

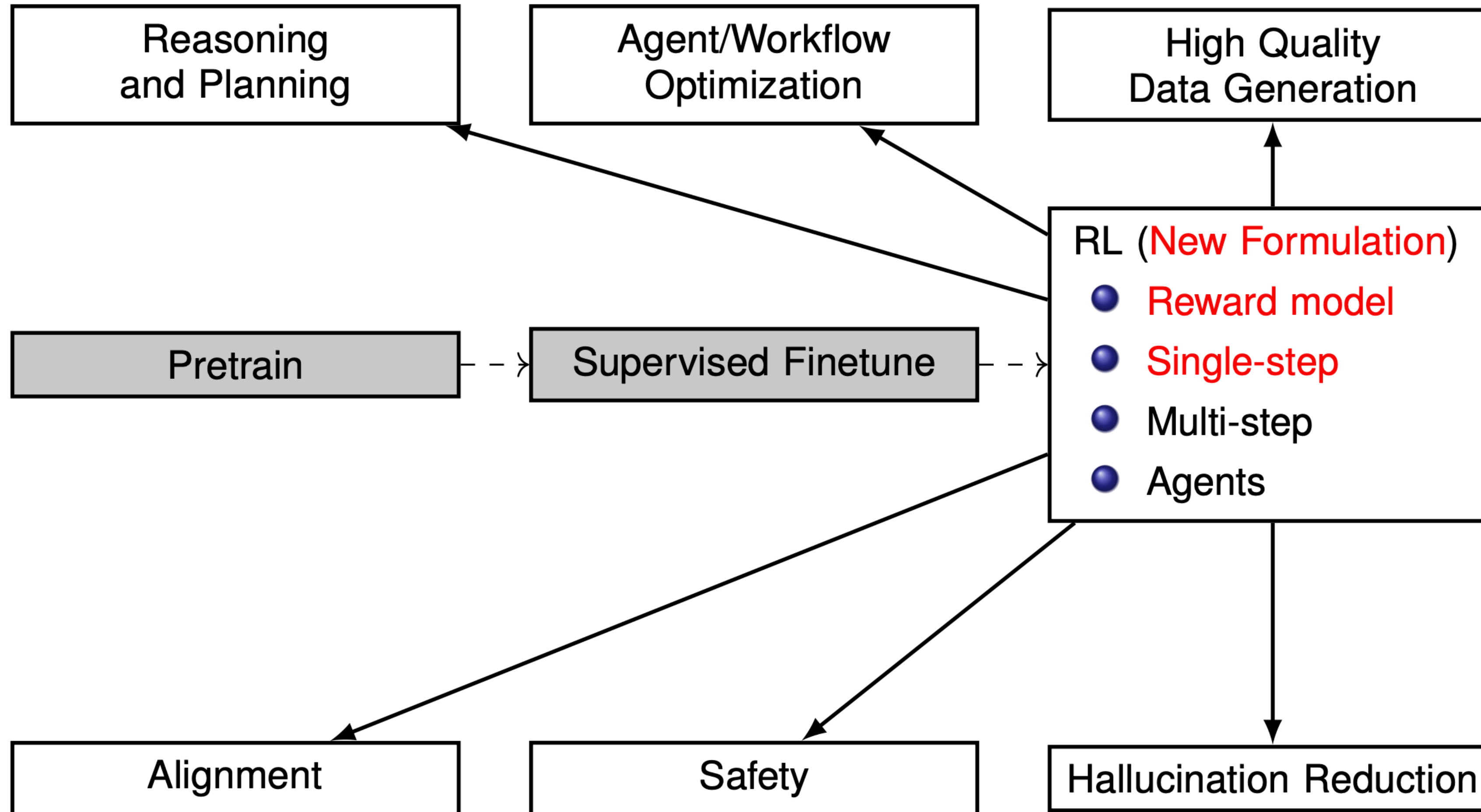
Reinforcement Learning from Human Feedback: *From Theory to Algorithm*

Wei Xiong

University of Illinois Urbana-Champaign



RL Research for Large Language Models

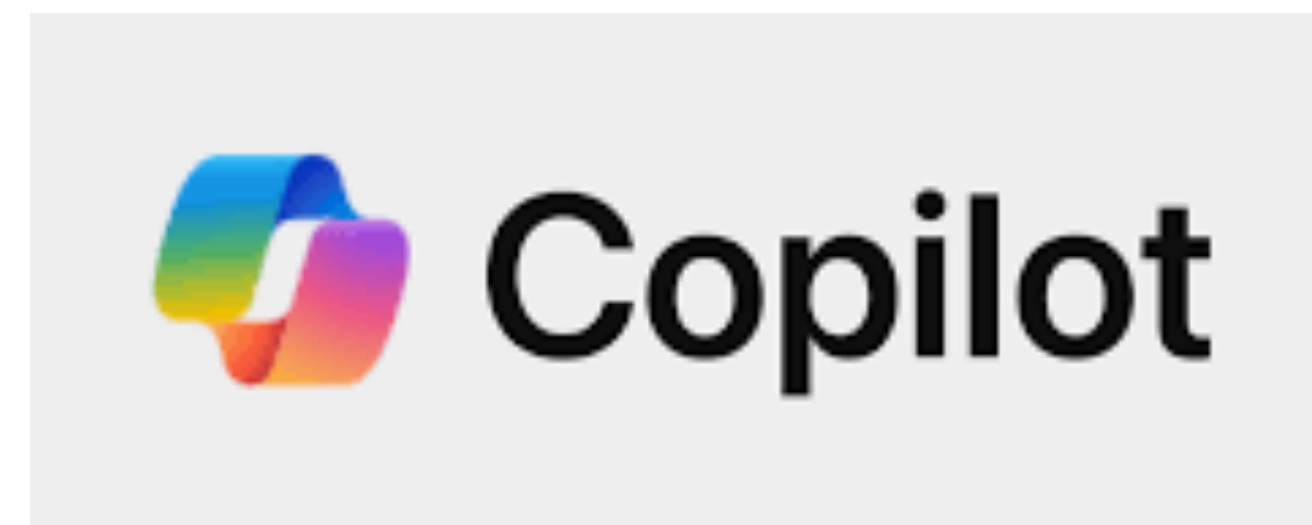


Foundation Generative Models

General ChatBot



Coding Assistant

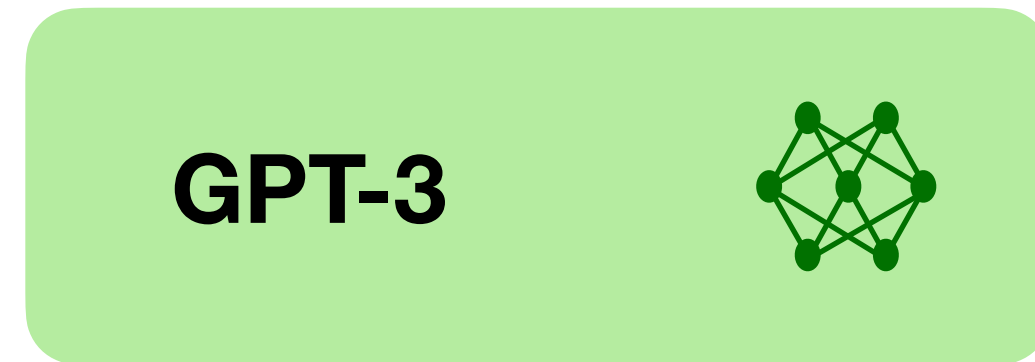
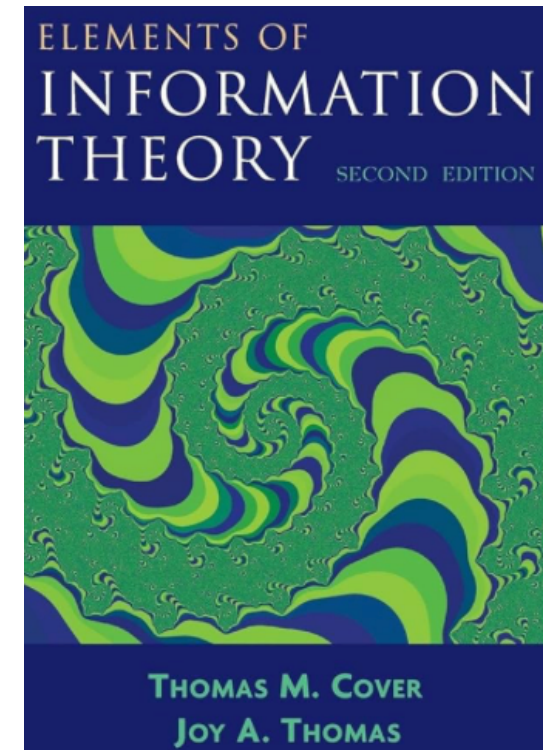


Music, Video, Image Generation



Foundation Model Pipeline

Pre-training

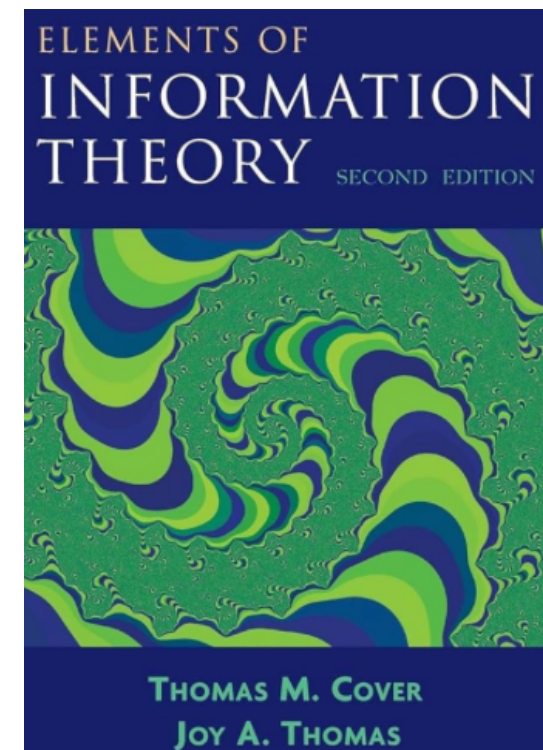


Instruction-following training

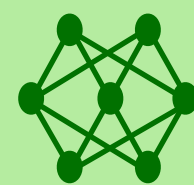
1. **LLM** is trained on a large amount of *unlabelled* data, to predict next token:
 $P(\text{next token} \mid \text{prior tokens})$;
2. Goal: acquire general knowledge.

Foundation Model Pipeline

Pre-training



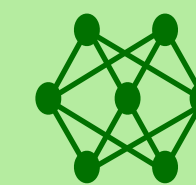
GPT-3



Instruction-following training

Ability to follow humans' instructions.

Text-davinci-002



... culture in Switzerland.
Sushi has been around for a
long time in Switzerland, ...

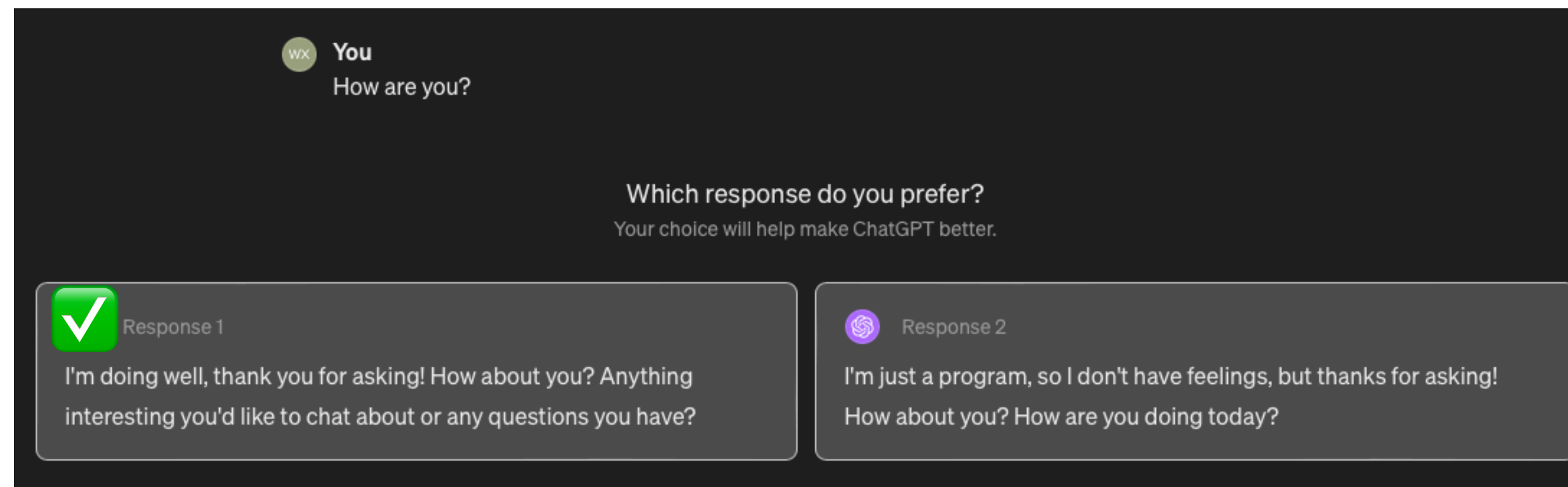
Tell me something
about the sushi

... Sushi is a traditional
Japanese dish that consists of
vinegared rice combined with
various ingredients

Reinforcement Learning from Human Feedback (RLHF)



1. RLHF is the leading technique to adapt the generation distribution to be **preferred by the humans**: *helpful, harmless, and honest*;
2. RLHF learns from *relative feedback*

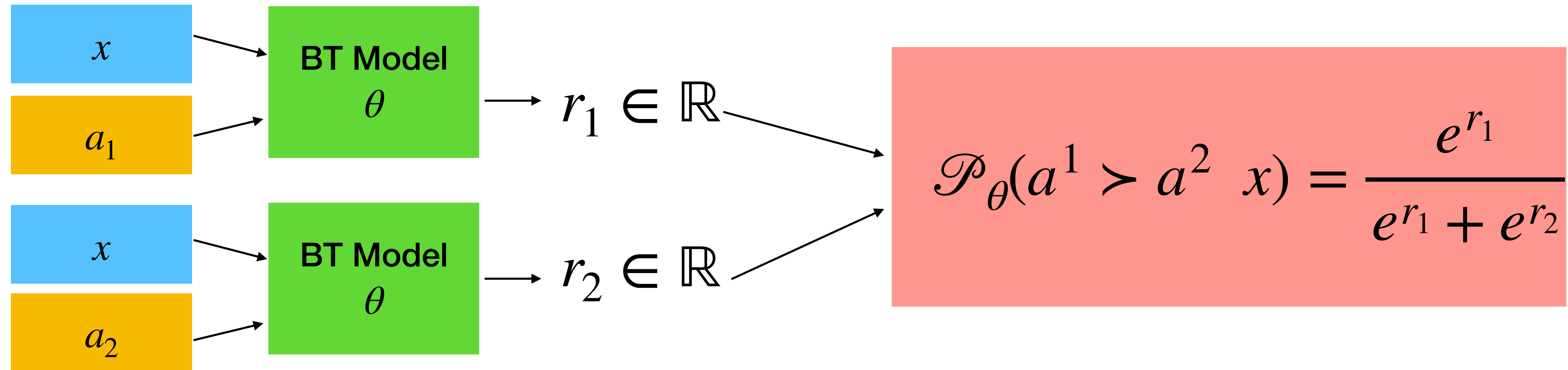


Formulation of LLM and RLHF

Language Model as RL/Bandit Agent

1. **Prompt** $x \in \mathcal{E}$: state from some distribution d_0
 1. Explain the moon landing to a 6 year old child.
2. **Response** $a \in \mathcal{A}$: action
 1. Explain gravity ...
 2. Explain war...
 3. Moon is natural satellite of ...
3. **LLM**: policy $\pi : \mathcal{X} \rightarrow \Delta(\mathcal{A})$
 1. Initial policy π_0 .

Bradley-Terry (BT) Model



- The Bradley-Terry model is a **proxy** of the Human preference
- Linear parameterization: $r^\star(x, a) = \langle \phi(x, a), \theta^\star \rangle$

RLHF as Reverse-KL Regularized Contextual Bandit

In practice, the following regularized learning objective is adopted:

$$\max_{\pi \in \Pi} J(\pi) = \max_{\pi \in \Pi} \mathbb{E}_{x \sim d_0} \left[\underbrace{\mathbb{E}_{a \sim \pi(\cdot | x)} [r^*(x, a)]}_{\text{Optimize Reward}} - \underbrace{\eta \text{KL}(\pi(\cdot | x) \| \pi_0(\cdot | x))}_{\text{Stay Close to } \pi_0} \right].$$

RLHF as Reverse-KL Regularized Contextual Bandit

In practice, the following regularized learning objective is adopted:

$$\max_{\pi \in \Pi} J(\pi) = \max_{\pi \in \Pi} \mathbb{E}_{x \sim d_0} \left[\underbrace{\mathbb{E}_{a \sim \pi(\cdot | x)} [r^*(x, a)]}_{\text{Optimize Reward}} - \underbrace{\eta \text{KL}(\pi(\cdot | x) \| \pi_0(\cdot | x))}_{\text{Stay Close to } \pi_0} \right].$$

- The BT model is not perfect: the major difference from traditional DRL
- The KL-constraint framework admits a stochastic optimal policy;
- The KL constraint optimization problem admits a closed-form solution:

$$\arg \max_{\pi} \left[\mathbb{E}_{a \sim \pi(\cdot | x)} [r(x, a)] - \eta \text{KL}(\pi(\cdot | x) \| \pi_0(\cdot | x)) \right] = \frac{1}{Z(x)} \cdot \pi_0(a | x) \exp\left(\frac{1}{\eta} r(x, a)\right).$$

- where $Z(x) = \sum_{a' \in \mathcal{A}} \pi_0(a' | x) \exp\left(\frac{1}{\eta} r(x, a')\right).$

- Assume the computational oracle: $\mathcal{O}(r, \eta, \pi_0)$

Instruct-GPT Framework to Make Chat-GPT

- **Preference Data Collection:**

- Contextual bandit: $x \sim d_0$, $a^1, a^2 \sim \pi_b(\cdot | x)$ (typically π_0)

- **Preference signal:** $y \sim \mathcal{P}_{BT}^*(\cdot | x, a^1, a^2)$

- **Learning Reward model as MLE:**

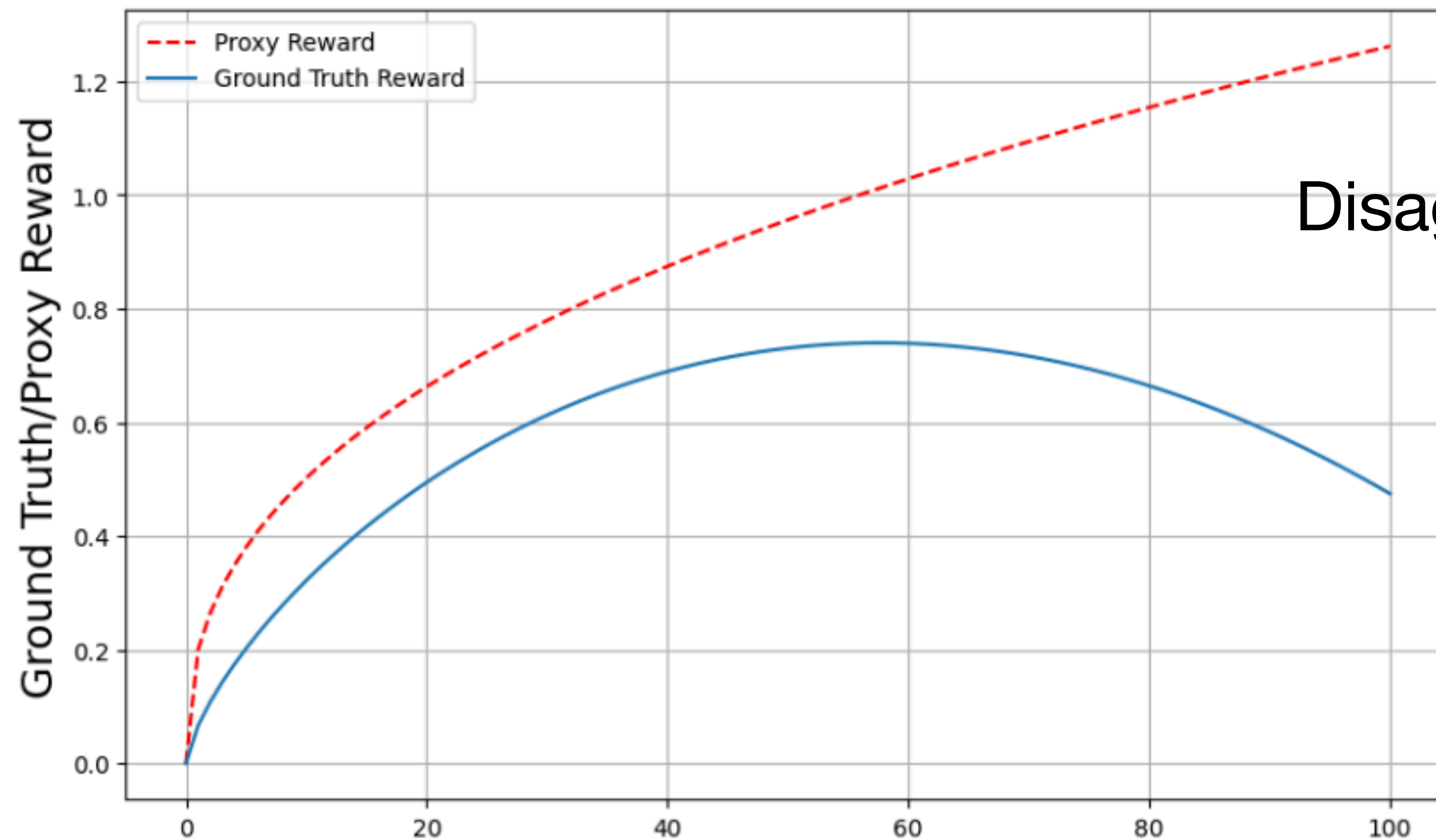
- $$\ell_{\mathcal{D}}(\theta) = \sum_{(x, a^w, a^l) \in \mathcal{D}} \log \left(\sigma \left(r_{\theta}(x, a^w) - r_{\theta}(x, a^l) \right) \right)$$

- **Optimize the learned reward using PPO.**

Fundamental Issue: Reward Hacking

- Heavily optimize the proxy reward leads to ***reward hacking***:
 - Higher reward
 - But worse performance
- The learned ***proxy reward*** are of **issues**:
 - SOTA RMs achieve accuracy ~75% (due to noise and human disagreement)
 - **Sensitivity to sampling distribution** (determined by the behavior policy)
 - Fine-tuning improves *in-distribution* generalization, but often performs poorly *out-of-distribution*.

Fundamental Issue: Reward Hacking



Disagreement between *proxy* and *gold*

Distribution shift: KL between π_0 and tuned policy

Offline Learning from a Fixed Preference Dataset

Insufficient Dataset Coverage

- **Unbalanced Preference Coverage**

- *Prompt A: Can you write a code for ...*

- A good code v.s. another good code;
- A good code v.s. a bad code;
- A bad code v.s. another bad code.
- ...

- *Prompt B: What is the best fitness app?*

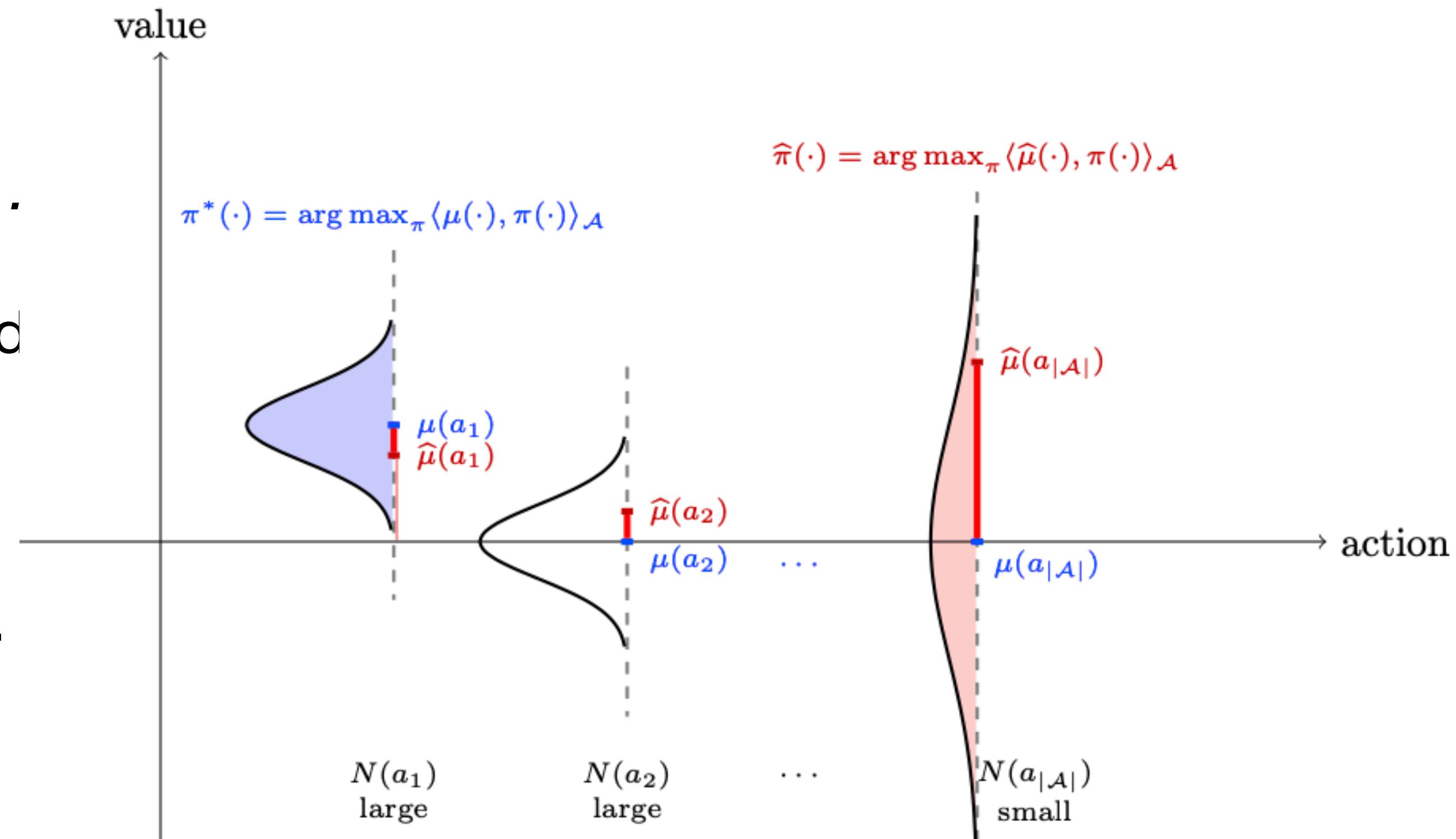
- a^1 : what is fitness app? v.s. a^2 : I am sorry, but I am an AI model...

Insufficient Dataset Coverage

- **Unbalanced Preference Coverage**

- *Prompt A: Can you write a code for ...*

- A good code v.s. another good code
- A good code v.s. a bad code;
- A bad code v.s. another bad code.
- ...



- *Prompt B: What is the best fitness app?*

- a^1 : what is fitness app? v.s. a^2 : I am sorry, but I am an AI model...

RLHF with Pessimism

- **Construct the *Pessimistic* Reward** Lower confidence bound (LCB)

- Compute $\hat{r}(x, a) = r_{\text{MLE}}(x, a) - c \cdot \sqrt{d} \|\phi(x, a) - \underbrace{\phi(x, \pi_0)}_{\text{reference}}\|_{\Sigma_{\text{off}}^{-1}}$,

- Where

$$\Sigma_{\text{off}} = \lambda I + \sum_{x, a^1, a^2 \in \mathcal{D}_{\text{off}}} (\phi(x, a^1) - \phi(x, a^2))(\phi(x, a^1) - \phi(x, a^2))^\top.$$

- **Planning with the Pessimistic Reward:**

- $\hat{\pi}(\cdot | x) = \mathcal{O}(r, \eta, \pi_0)$.

RLHF with Pessimism

Theorem: Guarantee for the Pessimistic RLHF

If the offline dataset covers the target (π^\star, π_0) well:

$$\mathbb{E}_{x \sim d_0, a^1 \sim \pi^\star(\cdot | x), a^2 \sim \pi_0(\cdot | x)} \|\phi(x, a^1) - \phi(x, a^2)\|_{\Sigma_{\text{off}}^{-1}} \leq \frac{C^\star}{\sqrt{n_{\text{off}}}},$$
 then with probability at

least $1 - \delta$, we have

$$J(\pi^\star) - J(\hat{\pi}) + \eta \text{KL}(\pi^\star \| \hat{\pi}) \lesssim \frac{\sqrt{d} \cdot C^\star}{\sqrt{n_{\text{off}}}}$$

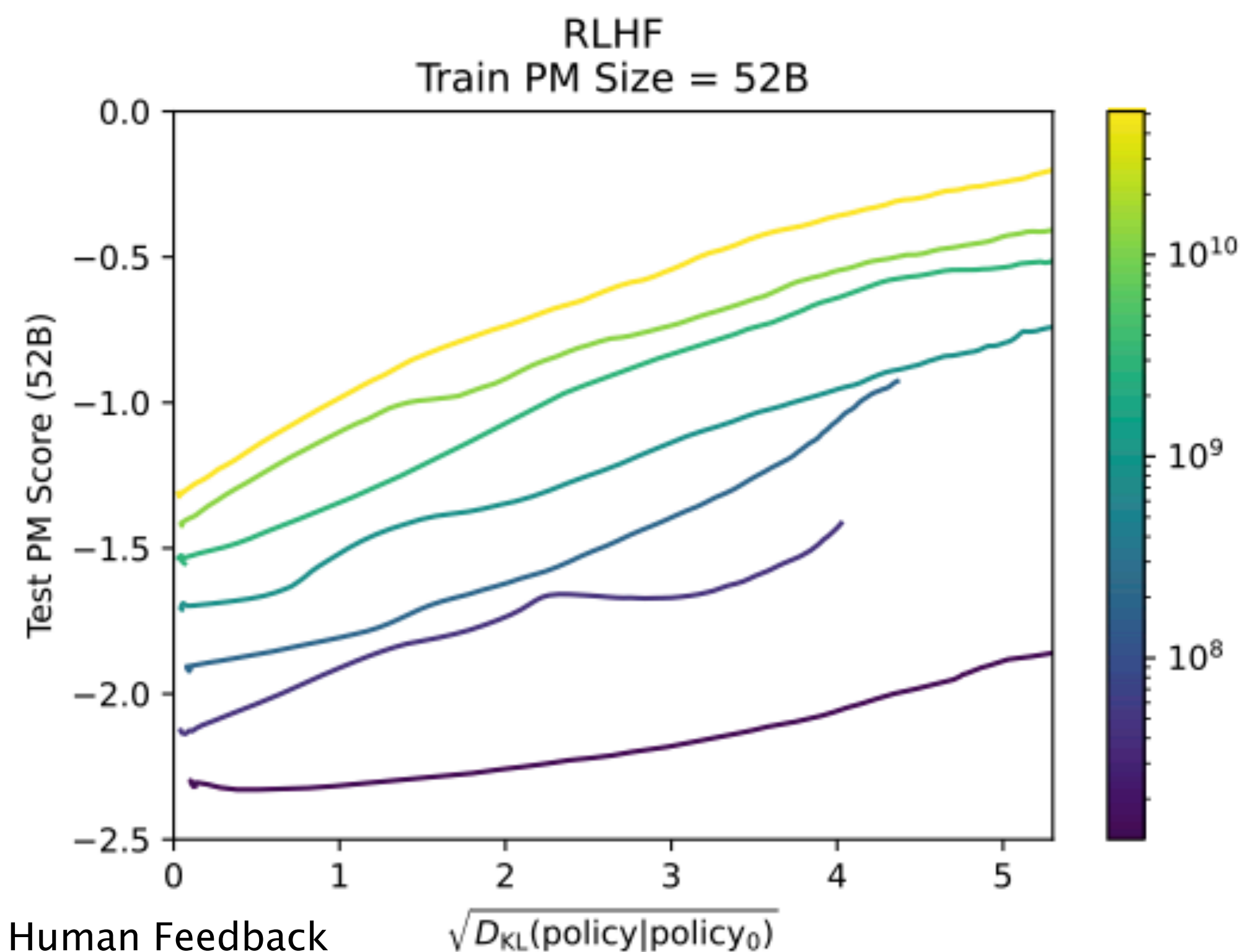
- **Partial coverage:**

- C^\star : *distribution shift* between behavior policy and target policy (π^\star, π_0)

Is a Good Coverage Assumption Practical?

- C^\star : *distribution shift* between behavior policy and coverage target
- Significant shift in open-source dataset due to **the long sequence nature**

$$\text{Average } \frac{\pi_{\text{Mistral-7B-v0.1}}(a \ x)}{\pi_{\text{Gemma-2B-it}}(a \ x)} \approx \exp(80)$$

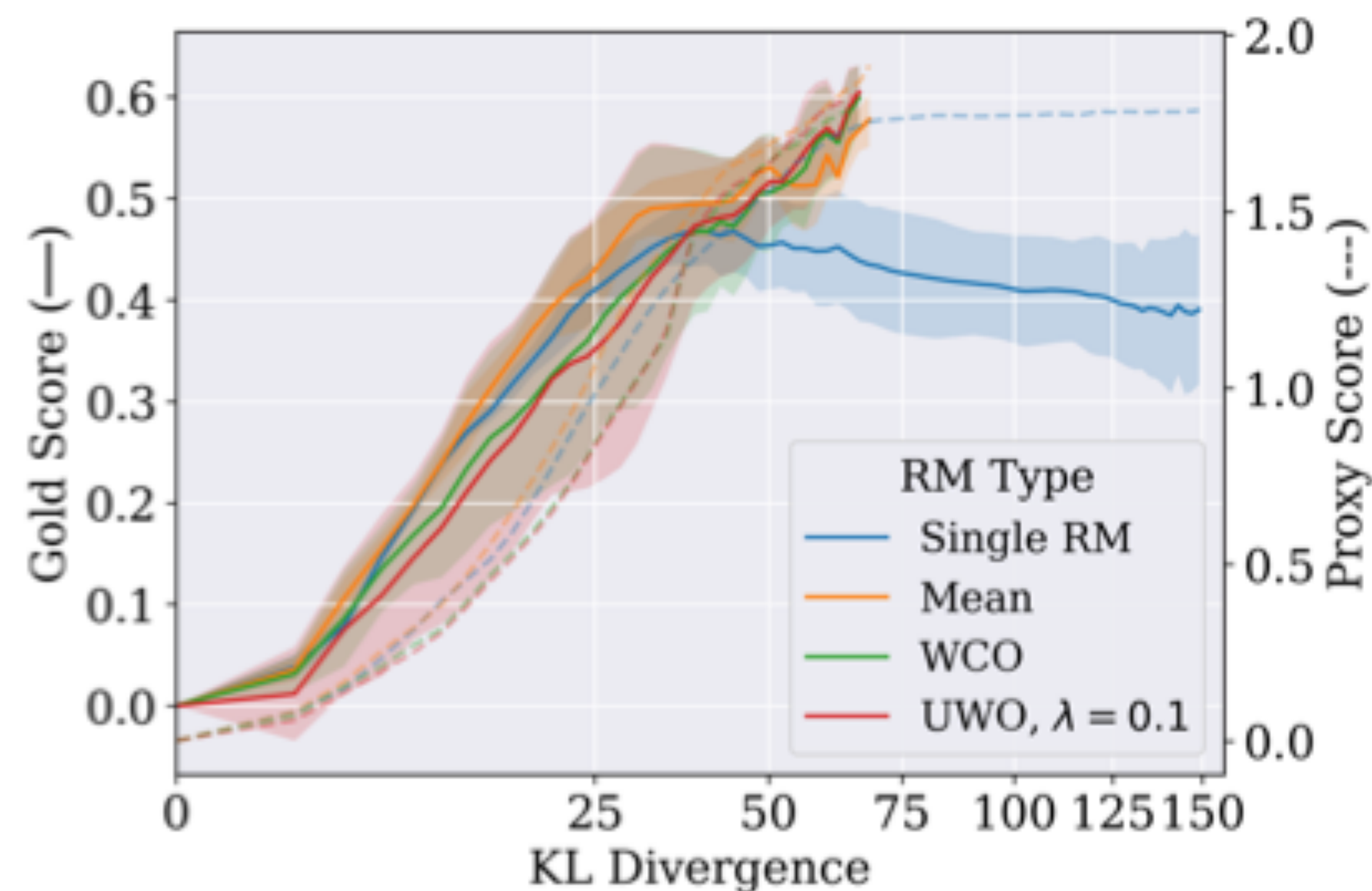


RLHF with Pessimism

- **Pessimism by Ensemble**

- A popular heuristic implementation of pessimism is based on ensemble

$$\hat{r}(x, a) = \min_{k=1, \dots, 5} r_k(x, a) \text{ where } r_k \text{ are independently trained}$$



Batch Hybrid Learning with Online Exploration

RLHF with Only Exploration

- **Batch Hybrid Learning**

- Hybrid: we start with an offline set but can also **query the human during training**
- Batch: we use a large batch size for a sparse update
- **Remark:** PPO with a fixed learned reward: offline learning

- **Intuition: Online Exploration Improves RLHF Policy**

- π_0 can only sample low-reward responses (in-distribution for learned reward);
- During PPO training, the reward gets higher and higher (out-of-distribution);
- Querying human feedback for these high-reward responses mitigates the OOD issue.

Online Iterative RLHF

Initialized with $\mathcal{D} = \mathcal{D}_{\text{off}}$ and define the covariance matrix:

- **For $t = 1, 2, 3, \dots$**
$$\Sigma_{t,m} = \lambda I + \frac{1}{m} \sum_{i=1}^{t-1} \sum_{j=1}^m (\phi(x_{i,j}, a_{i,j}^1) - \phi(x_{i,j}, a_{i,j}^2))(\phi(x_{i,j}, a_{i,j}^1) - \phi(x_{i,j}, a_{i,j}^2))^\top.$$
 - **Exploitation with the main agent:** $\pi_t^1 = \mathcal{O}(\hat{r}_t, \eta, \pi_0)$, with \hat{r}_t as the MLE on \mathcal{D} ;
 - **Choose the enhancer policy:**
 - **(1)** $\pi_t^2 = \arg \max_{\pi' \in \Gamma_t} \|\phi(x, \pi') - \phi(x, \pi_t^1)\|_{\Sigma_{t,m}^{-1}}$
Confidence set: $\Pi_t = \{\pi' : \beta \|\phi(x, \pi') - \phi(x, \pi_t^1)\|_{\Sigma_{t,m}^{-1}} \geq \eta \text{KL}(\pi'(\cdot | x) \| \pi_t^1(\cdot | x))\}$
 - **(2)** $\pi_t^2 = \pi_0$;
 - Collect the m new samples $x_{t,j}, a_{t,j}^1, a_{t,j}^2, y_{t,j} \sim (d_0, \pi_t^1, \pi_t^2, \mathcal{P}_{BT}^\star)$ into \mathcal{D} .

Online Iterative RLHF

Theorem 2 Part 1: Guarantee for the Online Iterative RLHF with optimism

With Option I, if we run the online iterative RLHF with batch size $m = c \cdot \frac{d}{\epsilon^2}$ for $T = \tilde{\Omega}(d)$ times, w.p. at least $1 - \delta$, we can find a $t_0 \in [T]$ such that

$$J(\pi^\star) - J(\pi_{t_0}^1) + \eta \text{KL}(\pi^\star \parallel \pi_{t_0}^1) \leq \epsilon$$

Online Iterative RLHF

Theorem 2 Part 2: Guarantee for the Online Iterative RLHF with offline dataset

With Option II, if we run the hybrid iterative RLHF with batch size $m = c \cdot \frac{d}{\epsilon^2}$ for $T = \tilde{\Omega}(d)$ times, w.p. at least $1 - \delta$, we can find a $t_0 \in [T]$ such that

$$J(\pi^\star) - J(\pi_{t_0}^1) + \eta \text{KL}(\pi^\star \parallel \pi_{t_0}^1) \leq \epsilon + \sqrt{d} \|\mathbb{E}[\phi(x, \pi^\star) - \phi(x, \pi_0)]\|_{\Sigma_{\text{off}+1:t_0}^{-1}}.$$

- **Offline v.s. Hybrid :** under the offline coverage condition, $\pi_t \rightarrow \pi^\star$, online data collected by (π_t, π_0) may cover (π^\star, π_0) better;
- **Online v.s. Hybrid:** optimism v.s. additional offline dataset coverage.

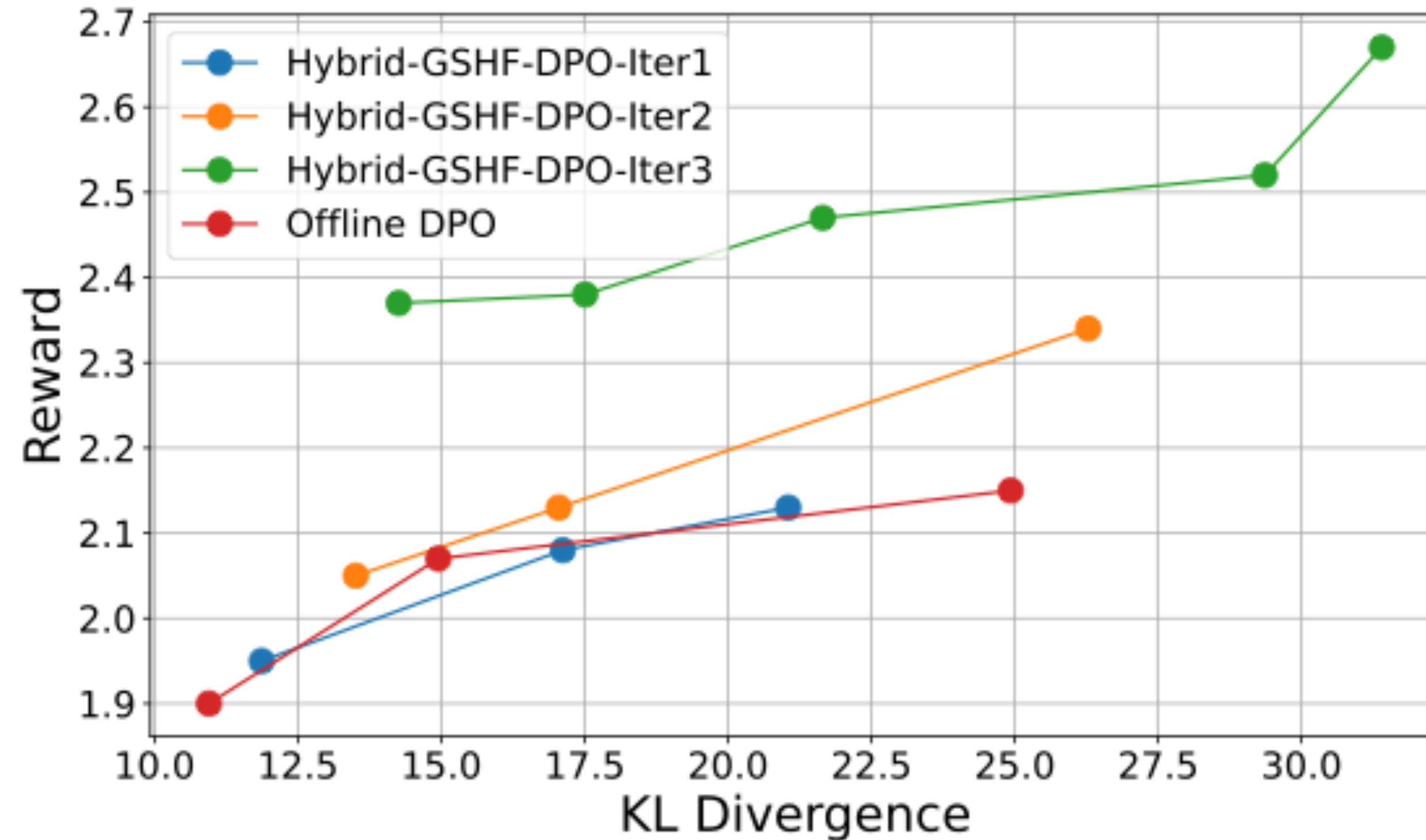
Practical Algorithm: Approximate the Computational Oracle

Computation oracle: $\mathcal{O}(r, \eta, \pi_0) := \arg \max_{\pi} \mathbb{E}_{a \sim \pi(\cdot | x)} [r(x, a) - \eta \text{KL}(\pi(\cdot | x) \| \pi_0(\cdot | x))]$

- **PPO** with regularized reward $\hat{r}(x, a) = r(x, a) - \eta \log \frac{\pi(a | x)}{\pi_0(a | x)}$.
 - Loading 4 models at the same time: tuned model, critic, reward, and π_0 .
- **DPO**, SLiC, IPO, InfoNCA, GPO: different choices of the binary classification loss
 - Direct Preference Optimization skips the reward modeling and optimize

$$L(\theta, \eta, \pi_0) = - \sum_{(x, a^w, a^l) \in \mathcal{D}} \log \sigma \left(\eta \log \frac{\pi_{\theta}(a^w | x)}{\pi_0(a^w | x)} - \eta \log \frac{\pi_{\theta}(a^l | x)}{\pi_0(a^l | x)} \right).$$

Online Iterative RLHF: Experimental Result 1

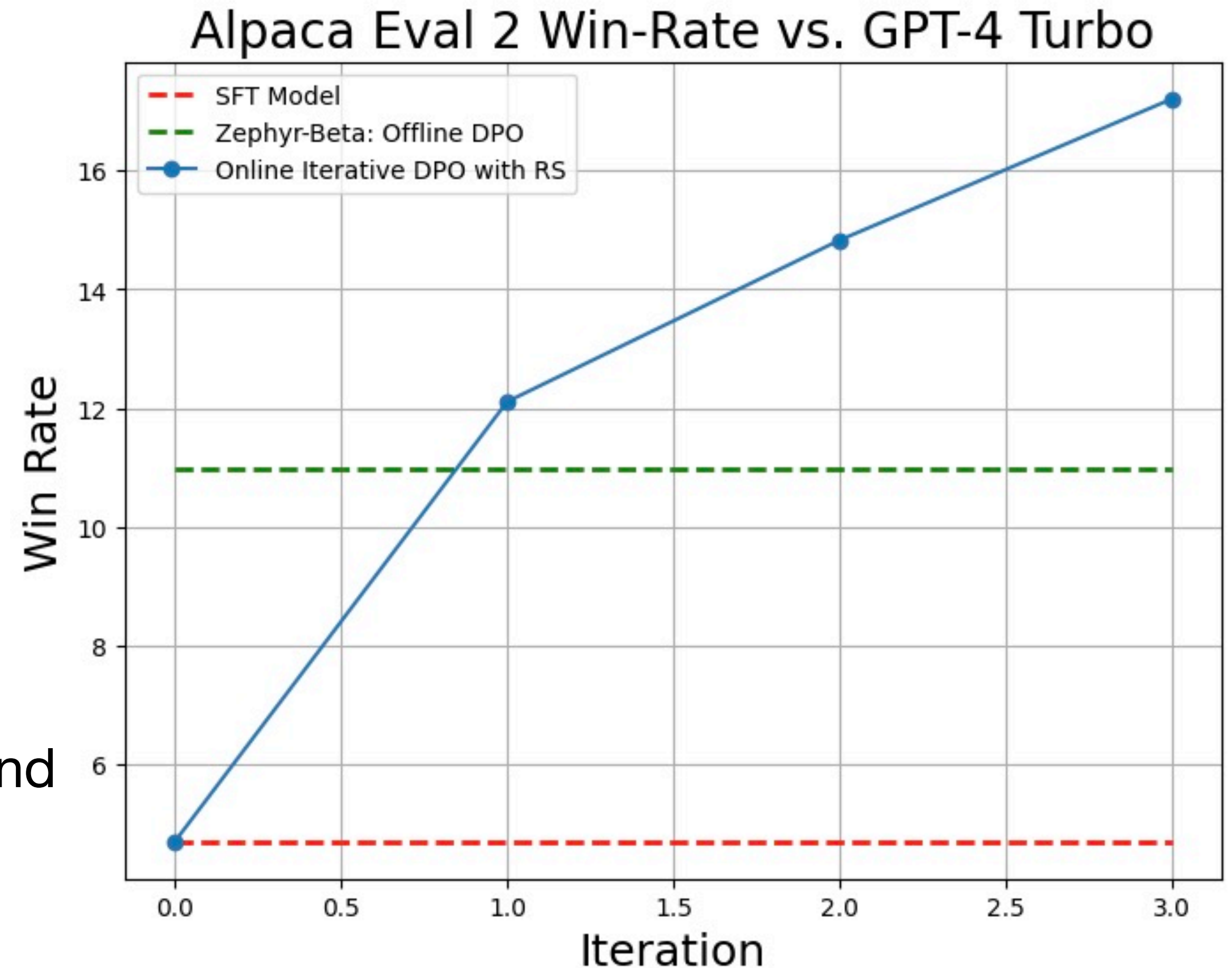


- **Setup**

- Model: Open-LLaMA-3B; Dataset: HH-RLHF (multi-round conversation); Gold reward: Ultra-LLaMA-13B RM to *approximate* human
- Main message: sampling new data from online exploration is far more efficient than sample more in-distribution data from π_0

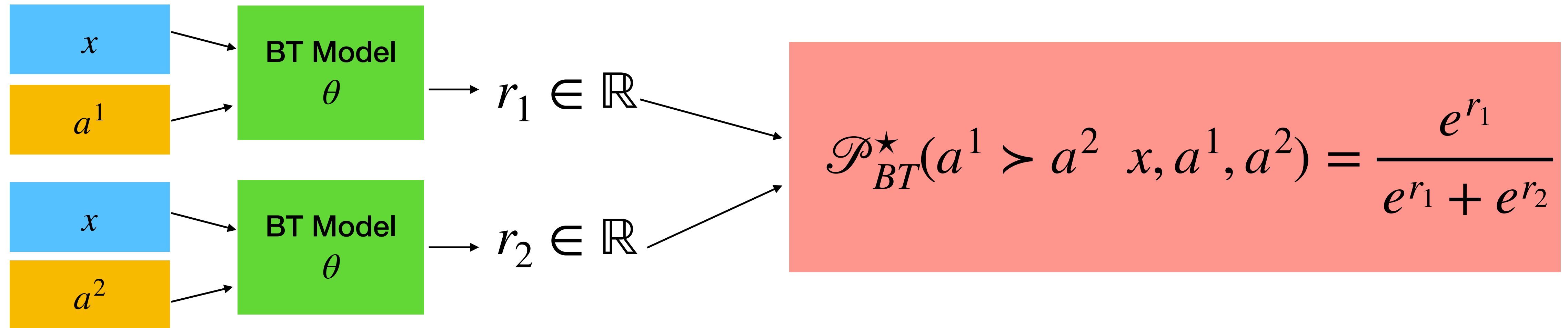
Online Iterative RLHF: Experimental Result 2

1. The same setup but with
 1. Model: Zephyr trained from Mistral-7B-v0.1
 2. Prompt set: Ultra feedback 60K
2. Online Exploration
 1. Exploitation: close to π_t^1 (MLE);
 2. Exploration: maximize policy difference;
 3. *Rejection sampling*: we sample 4 responses and use the best sample.



Beyond the Reward-based Framework: RLHF with General Preference

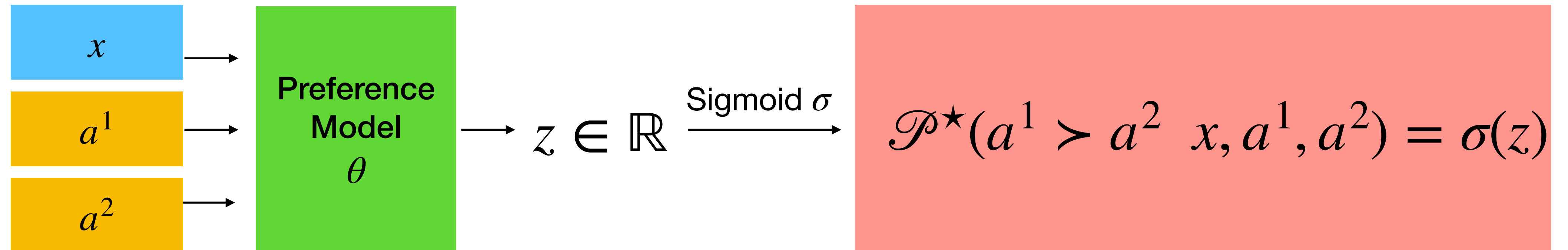
Bradley-Terry (BT) Model



- The Bradley-Terry model is a **proxy** of the preference oracle with **issues**:
- Its **transitivity** may not hold in practice

$$P(a^1 \prec a^2) > 0.5 \ \& \ P(a^2 \prec a^3) > 0.5 \ \Rightarrow \ P(a^1 \prec a^3) > 0.5$$

Preference Model



- The Preference Model is a **proxy** of the preference oracle **with larger capacity**:

- It doesn't impose the **transitivity** ($a^1 < a^2 \ \& \ a^2 < a^3 \Rightarrow a^1 < a^3$)

- Anti-symmetric Relative preference

$$R^*(x, a^1, a^2) = \log \frac{\mathcal{P}^*(a^1 \succ a^2 \mid x, a^1, a^2)}{\mathcal{P}^*(a^1 < a^2 \mid x, a^1, a^2)} = \underbrace{r^*(x, a^1) - r^*(x, a^2)}_{\text{If BT is true.}}$$

RLHF with General Preference

KL-Regularized Two-player Game:

$$(\pi^*, \pi^*) = \max_{\pi} \min_{\pi'} R^*(\pi, \pi') - \eta \text{KL}(\pi \| \pi_0) + \eta \text{KL}(\pi' \| \pi_0)$$

With the KL terms, the regularized objective enjoy following benefits:

- The KL regularization can (potentially) **mitigate reward hacking** and guarantee the optimal policy to be **stochastic** (diverse)
- The objective becomes **strongly** concave-convex \rightarrow **unique symmetric** Nash equilibrium

Online Iterative RLHF with General Preference

Computation oracle: $\mathcal{O}(R, \pi_0, \eta) = \arg \max_{\pi} \arg \min_{\pi'} R(\pi, \pi') - \eta \text{KL}(\pi \parallel \pi_0) + \eta \text{KL}(\pi' \parallel \pi_0)$

Initialized with $\mathcal{D} = \emptyset$, for $t=1,2,3,\dots$

- **Main agent:** compute the MLE \hat{R}_t on \mathcal{D} and take $\pi_t^1 = \mathcal{O}(\hat{R}_t, \pi_0, \eta)$

- **Choose the enhancer policy:** Information ratio

$$\pi_t^2 = \arg \min_{\pi^2 \in \Pi} \mathbb{E}_{a^1 \sim \pi_t^1, a^2 \sim \pi^2} \sup_{R \in \mathcal{R}} \frac{R(x, \pi_t^1, \pi^2) - \hat{R}_t(x, \pi_t^1, \pi^2)}{\sqrt{\lambda + \frac{1}{m} \sum_{s=1}^{t-1} \sum_{j=1}^m (R(x_{s,j}, a_{s,j}^1, a_{s,j}^2) - \hat{R}_t(x_{s,j}, a_{s,j}^1, a_{s,j}^2))^2}}$$

- Collect the m new samples $a_{t,j}^1, a_{t,j}^2 \sim (\pi_t^1, \pi_t^2)$, $y_{t,j} \sim \mathcal{P}^*$ into \mathcal{D} .

Online Iterative RLHF

Theorem 3: Guarantee for the Online Iterative RLHF with General Preference

If we run the algorithm with batch size $m = c \cdot \frac{d}{\epsilon^2}$ for $T = \tilde{\Omega}(d)$ times, w.p. at least $1 - \delta$, we can find a $t_0 \in [T]$ such that

$$J(\pi^*, \pi^*) - \min_{\pi'} J(\pi_{t_0}^1, \pi') = - \min_{\pi'} \left[R^*(x, a^1, a^2) - \eta \text{KL}(\pi_{t_0}^1 \| \pi_0) + \eta \text{KL}(\pi' \| \pi_0) \right] \leq \epsilon$$

1. With small η, ϵ , the model consistently outperform any competing policy

$$\min_{\pi' \in \Pi} \mathbb{E}_{x \sim d_0} \mathbb{E}_{a^1 \sim \pi_{t_0}^1, a^2 \sim \pi'} \mathcal{P}(a^1 > a^2 \mid x, a^1, a^2) > 0.5.$$

3. With the BT model,

$$\mathbb{E}_{x \sim d_0} \mathbb{E}_{a^1 \sim \pi_{t_0}^1} \left[r^*(x, a^1) - \eta \text{KL}(\pi_{t_0}^1 \| \pi_0) \right] \geq \max_{\pi' \in \Pi} \mathbb{E}_{x \sim d_0} \mathbb{E}_{a^2 \sim \pi'} \left[r^*(x, a^2) - \eta \text{KL}(\pi' \| \pi_0) \right] - \epsilon.$$

On-going Challenges and Future Directions

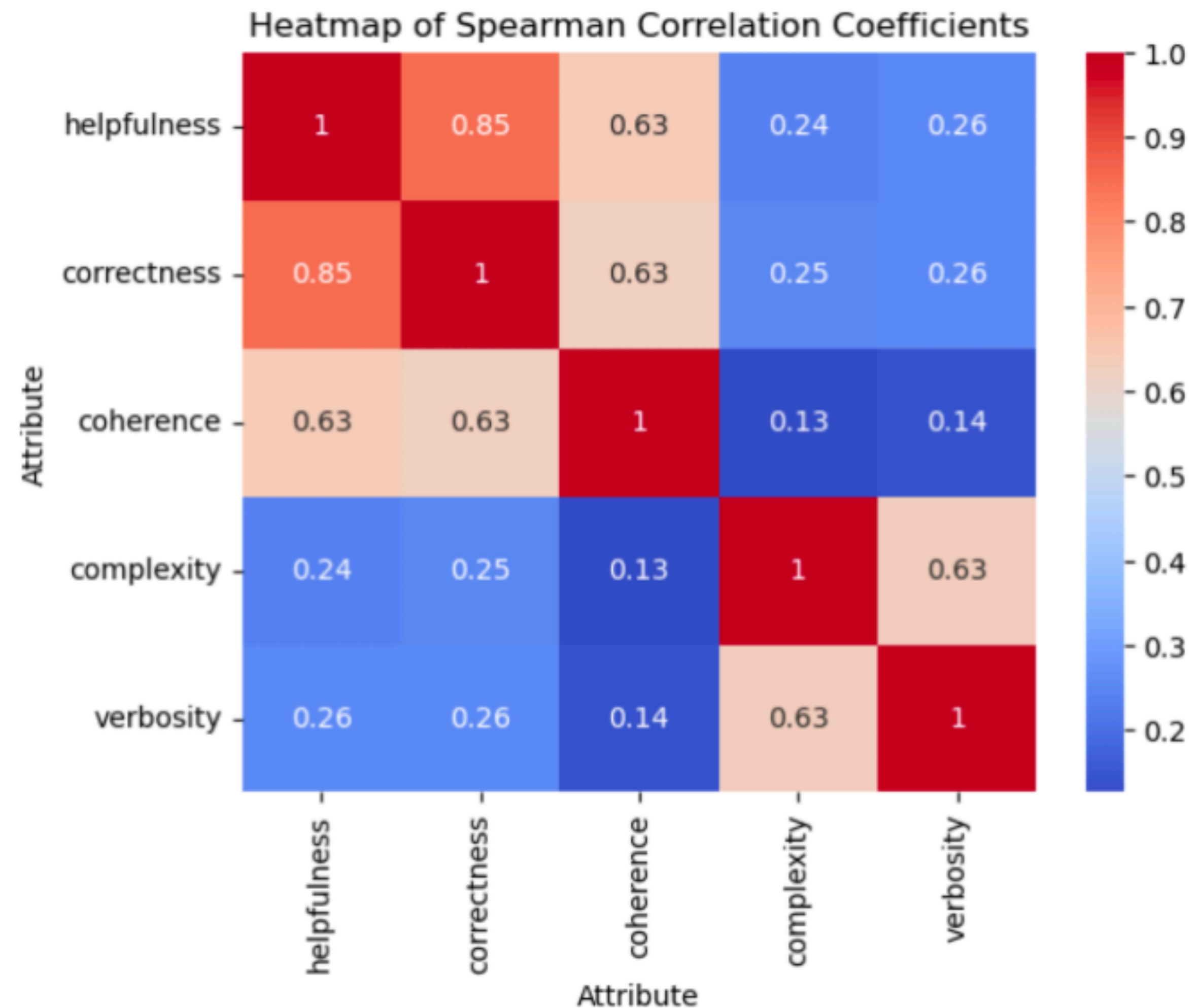
Challenge 1: Preference Conflict

- The agreement rate among humans is only 70%;
- Even the LLMs have different preferences.

Helpfulness					Understandability				
	MTurk	Scale	GPT4	Claude		MTurk	Scale	GPT4	Claude
MTurk	1.00				MTurk	1.00			
Scale	0.53	1.00			Scale	0.31	1.00		
GPT4	0.59	0.48	1.00		GPT4	0.36	0.28	1.00	
Claude	0.41	0.36	0.50	1.00	Claude	0.37	0.30	0.65	1.00
Conciseness					Harmlessness				
	MTurk	Scale	GPT4	Claude		MTurk	Scale	GPT4	Claude
MTurk	1.00				MTurk	1.00			
Scale	0.33	1.00			Scale	0.77	1.00		
GPT4	0.44	0.34	1.00		GPT4	0.82	0.74	1.00	
Claude	0.25	0.29	0.47	1.00	Claude	0.69	0.67	0.69	1.00

Challenge 2: Insufficiency of Scalar Reward

Human possesses *intricate* and even *contradictory* targets



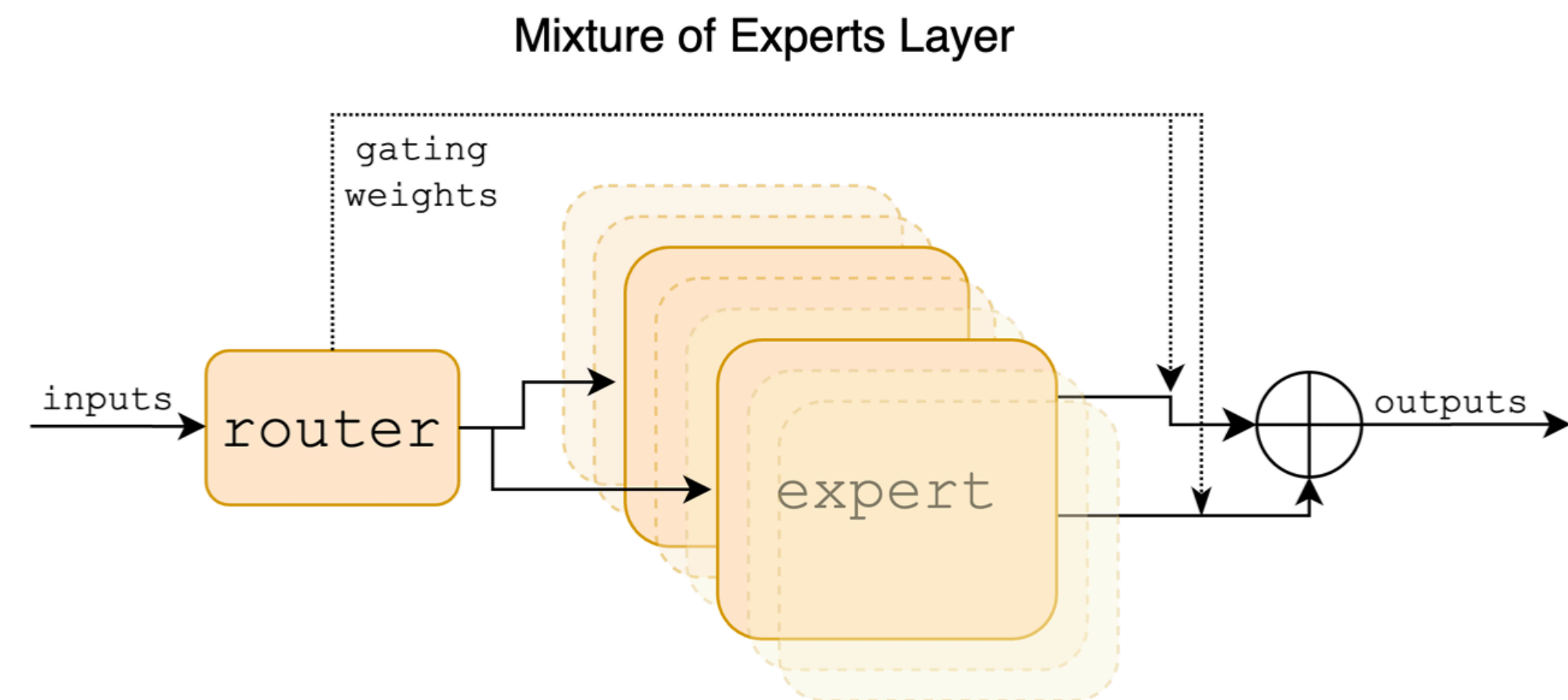
Multi-objective Reward

1. Reward Modeling: multi-objective rewards $\vec{r} = (r_1, r_2, \dots, r_k)$

1. Good performance

2. Multi-head + Mixture of Expert

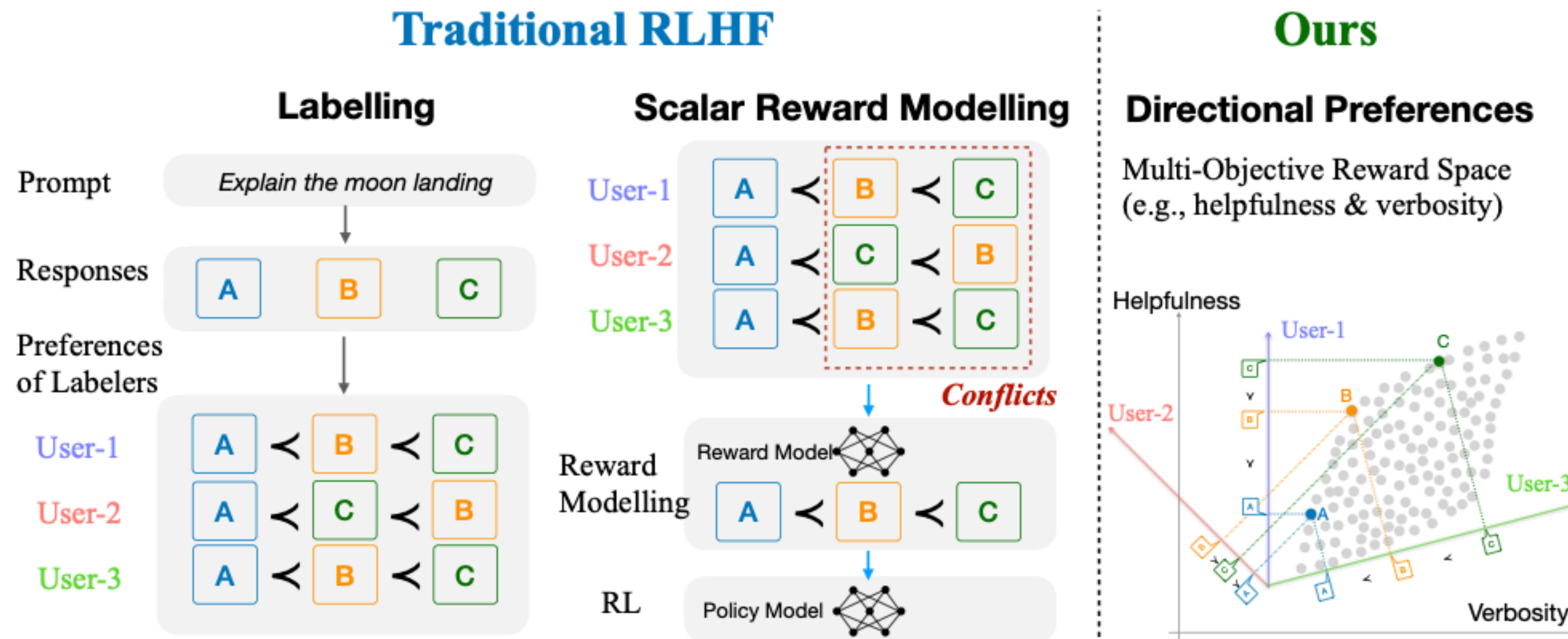
$$f(x, a) = \sum_{i=1}^k g(x)_i \cdot r_i(x, a)$$



User-preference-aware Alignment

1. User-preference-aware objective

$$J(\pi) = \mathbb{E}_{\nu \sim d_\nu} \left[\mathbb{E}_{x \sim d_0, a \sim \pi(\cdot, \nu, x)} f(\nu, x, a) \right]. \quad f(\nu, x, a) = \sum_{i=1}^k g(\nu, x)_i \cdot r_i(x, a)$$



End Note

Central problem: how to model the preference signal

1. Offline learning: pessimism;
2. Online iterative learning: collecting new online data;
3. Use more general preference modeling:
 1. General preference
 2. Multi-objective reward
 3. User-dependent preference
4. Structured problem: math, coding, and agent...

Thanks for listening!