
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*

Anthropic

Abstract

We study whether language models can evaluate the validity of their own claims and predict which questions they will be able to answer correctly. We first show that larger models are well-calibrated on diverse multiple choice and true/false questions when they are provided in the right format. Thus we can approach self-evaluation on open-ended sampling tasks by asking models to first propose answers, and then to evaluate the probability "P(True)" that their answers are correct. We find encouraging performance, calibration, and scaling for P(True) on a diverse array of tasks. Performance at self-evaluation further improves when we allow models to consider many of their own samples before predicting the validity of one specific possibility. Next, we investigate whether models can be trained to predict "P(IK)", the probability that "I know" the answer to a question, without reference to any particular proposed answer. Models perform well at predicting P(IK) and partially generalize across tasks, though they struggle with calibration of P(IK) on new tasks. The predicted P(IK) probabilities also increase appropriately in the presence of relevant source materials in the context, and to the presence of hints towards the solution of mathematical word problems. We hope these observations lay the groundwork for training more honest models, and for investigating how honesty generalizes to cases where models are trained on objectives other than the imitation of human writing.

*Correspondence to: {saurav, jared}@anthropic.com
Author contributions are listed at the end of the paper.

Contents

1	Introduction	3
1.1	Contributions	4
1.2	Models and Evaluation Tasks	5
1.3	Related Work	6
2	Larger Models are Calibrated on Diverse Multiple Choice Questions	7
3	From Calibration to Knowing What You Know	8
3.1	Replacing an Option with ‘None of the Above’ Harms Performance and Calibration	8
3.2	Models are Well-Calibrated on True/False Tasks	10
3.3	RLHF Policy Miscalibration Can Be Remediated with a Temperature Tuning	10
4	Ask the AI: Is your proposed answer True or False?	11
4.1	Basic Self-Evaluation	11
4.2	Showing Many $T = 1$ Samples Improves Self-Evaluation	12
5	Training Models to Predict Whether They Can Answer Questions Correctly	13
5.1	Evaluating P(IK) Training and Model Size Trends	14
5.2	Out of Distribution Generalization of P(IK)	14
5.3	P(IK) Generalizes to Account for Source Materials	15
5.4	P(IK) Generalizes to Account for Hints Towards GSM8k Solutions	19
5.5	Comparing Models Trained with Distinct Pretraining Distributions	20
6	Discussion	21
6.1	Limitations and Future Work	22
6.2	Broader Impacts	23
7	Contribution Statement	23
A	Metrics, Formatting Details, and P(IK) Training	24
B	Discriminating What Models Know with Entropy or Loss	27
C	More P(True) Evaluation Results and Details	31
D	Mixed-Arithmetic and Function Synthesis Dataset Descriptions	31

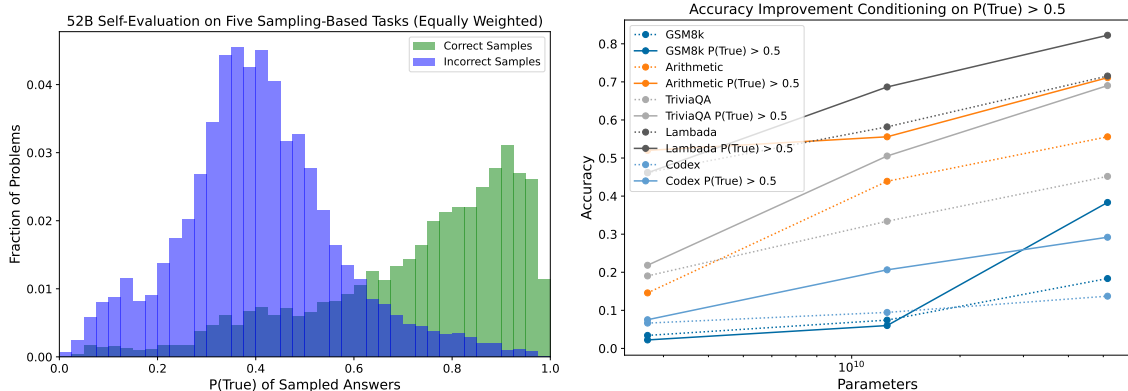


Figure 1 (left) We show the overall ability of a 52B language model to evaluate its own proposed answers (sampled at unit temperature) to questions from TriviaQA, Lambada, Arithmetic, GSM8k, and Codex HumanEval. We have weighted the overall contribution from each of these five datasets equally. We evaluate 20-shot using the method of section 4, where we show the model several of its own samples and then ask for the probability $P(\text{True})$ that a specific sample is correct. (right) We show the improvement in the accuracy on each sampling task when only including questions where a randomly sampled (unit temperature) response achieved $P(\text{True}) > 0.5$.

1 Introduction

We would eventually like to train AI systems that are honest, which requires that these systems accurately and faithfully evaluate their level of confidence in their own knowledge and reasoning. So AI systems must be able to recognize what they do and do not know, as a prerequisite. In this work, we study the extent to which Language Models (LMs) possess this ability and how it can be elicited and imparted.

As a starting point, we examine calibration: do the probabilistic predictions from language models match up with frequencies of occurrence? Language models can produce well-calibrated predictions for token probabilities on-distribution [Guo et al., 2017]. We show that large language models are also well-calibrated on a diverse array of multiple choice questions, as long as the questions are formatted appropriately. In particular, calibration improves with model size and few-shot prompting.

Good calibration opens up the possibility for using models to evaluate the accuracy of their own outputs (“self-evaluation”). For example, given any open-ended query, we can sample an answer from the model and then have the model evaluate $P(\text{True})$, the probability that its answer is correct. We may expect self-evaluation to be challenging, because the model may be overconfident that its own samples¹ are correct. Our self-evaluation procedure nevertheless distinguishes correct and incorrect samples, as summarized in Figure 1. Furthermore, as model size and capabilities increase, models improve at self-evaluation, which suggests that verification improves faster than generation quality in this context.

We also show that self-evaluation can be improved if we provide a model with *many* of its own samples, before asking it to evaluate any single sample. That is, ‘brainstorming other possibilities’ helps large models to evaluate the validity of a given answer option.

These techniques address a question about the world, as they ask models to evaluate “according to accepted truth in the wider world (i.e. according to humans), is a particular answer to a question correct?” In the case of self-evaluation, the proposed answer was provided by the model, but its validity is nevertheless an external fact.

But we are also interested in having language models attempt to directly evaluate their own state of knowledge. To this purpose, we investigate what happens when we train models to predict whether or not they can correctly answer questions themselves. This is really a question about the model² since we are training the model to learn what sorts of questions *it*, in particular, can answer.

¹Another more subtle issue is that in our setup, models have no way to distinguish the tokens they’ve written from tokens they were given by a third party.

²This claim is subtle, since the model could be learning “how hard is this question in general?” rather than “do I know the answer to this?” We partially address this concern in section 5.5.

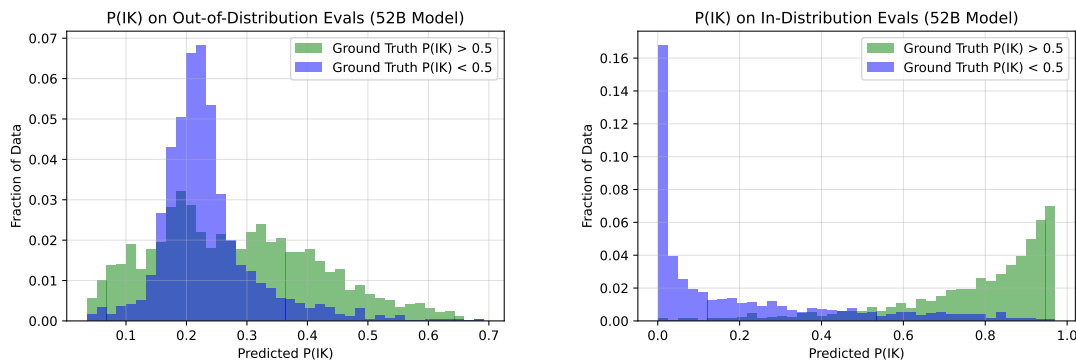


Figure 2 **Left:** We train a P(IK) classifier to predict whether or not a model knows the answer to TriviaQA questions, and then evaluate on Arithmetic, Python Function Synthesis, and Lambada questions. This histogram shows P(IK) scores exclusively from OOD questions. **Right:** We train a P(IK) classifier on TriviaQA, Arithmetic, Python Function Synthesis, and Lambada and histogram P(IK) scores for their test sets.

We find that language models can easily learn to perform well at evaluating P(IK), the probability that they know the answer to a question, on a given distribution (see Figure 3 for an illustration). More intriguingly, we also find some generalization across tasks, for example from trivia to story completion, math, and code, though models struggle with calibration OOD. We also observe some other types of generalization: although P(IK) was only trained on bare questions, it generalizes in such a way that it increases when we provide source materials that address these questions (for trivia) and when we provide hints for math word problems.

1.1 Contributions

Calibration: Multiple Choice, None of the Above, and True/False

- We show that when we use a format with visible lettered answer options, large models are very well calibrated on diverse multiple choice questions (e.g. from BIG Bench [Srivastava et al., 2022], MMLU [Hendrycks et al., 2021], and many other evaluations); see Figures 4, 5, and 6.
- Calibration improves with model size, and it also improves when we pass from zero-shot to few-shot evaluation; see Figure 4.
- Replacing an option with ‘none of the above’ reduces accuracy and calibration significantly with our models (see Figure 7). However, our models are also well calibrated on True/False distinctions (see Figure 8), with accuracy and calibration also increasing with model capability.
- We also show that RLHF policies [Bai et al., 2022] naively seem miscalibrated, but with a simple temperature adjustment they become fairly well-calibrated on several evaluations (Figure 9).

Self-Evaluation of Model-Generated Samples, without Finetuning

We evaluate on the generative tasks TriviaQA [Joshi et al., 2017], Lambada [Paperno et al., 2016], GSM8k [Cobbe et al., 2021], the Codex HumanEval [Chen et al., 2021], arithmetic problems, and natural function synthesis problems scraped from GitHub. See Figure 1 for a brief overview of results.

- Models can self-evaluate whether their own samples are True or False, though this tends to be a more challenging task (since models tend to find their own samples more plausible). Self-evaluations are well-calibrated few-shot, though models aren’t as well-calibrated zero-shot. In particular, larger k for k -shot self-evaluation seems to primarily help by improving calibration, rather than by improving the AUROC for separating correct and incorrect responses. See Figures 10 and 11 in the main text for representative results, and Figures 28, 29, and 30 in the appendix for complete results.
- Showing models many of their own $T = 1$ samples, along with a single sample to evaluate as True/False, can significantly improve their performance (this is somewhat reminiscent of self-consistency prompting [Wang et al., 2022]).

We conclude that language models can perform well at this task few-shot, with most measures of performance improving with model size, even though models are being asked to evaluate their own samples.

Finetuning to Identify the *Questions Models Can Correctly Answer*

We are also interested in whether models know, or can be taught, to specifically identify *questions* that they can and cannot answer, rather than simply evaluating whether answers to questions are in fact correct. Figure 2 provides a brief overview of results.

- We train models with a value head to predict the probability that they can answer a question correctly, which we refer to as $P(\text{IK})$. We find that models trained on TriviaQA have significant power to differentiate between math, lambda, and code questions that they can answer; see Figure 12. However, $P(\text{IK})$ tends to be poorly calibrated on these other distributions (see Figure 13). Generalization is perhaps most clearly illustrated in Figures 16 and 17.
- We study generalization of $P(\text{IK})$ to the inclusion of source materials and mathematical hints, see Figures 18 and 19. We find that $P(\text{IK})$ responds appropriately to sources, correct hints, and incorrect or distracting hints.
- We compare two models with roughly equal capability, but different pretraining data, in Figure 20. These models are somewhat better at predicting their own $P(\text{IK})$ rather than that for another model. We also try "crossing" the $P(\text{IK})$ training data for these models, and find a small effect suggesting that models generalize better when trained on what they know, rather than on what the other model knew.

Thus we conclude that we only find partial generalization on this task.

Glossary: Observables and Metrics

- **P(True)** – The probability a model assigns to the proposition that a specific sample is the correct answer to a question.
- **P(IK)** – The probability a model assigns to "I know", i.e. the proposition that it will answer a given question correctly when samples are generated at unit temperature. In this work, $P(\text{IK})$ is usually computed using a binary classification head on top of a language model.
- **Ground Truth P(IK)** – The fraction of unit temperature samples to a question that are correct.
- **Calibration Charts** - We often plot prediction probability vs frequency that a prediction was correct, see Figure 4 as an example. We use all predictions (not just predictions for the correct answer) and put the same number of predictions in each bin (rather than using equally spaced bins).
- **Expected or RMS Calibration Error** - To obtain a single number summarizing calibration, we compute the ECE as the mean of the absolute difference between probabilistic predictions and frequencies. For ECE we always use 10 bins, with an equal number of predictions in each. What we call the ECE has also been called the mean absolute deviation calibration error [Lin et al., 2022]. To more closely match other works, we only use the most likely predictions (for multiple choice) when computing the ECE, instead of using all predictions. We also include the RMS calibration error, which is better motivated theoretically, but seems to be less widely used in the literature.
- **AUROC** - We sometimes share the area under the receiver operating characteristic (AUROC) discriminating between questions models do or do not know the answer to, or discriminating between samples a model does or does not identify as correct. This captures discriminative power but is indifferent to calibration (note chance AUROC is 0.5, and larger scores are better).
- **(Conditional) Accuracy** - When models self-evaluate the probability $P(\text{True})$ that their own samples are valid, we are very interested in the accuracy of the samples that models label as 'True' (i.e. correct), and how this compares to the accuracy on the full distribution of problems in the task.
- **Brier Score** - In some cases we observe tradeoffs between discrimination (e.g. best AUROC) and calibration. Brier scores combine the discriminative power of self-evaluation with calibration (note the chance Brier score on binary choice tasks is 0.25, and smaller scores are better).

1.2 Models and Evaluation Tasks

Our goal in this study is to evaluate calibration and generalization on a diverse range of tasks. As such we include all of the multiple choice evaluations in BIG Bench [Srivastava et al., 2022], the MMLU

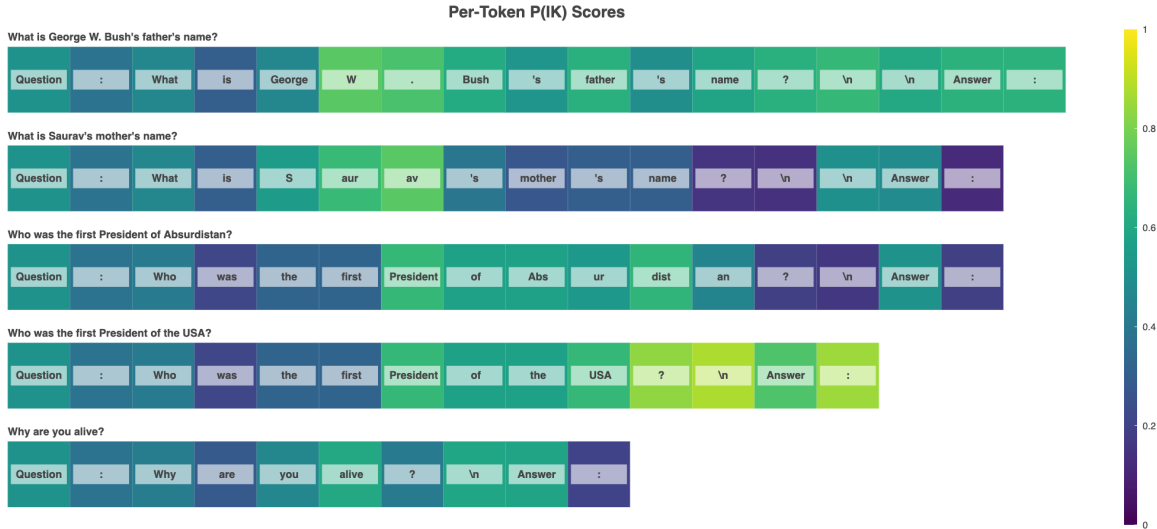


Figure 3 Examples of P(IK) scores from a 52B model. Token sequences that ask harder questions have lower P(IK) scores on the last token. To evaluate P(IK) on a specific full sequence, we simply take the P(IK) score at the last token. Note that we only train P(IK) on final tokens (and not on partial questions).

evaluation [Hendrycks et al., 2021], TruthfulQA [Lin et al., 2021], LogiQA [Liu et al., 2020], and QuALITY [Pang et al., 2021]. We are most interested in open-ended generation, so we study the sampling-based evaluations TriviaQA [Joshi et al., 2017], Lambada [Paperno et al., 2016], the Codex HumanEval [Chen et al., 2021], GSM8k [Cobbe et al., 2021], some basic arithmetic problems, and a dataset of additional web-scraped Python function synthesis problems. See Appendix D for more information on our arithmetic and function synthesis datasets. Ultimately, we would like to train models to express calibrated confidence levels when generating long-form responses in natural language dialogue.

When we perform few-shot evaluation, we simply stuff the context with randomly chosen examples from the (test) evaluation itself. For BIG Bench this means all few-shot examples come from within the specific subtask we are evaluating, though in the case of MMLU we randomize across the entire evaluation, without respecting subject boundaries.

We study a series of language models with 800M, 3B, 12B, 52B parameters. We do not include smaller models because they perform poorly on many of the evaluations we consider. The architecture and training setup for these models is identical to that in [Bai et al., 2022], except that the models we consider here were pretrained for 850B tokens, rather than the 400B tokens used in that work. For simplicity, we do not study models that have been finetuned on python code, though our pretraining distribution includes about 10% code. In section 3.3 we briefly study helpful and harmless RLHF policies finetuned (via the process in [Bai et al., 2022]) from these language models, but otherwise we only study pure language models. We show accuracies for our models on a few of the multiple choice tasks we study in Figure 37 in the appendix.

1.3 Related Work

Calibration for general ML predictions, and interventions to improve calibration, have been studied [Nguyen and O’Connor, 2015, Hendrycks and Gimpel, 2016, Nalisnick et al., 2019, Guo et al., 2017, Minderer et al., 2021, Hendrycks et al., 2018, Ovidia et al., 2019] for some time. Calibration for language model QA has also been studied [Jiang et al., 2021], but typically it has been found that to achieve good calibration predictions must be adjusted. Recently, the calibration of a wide range of models was analyzed on the diverse BIG Bench suite of tasks [Srivastava et al., 2022], where it was shown that language model calibration improves with model size. We are indebted to the BIG Bench collaboration for providing a convenient, huge, and diverse evaluation set. The authors of Gopher [Rae et al., 2021] briefly studied calibration on MMLU [Hendrycks et al., 2021] and found promising results, which led us to experiment with a variety of multiple choice formats.

Truthfulness [Evans et al., 2021] has been a recent focus of various works, including benchmarks [Lin et al., 2021] and the incorporation of web search and citation [Nakano et al., 2021, Menick et al., 2022]

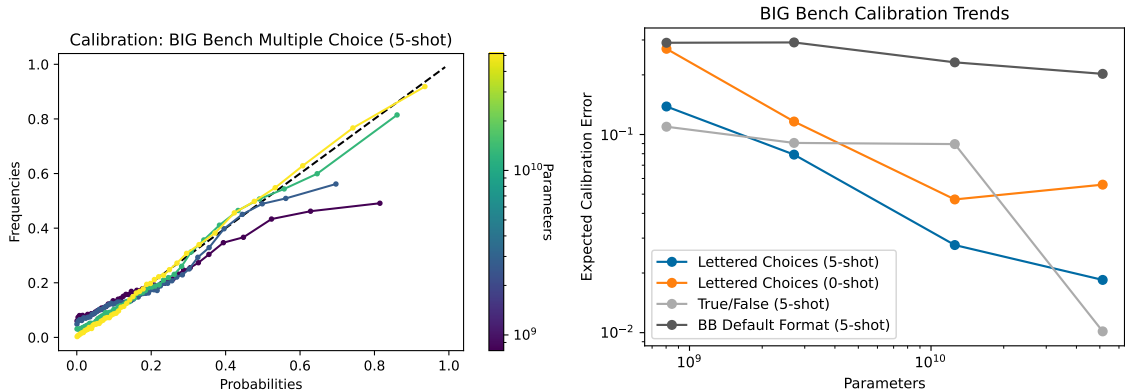


Figure 4 (left) We show calibration curves for various model sizes on all of the multiple choice tasks in BIG Bench, in the format described in section 2. We include a dashed line indicating perfect calibration. **(right)** Here we show trends in the expected calibration error on BIG Bench, for both multiple choice and a separate True/False format (see Section 3.2). We show the RMS calibration error in Figure 21 in the appendix.

into language models. That said, truthfulness focuses primarily on factual accuracy "in the world", rather than on self-knowledge, or eliciting latent knowledge [Christiano et al., 2021]. We use "honesty" [Askell et al., 2021] as an umbrella term for ideas including truthfulness, calibration, self-knowledge, explainability, and non-deceptiveness.

Perhaps the work most similar to ours is [Mielke et al., 2020], which is a very interesting application of metacognition/self-evaluation to improve natural language calibration. Another quite similar work is the very recent [Lin et al., 2022], where the authors train language models to express their calibration on arithmetic in words, and also study a signal analogous to $P(\text{True})$.

2 Larger Models are Calibrated on Diverse Multiple Choice Questions

A model makes calibrated predictions if the probability it assigns to outcomes coincides with the frequency with which these outcomes actually occur. Language models are known to produce calibrated token-level probabilities. In this section we will see that language models can produce well-calibrated probabilities when they are asked to choose the correct answer from among several explicit options. We believe calibration is interesting on its own, but it is especially relevant to honesty, since a model that can produce calibrated answers to meta-questions like 'do you know the answer to X?' must know something about what it knows. Generally we can use calibration as a way to bootstrap towards self-knowledge.

We find that when multiple choice problems are formatted in this way (as used by e.g. [Rae et al., 2021]):

```
Question: Who was the first president of the United States?
Choices:
(A) Barack Obama
(B) George Washington
(C) Michael Jackson
Answer:
```

and we identify the answers only by their labels, as e.g. '(B)', our largest models tend to produce a well-calibrated probability distribution among the available options. We show the calibration chart for all multiple choice BIG Bench tasks, in this format, in Figure 4. As can be seen in Figure 6, models are well-calibrated (in this format) even for somewhat adversarial datasets like TruthfulQA³ [Lin et al., 2021], as well as for QuALITY [Pang et al., 2021] and LogiQA [Liu et al., 2020].

It is crucial that the model gets to see the answer choices explicitly before choosing amongst them; without this, we would not expect a calibrated response, due to ambiguities and degeneracies among possible paraphrases and specializations of any given answer option (e.g. "Washington" vs "George Washington, the first

³Though note that in this format, where the model sees its options before making a choice, we do not observe anti-scaling with model size.

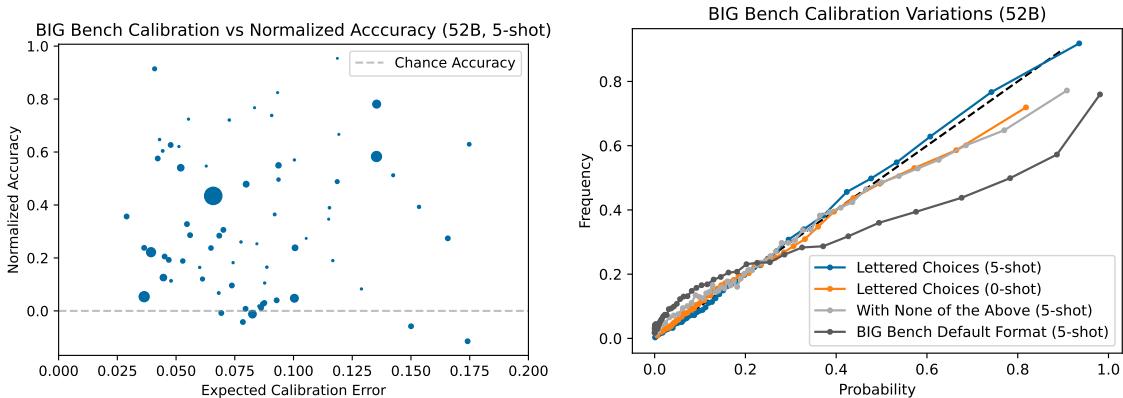


Figure 5 (left) We show expected calibration error versus normalized accuracy for all BIG Bench tasks; the number of problems in each task is represented by the marker sizes. We do not find any noticeable correlation between accuracy and calibration within BIG Bench. To normalize accuracies we linearly map chance accuracy to 0, keeping perfect accuracy at 1. (right) We compare calibration for several variations on BIG Bench evaluations: we vary between 0-shot and 5-shot, replace an answer option with "none of the above", and compare our format with letter-labeled choices to the default BIG Bench formatting.

US president"). As can be seen in figure 5, task formatting is important for achieving excellent calibration, and calibration improves as we pass from 0-shot to 5-shot evaluation. We expect calibration is also easier to achieve with this format because each answer option corresponds to a single token (this isn't the case in BIG Bench by default, see appendix A.4).

To simplify the interpretation of results, we reduce calibration curves to a single number by computing the expected calibration error (ECE), after binning the predictions in 10 equally-represented bins. On the right of Figure 4 we show scaling trends for calibration on BIG Bench. We typically find good calibration 0-shot, without any other prompt, though calibration improves as we pass from 0-shot to few-shot. We find that in almost all cases, calibration improves with model size and capability. Accuracy on the tasks also improves with model size, but as can be seen in Figure 5, we do not observe any obvious causal connection between accuracy and calibration. For details on how we obtain calibration charts and ECE see Appendix A.

In what follows we will work to leverage these calibration results to ask language models to evaluate what they do and do not know.

3 From Calibration to Knowing What You Know

If language models can answer multiple choice questions in a calibrated way, then one might hope that they can apply this ability to evaluate their own outputs. That is, we can simply ask models to generate potential answers to questions, and then have the model evaluate whether any of them are correct. In this section we will begin to explore this idea by reformulating existing tasks. Then in section 4 we will study self-evaluation.

3.1 Replacing an Option with ‘None of the Above’ Harms Performance and Calibration

We have seen that language models can produce calibrated probabilities for multiple choice questions, at least when the questions and choices are provided in the right format. However, to achieve this feat the model only needs to determine the relative weight for several concrete options, when they are compared to each other.

We are more interested in whether the model actually knows whether each of the answer options is correct, when judged independently. To probe this question, we modified our multiple choice evaluations by replacing their final option with “none of the above”. This procedure can make questions that do not actually have a unique correct answer ambiguous or impossible, but for many tasks it should result in a well-defined new evaluation. In particular this procedure appears to be sensible for the vast majority of questions in MMLU. Concretely this means that we took questions such as the example in section 2 and replaced them with:

Question: Who was the first president of the United States?
 Choices:
 (A) Barack Obama

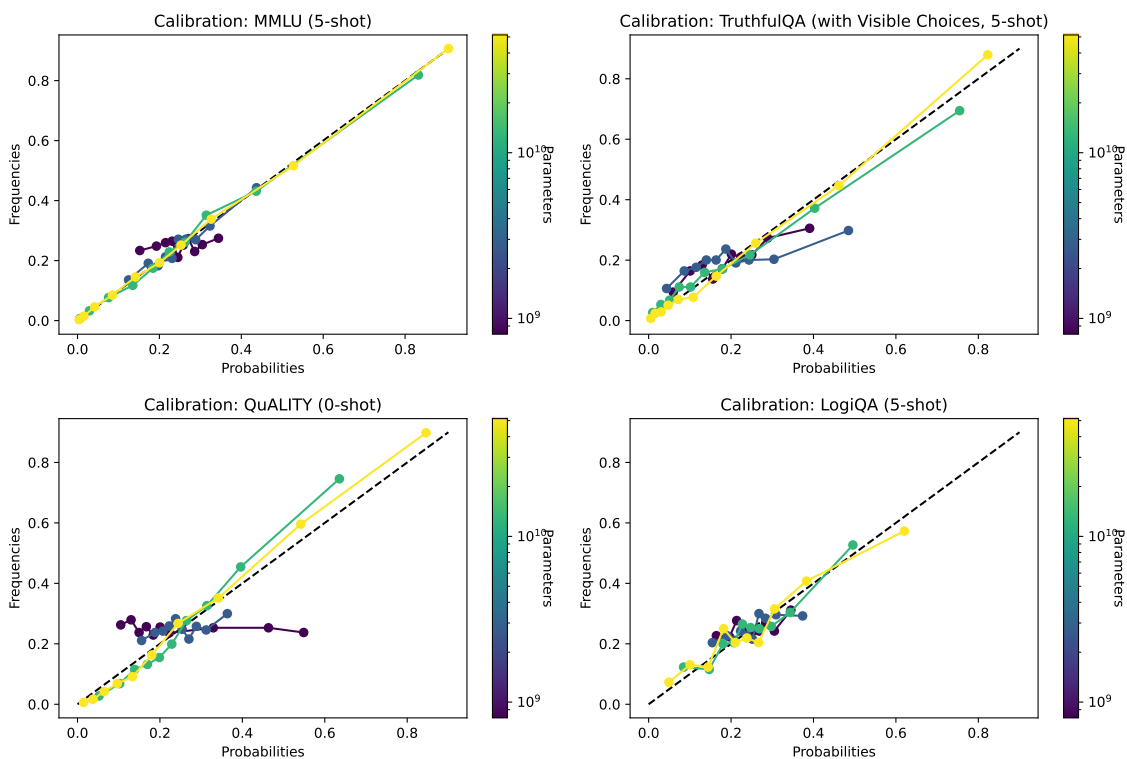


Figure 6 We show calibration curves for various model sizes on MMLU, TruthfulQA, QuALITY, and LogiQA in the format described in section 2. We emphasize that even on tasks that are difficult for LMs, like LogiQA, and on a somewhat adversarial evaluation like TruthfulQA, large models can achieve good calibration when the available answer options are presented to them in a favorable format. We include a dashed line indicating perfect calibration.

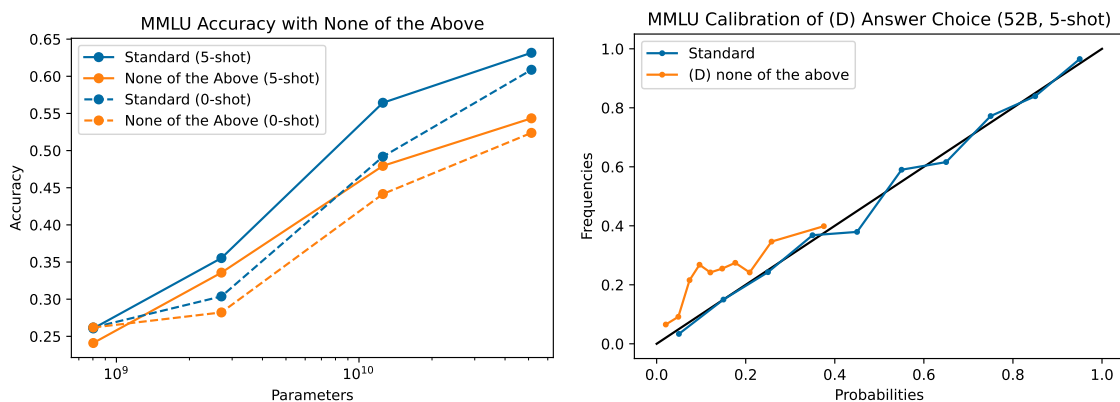


Figure 7 (left) We show accuracy on MMLU in the standard format, and after replacing option (D) with "none of the above". This replacement decreases accuracy very significantly. **(right)** We show calibration specifically for the (D) answer option, in the standard form of MMLU and with (D) as "none of the above". The latter makes calibration much worse, and in particular the model seems strongly biased against using this option, which also harms accuracy.

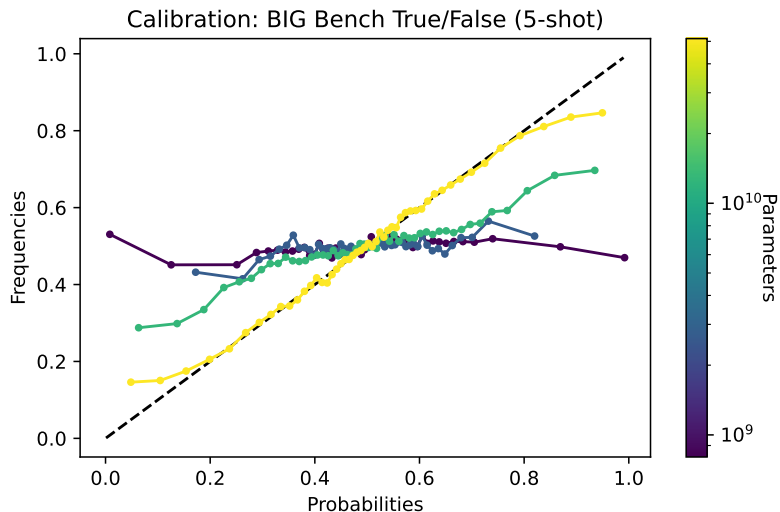


Figure 8 We show calibration curves for various model sizes on all of the multiple choice tasks in BIG Bench, reformulated as True/False questions on a mix of the correct answers, and randomly chosen incorrect answer options. The 52B model is very well-calibrated except near the tails, where it is overconfident.

```
(B) George Washington
(C) none of the above
Answer:
```

We found that this procedure degraded performance very significantly on evaluations; results for MMLU are shown in Figure 36 in the appendix. Furthermore, adding "none of the above" also harms calibration, as can be seen in Figures 5 and 7. It seems that even the 52B model is biased against using the "none of the above" option and failed to use it with appropriate frequency. This is particularly surprising for 5-shot evaluations; we also tried evaluating 20-shot and this also did not improve performance.

3.2 Models are Well-Calibrated on True/False Tasks

We saw in section 3.1 that language models seem to be confused by a "none of the above" option. Here we take a different approach, and simply ask models if a given answer is true or false. So we use the format:

```
Question: Who was the first president of the United States?
Proposed Answer: George Washington
Is the proposed answer:
(A) True
(B) False
The proposed answer is:
```

where we expect either '(A)' or '(B)' as an answer. If the model responses are correct at more than chance level, and especially if they are calibrated, then the probability $P(\text{True})$ indicates whether the model believes a response is valid.

As a first test of this approach, we can use answer options from existing multiple choice tasks. For this purpose, we take the correct answer and a randomly chosen incorrect answer, and create a new evaluation set with twice as many problems in the format above, asking models to determine if each answer is correct. In Figure 8 we show the calibration results from this method on BIG Bench. We see that the 52B model is quite well-calibrated in this context. We show similar results for MMLU in Figure 36 in the appendix, and scaling trends comparing a variety of evaluation methods in Figure 7.

3.3 RLHF Policy Miscalibration Can Be Remediated with a Temperature Tuning

Our focus in this paper is on pure language models, but as a quick experiment we also looked at calibration for a helpful and harmless RLHF policy, trained exactly as in [Bai et al., 2022] using the base language models

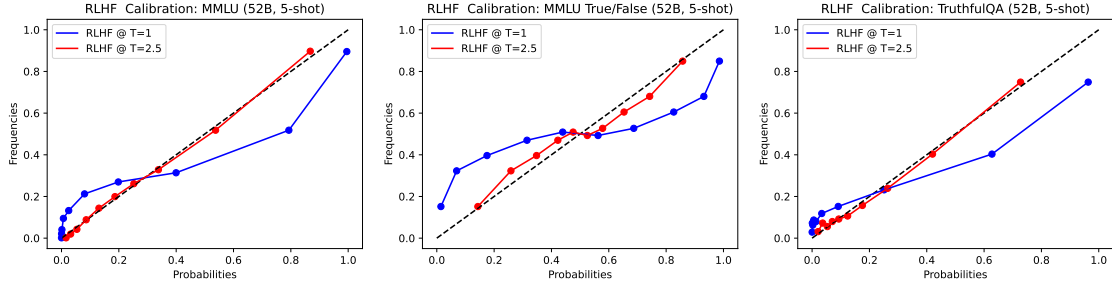


Figure 9 We show calibration curves for RLHF policies finetuned from our language models. Calibration of these models appears to be very poor, but simply adjusting the temperature of their probability distributions to $T = 2.5$ largely fixes calibration issues for three different evaluations.

we are studying here. We find that these policies naively appear very miscalibrated, which is not surprising, since RL finetuning tends to collapse language model predictions towards behaviors that receive the most reward. However, a simple temperature adjustment (with the same temperature $T = 2.5$ for all evaluations) largely fixes calibration issues with several independent evaluation tasks, with results shown in Figure 9. This also matches what was found for gender bias evaluations in [Bai et al., 2022], where RLHF policies had a bias score very similar to a basic language model evaluated at lower temperature. Of course more intensive RL training might distort calibration in ways that cannot be remedied in this way, but this at least provides hope that good calibration can survive some forms of finetuning.

4 Ask the AI: Is your proposed answer True or False?

We will now apply the True/False approach from section 3.2 to the samples models generated when trying to answer questions, including the short answer tasks arithmetic, Lambada, and TriviaQA, and the long-form answer tasks Codex HumanEval and GSM8k (technically GSM8k calls for a short answer, but we will be evaluating full written solution attempts, which have been solicited via chain-of-thought/scratchpad [Nye et al., 2021, Wei et al., 2022] prompting). We show the accuracies when sampling at a temperature of one in Figure 1.

In almost all cases self-evaluation performance improves with model size, and for our 52B models answers labeled with $P(\text{True}) > 50\%$ are far more likely to be correct as compared to generic responses (see the summary histogram and comparisons in Figure 1). We also find that showing the model many $T = 1$ samples for a single question significantly improves its ability to evaluate whether any given sample is correct. This is somewhat reminiscent of self-consistency [Wang et al., 2022], though here we are showing models their own samples, rather than externally judging self-consistency ourselves. One way to summarize these results is via the Brier scores for self-evaluation, which are shown in Figure 11.

We provide complete results in appendix C; since there are quite a few figures we only show representative examples from Lambada and Codex in the main text.

4.1 Basic Self-Evaluation

In section 3.2 we saw that large language models are well-calibrated on True/False questions. Our primary motivation for studying this issue was to ask language models about their own outputs. That is, we are interested in a process where we first ask a question like:

Question: Who was the first president of the United States?
 Answer:

and sample a response from the model. Then we ask the model about its own sample:

Question: Who was the first president of the United States?
 Proposed Answer: George Washington was the first president.
 Is the proposed answer:
 (A) True
 (B) False
 The proposed answer is:



Figure 10 Models self-evaluate their own samples by producing a probability $P(\text{True})$ that the samples are in fact correct. Here we show histograms of $P(\text{True})$ for the correct and incorrect samples, in the evaluation paradigm where models also see five $T = 1$ samples for the same question, in order to improve their judgment. Here we show results only for Lambda and Codex, as these are fairly representative of short-answer and long-answer behavior; for full results see Figure 28 in the appendix.

and evaluate the probabilities it assigns to the ‘(A)’ and ‘(B)’ options. We apply this approach to model generated answers from TriviaQA [Joshi et al., 2017], Lambda [Paperno et al., 2016], the Codex HumanEval [Chen et al., 2021], GSM8k [Cobbe et al., 2021], and basic arithmetic problems.

This True/False self-evaluation may be considerably more difficult than the tasks we studied in section 3.2, because there the model was presented with human-written possibilities, whereas here the model is forced to evaluate⁴ its own samples. These samples may lie close to the model’s own decision boundary for validity (or the model may simply be overconfident about its own samples), whereas options presented to the model by a third party may be easier to categorize. We observe this effect in several ways. Zero-shot, $P(\text{True})$ is poorly calibrated, and typically it lies close to 50% for typical samples (see Figure 38 in the appendix for illustrations). Furthermore, we show in Figure 33 in the appendix that samples from smaller models are universally easier to categorize as correct or incorrect, for models of all sizes.

4.2 Showing Many $T = 1$ Samples Improves Self-Evaluation

We can improve performance further by showing the model other $T = 1$ samples, for comparison. That is, we generate 5 samples in total, and then ask the model about the validity of one of these samples:

```
Question: Who was the third president of the United States?
Here are some brainstormed ideas: James Monroe
Thomas Jefferson
John Adams
Thomas Jefferson
George Washington
Possible Answer: James Monroe
Is the possible answer:
(A) True
(B) False
The possible answer is:
```

With this format, performance improves significantly on all of the short-form answer tasks, as compared to the version where we only show models a single proposed answer, as summarized in Figure 11. However, models benefit less from this approach on tasks requiring long-form answers (Codex and GSM8k). As noted in the last section, calibration of $P(\text{True})$ is relatively poor zero-shot, but it improves few-shot. In Figure 32 in the appendix we show the full calibration curves for 20-shot True/False self-evaluation.

A pragmatic comparison of self-evaluation techniques can be seen on the bottom of Figure 11. There we directly compare the overall accuracy of our models at the task, to the accuracies for the subset of responses

⁴Language models do not typically have an explicit way of knowing if tokens were provided to them by a third party, or are their own samples. This may make self-evaluation more difficult (or at least ambiguous), and can have other issues in an RL setting [Ortega et al., 2021].

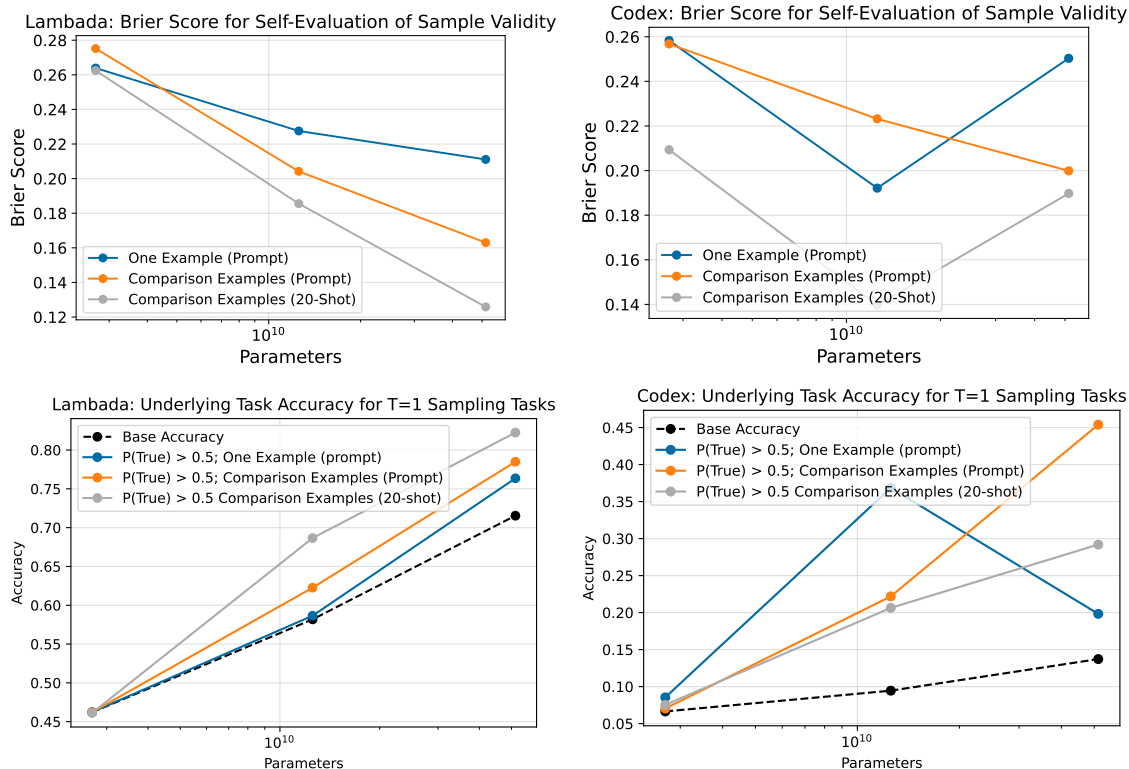


Figure 11 Here we show results only for Lambda and Codex, as these are fairly representative of short-answer and long-answer behavior; for full results see Figures 28, 29, 30, and 31 in the appendix. **Top:** Here we show the Brier scores for model self-evaluation with three methods: basic self-evaluation with a prompt, and self-evaluation with comparison samples, either with a fixed prompt or 20-shot. Note that the Brier score combines accuracy of the True/False determination with calibration, and 20-shot evaluation with comparison samples performs best in every case. Brier scores do not decrease with model size on evaluations like Codex because small model samples are almost always invalid, so that it’s relatively trivial to achieve a small Brier score. **Bottom:** We show the base accuracy of our models on various sampling tasks, and then the accuracy among the responses where via self-evaluation we have $P(\text{True}) > 0.5$. For $P(\text{True})$ we evaluate with a single example and a prompt, and then both 20-shot and with a prompt with five comparison examples. Few-shot evaluation is important for obtaining good calibration.

where the models chose $P(\text{True}) > 0.5$. We see that these conditional accuracies are substantially higher than the overall accuracy, with the separation between base and conditional accuracies growing with model size. This suggests that as capabilities improve and samples become more sophisticated, models seem to demonstrate *relative* improvement at self-evaluation, compared to their generative ability. This accords with the intuitive sense that verification is often easier than generation.

Overall, if given a few examples from a given distribution, models can generate samples and then self-evaluate them to productively differentiate correct and incorrect samples, with reasonably calibrated confidence.

5 Training Models to Predict Whether They Can Answer Questions Correctly

In this section, we will train models to predict whether they know the answer to any given free-form question, denoting the probability they assign as ‘P(IK)’ (for Probability that I Know the answer). This is fundamentally a question about the model itself, as different models will know the answers to different questions.

We considered two approaches:

- **Value Head:** We train $P(\text{IK})$ as the logit from an additional value ‘head’ added to the model (independent of the logits for language modeling). An advantage of this approach is that we can easily probe $P(\text{IK})$ at general token positions.
- **Natural Language:** We train $P(\text{IK})$ by asking the model to literally address "With what confidence could you answer this question?", and output an answer like 0%, 10%, 20%, ... 100%.

We had hoped to observe large benefits from few-shot evaluation out-of-distribution with the natural language approach. In early experiments we did not observe major gains, and so we will use the value head approach in what follows. But we believe it would be worth returning to the natural language approach in the future.

For each question, we generated 30 answer samples at $T = 1$. For a given question Q , if 20 of the model’s sampled answers were correct, and 10 were incorrect, our training set contained 20 copies of the (Q, IK) datapoint and 10 copies of the (Q, IDK) datapoint. This was a convenience to allow us to easily approximate⁵ a soft label for the ground-truth $P(\text{IK})$ by using many hard labels. We trained with a cross-entropy loss on these labels.

Figure 3 gives some examples of $P(\text{IK})$ scores from a 52 billion parameter model on a few example questions where the model obviously should or should not know the answers. Note that the value head is technically present at every token position. However, during training, we only backpropagate the loss through the head at the last token position of the input sequence. At test time, we also read off the $P(\text{IK})$ score for any given sequence as the output from our head at the final token position.

5.1 Evaluating $P(\text{IK})$ Training and Model Size Trends

Because we’re adding a new untrained head, language models do not perform well zero or few-shot at predicting $P(\text{IK})$, so we need to finetune them. Since TriviaQA has a large training set, we explore generalization by finetuning $P(\text{IK})$ only on trivia questions. In order to obtain ground-truth $P(\text{IK})$ scores that we use for training, we sample 30 answers (at temperature = 1) from each TriviaQA question with a 10-shot prompt constructed from other random TriviaQA questions and answers. We use a 10-shot prompt simply to ensure that the models almost always output answers in the correct format, which is important because correctness on TriviaQA questions is judged based on a string comparison.

Our dataset for training and evaluating the classifier then contains datapoints of the form (Few-Shot Prompt + Question, Ground Truth Label). During $P(\text{IK})$ training, we finetune the entire model along with the value head. In Figure 12, we then evaluate this classifier on a held-out set of TriviaQA test questions, and see that the model is able to separate the questions it got correct and incorrect quite well. In particular, $P(\text{IK})$ is very well calibrated on TriviaQA. As a note, in a later section we train $P(\text{IK})$ on Lambada, Arithmetic, and Python Function Synthesis problems as well. We used a 10-shot prompt for both Lambada and Arithmetic, while Python Function Synthesis was done 0-shot.

5.2 Out of Distribution Generalization of $P(\text{IK})$

Next, we study the generalization of $P(\text{IK})$ when training only on TriviaQA and then evaluating on Lambada, Arithmetic, GSM8k, Codex HumanEval, and a set of ‘naturally occurring’ python function synthesis tasks scraped from GitHub (we added this test set because the Codex evaluation is not very large). We are interested in how generalization scales across model sizes, and how performance compares to the case where we do train $P(\text{IK})$ on these distributions.

We treat GSM8k slightly differently, since it was harder than other tasks. As for TriviaQA, we generated 30 samples @ $T = 1$ per question from GSM8k using a 10-shot prompt of examples to ensure proper formatting. However, the 10-shot prompt for GSM8k included reasoning, as well as the final answer. This meant that each of the 30 samples included model-generated reasoning. Similarly to other tasks, we calculate a ground-truth $P(\text{IK})$ for each question as just the fraction of $T = 1$ samples that are correct. However, since there aren’t many problems with a ground truth $P(\text{IK}) > 0.5$, we sometimes binarize (i.e. split the distribution) using a threshold of 0.25, instead of 0.5. We only evaluate the largest model (52B) on GSM8k due to its difficulty.

Figure 14 gives an overview of generalization performance for $P(\text{IK})$ classifiers that are only trained on TriviaQA. Specifically, we see that generalization gets better as model size increases. Figures 39, 40, and

⁵In some cases $P(\text{IK})$ could be somewhat misleading – for instance, Owain Evans pointed out the nice example "Name a composite integer in the range [1,100]?" where by chance the model may achieve an apparent $P(\text{IK}) = 0.75$ simply by randomly sampling integers in [1,100].

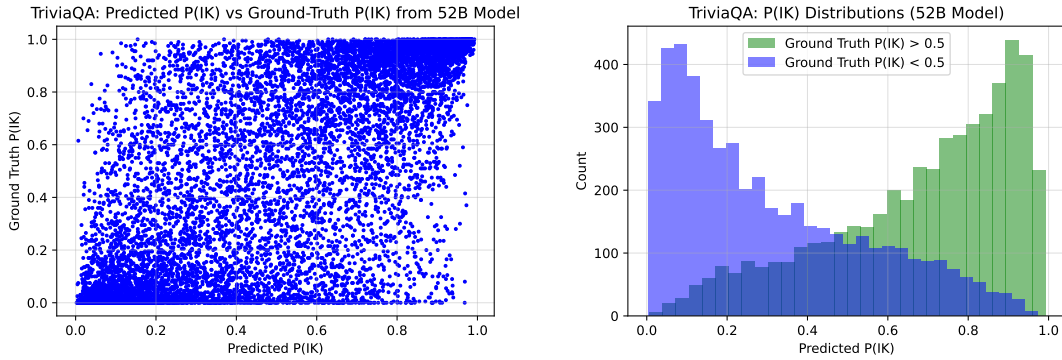


Figure 12 Testing a 52B classifier on a held-out set of TriviaQA questions. We see that the classifier predicts lower values of $P(\text{IK})$ for the questions it gets incorrect, and higher values of $P(\text{IK})$ for the questions it gets correct. We set the ground truth $P(\text{IK})$ as the fraction of samples at $T = 1$ that the model gets correct.

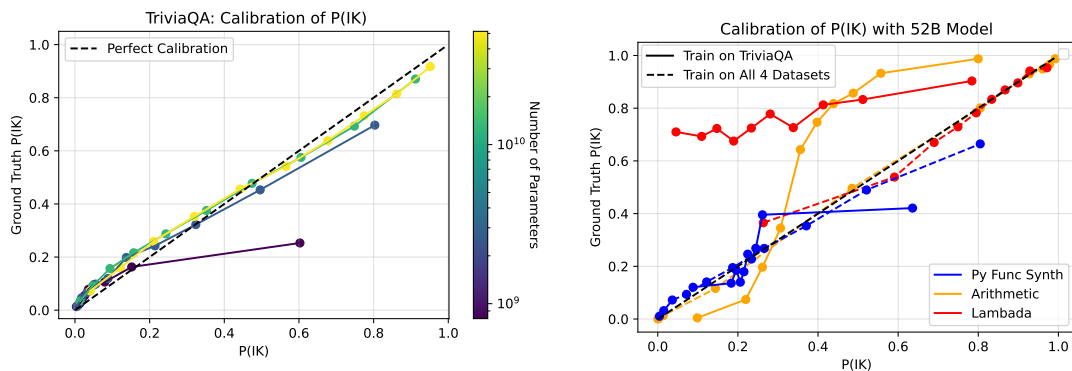


Figure 13 Left: Full calibration plot of $P(\text{IK})$ classifiers on TriviaQA over a range of model sizes. We see that the smallest models have higher calibration error than the biggest models. The larger classifiers are very well calibrated in-distribution. Right: We show calibration curves for $P(\text{IK})$ on three other sampling-based datasets, both in-distribution and out-of-distribution (trained only on TriviaQA). We see that OOD calibration of $P(\text{IK})$ is often quite poor, and for the most part models are underconfident.

41 show details of generalization to Mixed-Arithmetic, Python Function Synthesis, and Lambada. We see that there is a general trend where the AUROC of $P(\text{IK})$ increases with model size, and calibration gets better with model size. However, when testing on Lambada, calibration was terrible, because the model produces uniformly low $P(\text{IK})$ scores. However, training on all 4 tasks resolves this issue, as shown on the right side of Figure 41.

Table 1 gives an overview comparing generalization to in-distribution performance of $P(\text{IK})$ scores. Figure 16 gives a more detailed view of how the distributions of $P(\text{IK})$ changes depending on training data on the 52B model. We see that training on specific $P(\text{IK})$ distributions helps performance, indicating that there is a significant generalization gap to fill.

5.3 $P(\text{IK})$ Generalizes to Account for Source Materials

If we consider a fairly obscure question like

What state’s rodeo hall of fame was established in 2013?

then $P(\text{IK})$ appropriately predicts a low value, specifically 18% for a 52B model. However, if we prepend a Wikipedia article on the Idaho Rodeo Hall of Fame to the context:

⁶See section XYZ for details on the setup for GSM8k. In this table, we binarized the ground-truth $P(\text{IK})$ with a threshold of 0.5, like all other evals. Also, note that the Brier score for GSM8k tasks are somewhat misleading, since it is overwhelmingly dominated by questions the model gets incorrect and has low $P(\text{IK})$ for.

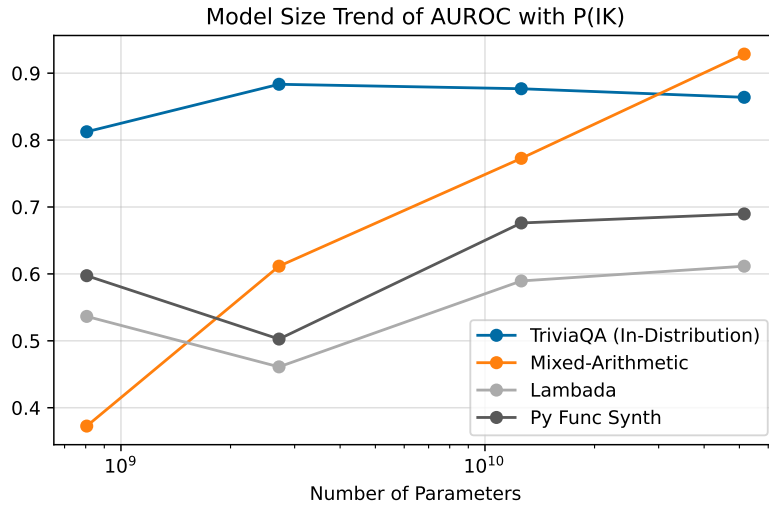


Figure 14 Model size trend of AUROC with P(IK), when training on only TriviaQA. We generally observe increasing AUROC as model size increases for all three out-of-distribution evals, suggesting that larger P(IK) classifiers are better at generalization.

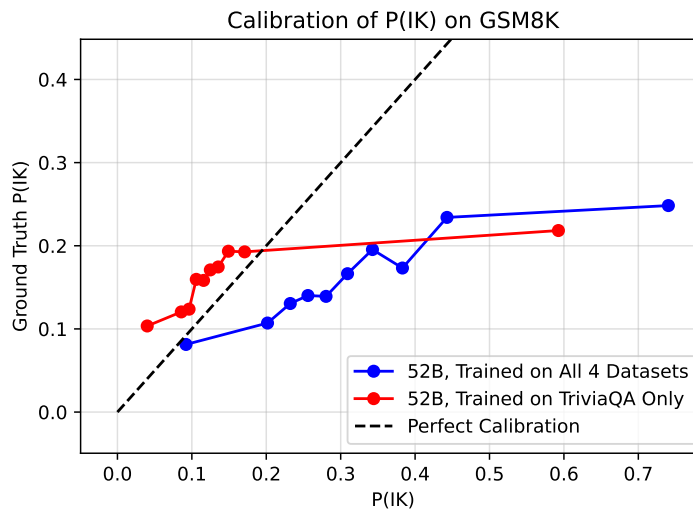


Figure 15 Calibration on GSM8k when training on only TriviaQA vs training on TriviaQA, LAMBADA, Mixed-Arithmetic, and Python Function Synthesis. We see that calibration does improve when training on more diverse data, rather instead of being mostly underconfident the model becomes overconfident. Note that GSM8k was significantly out of the training distribution in all cases.

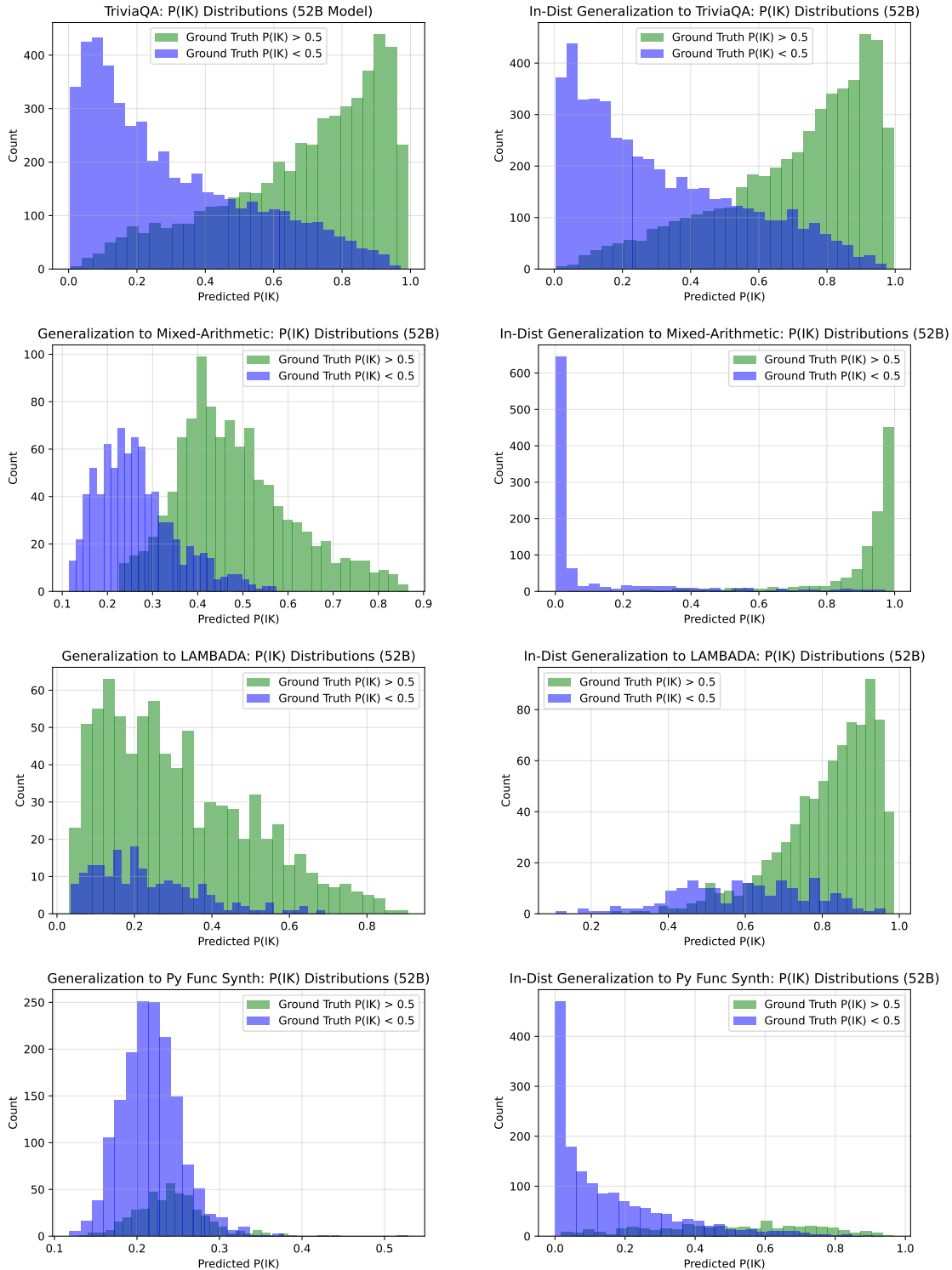


Figure 16 Generalization of $P(IK)$. We trained $P(IK)$ classifiers on just TriviaQA and on TriviaQA, Arithmetic, Python Function Synthesis, and LAMBADA. The left side of this figure includes distributions of $P(IK)$ from a 52B classifier that was trained on just TriviaQA, while the right side includes distributions of $P(IK)$ from a 52B classifier that was trained on all of these data distributions. We observe nontrivial generalization from TriviaQA to the other tasks, but training on the other tasks improves performance greatly.

	Training on TriviaQA (AUROC / Brier Score)	Training on All Tasks Except GSM8K (AUROC / Brier Score)
TriviaQA	0.864 / 0.151	0.873 / 0.145
Mixed-Arithmetic	0.928 / 0.194	0.987 / 0.042
LAMBADA	0.606 / 0.431	0.853 / 0.108
Python Func Synth.	0.687 / 0.164	0.881 / 0.109
GSM8K ⁶	0.624 / 0.200	0.752 / 0.121

Table 1 AUROC and Brier Scores of P(IK) on a variety of tasks, comparing training on just TriviaQA and training on everything. All values are computed using 52B parameter classifiers. All AUROC scores here are computed by comparing the model’s predicted P(IK) against the binarized label: ‘IK’ if the ground truth $P(IK) > 0.5$, and ‘IDK’ otherwise. Even when we only train on TriviaQA, we see decent generalization to other tasks. However, training on everything does help across all tasks. *Need to also add RMSCE to this table.*

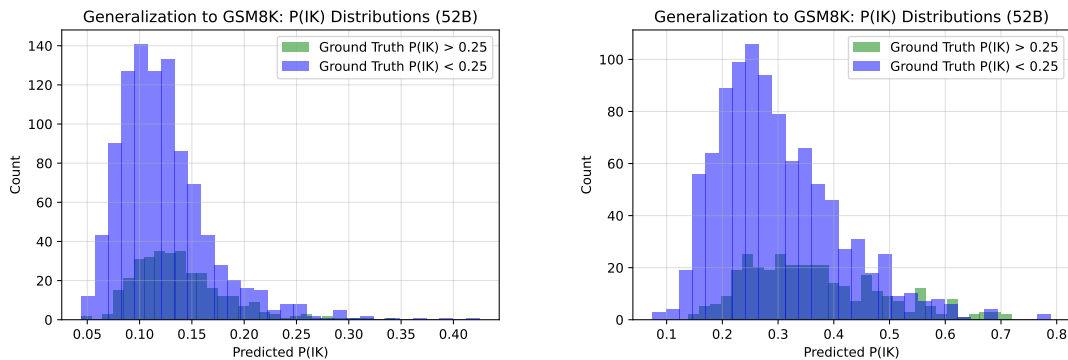


Figure 17 Left: P(IK) scores on GSM8k when training on only TriviaQA. Right: P(IK) scores on GSM8k when training on TriviaQA, LAMBADA, Mixed-Arithmetic, and Python Function Synthesis. Note the threshold for Ground Truth P(IK) is 0.25 here, in contrast to 0.5 in the other histograms from Figure 16 and Table 1

Wikipedia: The Idaho Rodeo Hall of Fame was established as a 501 (c) (3) non-profit organization on May 6, 2013. Lonnie and Charmy LeaVell are the founders of the organization. The actual charitable nonprofit status was received from the IRS on February 19, 2014. The IRHF hosts a reunion and induction ceremony annually every October. The Idaho Hall of Fame preserves and promotes the Western lifestyle and its heritage. The hall exists to dedicate the men and women in rodeo who contribute to ranching and farming through their sport. It also extends its reach to continue these western ways to the youth in the communities to ensure that these traditions continue for many generations. In 2015, the hall was awarded the Historic Preservation Recognition Award by National Society of the Daughters of the American Revolution.

What state’s rodeo hall of fame was established in 2013?

then the P(IK) score rises to 78%. In other words, without any further training, P(IK) generalizes to address whether the language model can find answers to questions in source materials within its context.

We demonstrate this phenomenon quantitatively using questions from TriviaQA, by comparing P(IK) evaluated both with and without accompanying reference material. Questions from TriviaQA come with Wikipedia documents that are relevant to each questions. For each question, we then compute P(IK) both with an without the reference document. Specifically, the format for the prompts are as follows:

With Background Material:

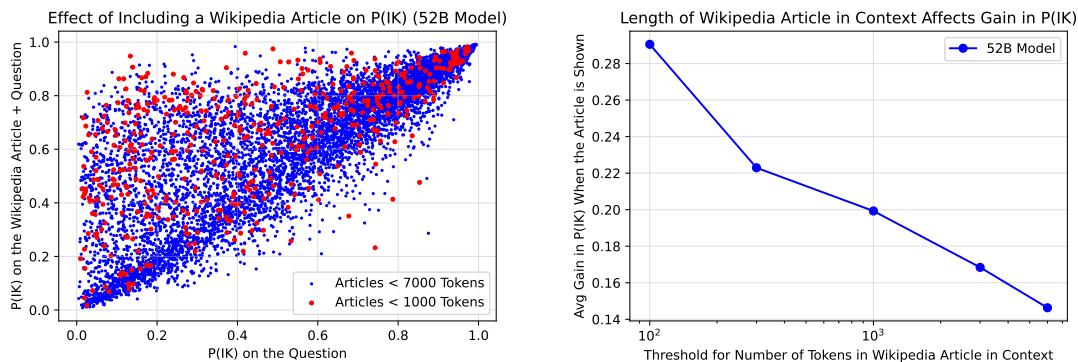


Figure 18 Effect of including Wikipedia article on P(IK) for TriviaQA Questions. We see that including a relevant Wikipedia article in the context boosts the average P(IK) on TriviaQA Questions. P(IK) increases more for shorter Wikipedia articles, from which it is presumably easier to identify the relevant facts.

Here is some background information material: <BACKGROUND_MATERIAL>
Now, answer the following question.

Question: Which Lloyd Webber musical premiered in the US on 10th
December 1993?

Answer:

Without Background Material:

Question: Which Lloyd Webber musical premiered in the US on 10th
December 1993?

Answer:

Whenever the full article was excessively long, we needed to truncate it to 7000 tokens so that the article and the question would always fit in the model context. Figure 18 summarizes the effects of including Wikipedia articles on P(IK). We see that including the article increases P(IK). Furthermore, shorter articles increase P(IK) more. Presumably this is because the correct answer is easier to extract from shorter articles than longer articles.

5.4 P(IK) Generalizes to Account for Hints Towards GSM8k Solutions

In this section we study how hints towards the solution of GSM8k problems affect P(IK) scores. Specifically, we add hints to the problem statement using the following format:

Question: Students in class 3B are collecting school points for behavior . If they get enough points in total, they can go on a trip. In the class, there are Adam, Martha, Betty, and Tom. Adam has collected 50 points. Betty was better than Adam and collected 30% more. Marta managed to collect 3 times more points than Tom, who has 30 points less than Betty. How many points is the class missing to go on the trip if the minimum threshold is 400 points?

Here is a hint: Betty has 30% more points than Adam, so it's $30/100 * 50 = \ll 30/100 * 50 = 15 \gg 15$ points more.

Betty's total is therefore $50 + 15 = \ll 50 + 15 = 65 \gg 65$ points.

Tom has 30 points less than Betty, so he has $65 - 30 = \ll 65 - 30 = 35 \gg 35$ points.

Marta has 3 times more points than Tom, so she has $3 * 35 = \ll 3 * 35 = 105 \gg 105$ points.

In total, all students collected $50 + 65 + 35 + 105 = \ll 50 + 65 + 35 + 105 = 255 \gg 255$ points.

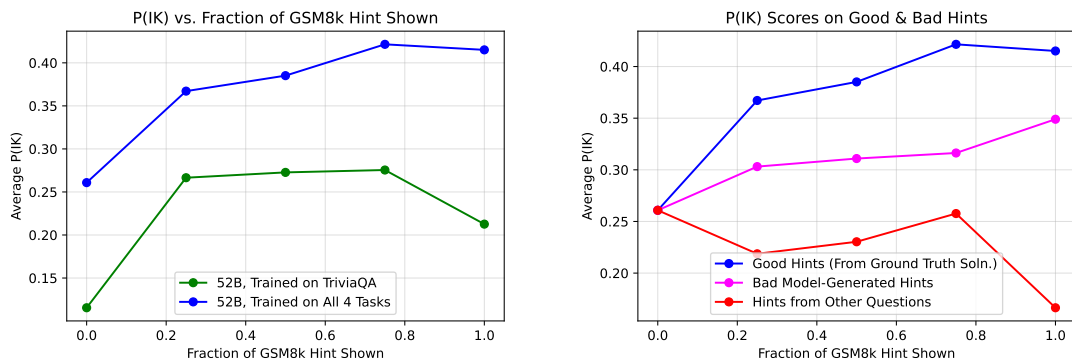


Figure 19 Effect of hints on P(IK) applied to GSM8k – all of these results represent generalization, as the models were not trained on GSM8k. Left: We see that showing more of the GSM8k hint results in higher P(IK). The effect is more consistent for the model trained on all 4 tasks (TriviaQA, LAMBADA, Arithmetic, and Python Function Synthesis), rather than the one trained on just TriviaQA. Right: We evaluate the model trained on all 4 other tasks on various hints. We see lower P(IK) scores for bad hints (though the models are partially fooled), and actual decreases in the P(IK) score when the hints are irrelevant because they come from other questions.

So the class is missing $400 - 255 = \ll 400-255=145 \gg 145$ points to go on the trip.

Answer:

We test two variations on hints. First, we vary the amount of information given away by the hint by truncating hints at fixed fractions of their total length. Second, we compare how P(IK) is affected by good, incorrect, and distracting hints. Bad hints are acquired by generating chain-of-thought samples from our 52B model and selecting only the samples that lead to an incorrect answer. Distracting hints are simply hints that were generated for a different question, so that they are irrelevant to the question at hand.

Figure 19 shows the result of evaluating GSM8k problems with hints using our 52B P(IK) model. We see that (1) showing more of the hint generally leads to higher P(IK), (2) good hints that lead to the correct answer result in higher P(IK) scores than bad hints, and (3) the P(IK) model that was trained on TriviaQA, LAMBADA, Arithmetic, and Python Function Synthesis performs better and more consistently, especially with partial hints.

5.5 Comparing Models Trained with Distinct Pretraining Distributions

We would like P(IK) to truly capture model self-knowledge. Thus we would like to distinguish between this and an alternative hypothesis, that P(IK) is merely capturing something like the intrinsic difficulty of tasks. In order to try to disentangle these explanations, we studied two 12B models (with identical architecture) that were pretrained on distinct data distributions – one was trained with four repetitions of a high quality dataset, while the other uses a single copy of that dataset mixed with a single copy of a larger but lower-quality distribution of webdata. We refer to these pretrained language models as *A* and *B* in this section. We finetuned both models for P(IK) on the questions from the TriviaQA training set that each model got correct.

These models get many of the same questions correct and incorrect. So our focus here will be on *the subset of questions that one model answers correctly and the other incorrectly*. In the TriviaQA test set there were 650 and 826 such questions, respectively, that model A or B got correct but that the other got wrong. Table 2 shows that each model has a noticeably higher P(IK) for the questions that they get correct, compared to the questions that the other model gets right. In Figure 20 we show a scatter plot of P(IK) for models A and B, colored by which model got the questions right. The differences between the distributions are small but noticeable.

We also tried a second experiment, in order to try to get insight as to whether P(IK) leverages features specifically relevant to self-knowledge. For this purpose we finetuned *both* the *A* and *B* pretrained models on the ground-truth P(IK) data *from each model*. So for example, we started from model *A*, and finetuned

	Questions that only A gets right	Questions only B gets right
A’s average P(IK)	0.463	0.408
B’s average P(IK)	0.409	0.477

Table 2 ‘Cross-Experiments’: Average P(IK) from for two distinct models on subsets of TriviaQA questions where one model is correct and the other is wrong. We see that the entries in the major diagonal are larger than the entries in the minor diagonal, showing that there is some signal that P(IK) is encoding model-specific information. However, the difference in P(IK) is only around 6%, so there is room for improvement from future work.

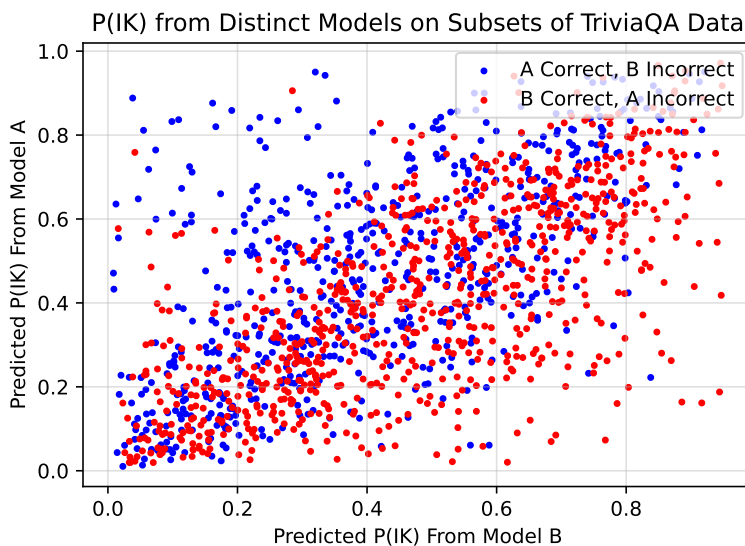


Figure 20 Scatterplot that disambiguates numbers in Table 2. We evaluate 2 distinct 12B models on TriviaQA, separating the data into questions each model gets correct and the other gets incorrect. The scatterplot depicts the P(IK) scores from each model on both of these data subsets.

it on the ground-truth P(IK) data from model *A* and, separately, on the data from model *B* (resulting in two distinct finetuned snapshots). We might hope to find that training a P(IK) classifier to predict whether or not model *A* knows the answer to a question would work better when starting from model *A* itself as the initial checkpoint, as compared to if we start from model *B*. Table 3 contains results for this experiment.

We find mixed but encouraging results here: when testing on the ground-truth P(IK) data from model *A*, both starting from model *A* and starting from model *B* seems to give comparable performance. However, when testing on ground-truth P(IK) data from model *B*, starting from model *B* seems to do better than starting from model *A*. We also tried focusing on only the questions where the two models differ, but we found similar results in that case.

6 Discussion

The long-term motivation underlying this work is to begin to understand aspects of *honesty* in AI models. We use honesty as an umbrella term including several overlapping⁷ ideas:

- Truthfulness: Does the AI provide factually accurate information, including finding, using, and evaluating source materials correctly?
- Calibration: Do the AI’s probabilistic predictions correspond with frequencies of occurrence?

⁷We are not attempting a precise taxonomy, but simply pointing at a collection of important ideas.

	Test on Ground-Truth from Model A	Test on Ground-Truth from Model B
	AUROC / Brier Score	AUROC / Brier Score
Starting from Model A	0.8633 / 0.1491	0.8460 / 0.1582
Starting from Model B	0.8631 / 0.1497	0.8717 / 0.1443

Table 3 ‘Cross-Experiments’: We trained P(IK) classifiers on the ground-truth data from two models, starting from both models. Ideally, starting from pretrained model X should do better than starting from model Y when training P(IK) using data from model X. We see some signal that starting from model B does better than starting from model A when testing on data from model B. However, we see no difference between both initializations when testing on data from model A.

- Self-knowledge: Do AI systems know what they know and make accurate predictions about their own behavior and reasoning?
- Explainability: Do AI systems reveal their ‘thinking’ completely and faithfully?
- Non-deceptiveness: Can we ensure AI systems do not learn to lie (e.g. when human preference data might encourage systematic mistakes or provide more reward for pleasant misconceptions)?

Here we have focused on aspects of calibration, self-knowledge, and truthfulness, but we are only scratching the surface of the larger subject. Our core findings are that large language models can be well-calibrated on diverse multiple choice questions, that they perform well at self-evaluation on a range of subjects, and that they can be trained to predict what they do and don’t know and exhibit some generalization to new domains and in-context information sources.

We found that calibration tends to improve with model size/capability and with additional few-shot examples. Self-evaluation also improves with model size, which is non-trivial since we expect the quality of model samples to also be improving as we scale up. This means that in effect, we are observing that verification has an advantage over generation. Within the scope of pretrained language models, we find these results encouraging, and expect they can be usefully leveraged to bootstrap more extensive forms of self or inter-model supervision, and to distill calibration back into open-ended natural language responses.

Another motivation for this work was to use self-knowledge as a test-bed for generalization. We are particularly interested in how honesty generalizes from easy to hard questions and across domains, because we are worried about how AI systems may behave out-of-distribution, or when they have some knowledge or insight that humans lack. We found that language models do exhibit a degree of generalization across domains, though calibration suffers out-of-distribution. We also found that although models are trained to predict P(IK) for standalone questions, they generalize in such a way that P(IK) increases significantly when models are provided with source materials that contain the answers to these questions, or hints towards the solution of math word problems. This suggests a relationship between the way models store longterm memory and the way they use information within their contexts, i.e. it suggests a connection between learning and in-context learning.

6.1 Limitations and Future Work

This work has a number of limitations:

- We have focused on pretrained language models, but models that have been finetuned for a specific purpose, such as RLHF policies [Bai et al., 2022], will not be so well-calibrated, and some of the methods we discussed may not work as well.
- Furthermore, language model pretraining is a form of human imitation. Some of the most interesting questions about honesty concern setups where advanced AI systems ‘know’ something that clashes with or extends what humans know, and so cannot have been grasped from pretraining. Our analysis does not differentiate between "the truth" and "what humans say", but eventually we would like to train AI systems that recognize this distinction and generalize appropriately.
- This work does not address the possibility that AI systems may learn to behave deceptively (in order to e.g. maximize human preference rewards), and intentional deception would counteract simple trends in honest self-evaluation.

- We were interested in the generalization of honesty because we would like to predict whether AI systems will extrapolate from training to exhibit safe and desirable behavior in new contexts. We found some interesting and potentially encouraging forms of generalization. But we only studied five sampling-based datasets, and our observations concerning capability trends and generalization were limited in power and scope. It would be interesting to investigate these more thoroughly and precisely.

With that said, we believe that the simple methods we have demonstrated here lay the foundation for investigating some of these issues in the future.

6.2 Broader Impacts

We hope that the broader impacts of this work will be positive. Pretrained language models and other AI systems can be dishonest in a number of ways, and we hope that this work will make it easier to identify and correct failures of honesty in deployed systems. That said, pretrained language models may have other failure modes, and the interventions we study here may not correct errors that are perpetuated by language model training data and human imitation.

7 Contribution Statement

Model Training: Model pretraining was led by Sam McCandlish, Nicholas Joseph, Tom Brown, and Jared Kaplan, and the majority of Anthropic’s technical staff contributed to the development of our efficient distributed training infrastructure and the underlying machine learning systems. Core contributors include Tom Henighan, Scott Johnston, Sheer El Showk, Nicholas Joseph, Nelson Elhage, and Ben Mann. Scott Johnston and Sheer El-Showk in particular worked on optimizing pretraining for ML efficiency.

Sampling and Evaluation: Efficient sampling efforts were led by Tom Brown, and Tom Conerly carried out major aspects of the design, implementation and support for the system, with help from Zac Hatfield Dodds. Many members of Anthropic worked on evaluations, including Saurav Kadavath, Nicholas Schiefer, Nick Joseph, Tom Henighan, Amanda Askell, Jared Kaplan, Andy Jones, and Sam McCandlish.

Cluster: Nova DasSarma and Eli Tran-Johnson managed the research cluster our research depended on and maintained its stability, making this research possible. Many others helped with these efforts, including Ben Mann, Tom Henighan, Sam McCandlish, Andy Jones, and Tristan Hume.

Research: Saurav Kadavath and Jared Kaplan designed and carried out most of the experiments. Saurav built much of the relevant infrastructure for the experiments, including for P(IK) training and large scale evaluations. Amanda Askell and Ethan Perez helped with experiments and design. Tom Henighan carried out early experiments surveying a variety of evaluation formats. Dawn Drain helped set up the code evaluations, and obtained the python function synthesis examples with test coverage. Anna Chen did early work training models to identify relevant source materials.

Writing: This paper was drafted by Jared Kaplan and Saurav Kadavath. Other members of Anthropic made miscellaneous contributions and suggestions throughout the writing process.

Other contributions: The ideas explored in this paper developed in conversations with many of Anthropic’s staff, especially Yuntao Bai, Stan Fort, Deep Ganguli, Jackson Kernion, Dario Amodei, Catherine Olsson, Sam Bowman, Sam McCandlish, and Chris Olah.

Acknowledgments

We thank Paul Christiano for helpful discussions, and Owain Evans, Roger Grosse, Dan Hendrycks, Jacob Hilton, Geoffrey Irving, and Daniel Ziegler for comments on the draft. We’re also deeply grateful to Daniela Amodei, Jarrah Bloomfield, Jamie Kerr, Timothy Telleen-Lawton, Jia Yuan Loke, Jeffrey Ladish, Rebecca Raible, Rune Kvist, Rob Gilson, Guro Khundadze, Filipe Dobreira, and Sebastian Conybeare for their help and support.

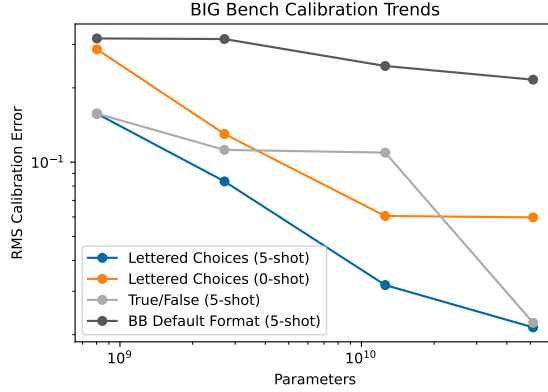


Figure 21 Here we show trends in the RMS calibration error on BIG Bench, for both multiple choice and a separate True/False format. It’s qualitatively very similar to the ECE pictured in Figure 4

A Metrics, Formatting Details, and P(IK) Training

A.1 Calibration Charts

To evaluate calibration on multiple choice problems, we obtain a list of all probabilities for all answer options (both correct and incorrect choices). We then sort these probabilities and bin them into 10 groups, each with an equal number of probabilities. We obtain the x-coordinate of calibration charts by computing the mean probability in each of these bins. To obtain the y-coordinate, we compute the fraction of the options that actually correspond to a correct answer within each bin. The result is a calibration chart such as Figure 6. Our method differs slightly from some others in the literature [Guo et al., 2017, Srivastava et al., 2022, Lin et al., 2022], where only the probabilities for the top prediction are included.

A.2 Expected Calibration Error

To compute the ECE, we simply evaluate

$$E = \frac{1}{N} \sum_i |y_i - x_i| \quad (\text{A.1})$$

for the (x_i, y_i) coordinates of our calibration charts (which have equal numbers of predictions in each bin). This results in plots like Figure 4. Note however that when computing the ECE we only use the top predictions for each multiple choice question, as this seems to be the convention in the literature (this change results in a larger ECE, compared to if we had used all predictions).

We also evaluate the RMS Calibration Error

$$E = \sqrt{\frac{1}{N} \sum_i (y_i - x_i)^2} \quad (\text{A.2})$$

which appears less often in the literature, though it has a sounder theoretical basis.

A.3 Brier Score

We use the standard prior score of

$$B = \frac{1}{N} \sum_i (p_i - c_i)^2 \quad (\text{A.3})$$

where $p_i = \text{P}(\text{True})$ for any given sample (i.e. the model’s self-evaluated probability that it’s sample was correct), and c_i is 0 if the sample is incorrect, and 1 if it is correct. In contexts where many samples have been generated at unit temperature, we binarize the ground-truth P(IK) via $\mathbb{1}\{\text{Ground-Truth P(IK)} > 0.5\}$.

A.4 BIG Bench Default Format

By default in BIG Bench [Srivastava et al., 2022] questions are posed in this way:

```
Question: Who was the first president of the United States?
choice: Barack Obama
choice: George Washington
choice: Michael Jackson
Answer:
```

Here models are required to re-write the complete responses. We find that calibration is poorer in this format, compared to a format with lettered choices, and where models need only write that letter.

A.5 Prompt for Self-Evaluation

We used this prompt for self-evaluation of P(True), when not taking a few-shot approach (which performs best, as it improves significantly on calibration). This was simply the first prompt we tried, and it was not otherwise optimized. It contains six examples, with some similarity to arithmetic, trivia, and fill-in-the-blank completions. This version contains extra "brainstormed" examples; we also used an otherwise identical version without these examples for the types of evaluation discussed in section 4.1:

```
Question: Who was the third president of the United States?
Here are some brainstormed ideas: James Monroe\n Thomas Jefferson\n Jefferson\n
    Thomas Jefferson\n George Washington
Possible Answer: James Monroe
Is the possible answer:
(A) True
(B) False
The possible answer is: (B)
```

```
Question: Calculate 33 + 4
Here are some brainstormed ideas: 37\n 37\n 40\n 36\n 37
Possible Answer: 37
Is the possible answer:
(A) True
(B) False
The possible answer is: (A)
```

```
Question: Fill in the blank in the sentence "I went to the grocery and then to
    the pharmacy. I was disappointed that they didn't have any vegetarian
    sausage at the ____."
Here are some brainstormed ideas: grocery\n store\n grocery\n refrigerator\n
    grocery
Possible Answer: grocery
Is the possible answer:
(A) True
(B) False
The possible answer is: (A)
```

```
Question: Name a celebrated civil rights leader.
Here are some brainstormed ideas: Martin Luther King\n Ghandhi\n Martin Luther
    King\n Barack Obama\n Martin Luther King
Possible Answer: Martin Luther King
Is the possible answer:
(A) True
(B) False
The possible answer is: (A)
```

```
Question: Calculate 33 * 849
Here are some brainstormed ideas: 28,347\n 1,490\n 27,488\n 3,409\n 34,561
Possible Answer: 28347
Is the possible answer:
(A) True
(B) False
The possible answer is: (B)
```

Question: Fill in the blank in the sentence "I shot the _____ and it went swish.
We walked away the winners of that battle!"
Here are some brainstormed ideas: gun\n bullet\n arrow\n basketball\n rifle
Possible Answer: gun
Is the possible answer:
(A) True
(B) False
The possible answer is: (B)

A.6 Training for P(IK)

In order to train P(IK) classifiers, we created datasets that consisted of (Q , IK / IDK Label) pairs. Given a question Q , such as a TriviaQA question that includes a few-shot prompt, we generated 30 candidate answer samples at $T = 1$. See Appendix A.7 for details on the formatting of Q on each of our tasks. We then scored each candidate answer sample as either correct or incorrect. For each candidate answer, we then create a datapoint (Q , True Label) based on whether or not the model got the answer correct. Thus, for each question, we have 30 datapoints of (Q , True Label). This is done as a simple way of approximating a soft label using many hard labels.

During fine-tuning, we used a batch size of 7680, and a learning rate that was $\frac{1}{3}$ of the original pretraining learning rate. We noticed that using a larger than normal batch size was important for learning because of our noisy soft training labels.

The evaluation datasets are constructed similarly to the above, except during evaluation, we focus on computing ground truth P(IK) scores for each question, instead of many IK/IDK labels for each question. The ground truth P(IK) is simply the fraction of $T = 1$ samples the model gets correct. We then compare this ground truth P(IK) score to the model's predicted P(IK) score on these evaluation questions in many plots throughout the paper.

A.7 Formatting of Questions for P(IK)

TriviaQA: TriviaQA was done 10-shot. For brevity, here is a 2-shot example:

Question: Anatomy. Where are the intercostal muscles situated? Answer: between the ribs Question: What is the thick watery substance filling the space between the lens and the retina of the eye? Answer:

Lambda: Lambda was done 10-shot. For brevity, here is a 2-shot example:

Question: Please complete the following passage by filling in the blank: John said, "Hi, this is the Telecommunications Exchange for the Deaf, and I have Gloria on the phone. She's hearing impaired, so I'm calling for her. Is this Alan?" "Yes." "OK, please hold." John told the deaf person that he had Alan on the line. Then she began to type, and John read her message to Alan: "Hi, Alan, this is ____." -> Answer: gloria
Question: Please complete the following passage by filling in the blank: He was good looking, but she was not in the mood to be picked up by anyone. "I'm McKenzie," said the man. He reached out his free hand to Ana. Ana hesitated for a moment, then shook McKenzie's hand and said, "Ana."

```
"Where are you from, Ana?"
"Look, if you are trying to pick up a girl, I am not it," said _____. ->

Answer:
```

Arithmetic: Arithmetic was done 10-shot. For brevity, here is a 2-shot example:

```
Question: What is 36 plus 32?

Answer: 68
Question: What is 7,781 minus 5,071?

Answer:
```

Python Function Synthesis: Python Function Synthesis was done 0-shot. The context for each Python Synthesis problem is a partial Python file, with a function definition and docstring at the very end. The model is then tasked with filling in the function so that it passes a test.

```
...
<Beginning of file is given as context>
...

def make_random_slice(upper):
    """Return a slice of an array with upper bound upper. Guaranteed to
       have
       at least one element."""
```

GSM8k: GSM8k was done 10-shot. For brevity, we have included a 2-shot example below. Note that the model is prompted to output reasoning as well as the correct answer. However, each candidate answer is scored based on the number given after the #####.

```
Question: Verna loves to eat fruit. She bought three apples at $1.50
         each, five oranges at $0.80 each, and six peaches at $0.75 each. If
         she gave $20, how much change did she receive?

Answer: three apples cost 3 x $1.50 = $<<3*1.5=4.50>>4.50.
five oranges cost 5 x $0.80 = $<<5*0.8=4>>4.
four peaches cost 6 x $0.75 = $<<6*0.75=4.50>>4.50.
thus, verna paid a total of $4.50 +$4+ $4.50 = $<<4.5+4+4.5=13>>13.
therefore, verna received $20 - $13 = $<<20-13=7>>7.
##### 7

Question: Frederick is making popsicles to sell and to save money he is
         making his own popsicle sticks. He can get 200 sticks from a 2 x 4
         piece of wood and 400 sticks from a 2 x 8 piece of wood. He has $24
         to buy wood for sticks. A 2 x 4 costs $4. A 2 x 8 costs $6. What is
         the most popsicle sticks he can make if he buys the cheapest lumber?

Answer:
```

B Discriminating What Models Know with Entropy or Loss

In this section we will compare methods that attempt to discriminate correct and incorrect samples, without achieving calibration.

B.1 Loss of the Sample

A very simple method is to generate a sample, and then look at the model's loss on this sample, averaged over all tokens. This has some power to discriminate between correct and incorrect samples, as shown in Figure 22 and 23.

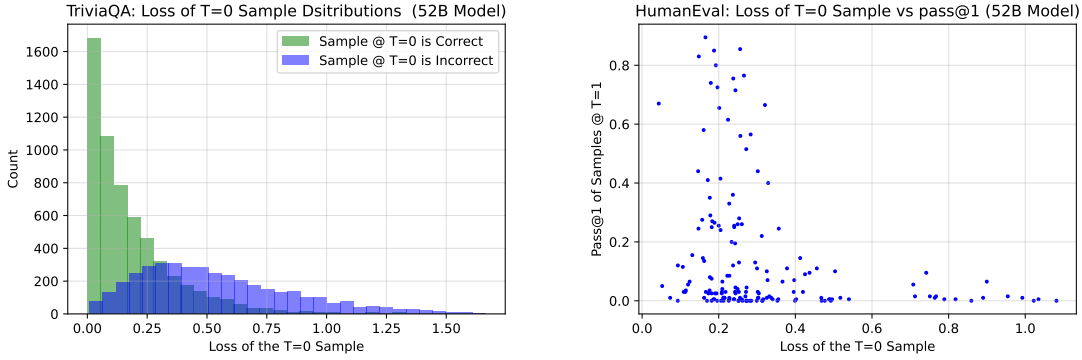


Figure 22 Using the model’s loss on the $T = 0$ sample to differentiate between problems it knows the answer to and problems it doesn’t know the answer to. **Left:** On TriviaQA, we see that the loss on the $T = 0$ sample is more commonly lower for answers that are correct. **Right:** On Codex HumanEval, we see that the loss on the $T = 0$ sample is somewhat indicative of the accuracy of the T=1 samples. Specifically, we see that our model performs poorly in terms of pass@ k on all questions that resulted in a high loss on the T=0 sample.

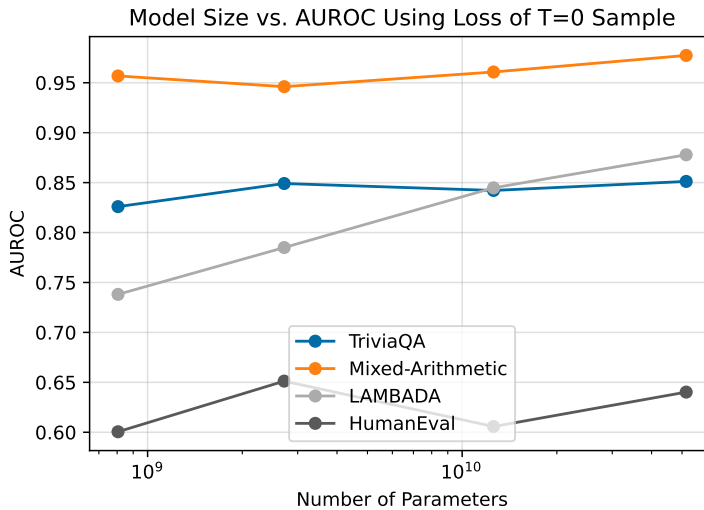


Figure 23 Model size trends of the AUROC, when using the loss of the $T = 0$ sample to predict whether or not the model will get the question correct. For the purposes of this chart, we consider HumanEval problems with a pass@10 > 0.5 as problems that the model got ‘correct’.

We considered summing the loss across all tokens as well. However, this would make the length of the candidate solution a confounding variable. For many evals, such as Codex HumanEval, more difficult questions naturally require longer answers.

B.2 Entropy of the Answer Distribution

One hypothesis about model hallucinations is that they are diverse. Specifically, we hypothesize that when a model knows the answer to a particular question, it is confident in its response, and sampling the answer many times at $T = 1$ would result in an answer distribution with small entropy. Conversely, when a model is unsure about its response, it will start "hallucinating" responses, leading to an answer distribution with high entropy. In order to investigate this, we sample $N = 200$ answers from each question and estimate the entropy of the answer distribution for a given question $H(A|Q)$ as:

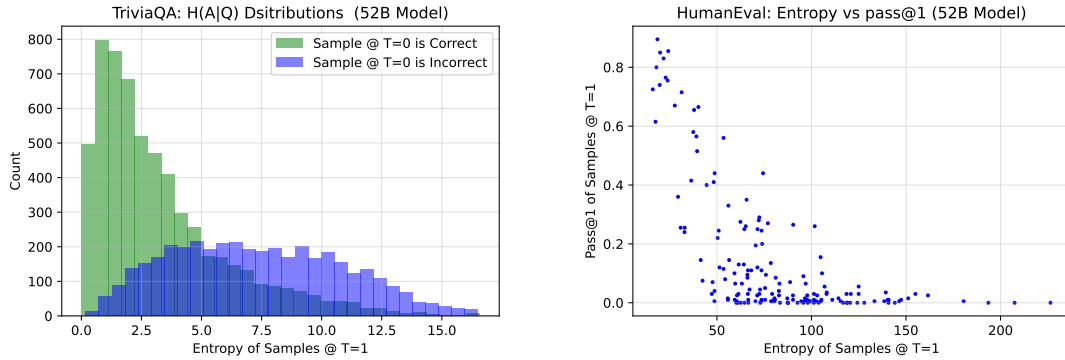


Figure 24 Entropy of samples from the 52B model on TriviaQA and HumanEval. On the left, we see that the TriviaQA questions that the model gets correct and incorrect at $T = 0$ have different entropy distributions. The average entropy of the questions the model gets correct is lower than that of the questions the model gets incorrect. On the right, we compute the entropy and pass@1 over many samples from each question in HumanEval. We see that as the entropy of the answer distribution decreases, models get higher pass@1 scores.

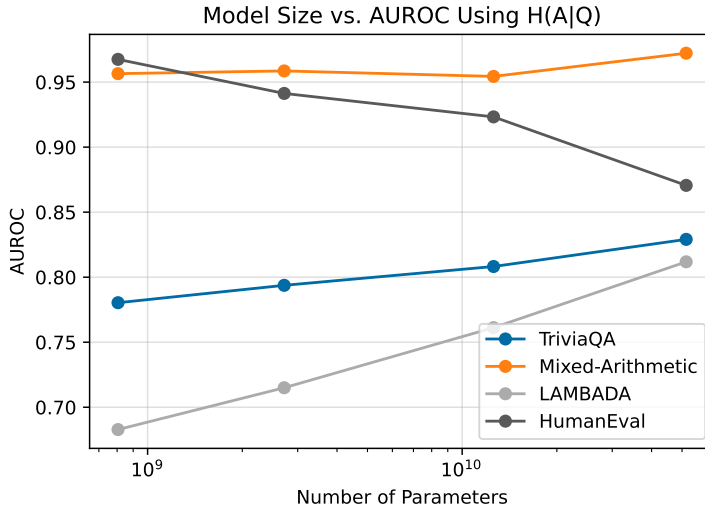


Figure 25 Model size vs. AUROC trends for several evals using the entropy of the answer distribution. Here we are attempting to distinguish whether the model knows the answer to given questions, not whether individual samples are valid. For the Codex HumanEval we threshold "correct" answers as those with Pass@10 > 0.5, whereas we use Pass@1 in the main text.

$$H(A|Q) = \mathbb{E}_{A \text{ sampled from model}} [-\log \mathbb{P}(A|Q)] = \mathbb{E}_A \left[\sum_{a_i \text{ tokens of } A} -\log \mathbb{P}(a_i|Q, a_0, \dots, a_{i-1}) \right]$$

In Figure 24, we look at how well $H(A|Q)$ performs as a signal for which questions the model gets correct vs. incorrect. The distribution of $H(A|Q)$ looks different depending on whether or not the model got the question correct, indicating that it has some predictive power. In Figure 25, we show model size trends for the AUROC using $H(A|Q)$ for many evals. It's interesting to note the negative trend of AUROC on HumanEval as we increase model size. We found that larger models solve harder HumanEval problems, but also often give a diverse set of correct answers. This is in conflict with the original hypothesis that when a model knows the answer to a question, its answer distribution is not diverse. Because larger models are able to give more diverse *and correct* answers, we believe that $H(A|Q)$ is not a robust measure of whether or not a model knows the answer to a question, especially as models increase in size.

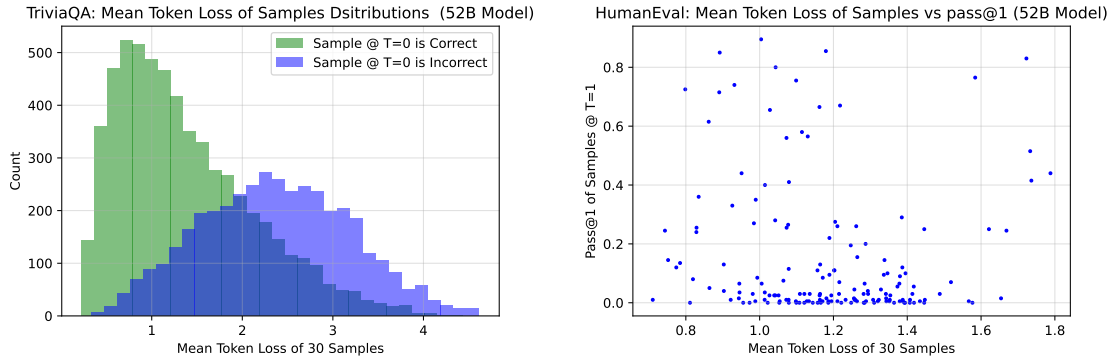


Figure 26 Token Loss of stuffed answers can sometimes provide signal as to whether the model knows the answer to a given question or not. On TriviaQA, there is a clear difference between the token loss of 30 samples when the model gets the underlying question correct vs. incorrect. On Codex HumanEval, there is much less of a correlation between these metrics.

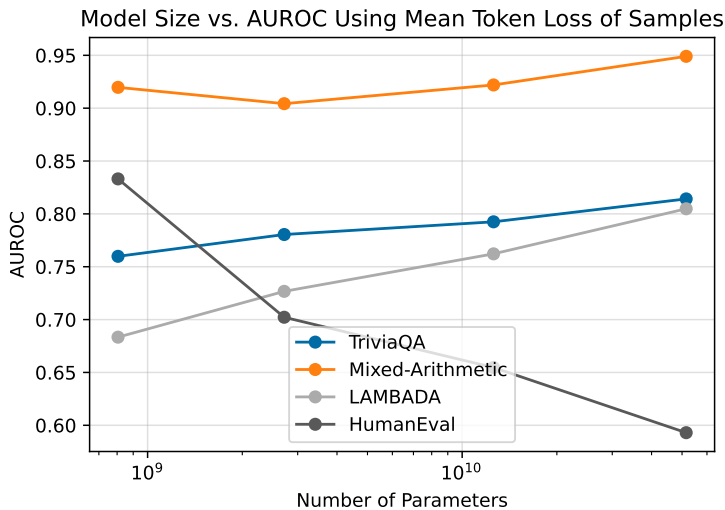


Figure 27 Model size vs. AUROC trends for several evals.

B.3 Loss of Sampled Answers Stuffed into a Single Context

Another way to measure diversity is to stuff many answer samples in the context of an LLM and compute the standard token-level language modelling loss on the stuffed context. We can then use the loss on the entire stuffed context as a measure of if the model knows the answer or not. The idea here is similar to the idea with the Entropy method - questions that the model knows the answer to will have less diverse answer distributions.

Here, we stuff 30 model-generated samples at $T = 1$ in the context window and compute the mean token loss across the sequence. We choose to take the mean token loss so that results aren't confounded by the length of the sampled answers, since for benchmarks like HumanEval, the length of correct answers tends to be correlated with the difficulty of the question. See Figure 26 and Figure 27 for results. We see that this method has some discriminative power for differentiating whether or not the model knows the answer. However, as expected, we see the a negative model size trend for Codex HumanEval. See Section B.2 for a short discussion on this negative trend - we believe that the same intuition applies here.

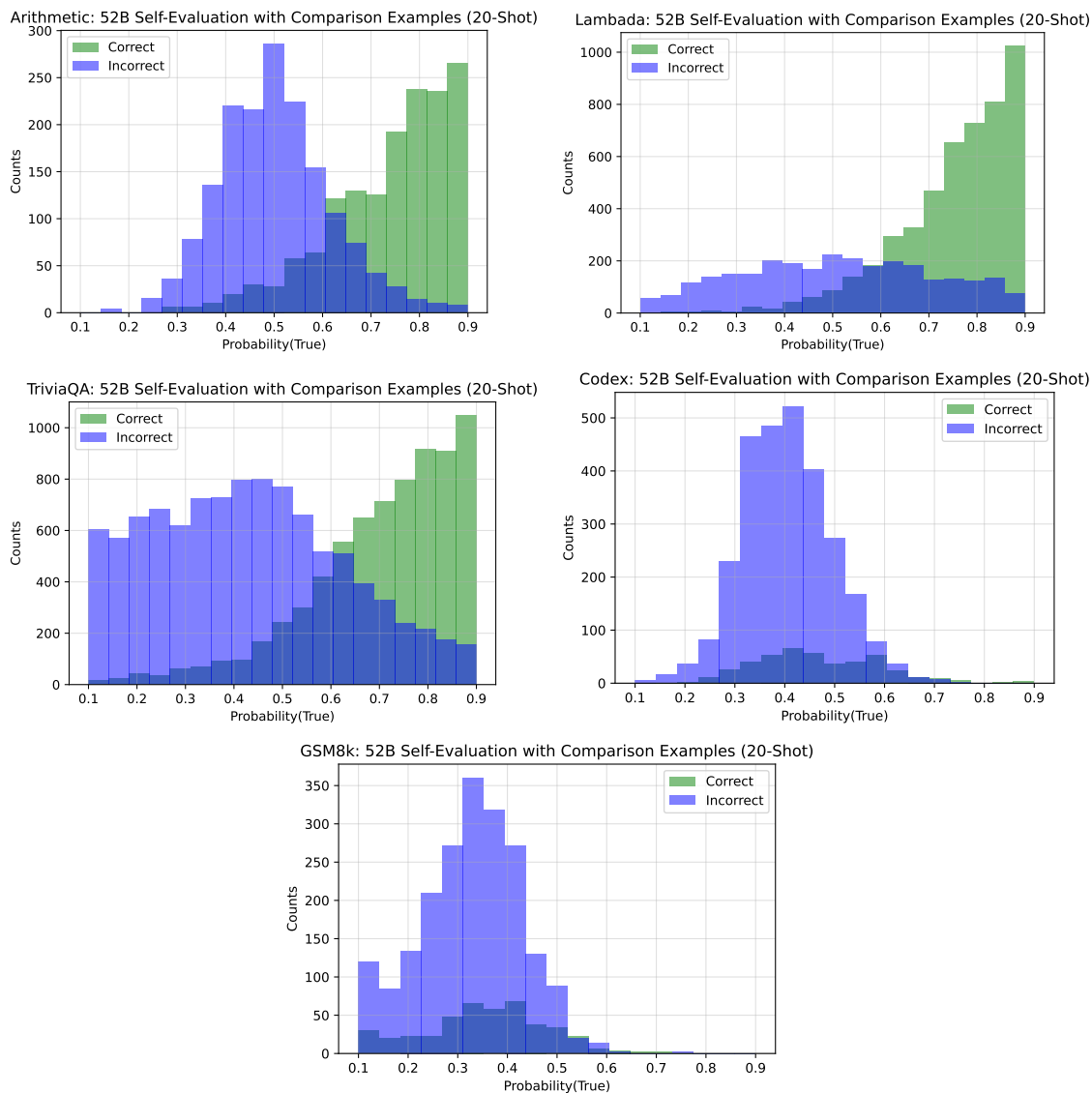


Figure 28 Models self-evaluate their own samples by producing a probability $P(\text{True})$ that the samples are in fact correct. Here we show histograms of $P(\text{True})$ for the correct and incorrect samples for each evaluation, in the evaluation paradigm where models also get to see a total of five $T = 1$ samples for the same question, in order to improve their judgment.

C More $P(\text{True})$ Evaluation Results and Details

Here we include some examples of the behavior of True/False self-evaluation 0-shot. In Figure 38 we see that models do a good job *separating* correct and incorrect samples, but their calibration for $P(\text{True})$ is quite poor. To obtain good calibration one must evaluate few-shot, as seen in Figure 28.

D Mixed-Arithmetic and Function Synthesis Dataset Descriptions

Our Mixed-Arithmetic dataset is a programmatically generated set of arithmetic problems. Table 4 gives an overview of the types of questions that were contained in the dataset.

Our Python function synthesis dataset was created by scraping Python repositories from GitHub that contained at least one file with 'test' in its name. For each repository, we called `pytest` with coverage, and grabbed

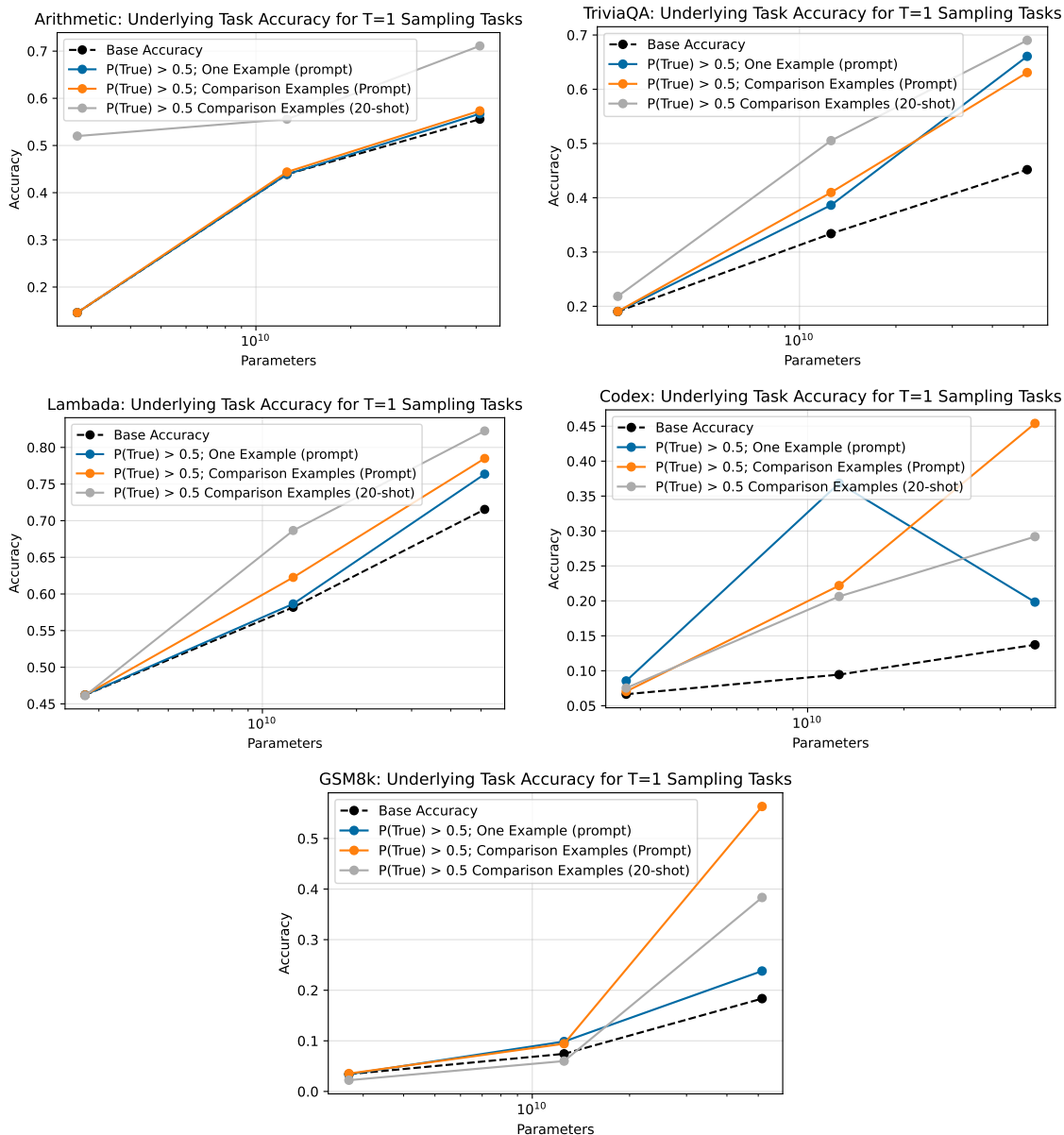


Figure 29 We show the base accuracy of our models on various sampling tasks, and then the accuracy among the responses where via self-evaluation we have $P(\text{True}) > 0.5$. For $P(\text{True})$ we evaluate both 20-shot and 0-shot with a prompt; in both cases we provide the model with five comparison examples to consider before it makes its judgment. Evaluating few-shot is crucial for obtaining good calibration for $P(\text{True})$, though it appears that the prompt actually performs better than few-shot for codex and GSM8k, possibly because these have long-form answers.

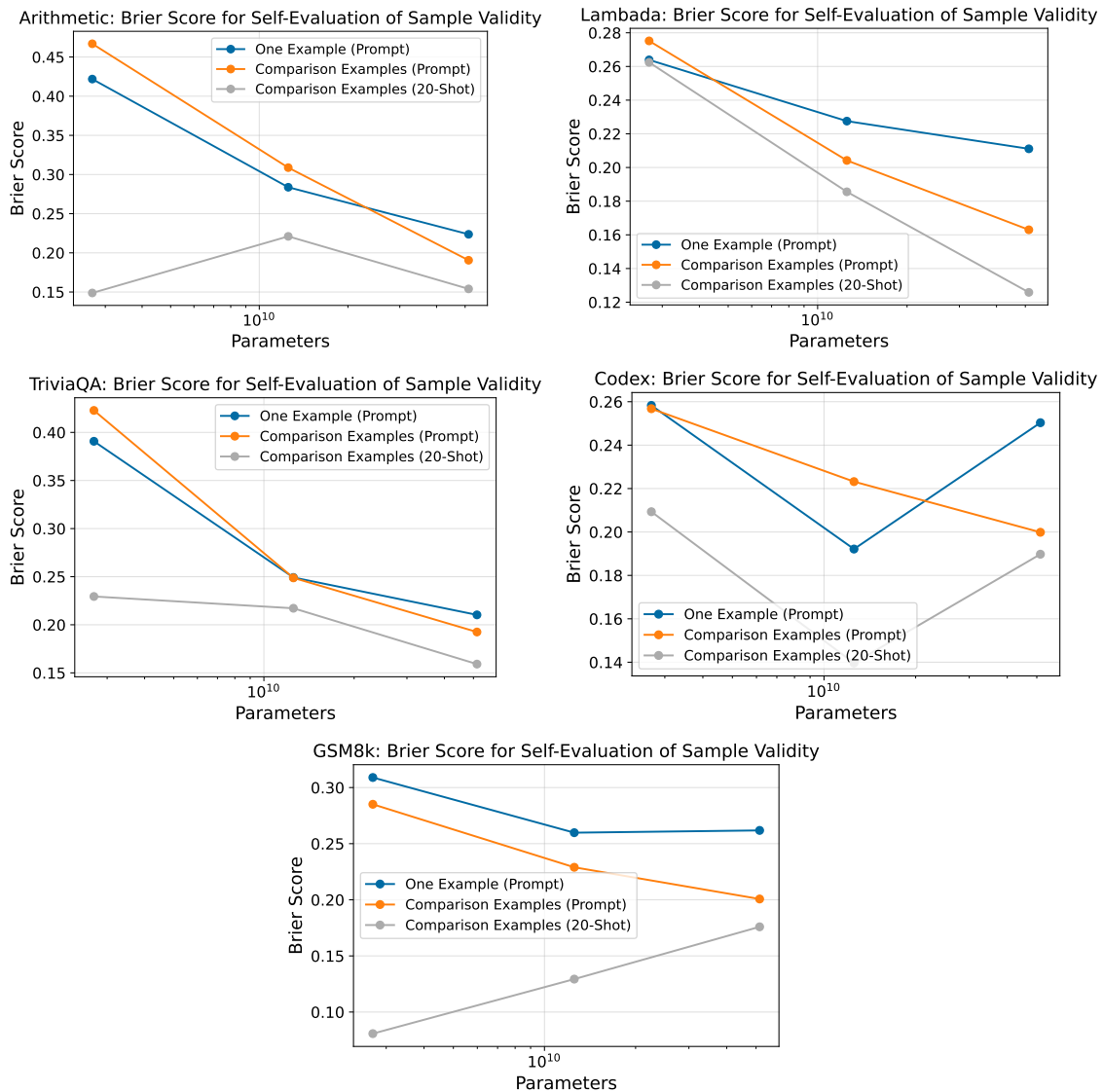


Figure 30 Here we show the Brier scores for model self-evaluation with three methods. Note that the Brier score combines accuracy of the True/False determination with calibration, and 20-shot evaluation with comparison samples performs best in every case. The model size trends in Brier score for Arithmetic, Codex HumanEval, and GSM8k may look surprisingly unpromising, but this is because smaller models have extremely poor performance on these tasks (see Figure 1), meaning that one can achieve a very low Brier score simply by predicting $P(\text{True}) \approx 0$ uniformly.

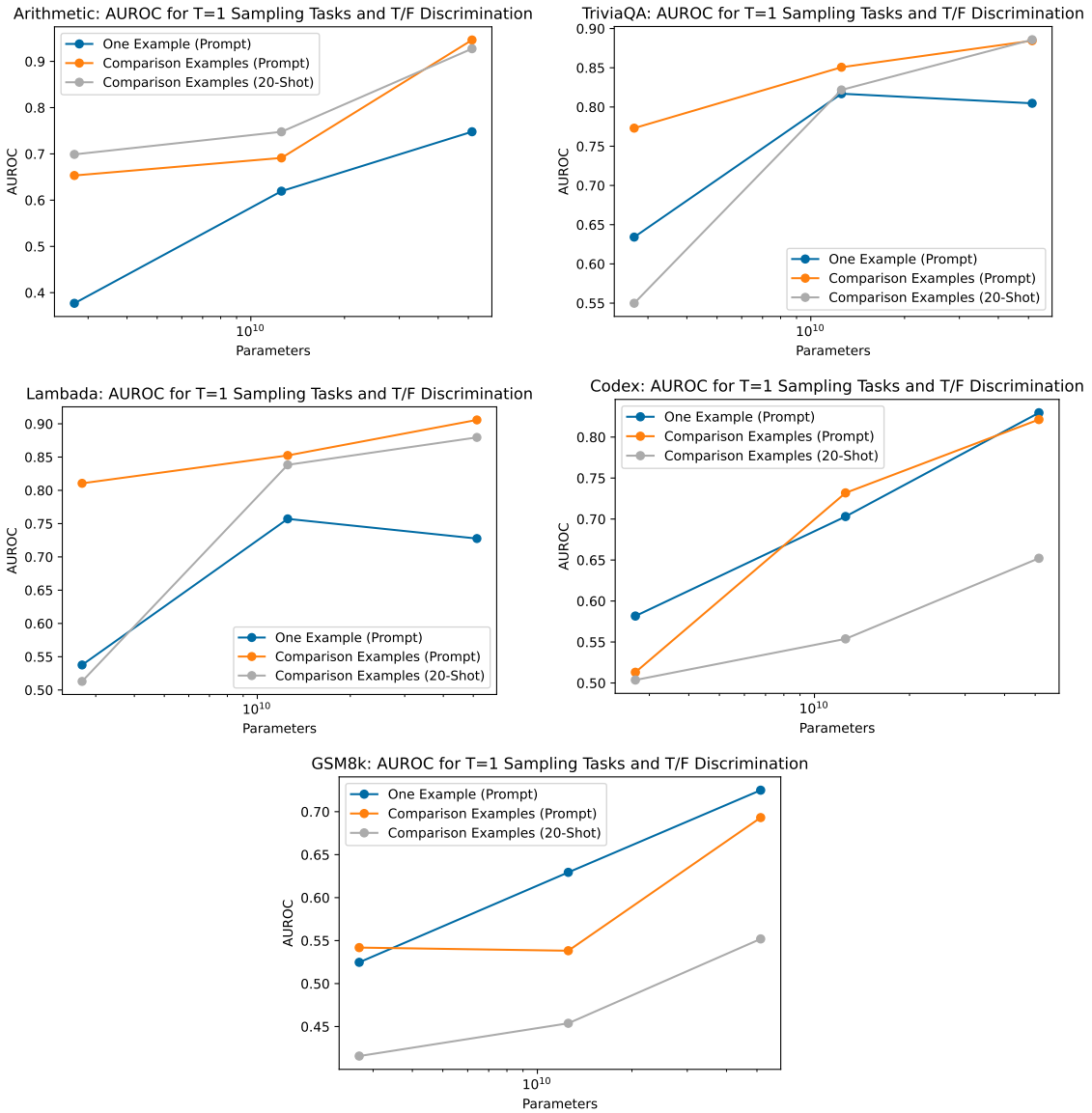


Figure 31 We show the AUROC scores for P(True) with several different methods – a fixed prompt and basic self-evaluation, a fixed prompt and self-evaluation with comparison examples, and 20-shot with comparison examples.

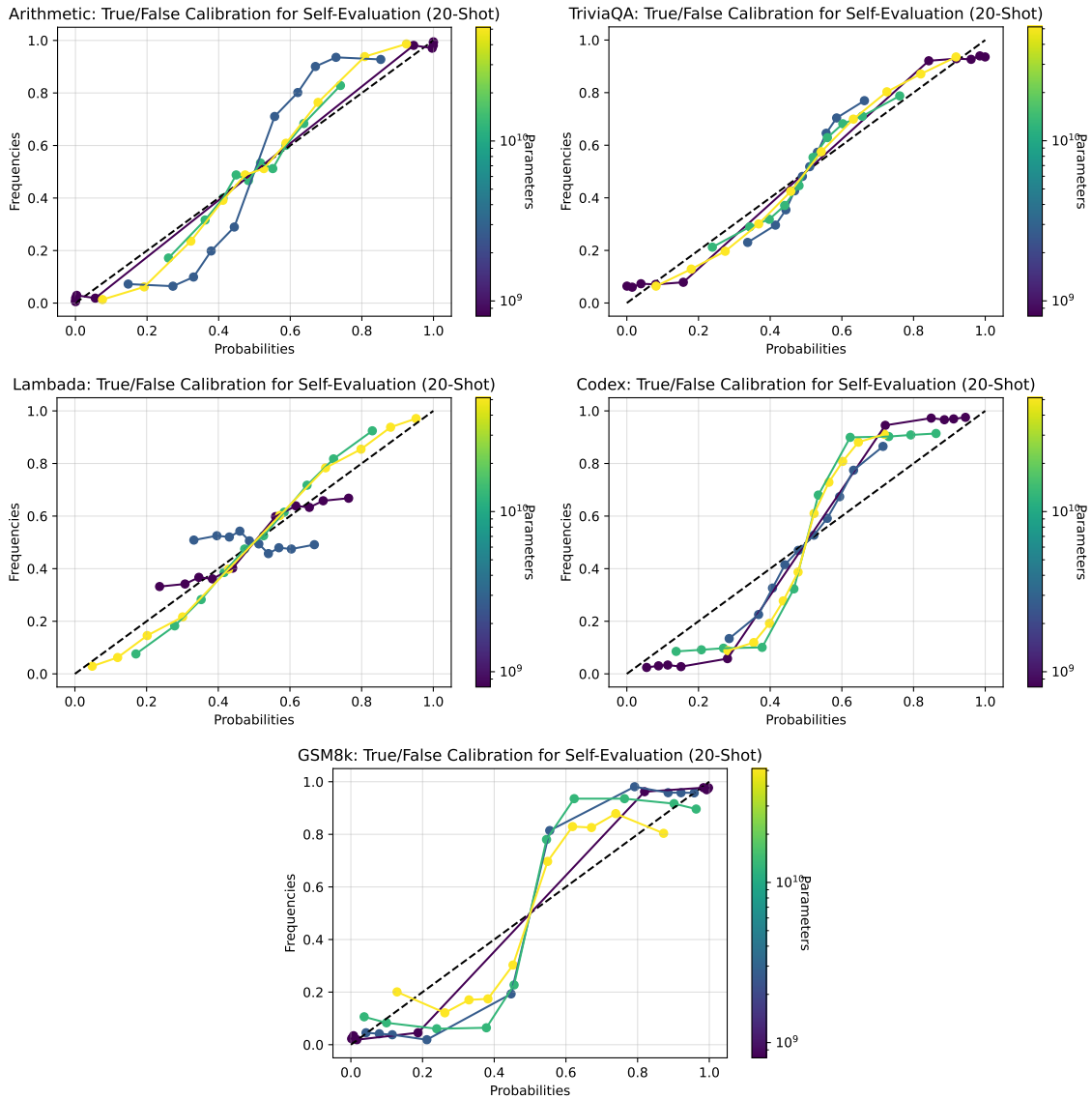


Figure 32 We show the calibration curves when models self-evaluate the likelihood that their own samples are in fact correct. It is worth noting that for some of the evaluations (GSM8k, Codex, Arithmetic), smaller models get almost every question wrong, which means that in these cases the small models are only well-calibrated because they are making trivial predictions.

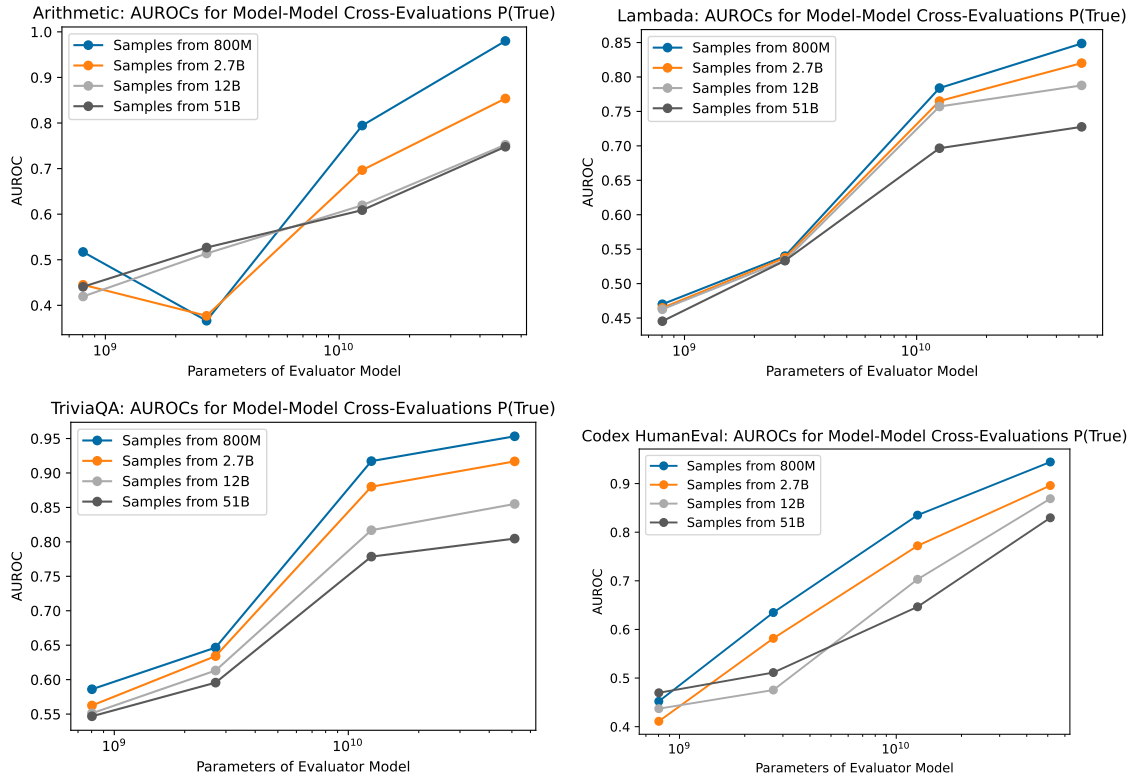


Figure 33 We show AUROCs for $P(\text{True})$ from cross-evaluation experiments where we generate samples from models of one size and then evaluate whether these samples are correct using models of a different size. We see that samples from smaller models are always easier to evaluate, and that larger models are better at evaluation. That said, correctness evaluation improves with the size of the evaluator model, even when it is evaluating its own samples.

all non-test functions where at least half the lines were covered by passing test(s). We then used these tests to evaluate model responses. Our final dataset consisted of 8000 Python functions and their corresponding tests, which was then separated out into a 6000/2000 train/test split.

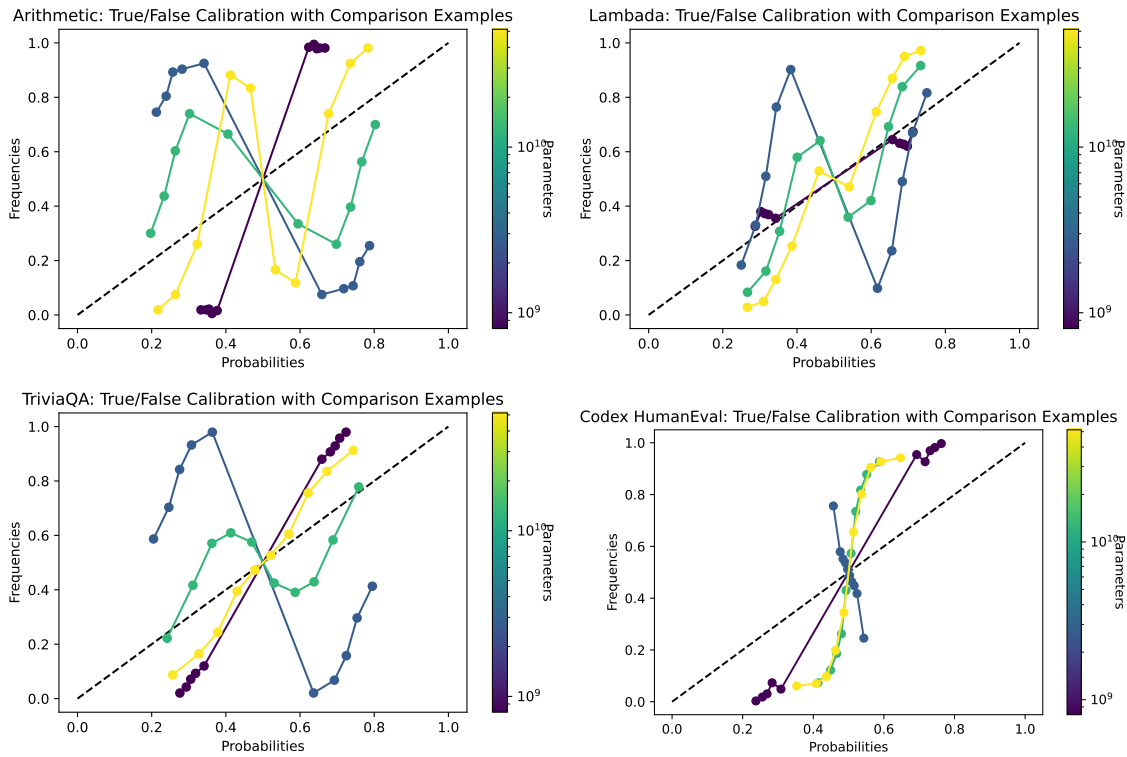


Figure 34 We show that when we ask models to self-evaluate their own samples as True or False **zero-shot**, the $P(\text{True})$ judgment is poorly calibrated, though in most cases it seems to be improving as models become larger and more capable.

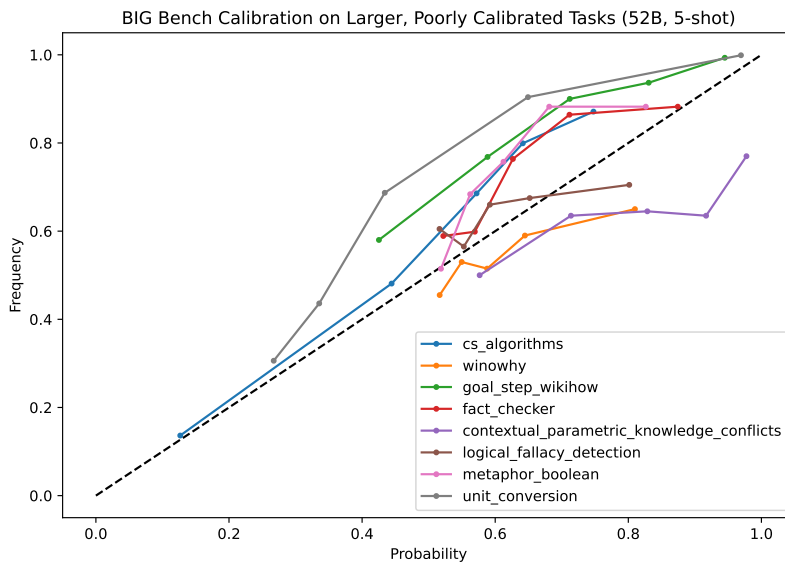


Figure 35 We show calibration curves for a subset of tasks that have both a large number of questions (for better statistics) and fairly bad calibration.

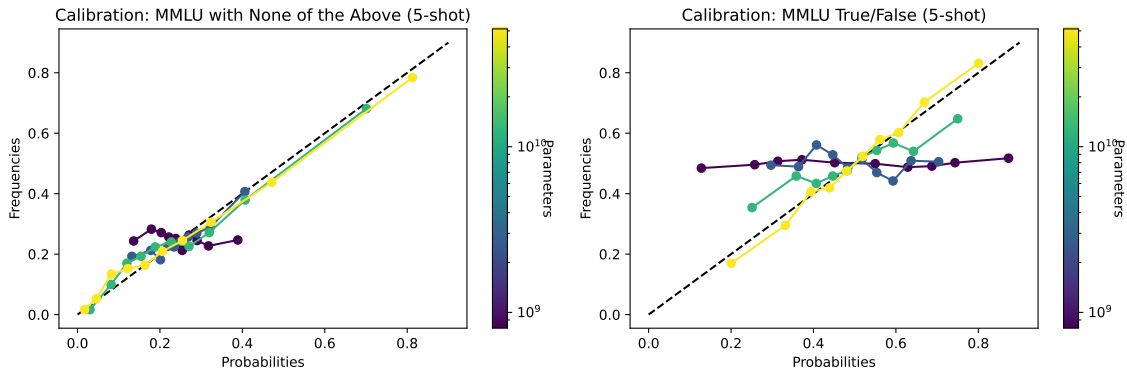


Figure 36 (left) We show calibration curves for MMLU when we replace option (D) with ‘none of the above’ in all questions, or (right) when we completely reformulate the task as a True/False decision as to whether randomly selected options are correct.

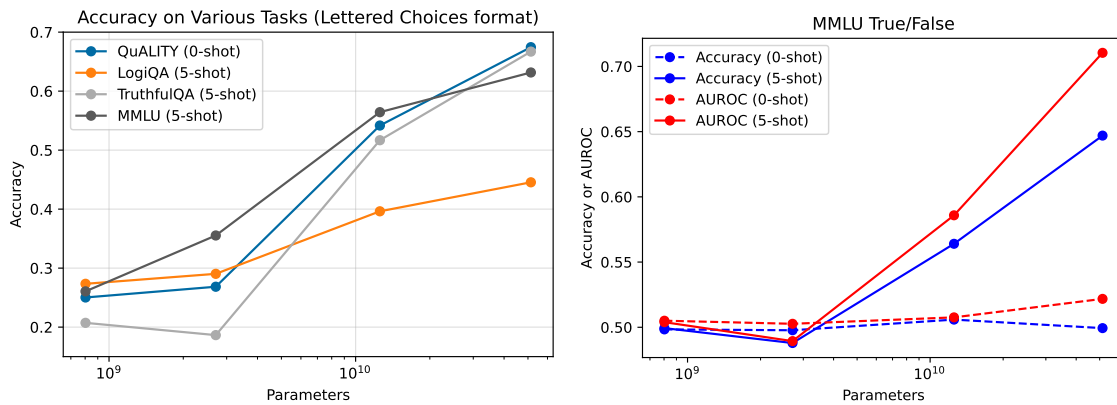


Figure 37 (left) We show accuracies on the specific multiple choice tasks we evaluate, MMLU, TruthfulQA, QuALITY, and LogiQA. (right) We show accuracy for MMLU in the True/False format, where the model must identify if a possible response to a question is true or false. Chance accuracy is 0.5. In order to connect with other methods that do not produce calibrated probabilities, we also show the AUROC when using the probabilities assigned to True/False to separate the correct and incorrect responses.

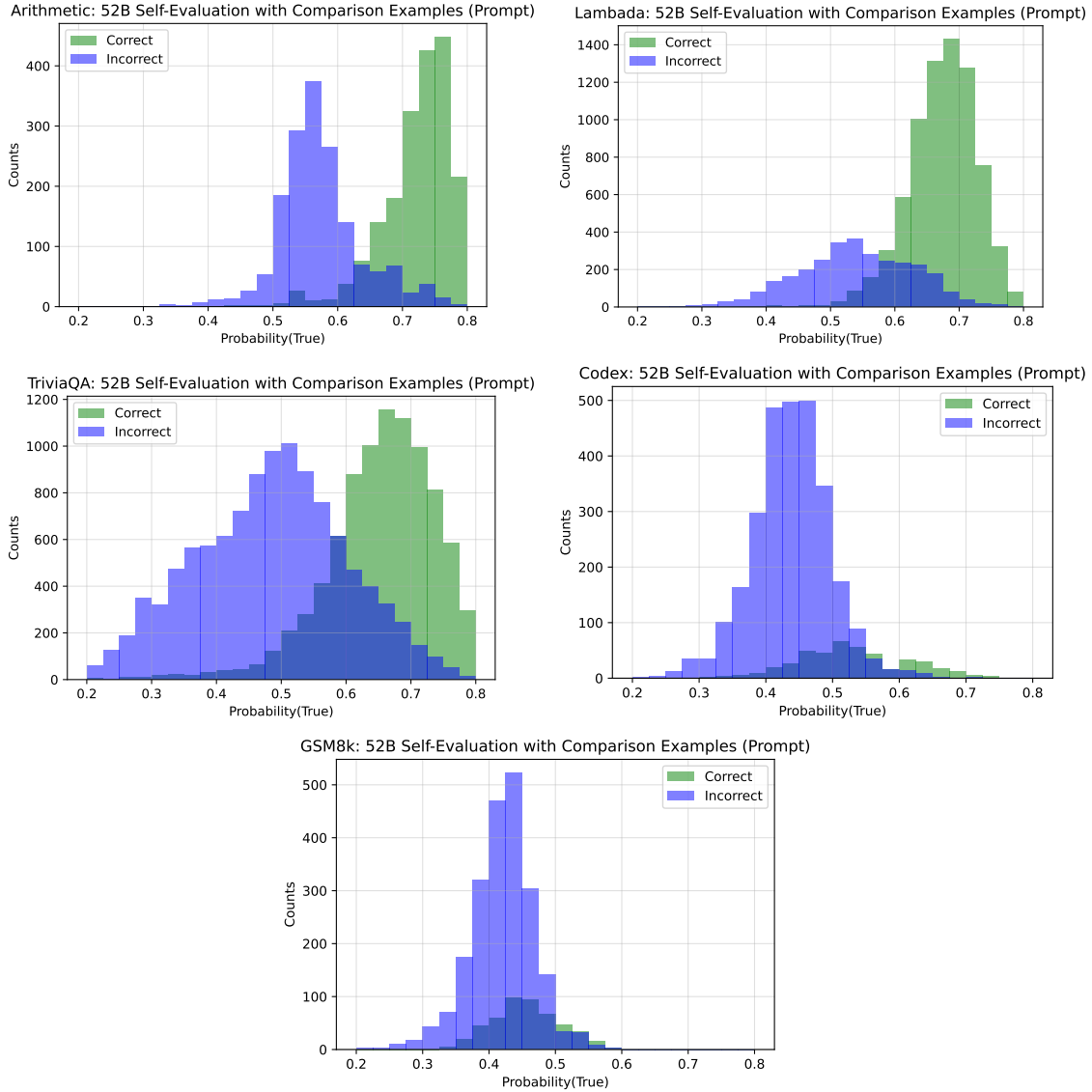


Figure 38 Models self-evaluate their samples by producing a probability $P(\text{True})$ that the samples are in fact correct. Here we show histograms of $P(\text{True})$ for the correct and incorrect samples for each evaluation, in the evaluation paradigm where models also get to see a total of five $T = 1$ samples for the same question, in order to improve their judgment. $P(\text{True})$ provides very noticeable separation between correct and incorrect samples with the 52B model, but the probability itself is not calibrated. In particular, almost all samples from arithmetic questions have $P(\text{True}) > 0.5$. These evaluations are all zero-shot, but they include a human-written prompt with six examples.

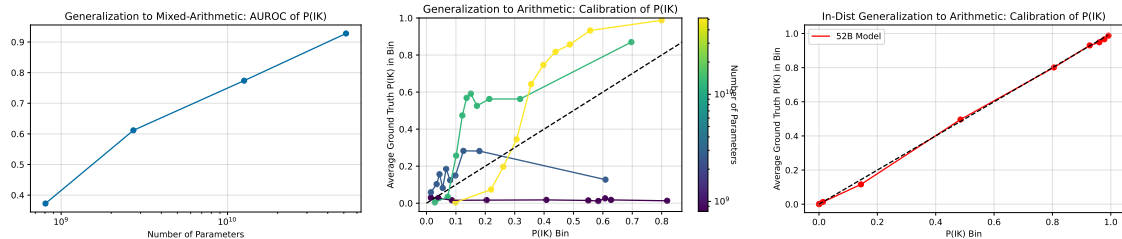


Figure 39 Left and Middle: Generalization of $P(\text{IK})$, trained on TriviaQA, to Arithmetic. Right: Calibration curve of a 52B model that was trained for $P(\text{IK})$ on all 4 tasks, on Arithmetic

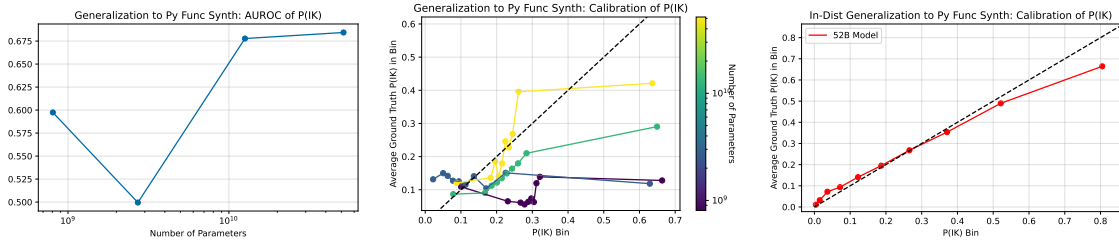


Figure 40 Left and Middle: Generalization of P(IK), trained on TriviaQA, to Python Function Synthesis. Right: Calibration curve of a 52B model trained for P(IK) on all 4 tasks, on Python Function Synthesis.

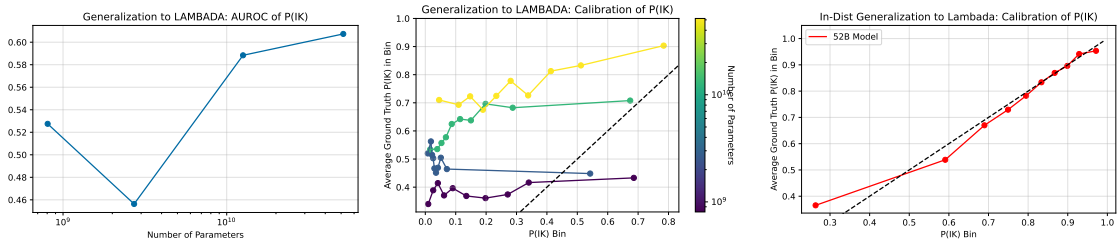


Figure 41 Left and Middle: Generalization of P(IK), trained on TriviaQA, to LAMBADA. Right: Calibration curve of a 52B model that was trained on all 4 tasks, on LAMBADA. Note calibration is extremely poor because P(IK) is systematically too small for all predictions; see Figure 16.

Name of Mixed-Arithmetic Subset	Example Question and Answer
add_digits_1_nlp_comma	Question: What is 4 plus 9?\n\nAnswer: 13
add_digits_2_nlp_comma	Question: What is 13 plus 88?\n\nAnswer: 101
add_digits_3_nlp_comma	Question: What is 423 plus 740?\n\nAnswer: 1,163
add_digits_4_nlp_comma	Question: What is 5,476 plus 4,136?\n\nAnswer: 9,612
add_digits_5_nlp_comma	Question: What is 95,837 plus 27,060?\n\nAnswer: 122,897
multiop_digits_1_nlp_comma	Question: What is 5 * 1 - 6?\n\nAnswer: -1
multiop_digits_2_nlp_comma	Question: What is 65 * 81 + 44?\n\nAnswer: 5,309
multiop_digits_3_nlp_comma	Question: What is 622 * 363 - 596?\n\nAnswer: 225,190
multiply_digits_1_nlp_comma	Question: What is 4 times 9?\n\nAnswer: 36
multiply_digits_2_nlp_comma	Question: What is 13 times 88?\n\nAnswer: 1,144
multiply_digits_3_nlp_comma	Question: What is 423 times 740?\n\nAnswer: 313,020
multisum_digits_1_nlp_comma	Question: What is 8 + 2 + 5 + 7 + 6?\n\nAnswer: 28
multisum_digits_2_nlp_comma	Question: What is 38 + 82 + 43 + 19 + 45?\n\nAnswer: 227
multisum_digits_3_nlp_comma	Question: What is 975 + 871 + 145 + 704 + 397?\n\nAnswer: 3,092
subtract_digits_1_nlp_comma	Question: What is 4 minus 9?\n\nAnswer: -5
subtract_digits_2_nlp_comma	Question: What is 13 minus 88?\n\nAnswer: -75
subtract_digits_3_nlp_comma	Question: What is 423 minus 740?\n\nAnswer: -317
subtract_digits_4_nlp_comma	Question: What is 5,476 minus 4,136?\n\nAnswer: 1,340
subtract_digits_5_nlp_comma	Question: What is 95,837 minus 27,060?\n\nAnswer: 68,777

Table 4 Example questions and answers from our programmatically generated Mixed-Arithmetic dataset.

References

- [Askell et al., 2021] Askell, A., Bai, Y., Chen, A., Drain, D., Ganguli, D., Henighan, T., Jones, A., Joseph, N., Mann, B., DasSarma, N., Elhage, N., Hatfield-Dodds, Z., Hernandez, D., Kernion, J., Ndousse, K., Olsson, C., Amodei, D., Brown, T., Clark, J., McCandlish, S., Olah, C., and Kaplan, J. (2021). A general language assistant as a laboratory for alignment.
- [Bai et al., 2022] Bai, Y., Jones, A., Ndousse, K., Askell, A., Chen, A., DasSarma, N., Drain, D., Fort, S., Ganguli, D., Henighan, T., Joseph, N., Kadavath, S., Kernion, J., Conerly, T., El-Showk, S., Elhage, N., Hatfield-Dodds, Z., Hernandez, D., Hume, T., Johnston, S., Kravec, S., Lovitt, L., Nanda, N., Olsson, C., Amodei, D., Brown, T., Clark, J., McCandlish, S., Olah, C., Mann, B., and Kaplan, J. (2022). Training a helpful and harmless assistant with reinforcement learning from human feedback.
- [Chen et al., 2021] Chen, M., Tworek, J., Jun, H., Yuan, Q., Pinto, H. P. d. O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G., et al. (2021). Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*.
- [Christiano et al., 2021] Christiano, P., Coira, A., and Xu, M. (2021). Eliciting latent knowledge.
- [Cobbe et al., 2021] Cobbe, K., Kosaraju, V., Bavarian, M., Hilton, J., Nakano, R., Hesse, C., and Schulman, J. (2021). Training verifiers to solve math word problems. *CoRR*, abs/2110.14168.
- [Evans et al., 2021] Evans, O., Cotton-Barratt, O., Finnveden, L., Bales, A., Balwit, A., Wills, P., Righetti, L., and Saunders, W. (2021). Truthful ai: Developing and governing ai that does not lie.
- [Guo et al., 2017] Guo, C., Pleiss, G., Sun, Y., and Weinberger, K. Q. (2017). On calibration of modern neural networks.
- [Hendrycks et al., 2021] Hendrycks, D., Burns, C., Basart, S., Zou, A., Mazeika, M., Song, D., and Steinhardt, J. (2021). Measuring massive multitask language understanding.
- [Hendrycks and Gimpel, 2016] Hendrycks, D. and Gimpel, K. (2016). A baseline for detecting misclassified and out-of-distribution examples in neural networks.
- [Hendrycks et al., 2018] Hendrycks, D., Mazeika, M., and Dietterich, T. (2018). Deep anomaly detection with outlier exposure.
- [Jiang et al., 2021] Jiang, Z., Araki, J., Ding, H., and Neubig, G. (2021). How Can We Know When Language Models Know? On the Calibration of Language Models for Question Answering. *Transactions of the Association for Computational Linguistics*, 9:962–977.
- [Joshi et al., 2017] Joshi, M., Choi, E., Weld, D. S., and Zettlemoyer, L. (2017). Triviaqa: A large scale distantly supervised challenge dataset for reading comprehension.
- [Lin et al., 2021] Lin, S., Hilton, J., and Evans, O. (2021). Truthfulqa: Measuring how models mimic human falsehoods.
- [Lin et al., 2022] Lin, S., Hilton, J., and Evans, O. (2022). Teaching models to express their uncertainty in words.
- [Liu et al., 2020] Liu, J., Cui, L., Liu, H., Huang, D., Wang, Y., and Zhang, Y. (2020). Logiqa: A challenge dataset for machine reading comprehension with logical reasoning.
- [Menick et al., 2022] Menick, J., Trebacz, M., Mikulik, V., Aslanides, J., Song, F., Chadwick, M., Glaese, M., Young, S., Campbell-Gillingham, L., Irving, G., and McAleese, N. (2022). Teaching language models to support answers with verified quotes.
- [Mielke et al., 2020] Mielke, S. J., Szlam, A., Boureau, Y.-L., and Dinan, E. (2020). Linguistic calibration through metacognition: aligning dialogue agent responses with expected correctness.
- [Minderer et al., 2021] Minderer, M., Djolonga, J., Romijnders, R., Hubis, F., Zhai, X., Houlsby, N., Tran, D., and Lucic, M. (2021). Revisiting the calibration of modern neural networks. In Ranzato, M., Beygelzimer, A., Dauphin, Y., Liang, P., and Vaughan, J. W., editors, *Advances in Neural Information Processing Systems*, volume 34, pages 15682–15694. Curran Associates, Inc.
- [Nakano et al., 2021] Nakano, R., Hilton, J., Balaji, S., Wu, J., Ouyang, L., Kim, C., Hesse, C., Jain, S., Kosaraju, V., Saunders, W., Jiang, X., Cobbe, K., Eloundou, T., Krueger, G., Button, K., Knight, M., Chess, B., and Schulman, J. (2021). Webgpt: Browser-assisted question-answering with human feedback. *CoRR*, abs/2112.09332.

- [Nalisnick et al., 2019] Nalisnick, E., Matsukawa, A., Teh, Y. W., Gorur, D., and Lakshminarayanan, B. (2019). Do deep generative models know what they don’t know? In *International Conference on Learning Representations*.
- [Nguyen and O’Connor, 2015] Nguyen, K. and O’Connor, B. (2015). Posterior calibration and exploratory analysis for natural language processing models. In *Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing*, pages 1587–1598, Lisbon, Portugal. Association for Computational Linguistics.
- [Nye et al., 2021] Nye, M., Andreassen, A. J., Gur-Ari, G., Michalewski, H., Austin, J., Bieber, D., Dohan, D., Lewkowycz, A., Bosma, M., Luan, D., Sutton, C., and Odena, A. (2021). Show your work: Scratchpads for intermediate computation with language models.
- [Ortega et al., 2021] Ortega, P. A., Kunesch, M., DeLá@tang, G., Genewein, T., Grau-Moya, J., Veness, J., Buchli, J., Degraeve, J., Piot, B., Perolat, J., Everitt, T., Tallec, C., Parisotto, E., Erez, T., Chen, Y., Reed, S., Hutter, M., de Freitas, N., and Legg, S. (2021). Shaking the foundations: delusions in sequence models for interaction and control.
- [Ovadia et al., 2019] Ovadia, Y., Fertig, E., Ren, J., Nado, Z., Sculley, D., Nowozin, S., Dillon, J. V., Lakshminarayanan, B., and Snoek, J. (2019). Can you trust your model’s uncertainty? evaluating predictive uncertainty under dataset shift.
- [Pang et al., 2021] Pang, R. Y., Parrish, A., Joshi, N., Nangia, N., Phang, J., Chen, A., Padmakumar, V., Ma, J., Thompson, J., He, H., and Bowman, S. R. (2021). Quality: Question answering with long input texts, yes!
- [Paperno et al., 2016] Paperno, D., Kruszewski, G., Lazaridou, A., Pham, Q. N., Bernardi, R., Pezzelle, S., Baroni, M., Boleda, G., and Fernández, R. (2016). The lambada dataset: Word prediction requiring a broad discourse context.
- [Rae et al., 2021] Rae, J. W., Borgeaud, S., Cai, T., Millican, K., Hoffmann, J., Song, H. F., Aslanides, J., Henderson, S., Ring, R., Young, S., Rutherford, E., Hennigan, T., Menick, J., Cassirer, A., Powell, R., van den Driessche, G., Hendricks, L. A., Rauh, M., Huang, P., Glaese, A., Welbl, J., Dathathri, S., Huang, S., Uesato, J., Mellor, J., Higgins, I., Creswell, A., McAleese, N., Wu, A., Elsen, E., Jayakumar, S. M., Buchatskaya, E., Budden, D., Sutherland, E., Simonyan, K., Paganini, M., Sifre, L., Martens, L., Li, X. L., Kuncoro, A., Nematzadeh, A., Gribovskaya, E., Donato, D., Lazaridou, A., Mensch, A., Lespiau, J., Tsimpoukelli, M., Grigorev, N., Fritz, D., Sottiaux, T., Pajarskas, M., Pohlen, T., Gong, Z., Toyama, D., de Masson d’Autume, C., Li, Y., Terzi, T., Mikulik, V., Babuschkin, I., Clark, A., de Las Casas, D., Guy, A., Jones, C., Bradbury, J., Johnson, M., Hechtman, B. A., Weidinger, L., Gabriel, I., Isaac, W. S., Lockhart, E., Osindero, S., Rimell, L., Dyer, C., Vinyals, O., Ayoub, K., Stanway, J., Bennett, L., Hassabis, D., Kavukcuoglu, K., and Irving, G. (2021). Scaling language models: Methods, analysis & insights from training gopher. *CoRR*, abs/2112.11446.
- [Srivastava et al., 2022] Srivastava, A., Rastogi, A., Rao, A., Shoeb, A. A. M., Abid, A., Fisch, A., Brown, A. R., Santoro, A., Gupta, A., Garriga-Alonso, A., et al. (2022). Beyond the imitation game: Quantifying and extrapolating the capabilities of language models.
- [Wang et al., 2022] Wang, X., Wei, J., Schuurmans, D., Le, Q., Chi, E., Narang, S., Chowdhery, A., and Zhou, D. (2022). Self-consistency improves chain of thought reasoning in language models.
- [Wei et al., 2022] Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., and Zhou, D. (2022). Chain of thought prompting elicits reasoning in large language models.