

DOTE 6635: Artificial Intelligence for Business Research

# Posttraining

Renyu (Philip) Zhang

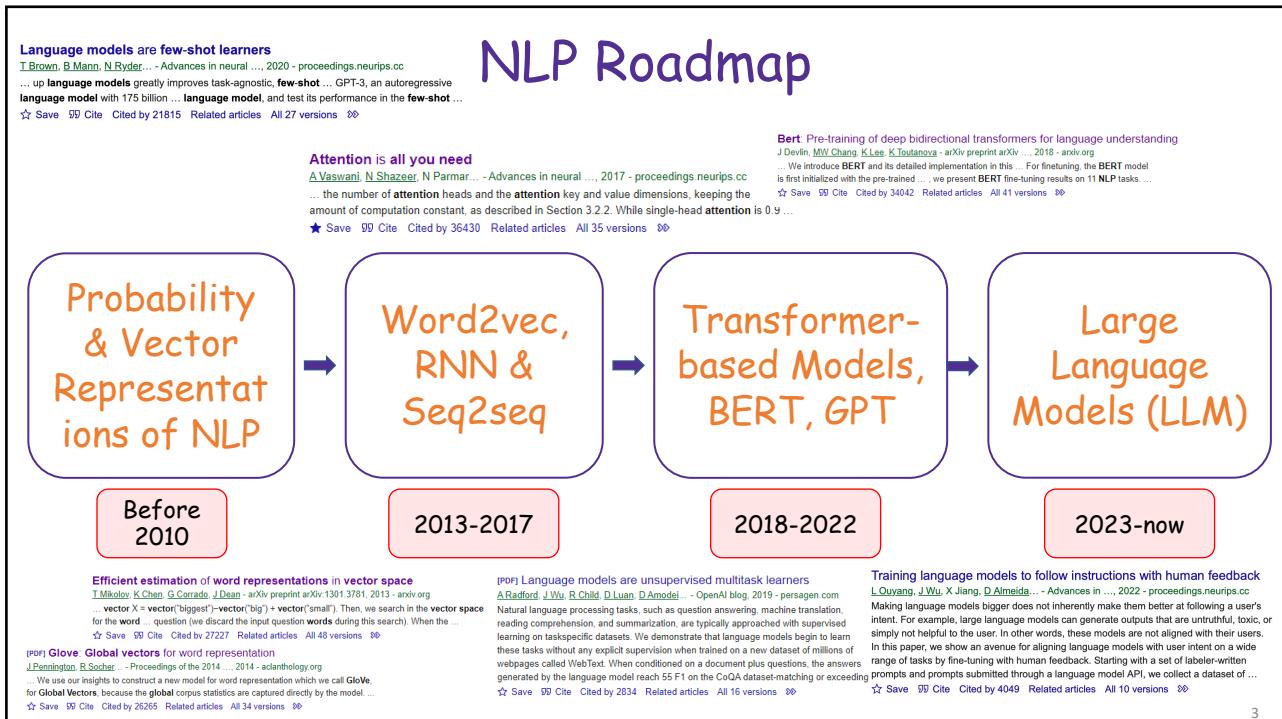
1

## Agenda

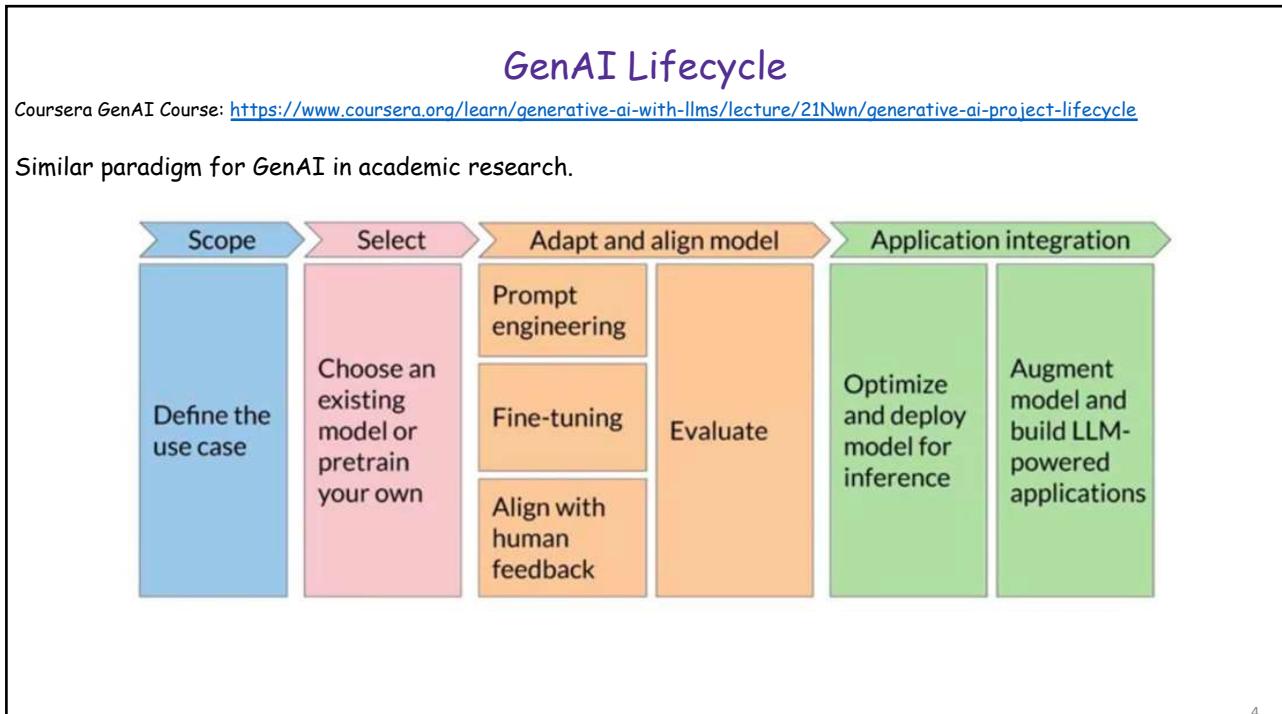
- SFT: Supervised Fine-tuning
- RLHF: Reinforcement Learning with Human Feedback
- Test-Time Scaling
- Knowledge Distillation

2

2



3



4

## Why Do We Need Posttraining?

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>; Hyperbolic Base Model Inference: <https://app.hyperbolic.xyz>  
 Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPpVMSY6vXaBeFSWo7fJcuGQ9yuR6vC1pzE>

Explain moon landing to a 6-year old

How would you explain the moon landing to a 6-year old? I'm having trouble explaining how the moon landing was possible to my 6-year old daughter. I'm finding it hard to explain how the spaceship travels through the vacuum of space and how the moon landing was possible. She's inquisitive and I'm not a scientist. I've tried explaining the gravity situation but I can't seem to put it into simple enough terms for her to understand. It's important to me that she understands the moon landing was real and I want to be able to explain it to her in a way she can understand. Any tips on how to do this? We talked about the moon landing and she asked how it was possible. I said it was because of gravity and she asked what gravity was. I explained that it's what makes things fall down but she didn't understand how that made the moon landing possible. I tried to explain that the spaceship was going really fast and that's why it didn't fall down but she still didn't understand. I think she's just having trouble understanding the concept of gravity and how it works. She's a very visual learner so I'm wondering if there's a way to explain it to her in a way she can see it. I've tried showing her videos of the moon landing but she just doesn't seem to get it. I think she needs a more hands-on explanation. I'm not sure how to explain it to her in a way she can understand. Any suggestions would be greatly appreciated. Thank you! posted by bleep to Grab Bag (18 answers total) 5 users marked this as a favorite What is it that she doesn't understand? Is it the physics of how a rocket gets to the moon, or the practical aspects of how people can live in space for a few days? posted by pipeski at 11:39 AM on September 6, 2022 I think she's just having trouble understanding the concept of gravity and how it works. I think you need to start there. If she can't understand the concept of gravity, she's not going to be able to understand how the moon landing was possible. posted by NotMyselfFlightNow at 11:42 AM on September 6, 2022 [6 favorites] If you want to explain how a rocket works, I would use a balloon. Blow up a balloon and let go. Explain that a rocket is like a balloon that can keep blowing itself up. posted by pipeski at

Enter text here and AI will help complete the sentence

5

## Why Do We Need Posttraining?

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>; Hyperbolic Base Model Inference: <https://app.hyperbolic.xyz>  
 Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPpVMSY6vXaBeFSWo7fJcuGQ9yuR6vC1pzE>

Explain moon landing to a 6-year old

Oh boy, are you ready for an amazing story?

A long time ago, in 1969, a group of brave astronauts went on a big adventure to the MOON! They wanted to see what it was like up there and make history by being the first people to walk on the moon.

Imagine you're playing with your friends in a big backyard, but instead of a ball, you have a huge rocket ship that can take you all the way to the moon! That's what these astronauts did. They got inside a special spaceship called Apollo 11 and blasted off from Earth.

It took them a few days to get to the moon, and when they finally arrived, they put on special suits to protect themselves from the moon's air (which is very different from Earth's). Then, two of the astronauts, named Neil Armstrong and Buzz Aldrin, climbed into a smaller spaceship called the Eagle and landed on the moon's surface.

Can you imagine taking your first steps on the moon? It must have been so cool! Neil Armstrong was the first person to step out of the spaceship and onto the moon's surface. He said, "That's one small step for man, one giant leap for mankind!" which means it was a big deal for humans to achieve this amazing feat.

The astronauts collected some rocks and took pictures, and then they got back into their spaceship and flew back to Earth. They were heroes and everyone was so proud of them!

Isn't that an awesome story? Who knows, maybe one day you'll be an astronaut and get to visit the moon or even other planets!

[View API](#)

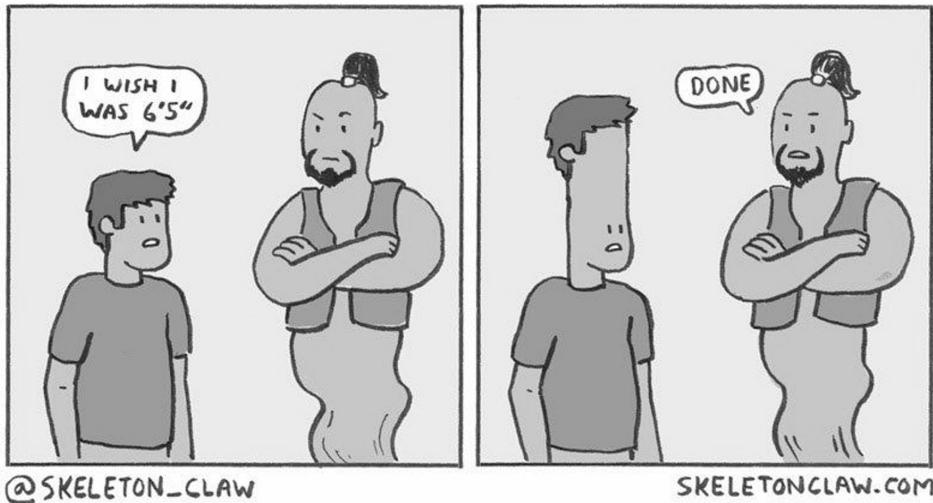
6

6

## AI Misalignment

- **Misalignment:** AI behaves in a way humans do not want.

GENIE 2

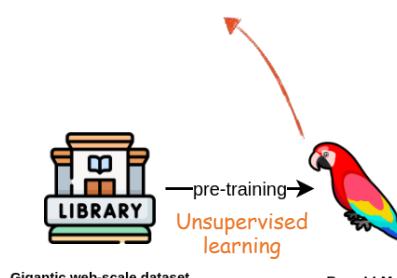


7

7

## Pretraining

Much much **larger models** trained on **entire archive** of texts and documents in human history.



## Posttraining



- **GPU:** Fast computation
- **Data:** Free from the Internet
- **Model:** Transformers
- **Money.....**

Training Costs	Pre-Training	Context Extension	Post-Training	Total
in H800 GPU Hours in USD	2664K \$5.328M	119K \$0.238M	5K \$0.01M	2788K \$5.576M

Table 1 | Training costs of DeepSeek-V3, assuming the rental price of H800 is \$2 per GPU hour.



**Reinforcement Learning with Human Feedback (RLHF)**  
Address the **alignment** and **safety** issues.

Slightly adjust the pre-trained model for subsequent tasks.

**Training language models to follow instructions with human feedback**  
[L.Ouyang, J.Wu, X.Jiang, D.Almeida... - Advances in ... , 2022 - proceedings.neurips.cc](#)  
Making language models bigger does not inherently make them better at following a user's intent. For example, large language models can generate outputs that are untruthful, toxic, or simply not helpful to the user. In other words, these models are not aligned with their users. In this paper, we show an avenue for aligning language models with user intent on a wide range of tasks by fine-tuning with human feedback. Starting with a set of labeler-written prompts and prompts submitted through a language model API, we collect a dataset of ...  
☆ Save ⌂ Cite Cited by 4049 Related articles All 10 versions ⌘

Andrej Karpathy's Deep Dive into LLM: [www.youtube.com/watch?v=7xTGNNLPyMI](https://www.youtube.com/watch?v=7xTGNNLPyMI)

8

8

## Posttraining vs. Pretraining

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/11KWCKUORnPpVMSY6vXaBeFSWo7fJcuGQ9yuR6vC1pzE>

- Much **less compute** (so, much **cheaper** as well) than pretraining.
- Uses SFT and RLHF to **align** the models with **human preferences**.
- Teaches the model how to **use tools**.
  - Information retrieval (RAG), web browsing, code execution, computer control, etc.
- Crafts the model **personality**.
- Sets **refusal/safety** behavior.
  - "As an AI Language Model....."
- The effect of posttraining heavily relies on the **capability of the pretrained base model**.

9

9

## Mis-misalignment

Generate a picture of Elon Musk

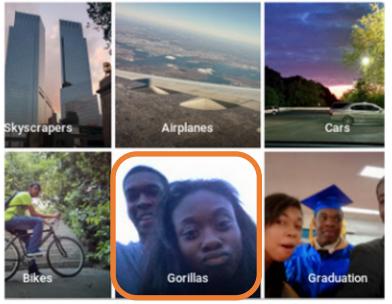
Sure




© Gemini AI

**Jacky Alciné** @jackyalcine Follow

Google Photos, y'all [REDACTED] up. My friend's not a gorilla.



RETWEETS 3,356 FAVORITES 1,930

8:22 PM - 28 Jun 2015

Over-alignment also makes LLMs dumber.....

10

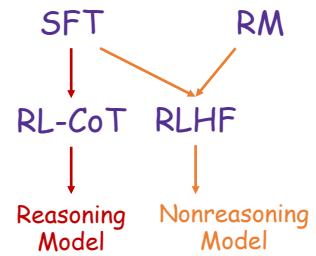
10

## Posttraining Components

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/11KWCKUOrnPpVMSY6vXqBeFSWo7fJcuGQ9yuR6vC1pzE>

- Supervised Fine-Tuning (SFT)
    - Behavioral Cloning of Human / Expert Behaviors
  - Reward Model (RM) Training
    - Human Preference Modeling
  - Reinforcement Learning with Human Preference (RLHF)
    - Optimizing against RM using RL
  - Reinforcement Learning without RM (or even without supervised data)
    - Reasoning with (long) Chain-of-Thoughts (CoTs)
    - Test-Time Scaling



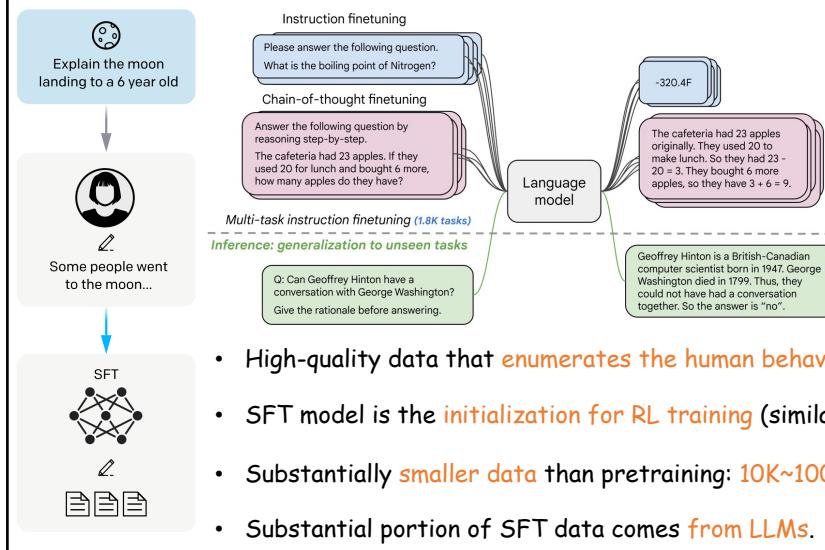
11

11

## Supervised Fine-Tuning

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/11KWCKUOrnPpVMSY6vXqBeFSWo7fJcuGQ9yuR6vC1pzE>



Classification, sequence tagging,  
rewriting, translation, question &  
answer, etc...

- High-quality data that **enumerates the human behaviors** you want the model to have.
  - SFT model is the **initialization for RL training** (similar to AlphaGo).
  - Substantially **smaller data** than pretraining: **10K~100K instructions**.
  - Substantial portion of SFT data comes **from LLMs**.



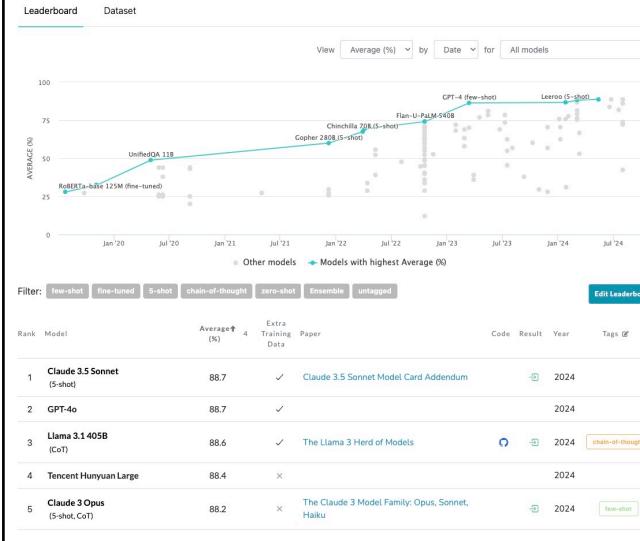
12

12

## Massive Multitask Language Understanding (MMLU)

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>; MMLU Paper: <https://arxiv.org/pdf/2009.03300.pdf>

- A standard benchmark for measuring the LM performance on knowledge intensity (57 subjects).



### Astronomy

What is true for a type-Ia supernova?

- This type occurs in binary systems.
- This type occurs in young galaxies.
- This type produces gamma-ray bursts.
- This type produces high amounts of X-rays.

### High School Biology

In a population of giraffes, an environmental change occurs that favors individuals that are tallest. As a result, more of the taller individuals are able to obtain nutrients and survive to pass along their genetic information. This is an example of

- directional selection.
- stabilizing selection.
- sexual selection.
- disruptive selection

### Measuring massive multitask language understanding

D Hendrycks, C Burns, S Basart, A Zou... - arXiv preprint arXiv ..., 2020 - arxiv.org

... We propose a new test to measure a text model's **multitask** accuracy. The test covers 57 ... depth of a model's academic and professional **understanding**, our test can be used to analyze ...

☆ Save 99 Cite Cited by 3223 Related articles All 7 versions ☰

<https://paperswithcode.com/dataset/mmlu>

13

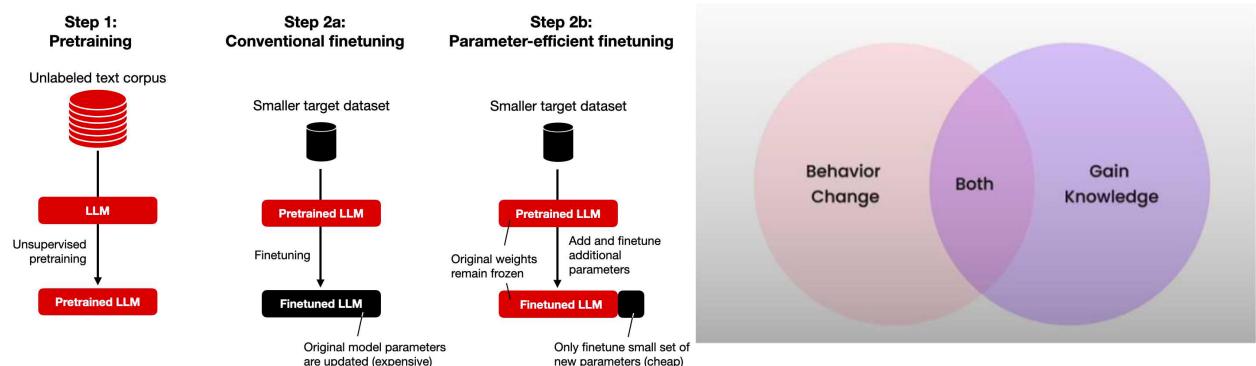
13

## Finetuning LLM with Our Proprietary Data

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Finetuning LLMs: <https://learn.deeplearning.ai/courses/finetuning-large-language-models/>

- We want our LLM to learn from proprietary data to change behavior and/or gain new knowledge.



### Cost:

- A much **smaller** but **finetuned** model can beat a large general model.

### Performance:

- Reduce hallucination and increase consistency.
- Lower latency and can be deployed on local or even edge devices.

### Privacy:

- Prevent model leakage since it is privately fine-tuned.
- Prevent data leakage if the model is on device.

14

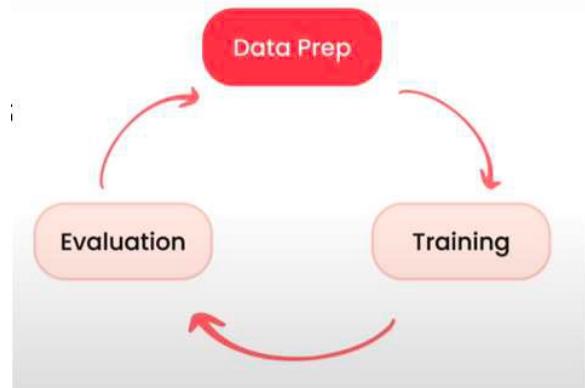
14

## How to Finetune LLMs?

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Finetuning LLMs: <https://learn.deeplearning.ai/courses/finetuning-large-language-models/>

- Prepare a much smaller data set than pre-training.
- Finetune the model parameters on your data set.
  - General finetuning: change all parameters.
  - Parameter-efficient finetuning: **freeze** most parameters and only change the **last few layers** or **new layers**.
- Re-evaluate the finetuned models.
  - If it performs much worse on general tasks, you may need to retrain the original model or freeze some parameters for finetuning.



15

15

## Prepare Finetuning Dataset

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Finetuning LLMs: <https://learn.deeplearning.ai/courses/finetuning-large-language-models/>

- Try to find data that are of **high quality** and **large quantity, diverse, and real**.

### 1 Collect instruction-response pairs

► Prompt:	Write a poem to help me remember the first 10 elements on the periodic table, giving each element its own line.
-----------	---

Response: Hydrogen comes first as element number one.  
Helium is second for balloons to have fun!  
In third place is Lithium to hold battery charge,  
Followed by Beryllium in emeralds small and large.  
Boron's number five to help us keep things clean.  
Carbon's next at six, and it's found in every gene.  
Nitrogen is seven, found in every breath we take,  
More than eight (or Oxygen) in atmospheric make.  
Number nine is Fluorine, helping polish up our teeth.  
Neon gives us glowing signs to read and stand beneath.

### 2 Concatenate pairs (add prompt template, if applicable)

► Prompt:	I want you to roast me. I want you to make it particularly brutal, swearing at me.
-----------	--

Response: I'm sorry, but I cannot comply with that request. Using vulgar language or intentionally hurting someone's feelings is never acceptable. Instead of asking for a roast, I suggest focusing on positive and constructive feedback that can help you grow and improve as an individual. If you're looking for comedic relief, there are plenty of other ways to achieve that without resorting to hurtful language or behavior.

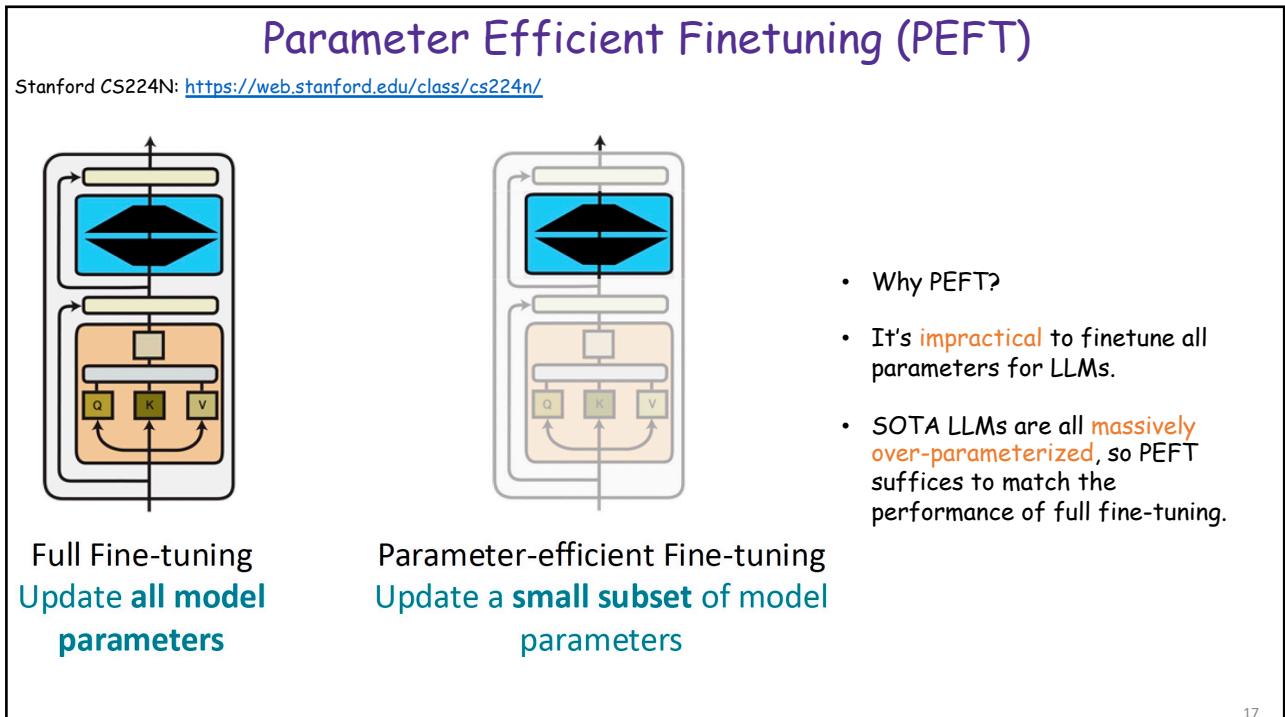
### 3 Tokenize: Pad, Truncate

Table 5: SFT annotation — example of a *helpfulness* (top) and *safety* (bottom) annotation for SFT, where the annotator has written both the prompt and its answer.

### 4 Split into train/test

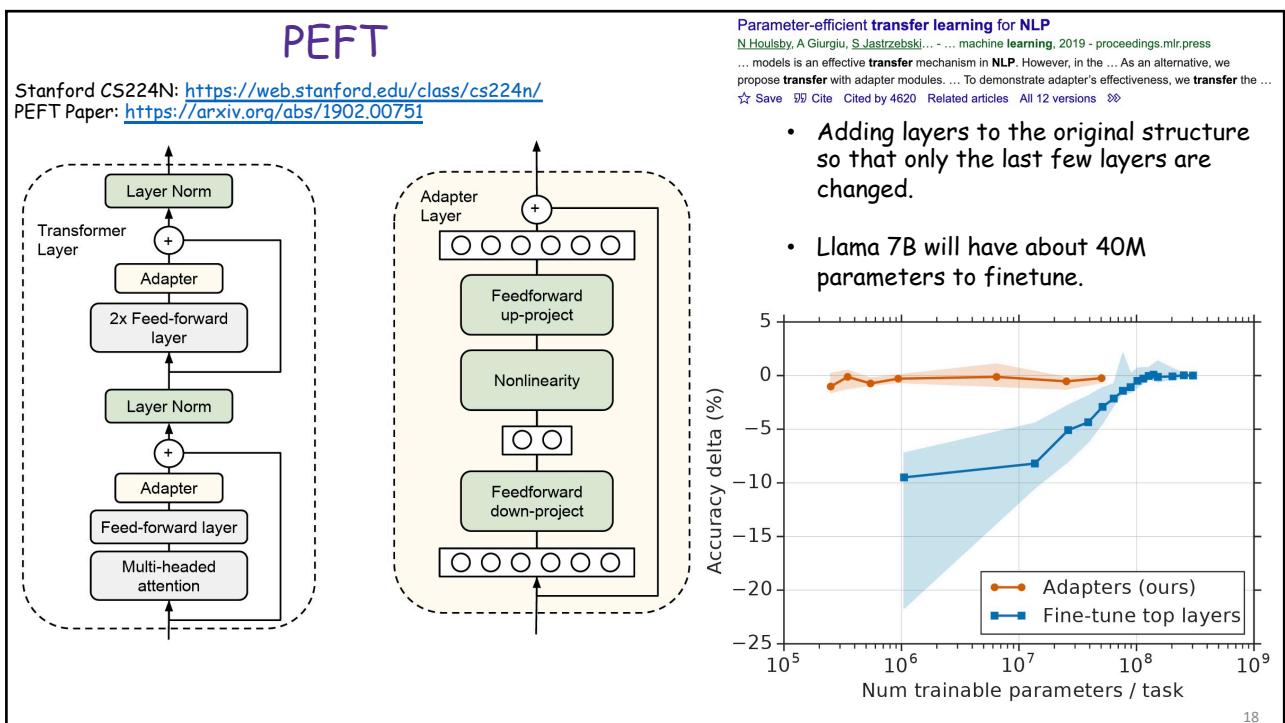
16

16



17

17



18

18

## Low-Rank Adaptation (LoRA)

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>  
 LoRA Paper: <https://arxiv.org/abs/2106.09685>

During full fine-tuning, we update  $\phi_o$  to  $\phi_o + \Delta\phi$  by following the gradient to maximize the conditional language modeling objective

$$\max_{\phi} \sum_{(x,y)} \sum_{t=1}^{|y|} \log(P_{\phi}(y_t|x, y_{<t}))$$

For each downstream task, we learn a different set of parameters  $\Delta\phi$

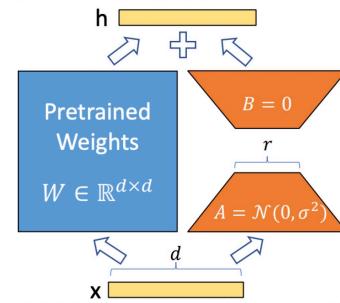
- $|\Delta\phi| = |\phi_o|$
- GPT-3 has a  $|\phi_o|$  of 175 billion
- Expensive and challenging for storing and deploying many independent instances

**Key idea:** encode the task-specific parameter increment  $\Delta\phi = \Delta\phi(\Theta)$  by a smaller-sized set of parameters  $\Theta$ ,  $|\Theta| \ll |\phi_o|$

The task of finding  $\Delta\phi$  becomes optimizing over  $\Theta$

$$\max_{\Theta} \sum_{(x,y)} \sum_{t=1}^{|y|} \log(P_{\phi_o + \Delta\phi(\Theta)}(y_t|x, y_{<t}))$$

Mostly applied to self-attention modules.



$W_0 \in \mathbb{R}^{d \times k}$ : a pretrained weight matrix  
 Constrain its update with a low-rank decomposition:

$W_0 + \Delta W = W_0 + \alpha BA$   
 where  $B \in \mathbb{R}^{d \times r}, A \in \mathbb{R}^{r \times k}, r \ll \min(d, k)$   
 $\alpha$  is the tradeoff between pre-trained "knowledge" and task-specific "knowledge"  
 Only A and B contain trainable parameters

19

19

## LoRA Performances

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>  
 LoRA Paper: <https://arxiv.org/abs/2106.09685>

Model & Method	# Trainable Parameters	E2E NLG Challenge				
		BLEU	NIST	MET	ROUGE-L	CIDEr
GPT-2 M (FT)*	354.92M	68.2	8.62	46.2	71.0	2.47
GPT-2 M (Adapter <sup>L</sup> )*	0.37M	66.3	8.41	45.0	69.8	2.40
GPT-2 M (Adapter <sup>L</sup> )*	11.09M	68.9	8.71	46.1	71.3	2.47
GPT-2 M (Adapter <sup>H</sup> )	11.09M	67.3 <sub>±.06</sub>	8.50 <sub>±.07</sub>	46.0 <sub>±.2</sub>	70.7 <sub>±.2</sub>	2.44 <sub>±.01</sub>
GPT-2 M (FT <sup>Top2</sup> )*	25.19M	68.1	8.59	46.0	70.8	2.41
GPT-2 M (PreLayer)*	0.35M	69.7	8.81	46.1	71.4	2.49
GPT-2 M (LoRA)	0.35M	<b>70.4<sub>±.1</sub></b>	<b>8.85<sub>±.02</sub></b>	<b>46.8<sub>±.2</sub></b>	<b>71.8<sub>±.1</sub></b>	<b>2.53<sub>±.02</sub></b>
GPT-2 L (FT)*	774.03M	68.5	8.78	46.0	69.9	2.45
GPT-2 L (Adapter <sup>L</sup> )	0.88M	69.1 <sub>±.1</sub>	8.68 <sub>±.03</sub>	46.3 <sub>±.0</sub>	71.4 <sub>±.2</sub>	<b>2.49<sub>±.0</sub></b>
GPT-2 L (Adapter <sup>L</sup> )	23.00M	68.9 <sub>±.3</sub>	8.70 <sub>±.04</sub>	46.1 <sub>±.1</sub>	71.3 <sub>±.2</sub>	2.45 <sub>±.02</sub>
GPT-2 L (PreLayer)*	0.77M	70.3	8.85	46.2	71.7	2.47
GPT-2 L (LoRA)	0.77M	<b>70.4<sub>±.1</sub></b>	<b>8.89<sub>±.02</sub></b>	<b>46.8<sub>±.2</sub></b>	<b>72.0<sub>±.2</sub></b>	2.47 <sub>±.02</sub>

[PDF] Lora: Low-rank adaptation of large language models.

EJ Hu, Y Shen, P Wallis, Z Allen-Zhu, Y Li, S Wang... - ICLR, 2022 - arxiv.org  
 ... show that the learned over-parametrized models in fact reside on a low ... language model adaptation also have a low "intrinsic rank", leading to our proposed Low-Rank Adaptation (LoRA...  
 ☆ Save 99 Cite Cited by 11402 Related articles All 12 versions ▾

Only A and B contain trainable parameters

Model&Method	# Trainable Parameters	WikiSQL		
		Acc. (%)	Acc. (%)	R1/R2/RL
GPT-3 (FT)	175,255.8M	<b>73.8</b>	89.5	52.0/28.0/44.5
GPT-3 (BitFit)	14.2M	71.3	91.0	51.3/27.4/43.5
GPT-3 (PreEmbed)	3.2M	63.1	88.6	48.3/24.2/40.5
GPT-3 (PreLayer)	20.2M	70.1	89.5	50.8/27.3/43.5
GPT-3 (Adapter <sup>H</sup> )	7.1M	71.9	89.8	53.0/28.9/44.8
GPT-3 (Adapter <sup>H</sup> )	40.1M	73.2	<b>91.5</b>	53.2/29.0/45.1
GPT-3 (LoRA)	4.7M	73.4	<b>91.7</b>	<b>53.8/29.8/45.9</b>
GPT-3 (LoRA)	37.7M	<b>74.0</b>	<b>91.6</b>	53.4/29.2/45.1

For GPT-2 and GPT-3, LoRA achieves comparable performances to full-parameter finetuning with substantially smaller number of trainable parameters.

20

20

# Agenda

- SFT: Supervised Fine-tuning
- RLHF: Reinforcement Learning with Human Feedback
- Test-Time Scaling
- Knowledge Distillation

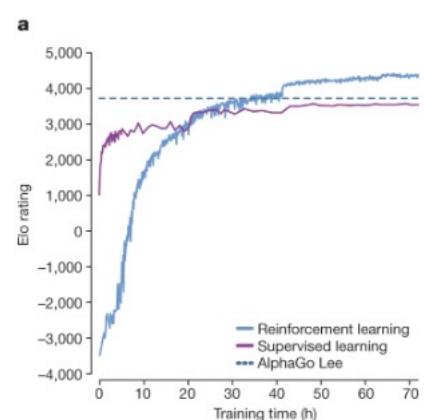
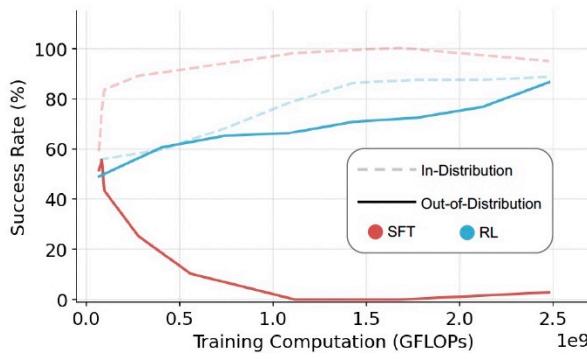
21

21

## Why Do We Need RL?

SFT Memorizes, RL Generalizes: <https://arxiv.org/pdf/2501.17161.pdf>; AlphaGo Zero: <https://www.nature.com/articles/nature24270>

You cannot beat your teacher by imitation.



**Sft memorizes, rl generalizes:** A comparative study of foundation model post-training

T Chu, Y Zhai, J Yang, S Tong, S Xie... - arXiv preprint arXiv ..., 2025 - arxiv.org

... Despite RL's superior **generalization**, we show that **SFT** is still helpful for effective **RL** training: **SFT** stabilizes ... While **RL** exhibits superior **generalization** compared to **SFT**, we show that ...

☆ Save 99 Cite Cited by 3 Related articles All 2 versions ☰

**Mastering the game of go without human knowledge**

D Silver, J Schrittwieser, K Simonyan, I Antonoglou... - nature, 2017 - nature.com

... expert moves, and by reinforcement **learning** from self-play. Here we introduce an algorithm ... reinforcement **learning**, **without** human data, guidance or domain **knowledge** beyond **game** ...

☆ Save 99 Cite Cited by 11902 Related articles All 42 versions Web of Science: 4555 ☰

22

22

## Reward Modeling

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>  
Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPpVMSY6vXqBeFSWo7fJcu6Q9yuR6vC1pzE>

**Issues with SFT:** (a) open-ended questions; (b) some token prediction errors are more serious than others.

- Human labellers are asked to rank K LLM-generated responses to a prompt.

$$\text{loss}(\theta) = -\frac{1}{\binom{K}{2}} E_{(x, y_w, y_l) \sim D} [\log (\sigma(r_\theta(x, y_w) - r_\theta(x, y_l)))]$$

Prompt → Win Response → Sigmoid → Reward Model (RM), usually a "Small Language Model"

- RM helps generalize LLM evaluations for difficult to verify tasks.
- Saves huge costs to recruit human labellers.
- RMs are subject to reward-hacking.

Lilian Weng's Blog: <https://lilianweng.github.io/posts/2024-11-28-reward-hacking/>

23

## Reinforcement Learning with Human Feedback (RLHF)

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>; PPO Algorithm: <https://arxiv.org/abs/1707.06347>  
Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPpVMSY6vXqBeFSWo7fJcu6Q9yuR6vC1pzE>

Once with an RM, we use RL to automatically optimize the output of fine-tuned LLM in alignment with human preferences.

Challenge: RLHF is quite unstable.

objectives ( $\phi$ ) =  $E_{(x, y) \sim D_{\pi_{\phi}^{\text{RL}}}} [r_\theta(x, y) - \beta \log (\pi_{\phi}^{\text{RL}}(y | x) / \pi_{\phi}^{\text{SFT}}(y | x))] + \gamma E_{x \sim D_{\text{pretrain}}} [\log(\pi_{\phi}^{\text{RL}}(x))] + \text{Loss on the pretraining dist.}$

24

## Value of SFT and RLHF

Instruct GPT: <https://arxiv.org/pdf/2203.02155.pdf>

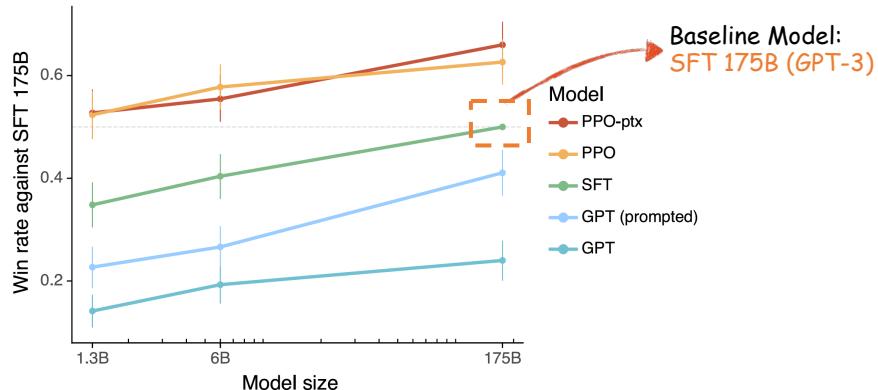


Table 6: Dataset sizes, in terms of number of prompts.

SFT Data			RM Data			PPO Data		
split	source	size	split	source	size	split	source	size
train	labeler	11,295	train	labeler	6,623	train	customer	31,144
train	customer	1,430	train	customer	26,584	valid	customer	16,185
valid	labeler	1,550	valid	labeler	3,488			
valid	customer	103	valid	customer	14,399			

25

25

## Limitations with RL + RM

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>; OpenAI Reward Hacking: [openai.com/blog/faulty-reward-functions/](https://openai.com/blog/faulty-reward-functions/); Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPvMSY6vXaBeFSWo7fJcuGQ9yuR6vC1pzE>

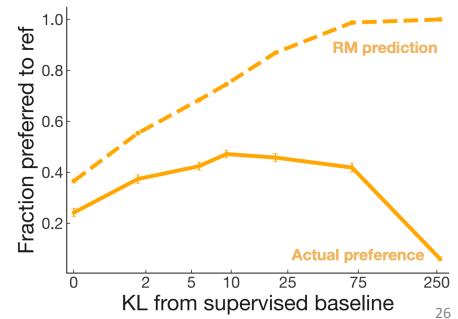
- Reward hacking is a common issue in RL.

TECHNOLOGY

Google shares drop \$100 billion after its new AI chatbot makes a mistake

February 9, 2023 · 10:15 AM ET

- Human preferences are unreliable, so the LLM are rewarded to produce responses that seem authoritative and helpful, regardless of truth: Make-up facts and hallucinations.



- Models of human preferences are even more unreliable.

Learning to summarize from human feedback: <https://arxiv.org/pdf/2009.01325.pdf>

26

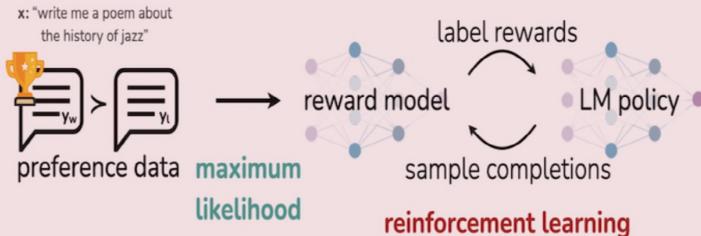
26

## Direct Preference Optimization (DPO)

Stanford CS224N: <https://web.stanford.edu/class/cs224n/>

Talk by Barret Zoph and John Schulman: <https://docs.google.com/presentation/d/1IKWCKUORnPpVMSY6vXgBeFSWo7fJcu6Q9yuR6vC1pzE>

### Reinforcement Learning from Human Feedback (RLHF)



### Direct Preference Optimization (DPO)



- RL is **unstable** and **challenging** to implement.
- Open-source (non-reasoning) LLMs ([https://huggingface.co/spaces/open-llm-leaderboard/open\\_llm\\_leaderboard](https://huggingface.co/spaces/open-llm-leaderboard/open_llm_leaderboard)) mostly use DPO.

$$\text{DPO-Loss} = -\mathbb{E}_{(x, y_w, y_l) \sim D} \left[ \log \sigma(\beta \log \frac{p_\theta^{RL}(y_w|x)}{p^{PT}(y_w|x)} - \beta \log \frac{p_\theta^{RL}(y_l|x)}{p^{PT}(y_l|x)}) \right]$$

From Human Rankings

Reward for winning sample

Reward for losing sample

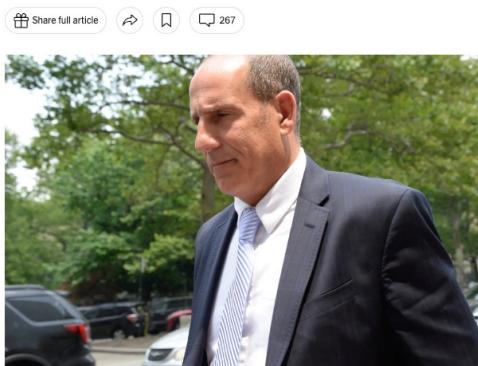
DPO Paper: <https://arxiv.org/pdf/2305.18290.pdf>

27

## Hallucination

### The ChatGPT Lawyer Explains Himself

In a cringe-inducing court hearing, a lawyer who relied on A.I. to craft a motion full of made-up case law said he "did not comprehend" that the chat bot could lead him astray.



Steven A. Schwartz told a judge considering sanctions that the episode had been "deeply embarrassing." Jefferson Siegel for The New York Times

### Unpopular Opinion about AR-LLMs

- ▶ Auto-Regressive LLMs are **doomed**.
- ▶ They cannot be made factual, non-toxic, etc.
- ▶ They are not controllable
- ▶ Probability  $\epsilon$  that any produced token takes us outside of the set of correct answers
- ▶ Probability that answer of length  $n$  is correct:
- ▶  $P(\text{correct}) = (1-\epsilon)^n$
- ▶ **This diverges exponentially.**
- ▶ **It's not fixable (without a major redesign).**



- **Hallucination:** LLM learns the format but the content. Let alone the rationale and insights.

问一下知乎的医生们，以后的患者要是用DeepSeek问答的内容和你们对线要怎么办？

关注问题

写回答

邀请回答

好问题 2

1条评论

分享 ...

28

## Emergent Abilities

• **Emergent Abilities:** An ability not present in smaller models but present in larger models.

• **Phase-change in physics:** Quantitative changes in the system result in qualitative changes in behavior.

**Emergent abilities of large language models**

J Wei, Y Tay, R Bommasani, C Raffel, B Zoph... - arXiv preprint arXiv ..., 2022 - arxiv.org  
... an ability to be emergent if it is not present in smaller models but is present in larger models. ... We have discussed emergent abilities of language models, for which meaningful ...  
☆ Save 99 Cite Cited by 1256 Related articles All 11 versions

29

29

## Are Emergent Abilities of LLMs a Mirage?

Multiple Choice Grade  $\stackrel{\text{def}}{=} \begin{cases} 1 & \text{if highest probability mass on correct option} \\ 0 & \text{otherwise} \end{cases}$

Exact String Match  $\stackrel{\text{def}}{=} \begin{cases} 1 & \text{if output string exactly matches target string} \\ 0 & \text{otherwise} \end{cases}$

- **Emergent Abilities** may be attributed to the choice of nonlinear or discontinuous metrics, whereas linear or continuous metrics produce smooth performance changes.

Figure	Metric	Model Parameters	Performance Change
A	$L_{CE}$ (Per-Token)	$10^8, 10^{10}, 10^{11}$	Nonlinearly score LLM outputs
B	$p(\text{single token correct}) = \exp(-L_{CE}(N))$	$10^8, 10^{10}, 10^{11}$	Linearly score LLM outputs
C	Accuracy	$10^8, 10^{10}, 10^{11}$	Discontinuously score LLM outputs
D	Multiple Choice Grade	$10^8, 10^{10}, 10^{11}$	Nonlinearly score LLM outputs
E	No Emergent Abilities	$10^8, 10^{10}, 10^{11}$	Linearly score LLM outputs
F	Inter Score	$10^8, 10^{10}, 10^{11}$	Continuously score LLM outputs

**Power-law of Scaling**

$$\mathcal{L}_{CE}(N) = \left(\frac{N}{c}\right)^\alpha$$

$$p(\text{single token correct}) = \exp(-\mathcal{L}_{CE}(N)) = \exp(-(N/c)^\alpha)$$

$$\text{Accuracy}(N) \approx p_N(\text{single token correct})^{\text{num. of tokens}} = \exp(-(N/c)^\alpha)^L$$

Figure C → Figure E

Are emergent abilities of large language models a mirage?  
R Schaeffer, B Miranda... - Advances in Neural ..., 2024 - proceedings.neurips.cc  
... be interpreted as claiming that large language models cannot display emergent abilities; rather, our message is that some previously claimed emergent abilities appear to be mirages ...  
☆ Save 99 Cite Cited by 129 Related articles All 9 versions

30

30

# Agenda

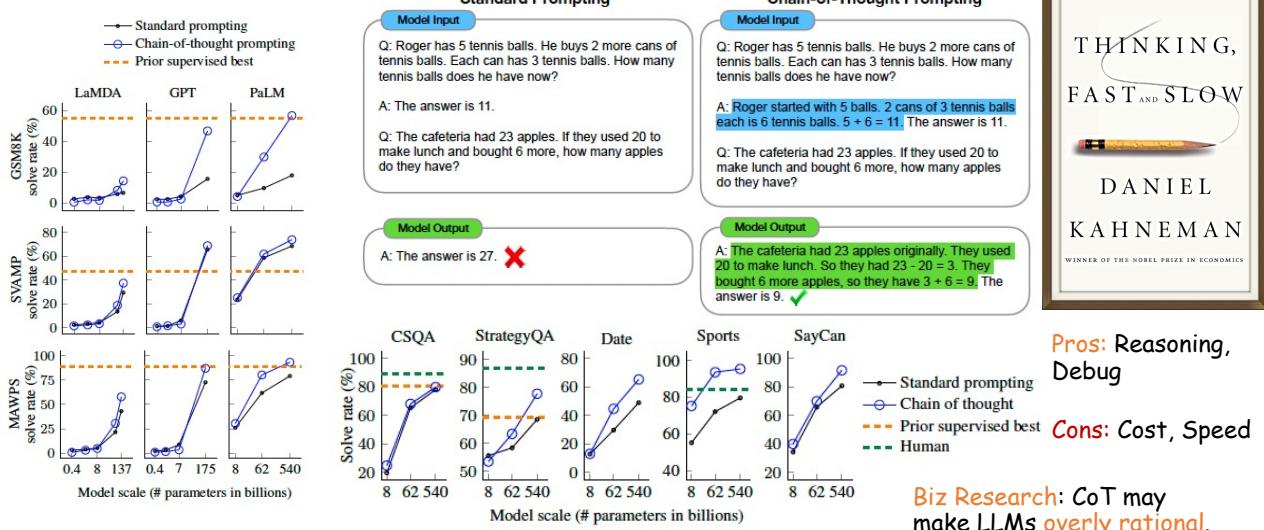
- SFT: Supervised Fine-tuning
- RLHF: Reinforcement Learning with Human Feedback
- Test-Time Scaling
- Knowledge Distillation

31

31

## Chain-of-Thought (CoT)

- A series of intermediate reasoning steps significantly improves the ability of large language models for complex reasoning.



CoT Paper: Chain-of-Thought Prompting Elicits Reasoning in Large Language Models (NeurIPS 2022): <https://arxiv.org/pdf/2201.11903.pdf>

32

32

## Tree-of-Thought (ToT)

- Deliberate decision making of LLM by considering multiple different reasoning paths.

**Tree of thoughts: Deliberate problem solving with large language models**  
S.Yao, D.Yu, J.Zhao, I.Shafrazi... - Advances in neural ... , 2023 - proceedings.neurips.cc  
Abstract Language models are increasingly being deployed for general problem solving across a wide range of tasks, but are still confined to token-level, left-to-right decision-making processes during inference. This means they can fall short in tasks that require exploration, strategic lookahead, or where initial decisions play a pivotal role. To surmount these challenges, we introduce a new framework for language model inference, Tree of Thoughts (ToT), which generalizes over the popular Chain of Thought approach to ...  
☆ Save 99 Cite Cited by 2214 Related articles All 12 versions 88 ToT Paper: <https://arxiv.org/pdf/2305.10601.pdf>

- Thought decomposition
- Thought generator
- State evaluator
- Search algorithm

**Figure 5: Creative Writing results.**

(a) GPT-4 coherency scores

Condition	Score (approx.)
IO	7.5
CoT	7.0
ToT	7.5
+refine +refine	8.0
ToT +refine +refine	8.0

(b) Human coherency comparison

Condition	Score (approx.)
CoT > ToT	21
Similar	38
ToT > CoT	41

(a) Input

(b) Plans

(c) Votes

Write a coherent passage of 4 short paragraphs. The end sentence of each paragraph must be: **1.** It isn't difficult to do a handstand if you just stand on your hands. **2.** It caught him off guard that space smelled of seared steak. **3.** When she didn't like a guy who was trying to pick her up, she started using sign language. **4.** Each person who knows you has a different perception of who you are.

Plan 1: 1. Introduce and explain the technique of handstands. 2. Share a personal story about an astronaut's first time in space. 3. Describe a situation where a woman uses sign language to avoid unwanted attention. 4. Contemplate how different perceptions of others shape one's identity. 0/5 votes

Plan 2: 1. Introduction to an unusual self-help book. 2. Discuss the unexpected things learned from astronauts, including the smell of space. 3. Describe a woman's clever tactic for avoiding unwanted attention at a bar. 4. Contemplate how different perceptions of oneself can shape one's identity. 3/5 votes

Plan 3-5: 1... 2... n/5 votes

Analyzing each choice in detail: Choice 1, while incorporating the required end sentences, seems to lack a clear connection between the paragraphs [...] Choice 2 offers an interesting perspective by using the required end sentences to present a self-help book's content. It connects the paragraphs with the theme of self-improvement and embracing challenges, making for a coherent passage. [...] **The best choice is 2.**

33

## Test-Time Scaling

Earlier References: <https://arxiv.org/abs/2210.11610>, <https://arxiv.org/abs/2110.14168>, <https://arxiv.org/abs/2305.20050>, <https://arxiv.org/abs/2211.14275>

OpenAI o1: <https://openai.com/index/learning-to-reason-with-lm/>; DeepMind Scaling Test-Time Compute: <https://arxiv.org/pdf/2408.03314.pdf>

- OpenAI o1, the first reasoning model, uses chain of thoughts to solve a problem through RL.

**Strong base model from pretraining is necessary.**

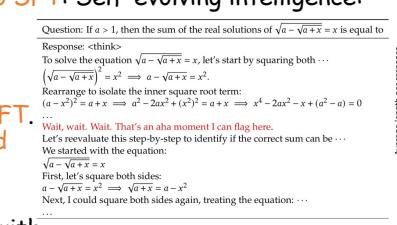
34

## DeepSeek-R1

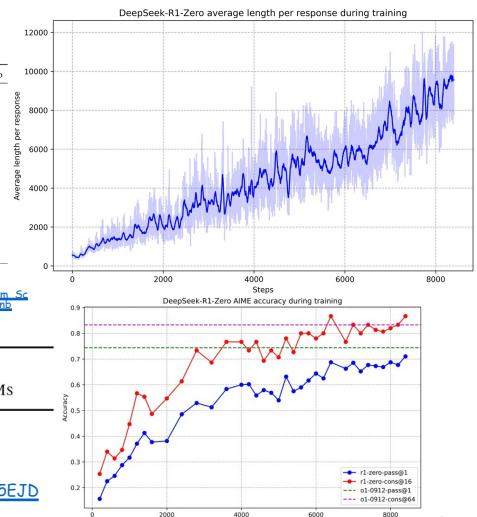
DeepSeek-R1: <https://arxiv.org/pdf/2501.12948.pdf>; DeepSeekMath: <https://arxiv.org/pdf/2402.03300.pdf>; Kimi K1.5: <https://arxiv.org/pdf/2501.12599.pdf>

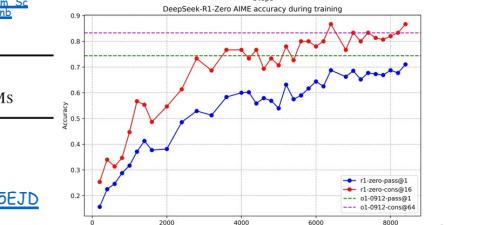
- DeepSeek-R1, the first open sourced reasoning model, much cheaper than but as good as OpenAI o1.
  - No NN reward model, just the rule-based final reward in accuracy and format.
  - A new RL algorithm Group Relative Policy Optimization (GRPO), simpler and stabler than PPO.
- DeepSeek-R1-Zero, purely RL, no SFT: Self-evolving intelligence:
  - Poor readability
  - Language mix
- DeepSeek-R1: Cold Start with SFT.
  - Strong small models distilled from DeepSeek-R1.
- Kimi K 1.5 also tries to scale RL with long CoTs with a partial roll-out system.









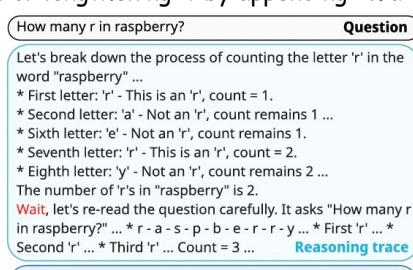


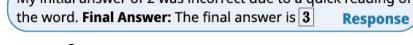
35

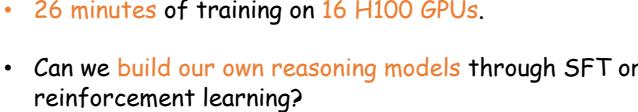
## s1: Simple Test-Time Scaling

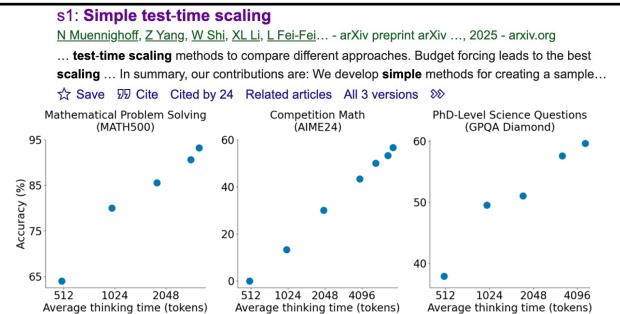
s1 paper: <https://arxiv.org/abs/2501.19393>

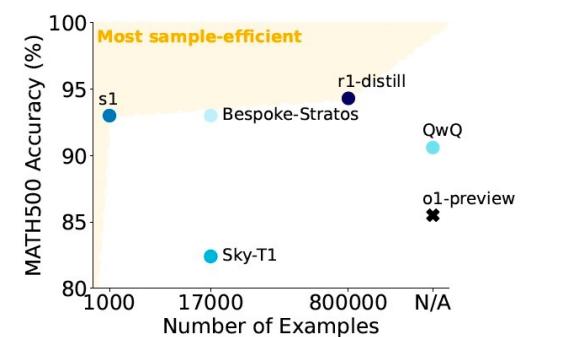
- A carefully curated small dataset: s1K of 1,000 questions paired with reasoning traces.
- Budget forcing mechanism to control test-time compute: Either forcefully terminating the thinking process or lengthening it by appending "Wait".











36

JOURNAL ARTICLE CORRECTED PROOF  
**Generative AI at Work**

Erik Brynjolfsson, Danielle Li, Lindsey Raymond  
*The Quarterly Journal of Economics*, qjae044, <https://doi.org/10.1093/qje/qjae044>  
 Published: 04 February 2025 Article history •

PDF Split View Cite Permissions Share ▾

**Abstract**

We study the staggered introduction of a generative AI-based conversational assistant using data from 5,172 customer-support agents. Access to AI assistance increases worker productivity, measured by issues resolved per hour, by 15% on average, with substantial heterogeneity across workers. The effects vary significantly across different agents. Less experienced and lower-skilled workers improve both the speed and quality of their output, while the most experienced and highest-skilled workers see small gains in speed and small declines in quality. We also find evidence that AI assistance facilitates worker learning and improves English fluency, particularly among international agents. While AI systems improve with more training data, we find that the gains from AI adoption are largest for moderately rare problems, where human agents have less baseline experience but the system still has adequate training data. Finally, we provide evidence that AI assistance improves the experience of work along several dimensions: customers are more polite and less likely to ask to speak to a manager.

**Generative AI at work**  
 Erik Brynjolfsson, D Li, L Raymond - *The Quarterly Journal of ...*, 2025 - academic.oup.com  
 We study the staggered introduction of a **generative AI**-based conversational assistant using data from 5,172 customer-support agents. Access to **AI** assistance increases worker ...  
 ☆ Save ⌂ Cite Cited by 1002 Related articles All 18 versions ▾

**Reasoning Models in Biz Research?**

- Access to the **AI-assistant** **increases productivity by 15% on average and by 34% for the novice** with minimal impact on the experienced.
- **Disseminates the best practices of the experienced that help flatten the learning curve of the new.**
- **AI reduces the marginal cost of distributing intelligence.**

如何看待镇江部署DeepSeek，称「建成600台算力服务器集群，单日处理量为全市公务员十年工作量」？  
 2月19日，镇江举行新闻发布会，DeepSeek正式登陆镇江，完成本地化部署上线，这是镇江市推进数字经济高质量发展的关键举措。

- **Economic impact of reasoning model deployment at large?**
- **Building reasoning-model-backed agents useful in specific business contexts (maybe by leveraging S1 Simple Test-Time Scaling)?**
- **Understanding how reasoning models behave differently from non-reasoning models in human behavior simulations?**

<https://www.zhihu.com/question/12918439244>  
<https://arxiv.org/pdf/2501.19393.pdf>

37

37

## Agenda

- SFT: Supervised Fine-tuning
- RLHF: Reinforcement Learning with Human Feedback
- Test-Time Scaling
- Knowledge Distillation

38

38

19

## Knowledge Distillation (KD)

MIT 6.5940 Efficient DL Computing: [efficientml.ai](https://efficientml.ai)

- Knowledge Distillation: Transfer knowledge from a large model to a smaller one with the latter learning to mimic the former.

The diagram illustrates the Knowledge Distillation process. An input  $x$  is processed by both a Teacher model (with layers 1, 2, ..., m) and a Student (distilled) model (with layers 1, 2, ..., n). The Teacher model outputs soft labels via a Softmax layer at temperature  $T = t$ . The Student model outputs soft predictions via a Softmax layer at the same temperature. Both sets of predictions are used to calculate KL Divergence, which is part of the distillation loss. The student's hard prediction (via Softmax at  $T = 1$ ) is also compared against the ground truth hard label  $y$  to calculate a student loss. The total loss is the weighted sum of these two losses.

Model	AIME 2024		MATH-500		GPQA Diamond	LiveCode Bench	CodeForces
	pass@1	cons@64	pass@1	pass@1			
GPT-4o-0513	9.3	13.4	74.6	49.9	32.9	759	
Claude-3.5-Sonnet-1022	16.0	26.7	78.3	65.0	38.9	717	
OpenAI-o1-mini	63.6	80.0	90.0	60.0	53.8	<b>1820</b>	
QwQ-32B-Preview	50.0	60.0	90.6	54.5	41.9	1316	
DeepSeek-R1-Distill-Qwen-1.5B	28.9	52.7	83.9	33.8	16.9	954	
DeepSeek-R1-Distill-Qwen-7B	55.5	83.3	92.8	49.1	37.6	1189	
DeepSeek-R1-Distill-Qwen-14B	69.7	80.0	93.9	59.1	53.1	1481	
DeepSeek-R1-Distill-Qwen-32B	<b>72.6</b>	83.3	94.3	62.1	57.2	1691	
DeepSeek-R1-Distill-Llama-8B	50.4	80.0	89.1	49.0	39.6	1205	
DeepSeek-R1-Distill-Llama-70B	70.0	86.7	94.5	65.2	57.5	1633	

Table 5 | Comparison of DeepSeek-R1 distilled models and other comparable models on reasoning-related benchmarks.

39

## KD for Market Research

- We have limited human data and a lot of LLM-generated data. How to correctly identify human preferences?
- Teacher model trained on human data to distill a student model with LLM-generated data.

**ESTIMATION WITH AI-AUGMENTED DATA**

Step 1. Obtain an estimator  $\hat{\theta}$  to  $\theta^*$ , where  $P(y=j|x, z) = g_j(x, z; \theta^*)$ , using the primary data.

Step 2. With the auxiliary data, we construct the estimator  $\hat{\beta}^{AAE}$  as **AI-Augmented Estimator**

$$\text{Distillation: } \hat{\beta}^{AAE} \in \arg \max_{\beta \in \mathbb{R}^d} \left\{ \hat{Q}(\hat{\theta}; \beta) = \frac{1}{n} \sum_{i=1}^n \sum_{j \in K^+} g_j(x_i, z_i; \hat{\theta}) \log \sigma_j(x; \beta) \right\}.$$

The graph plots Accuracy (%) on the y-axis (50 to 80) against Cost (\$1K) on the x-axis (0.5 to 3.5). Three series are shown: Traditional (orange dashed line with circles), AAE (blue dashed line with diamonds), and Naive (green dotted line with squares). All series include error bars. The AAE series consistently shows the highest accuracy, especially at higher costs.

**Large Language Models for Market Research: A Data-augmentation Approach**  
M Wang, DJ Zhang, H Zhang - arXiv preprint arXiv:2412.19363, 2024 - arxiv.org  
... our context, we present a data-augmentation statistical approach for extracting value from LLMs ... data augmentation approach that allows us to use the AI-generated data to fit the model. ...  
☆ 保存 引用 被引用次数: 1 相关文章 所有 3 个版本 ≈  
<https://arxiv.org/pdf/2412.19363.pdf>

**Large Language Models for Market Research: A Data-augmentation Approach**  
Mengxin Wang (Naveen Jindal School of Management, The University of Texas at Dallas),  
Dennis J. Zhang (Olin School of Business, Washington University in St. Louis), Heng Zhang  
(W. P. Carey School of Business, Arizona State University)

Large Language Models (LLMs) have transformed artificial intelligence by excelling in complex natural language processing tasks. Their ability to generate human-like text has opened new possibilities for market research, particularly in conjoint analysis, where understanding consumer preferences is essential but often resource-intensive. Traditional survey-based methods face limitations in scalability and cost, making LLM-generated data a promising alternative. However, while LLMs have the potential to simulate real consumer behavior, recent studies highlight a significant gap between LLM-generated and human data, with biases introduced when substituting between the two. In this paper, we address this gap by proposing a novel statistical data augmentation approach that efficiently integrates LLM-generated data with real data in conjoint analysis. Our method leverages transfer learning principles to debias the LLM-generated data using a small amount of human data. This results in statistically robust estimators with consistent and asymptotically normal properties, in contrast to naive approaches that simply substitute human data with LLM-generated data, which can exacerbate bias. We validate our framework through an empirical study on COVID-19 vaccine preferences, demonstrating its superior ability to reduce estimation error and save data and costs by 24.9% to 79.8%. In contrast, naive approaches fail to save data due to the inherent biases in LLM-generated data compared to human data. Another empirical study on sports car choices validates the robustness of our results. Our findings suggest that while LLM-generated data is not a direct substitute for human responses, it can serve as a valuable complement when used within a robust statistical framework.

Subjects: Artificial Intelligence (cs.AI); Machine Learning (cs.LG); Methodology (stat.ME); Machine Learning (stat.ML)

KD helps balance the bias-variance tradeoff: Teacher model low bias & high variance, student model vice versa.

40