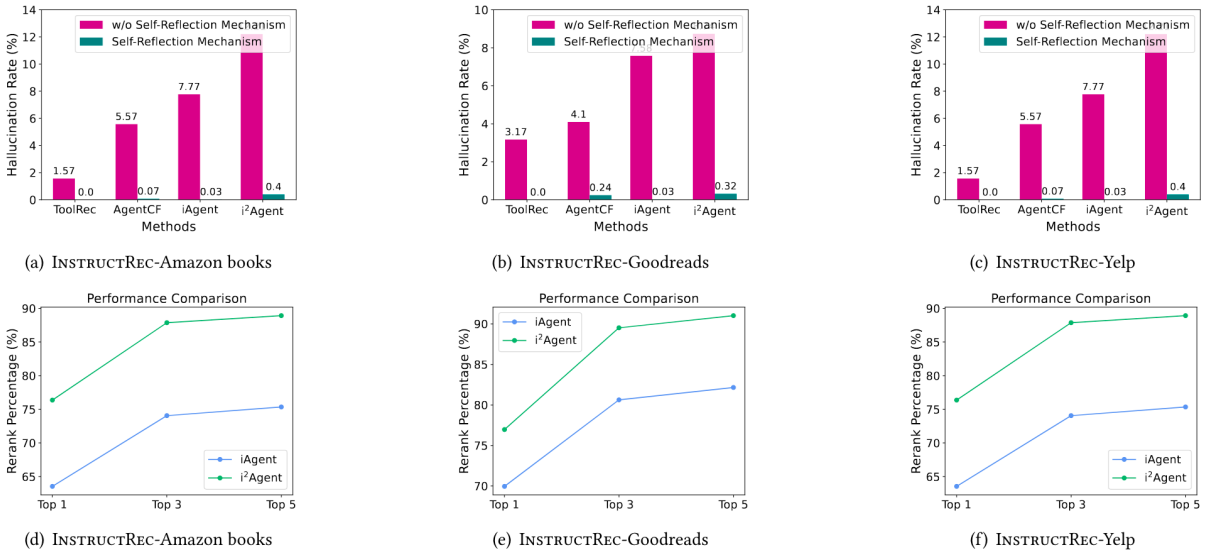
  Self-reflection slashes hallucination rates by **≥ 20×** for both models.

- **Limitations**

  Instruct2Agent shows the highest residual error—longer input sequences cause partial information loss.

- **Take-away**

  Self-reflection is an effective, lightweight safeguard against LLM-induced hallucinations.



(a) InstructRec-Amazon books (b) InstructRec-Goodreads (c) InstructRec-Yelp

(d) InstructRec-Amazon books (e) InstructRec-Goodreads (f) InstructRec-Yelp

Figure 4: The first row presents the hallucination rate with and without the self-reflection mechanism, while the second row illustrates the probability of changes in the ranking list after our reranker.

- **Procedure:**

  1. Generate initial ranked list.
  2. Apply model's re-ranking step.
  3. Compare positions in the top-1/3/5 slices.

- **Finding:**

  Near-universal position shifts—almost every query triggers at least one change.

- **Interpretation:**

  The agent **actively personalises** results rather than pass-through sorting, demonstrating an adaptive final-step refinement.

Conclusions

- We first establish an instruction-aware recommendation benchmark.
- Design a straightforward instruction-aware agent (InstructAgent).
- To enhance the agent's personalized abilities, we propose individual instruction-aware agent (Instruct2Agent), with integrated with dynamic memory mechanism to learn from user's personal feedback and extracts the dynamic interests.

Thank you all for your time and attention!!

- Contact: wujiang.xu@rutgers.edu, Yunxiao.Shi@student.uts.edu.au