

Lecture 8: Imitation Learning and RLHF

Emma Brunskill

CS234 Reinforcement Learning.

Spring 2024

Select all that are true

- (a) Maximizing a lower bound on the performance gap between a new policy and old policy can ensure monotonic convergence T
- (b) Behavior cloning requires knowing the dynamics model F
- (c) DAGGER uses demonstrations from experts but no further interactions F
- (d) Not sure

Select all that are true

- (a) Maximizing a lower bound on the performance gap between a new policy and old policy can ensure monotonic convergence
- (b) Behavior cloning requires knowing the dynamics model
- (c) DAGGER uses demonstrations from experts but no further interactions
- (d) Not sure

How Can RL Enable This?

PM You

Please write me a program to demonstrate how RLHF works. Please be brief in your explanations and only say 1-2 sentences before you show me the code.

ChatGPT

Reinforcement Learning from Human Feedback (RLHF) trains a model to perform tasks based on human-derived feedback. Here's a simplified Python program that demonstrates RLHF using a scenario where an AI chooses responses in a conversation.

```
python                                Copy code

import numpy as np

# Define possible actions (responses) the AI can use
actions = ["I'm doing well, thanks!", "I'm not sure how I feel.", "Let's talk about RLHF"]
q_table = np.zeros(len(actions))  # Initialize Q-values for each action to zero

def human_feedback(action):
    feedback = {"I'm doing well, thanks!": 10, "I'm not sure how I feel.": -5, "Let's talk about RLHF": 0}
    return feedback[action]

# Hyperparameters
learning_rate = 0.1
discount_factor = 0.6

# Training loop
for episode in range(100):
    action_index = np.random.choice(len(actions))  # Randomly choose an action
```

- Last time: Policy search continued and Imitation Learning
- This time: Imitation Learning and RLHF
- Next time: Author of Direct Preference Optimization (best paper runner up at top ML conference) guest lecture

- Imitation Learning
 - Max entropy inverse RL
- Human feedback
 - RLHF

- Expert provides a set of **demonstration trajectories**: sequences of states and actions
- Imitation learning is useful when it is easier for the expert to demonstrate the desired behavior rather than:
 - Specifying a reward that would generate such behavior,
 - Specifying the desired policy directly

Problem Setup

- Input:
 - State space, action space
 - Transition model $P(s' | s, a)$ (sometimes)
 - No reward function R
 - Set of one or more expert's demonstrations $(s_0, a_0, s_1, a_1, \dots)$
(actions drawn from expert's policy π^*)
- Behavioral Cloning:
 - Can we directly learn the expert's policy using supervised learning?
- Inverse RL:
 - Can we recover R ?
- Apprenticeship learning via Inverse RL:
 - Can we use R to generate a good policy?



DAGGER

Recall: Feature Matching

$\pi \rightarrow \gamma \rightarrow (s, a)$ distrib

- Want to find a reward function such that the expert policy outperforms other policies.
- For a policy π to be guaranteed to perform as well as the expert policy π^* , sufficient if its discounted summed feature expectations match the expert's policy [Abbeel & Ng, 2004].
- More precisely, if

$$\|\mu(\pi) - \mu(\pi^*)\|_1 \leq \epsilon$$

then for all w with $\|w\|_\infty \leq 1$ (uses Holder's inequality):

$$|w^T \mu(\pi) - w^T \mu(\pi^*)| \leq \epsilon$$

- where here μ is used to represent the features experienced under π

Recall: Ambiguity

- There is an infinite number of reward functions with the same optimal policy.
- There are infinitely many stochastic policies that can match feature counts
- Which one should be chosen?

- Many different approaches
- Two of the key papers are:
 - Maximum Entropy Inverse Reinforcement Learning (Ziebart et al. AAAI 2008)
 - Generative adversarial imitation learning (Ho and Ermon, NeurIPS 2016)

Max Entropy Inverse RL. Ziebart et al. 2008. Note: Much of this presentation follows the slides from Katerina Fragkiadaki's Deep Reinforcement Learning and Control Lecture on Maximum Entropy Inverse RL.

$$\sum_s p(s) = 1 \quad \text{prob dist'n}$$

- Recall that entropy of a distribution $p(s)$ is $-\sum_{s'} p(s = s') \log p(s = s')$
- Principle of max entropy: The probability distribution which best represents the current state of knowledge is the one with the largest entropy, given the constraints of precisely stated prior data.
- Intuitively: consider all probability distributions consistent with observed data, and select the probability distribution with the maximum entropy.

- Recall that entropy of a distribution $p(s)$ is $-\sum_{s'} p(s = s') \log p(s = s')$
- Principle of max entropy: The probability distribution which best represents the current state of knowledge is the one with the largest entropy, given the constraints of precisely stated prior data.
- Intuitively: consider all probability distributions consistent with observed data, and select the probability distribution with the maximum entropy.
- In the linear reward case, this is equivalent to specifying the weights w that yield a policy with the max entropy constrained to matching the feature expectations:

$$\max_P - \sum_{\tau} P(\tau) \log P(\tau) \text{ s.t. } \sum_{\tau} P(\tau) \mu(\tau) = \frac{1}{|\mathcal{D}|} \sum_{i \in \mathcal{D}} \mu(\tau_i) \quad \sum_{\tau} P(\tau) = 1$$

experts (1)

- where $\mu(\tau)$ are the features for trajectory τ and \mathcal{D} is the observed expert data

- In the linear reward case, this is equivalent to specifying the weights w that yield a policy with the max entropy constrained to matching the feature expectations:

$$\max_P - \sum_{\tau} P(\tau) \log P(\tau) \text{ s.t. } \sum_{\tau} P(\tau) \mu(\tau) = \frac{1}{|\mathcal{D}|} \sum_{i \in \mathcal{D}} \mu(\tau_i) \quad \sum_{\tau} P(\tau) = 1 \quad (2)$$

- where $\mu(\tau)$ are the features for trajectory τ and \mathcal{D} is the observed expert data
- In general, would like to find a policy π that induces a distribution over trajectories $p(\tau)$ which has the same expected reward as the expert's demonstrations $\hat{P}(\tau)$ given a reward function r_ϕ

$$\max_{p(\tau)} - \sum_{\tau} p(\tau) \log p(\tau) \quad \text{s.t.} \quad \sum_{\tau} p(\tau) r_\phi(\tau) = \sum_{\tau} \hat{P}(\tau) r_\phi(\tau) \quad \sum_{\tau} p(\tau) = 1$$

expert (3)

Matching Rewards to Learning Policies

- In the linear reward case, this is equivalent to specifying the weights w that yield a policy with the max entropy constrained to matching the feature expectations:

$$\max_P - \sum_{\tau} P(\tau) \log P(\tau) \text{ s.t. } \sum_{\tau} P(\tau) \mu(\tau) = \frac{1}{|\mathcal{D}|} \sum_{i \in \mathcal{D}} \mu(\tau_i) \quad \sum_{\tau} P(\tau) = 1 \quad (4)$$

- where $\mu(\tau)$ are the features for trajectory τ and \mathcal{D} is the observed expert data
- In general, would like to find a policy π that induces a distribution over trajectories $p(\tau)$ which has the same expected reward as the expert's demonstrations $\hat{P}(\tau)$ given a reward function r_ϕ

$$\max_{p(\tau)} - \sum_{\tau} p(\tau) \log p(\tau) \quad \text{s.t.} \quad \sum_{\tau} p(\tau) r_\phi(\tau) = \sum_{\tau} \hat{P}(\tau) r_\phi(\tau) \quad \sum_{\tau} p(\tau) = 1 \quad (5)$$

- To do so, will alternate between computing a reward function, using that reward function to learn an optimal policy, and then updating the trajectory / state frequencies needed to update the reward function
- Note: in original maximum entropy inverse RL paper, assumed dynamics / reward model is known

From Maximum Entropy to Probability over Trajectories

- given constrained obj. if we know the costs, what would be the form of the distib over τ ?

$$\mathcal{L}(\rho, \lambda) = \sum_{\tau} p(\tau) \log p(\tau) + \lambda_1 (\underbrace{\sum_{\tau} \hat{p}(\tau) r_{\phi}(\tau)}_{-\sum_{\tau} p(\tau) r_{\phi}(\tau)}) + \lambda_0 (\sum_{\tau} p(\tau) - 1)$$

$$\frac{d\mathcal{L}}{dp(\tau)} = \log p(\tau) + p(\tau) \cdot \frac{1}{p(\tau)} - \lambda_1 r_{\phi}(\tau) + \lambda_0 = 0$$

$$\log p(\tau) = -1 + \lambda_1 r_{\phi}(\tau) - \lambda_0$$

$$p(\tau) = e^{-1 + \lambda_1 r_{\phi}(\tau) - \lambda_0}$$

$$p(\tau) \propto e^{r_{\phi}(\tau)}$$

Maximizing Entropy Over $\tau \equiv$ Maximize Likelihood of Observed Data
Under Max Entropy (Exponential Family) Distribution (Jaynes 1957)

$$p(\gamma_i | \phi) = \frac{1}{Z(\phi)} e^{r_\phi(\gamma_i)}$$

$$Z(\phi) = \sum_{\gamma} e^{r_\phi(\gamma)}$$

$$p(\gamma_i | \phi) = \frac{1}{Z(\phi)} e^{\sum_{s_i \in \gamma_i} r_\phi(s_i)}$$

we don't know what r_ϕ is constraint
this observation (prob over γ that max 1
entropy looks like a normalized expn)
means we can now estimate / learn r_ϕ
by max prob of our observed data

Maximize (over r_ϕ) Likelihood of Observed Data Under Max Entropy

$$\max_{\phi} \log \prod_{Y^* \in D} p(Y^*)$$

$$\max_{\phi} \sum_{Y^* \in D} \log \left(\frac{e^{r_\phi(Y^*)}}{\sum e^{r_\phi(Y)}} \right)$$

$$= \max_{\phi} \sum_{Y^* \in D} r_\phi(Y^*) - \underbrace{\log \sum_Y e^{r_\phi(Y)}}_{J(\phi)}$$

$$J(\phi) = \max_{\phi} \sum_{Y^* \in D} r_\phi(Y^*) - |D| (\log \sum_Y e^{r_\phi(Y)})$$

$$\nabla_{\phi} J(\phi) = \sum_{Y^* \in D} \frac{d r_\phi(Y^*)}{d \phi} - |D| \underbrace{\frac{1}{\sum_Y e^{r_\phi(Y)}}}_{\text{Note} \Rightarrow p(Y|\phi)} \sum_Y e^{r_\phi(Y)} \frac{d r_\phi(Y)}{d \phi}$$

$$= \sum_{Y^* \in D} \frac{d r_\phi(Y^*)}{d \phi} - |D| \sum_Y p(Y|\phi) \frac{d r_\phi(Y)}{d \phi}$$

From Trajectories to States

$$p(\gamma) = p(s_1) \prod_{t=1}^T p(a_t | s_t) p(s_{t+1} | s_t, a_t)$$

$$p(\gamma) \propto e^{-r_p(\gamma)} = e^{-\sum_{s \in \gamma} r_\phi(s)}$$

$$\nabla_\theta J(\theta) = \sum_{s \in \gamma^* \in D} \frac{d r_\phi(s)}{d \theta} - |D| \sum_s p(s | \theta, \gamma) \frac{d r_\phi(s)}{d \theta}$$

State Densities

if tabular & dynamics known so π is given

$$\mu_t(s) = \rho(s_t)$$

for $t=1\dots T$ (time index t)

$$\mu_{t+1}(s) = \sum_a \sum_{s'} \mu_t(s') \rho(a|s') \rho(s|s; a)$$

$$\rho(s_t|\phi, \gamma) = \sum_t \mu_t(s)$$

$$\nabla_\phi J(\phi) = \sum_{s_t \in \text{ep}} \frac{\partial r_\phi(s)}{\partial \phi} - 1/D \sum_s \rho(s|\phi, T) \frac{\partial r_\phi(s)}{\partial \phi}$$

if $r_\phi(s) = \phi f_s$ (linear)

$$\frac{\partial r_\phi(s)}{\partial \phi} = f_s$$

Note: Assuming known dynamics model and linear rewards

- ① Input: expert demonstrations \mathcal{D}
- ② Initialize r_ϕ
- ③ Compute optimal $\pi(a|s)$ given r_ϕ e.g. with value iteration
- ④ Compute state visitation frequencies $p(s|\phi, T)$ (linear)
- ⑤ Compute gradient on reward model

$$\nabla J(\phi) = \frac{1}{M} \sum_{t_d \in \mathcal{D}} f_{t_d} - \sum_s p(s|\phi, T) f_s \quad (6)$$

- ⑥ Update ϕ with one gradient step
- ⑦ Go to step 3

Note: Assuming known dynamics model and linear rewards

- ① Input: expert demonstrations \mathcal{D}
- ② Initialize r_ϕ
- ③ Compute optimal $\pi(a|s)$ given r_ϕ e.g. with value iteration)
- ④ Compute state visitation frequencies $p(s(\phi, T))$
- ⑤ Compute gradient on reward model

$$\nabla J(\phi) = \frac{1}{M} \sum_{\gamma_d \in \mathcal{D}} f_\zeta - \sum_s p(s|\phi, \gamma) f_s \quad (7)$$

- ⑥ Update ϕ with one gradient step
 - ⑦ Go to step 3
- What steps in the above algorithm rely on knowing the dynamics model? (select all)
 - (1) Computing the optimal policy
 - (2) Computing the state visitation frequencies
 - (3) Computing the gradient
 - (4) No steps required it
 - (5) Not sure

Check Your Understanding: L8N2 Maximum entropy inverse RL Solutions

Note: Assuming known dynamics model and linear rewards

- ① Input: expert demonstrations \mathcal{D}
- ② Initialize r_ϕ
- ③ Compute optimal $\pi(a|s)$ given r_ϕ e.g. with value iteration
- ④ Compute state visitation frequencies $p(s|\phi, T)$
- ⑤ Compute gradient on reward model

$$\nabla J(\phi) = \quad (8)$$

- ⑥ Update ϕ with one gradient step
- ⑦ Go to step 3
 - What steps in the above algorithm rely on knowing the dynamics model? (select all)
 - (1) Computing the optimal policy
 - (2) Computing the state visitation frequencies
 - (3) Computing the gradient
 - (4) No steps required it
 - (5) Not sure

1 and 2

- Max entropy approach has been hugely influential
- Initial formulation (Ziebart et al) using linear rewards and assumed dynamics model is known
 - Check your understanding: was this needed in behavioral cloning?
- Finn et al. 2016 (Guided cost learning: Deep inverse optimal control via policy optimization) showed how to use general reward/cost functions and removed the need to know the dynamics model

- Imitation learning can greatly reduce the amount of data need to learn a good policy
- Challenges remain and one exciting area is combining inverse RL / learning from demonstration and online reinforcement learning
- For a look into some of the theory between imitation learning and RL, see Sun, Venkatraman, Gordon, Boots, Bagnell (ICML 2017)

- Define behavior cloning and how it differs from reinforcement learning
- Understand principle of maximum entropy, the resulting distribution over trajectories, and how this can be used to learn a reward function and fit a policy

Human Feedback and Reinforcement Learning from Human Preferences

- There are many ways for humans to help train RL agents
- This is relevant if we want RL agents that can match human performance and/or human values

Training a Robot Through Human and Environmental Feedback



Teachable robots: Understanding human teaching behavior to build more effective robot learners. AL
Thomaz, C Breazeal. Artificial Intelligence 2008

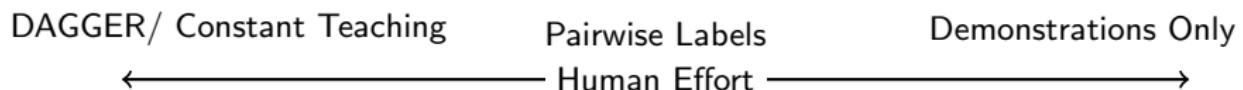
Table 1: Results of various Tetris agents.

Method	Mean Lines Cleared		Games for Peak
	at Game 3	at Peak	
TAMER	65.89	65.89	3
RRL-KBR [15]	5	50	120
Policy Iteration [2]	~ 0 (no learning until game 100)	3183	1500
Genetic Algorithm [5]	~ 0 (no learning until game 500)	586,103	3000
CE+RL [17]	~ 0 (no learning until game 100)	348,895	5000

Human Input for Training and Aligning RL Policies



Human Input for Training and Aligning RL Policies: Sweet Spot?



Comparing Recommendation Ranking Systems

RETRIEVAL FUNCTION A

CS 159 Purdue University

web.ics.purdue.edu/~cs159/ ▾ Purdue University ▾

Aug 16, 2012 - CS 159 introduces the tools of software development that have become essential for creative problem solving in Engineering. Educators and ...

CS159: Introduction to Parallel Processing | People | San Jo...

www.sjsu.edu ▾ ... ▾ Chun, Robert K ▾ Courses ▾ San Jose State University ▾

Jan 20, 2015 - Description. A combination hardware architecture and software development class focused on multi-threaded, parallel processing algorithms ...

CS 159: Introduction to Parallel Processing - Info.sjsu.edu

info.sjsu.edu ▾ ... ▾ Courses ▾ San Jose State University ▾

CS 159. Introduction to Parallel Processing. Description Major parallel architectures: shared memory, distributed memory, SIMD, MIMD. Parallel algorithms: ...

Guy falls asleep in CS159 lab Purdue - YouTube



<https://www.youtube.com/watch?v=vVciOgZwLag>

Mar 24, 2011 - Uploaded by james brand

Guy falls asleep in our 7:30 am lab so we take his phone turn the volume up to full and call him.

CS 159: Advanced Topics in Machine Learning - Yisong Yue

www.yisongyue.com/courses/cs159/ ▾

CS 159: Advanced Topics in Machine Learning (Spring 2016). Course Description. This course will cover a mixture of the following topics: Online Learning ...

CS159: Introduction to Computational Complexity

cs.brown.edu/courses/cs159/home.html ▾ Brown University ▾

Home | Course Info | Assignments | Syllabus And Lectures | Staff and Hours | LaTeX. An early model of parallel computation... Home Courses.

RETRIEVAL FUNCTION B

Guy falls asleep in CS159 lab Purdue - YouTube



<https://www.youtube.com/watch?v=vVciOgZwLag>

Mar 24, 2011 - Uploaded by james brand

Guy falls asleep in our 7:30 am lab so we take his phone turn the volume up to full and call him.

CS 159 Purdue University

web.ics.purdue.edu/~cs159/ ▾ Purdue University ▾

Aug 16, 2012 - CS 159 introduces the tools of software development that have become essential for creative problem solving in Engineering. Educators and ...

CS159: Introduction to Parallel Processing | People | San Jo...

www.sjsu.edu ▾ ... ▾ Chun, Robert K ▾ Courses ▾ San Jose State University ▾

Jan 20, 2015 - Description. A combination hardware architecture and software development class focused on multi-threaded, parallel processing algorithms ...

CS 159: Introduction to Parallel Processing - Info.sjsu.edu

info.sjsu.edu ▾ ... ▾ Courses ▾ San Jose State University ▾

CS 159. Introduction to Parallel Processing. Description Major parallel architectures: shared memory, distributed memory, SIMD, MIMD. Parallel algorithms: ...

CS 159: Advanced Topics in Machine Learning - Yisong Yue

www.yisongyue.com/courses/cs159/ ▾

CS 159: Advanced Topics in Machine Learning (Spring 2016). Course Description. This course will cover a mixture of the following topics: Online Learning ...

CS159: Introduction to Computational Complexity

cs.brown.edu/courses/cs159/home.html ▾ Brown University ▾

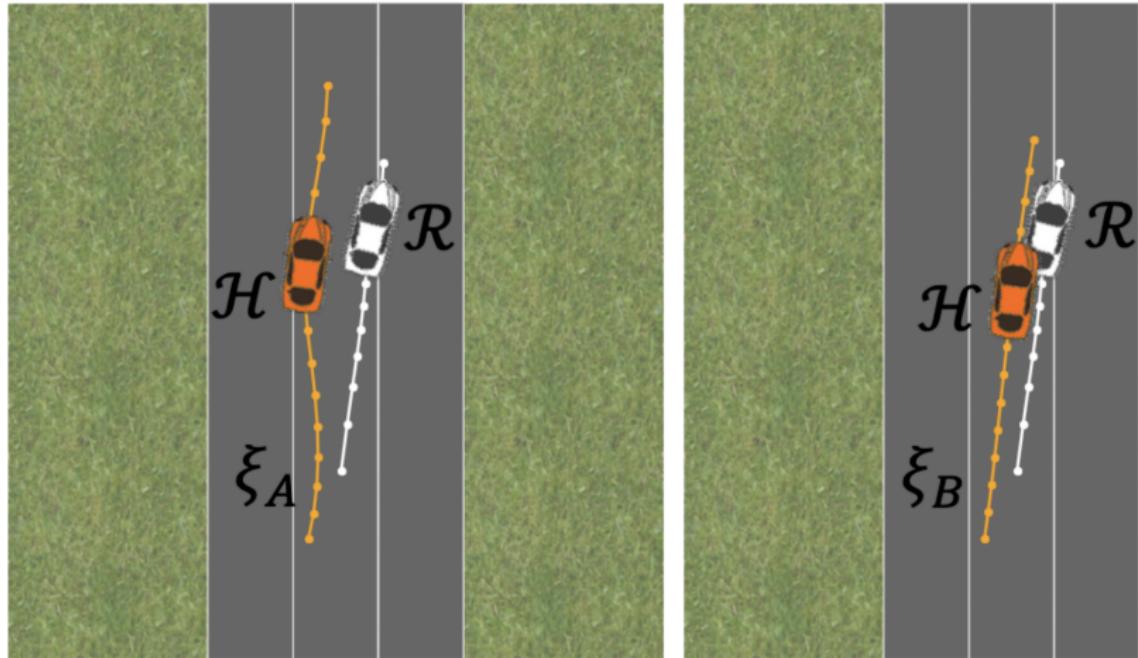
Home | Course Info | Assignments | Syllabus And Lectures | Staff and Hours | LaTeX. An early model of parallel computation... Home Courses.

Slide from Yisong Yue

http://www.yisongyue.com/courses/cs159/lectures/dueling_bandits_lecture.pdf



Active Learning of Preferences for Human Robot Interaction



Active preference-based learning of reward functions. D Sadigh, AD Dragan, S Sastry, SA Seshia. RSS
2017

- Often easier for people to make than hand writing a reward function
- Often easier than providing scalar reward (how much do you like this ad?)

- Already saw with no other assumptions, the latent reward model is not unique
- Now focus on a particular structural model
- First consider simpler setting of k -armed bandits¹: K actions b_1, b_2, \dots, b_k . No state/context.
- Assume a human makes noisy pairwise comparisons, where the probability she prefers $b_i \succ b_j$ is

$$P(b_i \succ b_j) = \frac{\exp(r(b_i))}{\exp(r(b_i)) + \exp(r(b_j))} = p_{ij} \quad (9)$$

- Transitive: p_{ik} is determined from p_{ij} and p_{jk}

¹We will see more on bandits later in the course

See: The K -armed dueling bandits problem. Y Yue, J Broder, R Kleinberg and T. Joachims. Journal of Computer and System Sciences. 2012.

Condorcet Winner

An item b_i is a Condorcet winner if for every other item b_j , $P(b_i \succ b_j) > 0.5$.

Copeland Winner

An item b_i is a Copeland winner if it has the highest number of pairwise victories against all other items. The score for an item is calculated as the number of items it beats minus the number of items it loses to.

Borda Winner

An item b_i is a Borda winner if it maximizes the expected score, where the score against item b_j is 1 if $b_i \succ b_j$, $(P(b_i \succ b_j) > 0.5)$ 0.5 if $b_i = b_j$, and 0 if $b_i \prec b_j$.

- Historically algorithms for k-armed or dueling ($k=2$) bandits focused on finding a copeland winner.

Preference learning

Fitting the Parameters of a Bradley-Terry Model

- First consider k -armed bandits²: K actions b_1, b_2, \dots, b_k . No state/context.
- Assume a human makes noisy pairwise comparisons, where the probability she prefers $b_i \succ b_j$ is

$$P(b_i \succ b_j) = \frac{\exp(r(b_i))}{\exp(r(b_i)) + \exp(r(b_j))} = p_{ij} \quad (10)$$

²We will see more on bandits later in the course

Fitting the Parameters of a Bradley-Terry Model

- First consider k -armed bandits³: K actions b_1, b_2, \dots, b_k . No state/context.
- Assume a human makes noisy pairwise comparisons, where the probability she prefers $b_i \succ b_j$ is

$$P(b_i \succ b_j) = \frac{\exp(r(b_i))}{\exp(r(b_i)) + \exp(r(b_j))} = p_{ij} \quad (11)$$

- Assume have N tuples of form (b_i, b_j, μ) where $\mu(1) = 1$ if the human marked $b_i \succ b_j$, $\mu(1) = 0.5$ if the human marked $b_i = b_j$, else 0 if $b_j \succ b_i$
- Maximize likelihood with cross entropy

$$\text{loss} = - \sum_{(b_i, b_j, \mu) \in \mathcal{D}} \mu(1) \log P(b_i \succ b_j) + \mu(2) \log P(b_j \succ b_i) \quad (12)$$

³We will see more on bandits later in the course

- Can also do this for trajectories
- Consider two trajectories, $\tau^1(s_0, a_7, s_{14}, \dots)$ and $\tau^2(s_0, a_6, s_{12}, \dots)$
- Let $R^1 = \sum_{i=0}^{T-1} r_i^1$ be the (latent, unobserved) sum of rewards for trajectory τ^1 and similarly for R^2 .
- Define the probability that a human prefers $\tau^1 \succ \tau^2$ as

$$\hat{P} [\tau^1 \succ \tau^2] = \frac{\exp \sum_{i=0}^{t-1} r_i^1}{\exp \sum_{i=0}^{t-1} r_i^1 + \exp \sum_{i=0}^{t-1} r_i^2}, \quad (13)$$

- Can also do this for trajectories
- Consider two trajectories, $\tau^1(s_0, a_7, s_{14}, \dots)$ and $\tau^2(s_0, a_6, s_{12}, \dots)$
- Let $R^1 = \sum_{i=0}^{T-1} r_i^1$ be the (latent, unobserved) sum of rewards for trajectory τ^1 and similarly for R^2 .
- Define the probability that a human prefers $\tau^1 \succ \tau^2$ as

$$\hat{P}[\tau^1 \succ \tau^2] = \frac{\exp \sum_{i=0}^{t-1} r_i^1}{\exp \sum_{i=0}^{t-1} r_i^1 + \exp \sum_{i=0}^{t-1} r_i^2}, \quad (14)$$

- Use learned reward model, and do PPO with this model

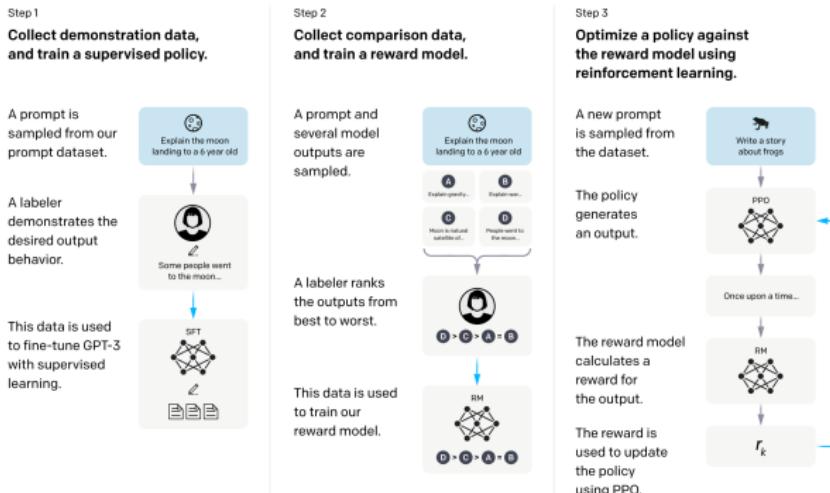
- Learning to backflip
- "needed 900 bits of feedback from a human evaluator to learn to backflip"
- https://player.vimeo.com/video/754042470?h=e64a40690d&badge=0&autoplay=0&player_id=0&app_id=58479

From Backflips to ChatGPT.⁴

⁴Slides from part of Tatsu Hashimoto's Lecture 11 in CS224N

- Next set of slides are from part of Tatsu Hashimoto's Lecture 11 in CS224N

High-level instantiation: ‘RLHF’ pipeline



- First step: instruction tuning!
- Second + third steps: maximize reward (but how??)