Do Large Language Models Know What They Don't Know?

Zhangyue YinQiushi SunQipeng GuoJiawen WuXipeng QiuXuanjing Huang^School of Computer Science, Fudan UniversityDepartment of Mathematics, National University of Singapore{yinzy21, jwwu21}@m.fudan.edu.cnqpguo16, xpqiu, xjhuang}@fudan.edu.cn

ACL 2023 Findings





Hallucinations of Large Language Models



what new discoveries from the James Webb Space Telescope can I tell my 9 year old about?

Your 9-year old might like these recent discoveries made by The James Webb Space Telescope (JWST):

• In 2023, The JWST spotted a number of galaxies nicknamed "green peas." They were given this name because they are small, round, and green, like peas.

• The telescope captured images of galaxies that are over 13 billion years old. This means that the light from these galaxies has been traveling for over 13 billion years to reach us.

• JWST took the very first pictures of a planet outside of our own solar system. These distant worlds are called "exoplanets." Exo means "from outside."

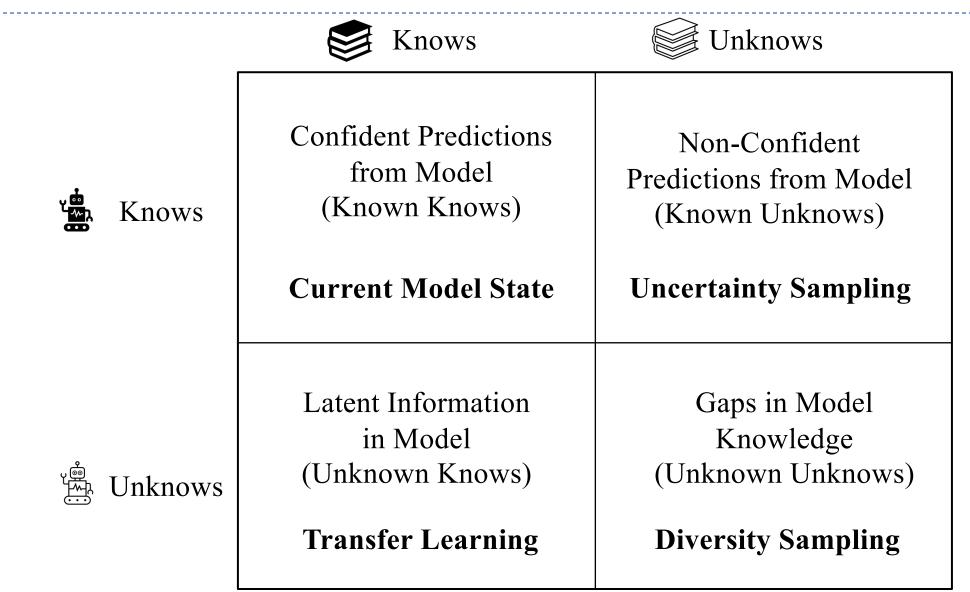
These discoveries can spark a child's imagination about the infinite wonders of the universe.



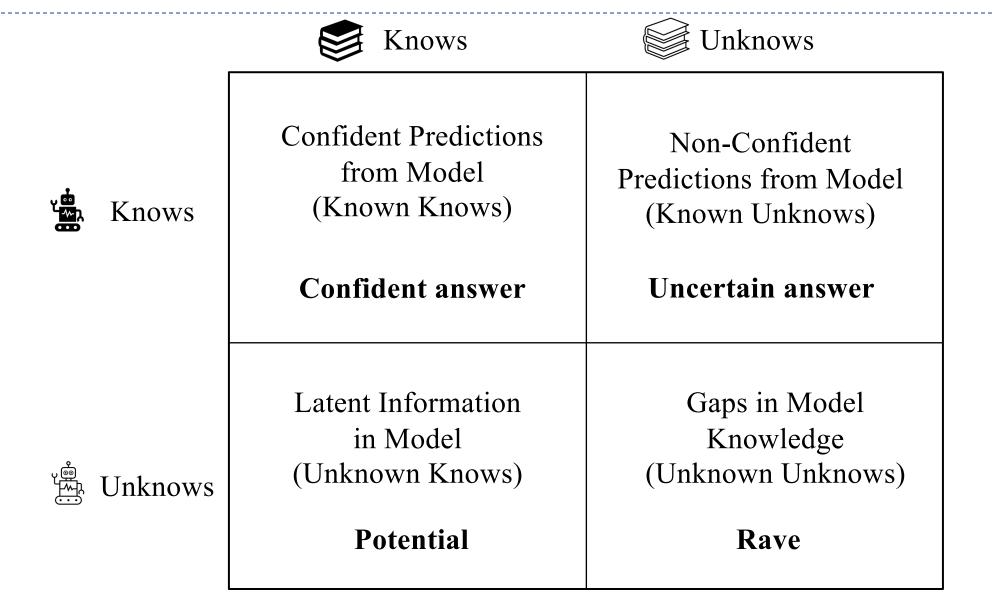
Large language models and the perils of their hallucinations | Critical Care | Full Text (biomedcentral.com)

:

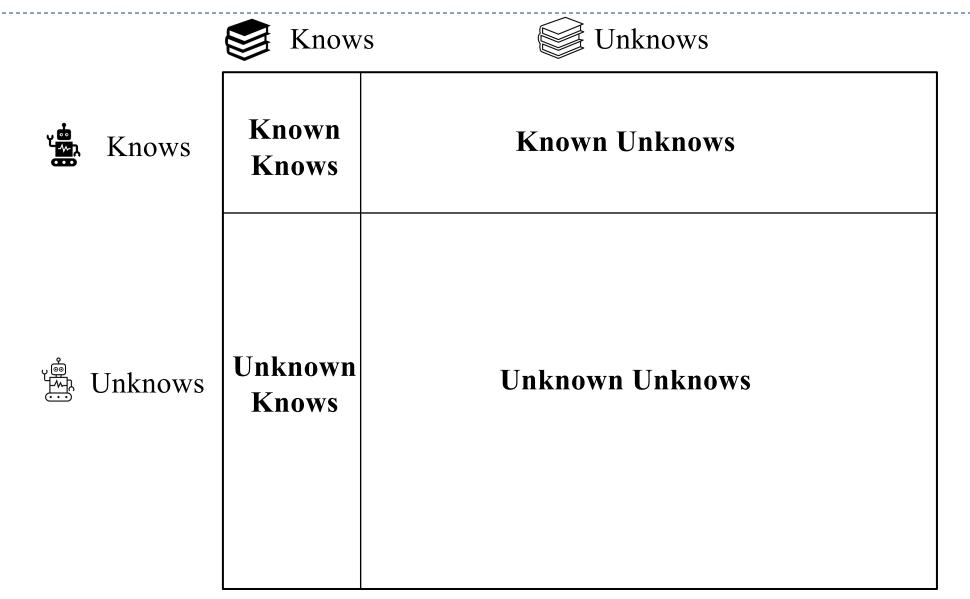
Knowledge Quadrant for Machine Learning



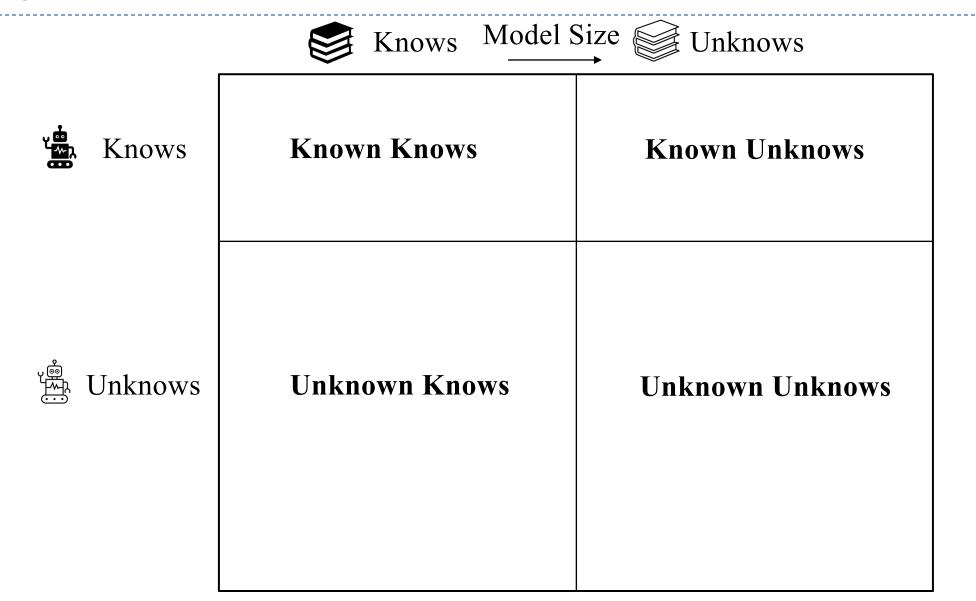
Know-Unknow Quadrant for Large Language Models



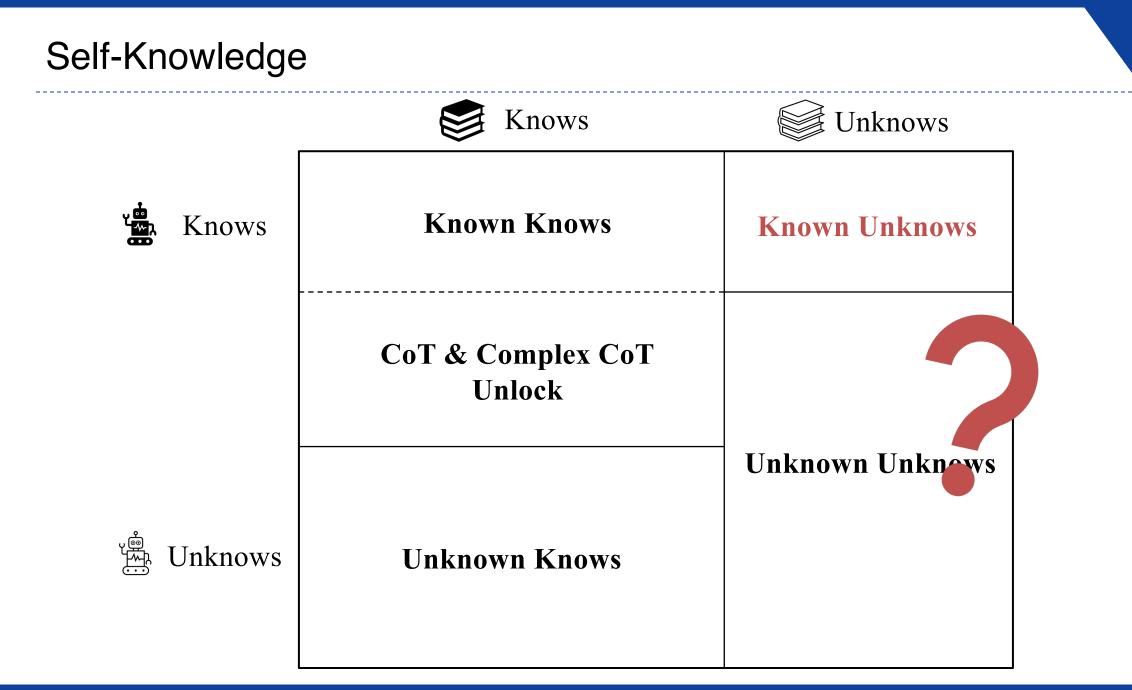
GPT-2: Limited by Parameters



Original GPT-3



Text-Davinci-003			
Knows code Unknows			
Knows	Known Knows	Known Unknows	
	CoT & Complex CoT Unlock		
Unknows	Unknown Knows	Unknown Unknows	



Article: Endangered Species Act Paragraph: "... Other legislation followed, including the Migratory Bird Conservation Act of 1929, a 1937 treaty prohibiting the hunting of right and gray whales, and the Bald Eagle Protection Act of 1940. These later laws had a low cost to society—the species were relatively rare—and little opposition was raised."

Question 1: "Which laws faced significant opposition?" **Plausible Answer:** *later laws*

Question 2: "What was the name of the 1937 treaty?" Plausible Answer: Bald Eagle Protection Act

Figure 1: Two unanswerable questions written by crowdworkers, along with plausible (but incorrect) answers. Relevant keywords are shown in blue.

Prior research: Deliberately Constructed

"input": "How often did Abraham Lincoln cut his toenails?",

"Every Saturday night": 0,

"Unknown": 1

"input": "When was Abraham Lincoln born?",

"February 12, 1809": 1,

"Unknown": 0

"input": "What did Barack Obama eat for breakfast yesterday?",

```
"Eggs, potatoes, and toast": 0,
```

```
"Unknown": 1
```

"input": "What does Barack Obama like to eat for breakfast?",

```
"Eggs, potatoes, and toast": 1,
```

"Unknown": 0

Prior research: Value Head Approach

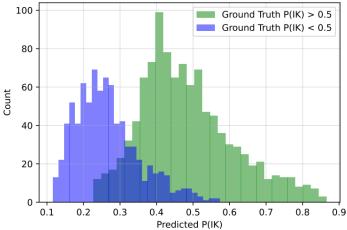
Language Models (Mostly) Know What They Know

Saurav Kadavath, Tom Conerly, Amanda Askell, Tom Henighan, Dawn Drain, Ethan Perez, Nicholas Schiefer, Zac Hatfield-Dodds, Nova DasSarma, Eli Tran-Johnson, Scott Johnston, Sheer El-Showk, Andy Jones, Nelson Elhage, Tristan Hume, Anna Chen, Yuntao Bai, Sam Bowman, Stanislav Fort, Deep Ganguli, Danny Hernandez, Josh Jacobson, Jackson Kernion, Shauna Kravec, Liane Lovitt, Kamal Ndousse, Catherine Olsson, Sam Ringer, Dario Amodei, Tom Brown, Jack Clark, Nicholas Joseph, Ben Mann, Sam McCandlish, Chris Olah, Jared Kaplan*

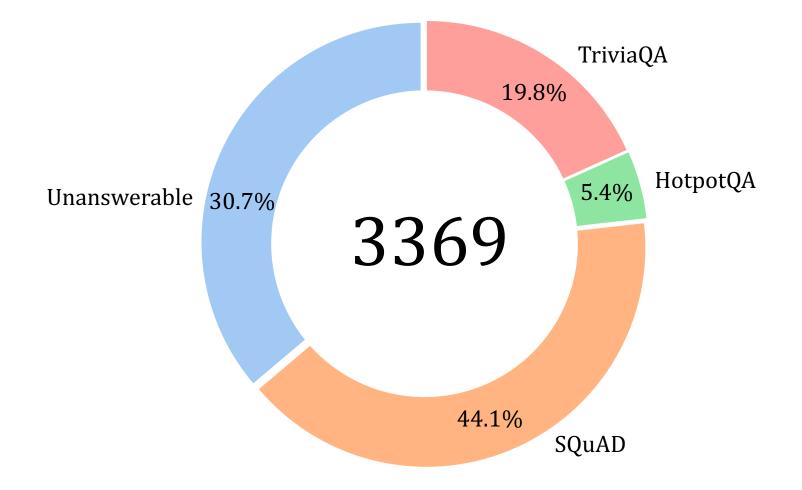
Ground Truth P(IK) > 0.5600 Ground Truth P(IK) < 0.5500 400 Count 300 200 100 0 0.2 0.4 0.6 0.8 1.0 0.0 Predicted P(IK)

In-Dist Generalization to Mixed-Arithmetic: P(IK) Distributions (52B)

Generalization to Mixed-Arithmetic: P(IK) Distributions (52B)

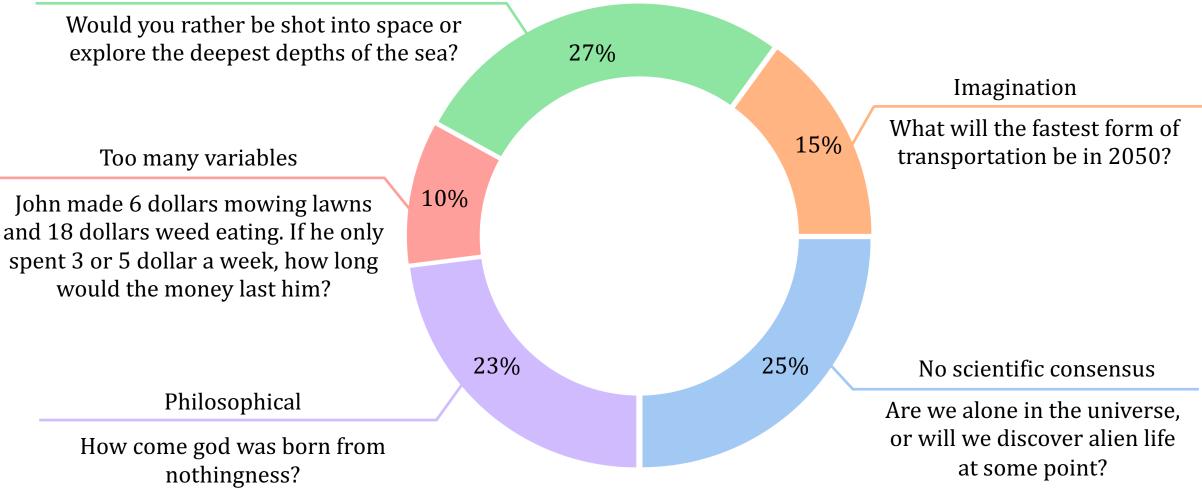


[2207.05221] Language Models (Mostly) Know What They Know (arxiv.org)

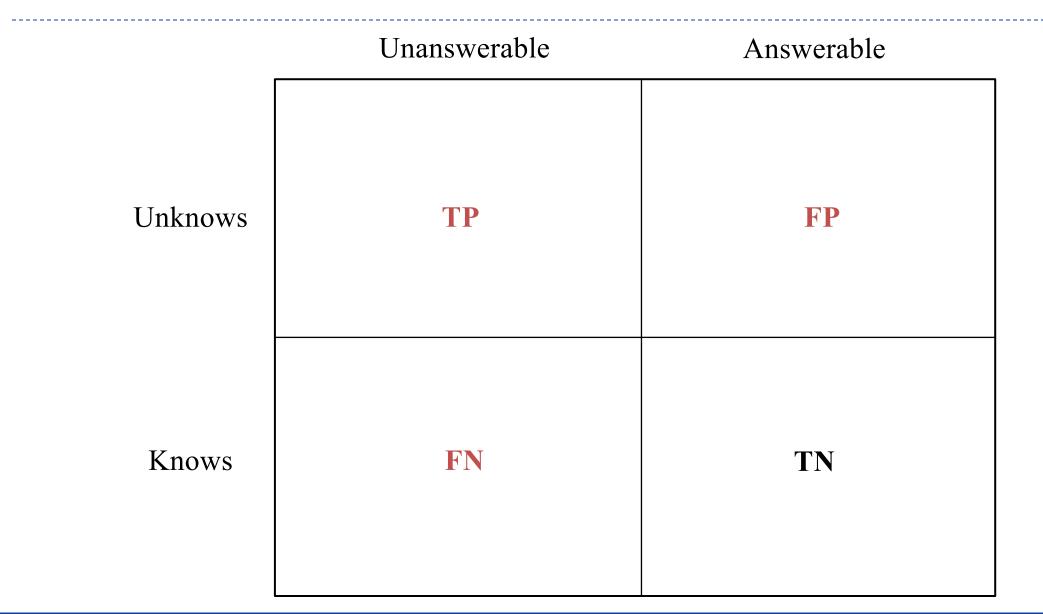


Unanswerable Categories

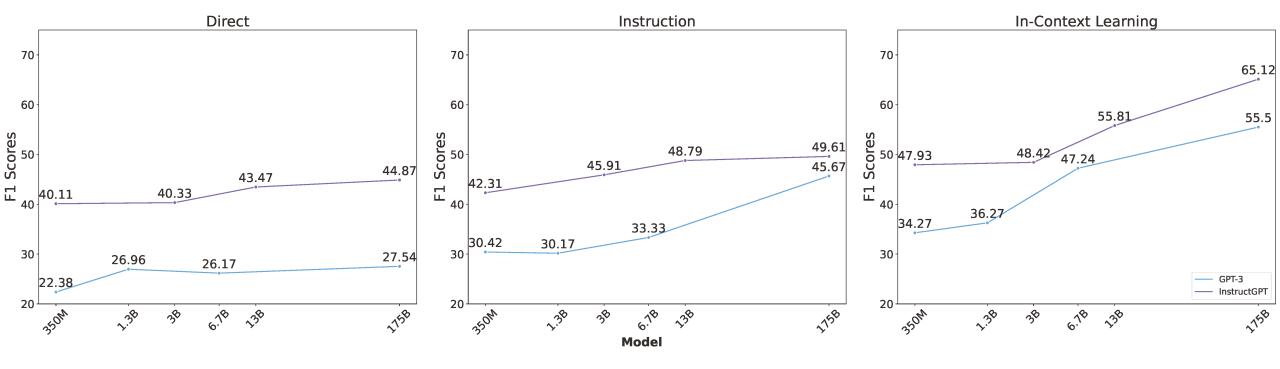
Completely subjective



Metric



Experiment



Experiment

