Open Peer Review on Qeios

RESEARCH ARTICLE

LLM Confidence Evaluation Measures in Zero-Shot CSS Classification

David Farr[1], Iain Cruickshank[2], Nico Manzonelli[3], Nicholas Clark[1], Kate Starbird[1], Jevin West[1]

1 University of Washington, United States
2 Carnegie Mellon University, United States
3 Independent researcher

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.

Abstract

Assessing classification confidence is critical for leveraging large language models (LLMs) in automated labeling tasks, especially in the sensitive domains presented by Computational Social Science (CSS) tasks. In this paper, we make three key contributions: (1) we propose an uncertainty quantification (UQ) performance measure tailored for data annotation tasks, (2) we compare, for the first time, five different UQ strategies across three distinct LLMs and CSS data annotation tasks, (3) we introduce a novel UQ aggregation strategy that effectively identifies low-confidence LLM annotations and disproportionately uncovers data incorrectly labeled by the LLMs. Our results demonstrate that our proposed UQ aggregation strategy improves upon existing methods and can be used to significantly improve human-in-the-loop data annotation processes.

Corresponding author: David Farr, dtfarr@uw.edu

1. Introduction

Large Language Models (LLMs) have transformed the way artificial intelligence is integrated into professional workflows, with applications that span healthcare[1], academia[2], cybersecurity[3], software development[4], and many others. However, research shows that users struggle to identify incorrect LLM responses which poses a problem because LLMs are less likely to refrain from answering questions they do not know as they scale with size and complexity[5]. Despite these challenges, LLMs have proven effective in synthesizing vast amounts of data and applying contextual understanding, making them a popular choice for integration into natural language processing tasks, particularly in zero-shot classification settings where prior training data is unavailable[6].

With broad applications in critical industries, LLM-generated responses that are assumed to be correct can lead to drastic second- and third-order consequences when answered incorrectly and integrated into decision-making processes. Although some LLMs incorporate expressions of uncertainty[7], developers often restrict the output of the model to a

predetermined set of responses to manage nondeterministic behavior or reduce token generation cost[8]. However, these constraints can cause LLMs to provide confident answers even when they lack the correct knowledge. While LLMs are useful for large-scale data annotation tasks, there remains uncertainty as to which labels are correct or how to best quantify label confidence in LLM-generated annotations, especially in multi-modal systems.

This paper evaluates various Uncertainty Quantification (UQ) methods to assess LLM confidence in data annotation tasks applied to Computational Social Science (CSS) problems. Based on these results, we present a simple UQ aggregation strategy to help identify misclassified LLM-labeled data. We constrain our settings to realistic industry scenarios where previously labeled data is unavailable to simulate common, real-world problems. Additionally, we propose a new evaluation metric that assesses the recall of misclassified LLM-labeled data at low-confidences and compare UQ techniques using the Area Under Curve (AUC) analysis by applying thresholds based on percentiles of confidence scores. Our methodology has significant implications for systems that use human-machine teaming for data annotation tasks by better identifying data on which humans should spend finite resources.

2. Related Works

[5] show that as LLMs scale, they become more confident and less avoidant in answering questions. However, this increased confidence comes at a cost: they answer questions incorrectly more frequently compared to smaller LLMs, which were more likely to avoid answering altogether. In a related study,[8] demonstrate the importance of constraining LLM outputs in software development workflows to ensure predictability. Together, these works highlight both the internal challenge of larger LLMs being more prone to incorrect answers instead of avoidance, as well as the common practice of imposing constraints on LLM outputs to improve workflow predictability.

In the field of LLM UQ techniques[9] demonstrates an effective method of UQ via supervised calibration from utilizing hidden activation layers[10] integrate a human annotated training set to train an external BERT-based verifier to select data that the LLM was likely to mislabel for later external human annotation. However, these methods require a labeled dataset for training an external supervised ML model which is not available in many contexts.

As such, recent research has investigated zero-shot UQ techniques for LLMs[11] and[7] show that an effective technique to assess confidence in LLMs tuned with reinforcement learning human feedback (RLHF) is prompting the model to evaluate its confidence in its own answer[12] find that the uncertainty estimates from conformal prediction are closely correlated with the accuracy of the prediction.

Instead of relying on the LLM to self-report confidence, other approaches analyze model output. For example[13] show that the approximation of entropy using measurements on a restricted set of returned tokens is a valid mechanism to assess confidence in multiple-choice questions. Additionally[14] present an effective mechanism for identifying mislabeled data is using the absolute difference between the two highest log probability values returned. Finally[15] look for semantic differences in responses can inform uncertainty. Our work builds on the existing literature by comparing a sample of the aforementioned UQ mechanisms for zero-shot classification while proposing a new methodology that takes advantage of

existing UQ techniques through an ensemble method.

3. Uncertainty Quantification Techniques

In this section we describe the five UQ techniques used in the study.

3.1. Quantitative and Qualitative Self-report

Our first and second UQ techniques are driven by the work of[7], who show that RLHF tuned LLMs can self-assess answer confidence. We accomplish this by prompting the model to give a quantitative assessment of its confidence on a scale between 0 and 100. We also assess the ability of language models to map its uncertainty in qualitative terms. Our hypothesis being that open-source LLMs may perform better using normal language as opposed to probabilistic quantitative values. We accomplish this by asking models to report either *no*, *low*, *medium*, *high*, or *absolute* confidence in their responses. Then we map those responses to quantitative values of 0, 0.25, 0.50, 0.75, and 1 to allow comparability to other confidence measures. Access to all prompt examples and datasets can be found in the availability section.

3.2. Confidence Score

We use the confidence score method from[14], where the authors define the confidence score as the absolute value of the difference between the highest token label log probability and the second-highest token label log probability within a constrained set of tokens. Let T represent the set of given tokens, and $P(t)$ denote the distribution of log probabilities across each token $t \in T$. The log probability is then computed using the formula

$$C = \left| \max_{t \in T} P(t) - \max_{t \in T t^*} P(t) \right|,$$

where t^* is the token corresponding to the highest probability $\max_{t \in T} P(t)$. We refer to this metric as C_score in our results section.

3.3. Log Inverse

We additionally test a commonly used method to convert the logarithmic probability of the highest returned token into a probability. This allows us to investigate whether the difference between the confidence score (based on the top two token probabilities) and the direct probability of the highest token leads to significant differences in sampling outcomes. Specifically, let t^* represent the token with the highest probability, and let $\log P(t^*)$ denote the log probability of this token. The probability for the token t^* is obtained by exponentiating the log probability.

For our results, we refer to this methodology as the *log inverse*.

3.4. Confidence Ensemble

Finally, we introduce the following UQ aggregation strategy, which is more resource intensive than the previous three, requiring the aforementioned confidence score from multiple LLMs, but is meant to reward LLMs for converging on a single label, while not penalizing a divergence of LLM-responses. This is especially important in classification tasks with multiple target classes.

Let L represent the set of LLMs, and for each LLM L_i, the token with the highest probability is denoted by $t^*_{L_i}$, and the corresponding confidence score C_{L_i} is given in Equation 1. To aggregate confidence scores when multiple LLMs provide the same answer t^*, the overall confidence score C_{agg} is calculated as

$$C_{\text{agg}} = \sum_{\{L_i \in \mathrm{L} \mid t^*_{L_i} = t^*\}} C_{L_i},$$

where t^* is the common token predicted by the LLMs. For our results section, this methodology is referred to as *C_ensemble*.

4. Experimental Design

We evaluated our five UQ techniques across three different LLMs and three distinct CSS tasks. For each LLM and task, we rank all annotated data from least confident to most confident, allowing us to sample low-confidence data for human-in-the-loop labeling or high-confidence data for downstream classifiers. Each CSS task is pulled from common benchmark datasets for stance, ideology, and frame detection. For stance detection, we use the SemEval-2016 dataset[16]. For ideology detection, we use the ideological books corpus (IBC) from[17] with sub-sentential annotations[18]. For frame detection, we use the Gun Violence Frames Corpus (GVFC) from[19]. The LLMs chosen were Llama-3.1 8B Instruct, Flan UL2, and GPT-4o. This selection was intentional to show a variety of parameter sizes and the integration of a RLHF-tuned model to show utility in sampling strategy mechanisms across different LLMs.

4.1. Evaluation Metric

In order to demonstrate the efficacy of each UQ strategy, we devise a metric that measures a confidence scoring techniques' ability to recall misclassified LLM-labeled data at low-confidences. When used to inform sampling for human-in-the-loop labeling, we would like to send a small sample of LLM labeled data to human data annotators for evaluation. Ideally, human evaluation is only applied to the data that the LLM is likely to misclassify, which boosts overall classification accuracy under the assumption that the human will correctly label data misclassified by the LLM. By selecting data based on the lowest percentile of confidence scores, we aim to select misclassfied examples for humans to evaluate. Therefore, we measure the percentage of falsely LLM-labeled data recalled as a function of the percentage of the total dataset evaluated based on the same the bottom percentile of confidence scores. This curve is depicted in Figure 1.

Our goal is to succinctly measure performance across UQ techniques, LLMs, and datasets. In order to accomplish this, we report the Area Under Curve (AUC) of the proportion of wrong examples to evaluated examples. As indicated in Figure 1, a higher AUC indicates a better UQ-informed, data sampling strategy. The AUC is calculated for the curve evaluating the dataset from none of the dataset to the full dataset. All graphs for evaluated models, sampling strategies, and datasets are shown in Appendix B. We also report the accuracy on each task for the LLM evaluated on the labeling tasks in Appendix A.

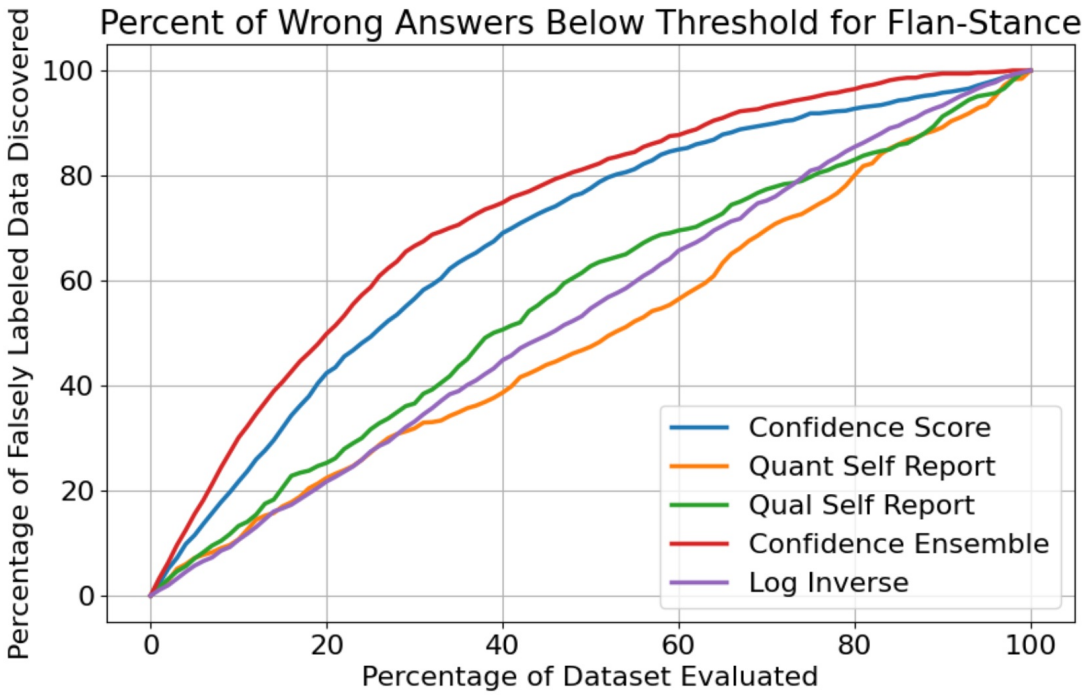


Figure 1. Graph depicts the percent of incorrect data annotations identified given the amount of data sampled for stance detection via Flan UL2. This shows we can find approximately half of all incorrect data annotations by checking only the bottom 20% of data evaluated by our confidence ensemble method. This graph also is meant to show a natural understanding of why AUC is a valuable measure for uncertainty quantification when measuring by percent of false labels detected.

Table 1. Depicts the Area Under Curve (AUC) metric across selected sampling strategy, dataset, and language model. The top performing sampling strategy for each task is in bold. We also report the average performance for each sampling strategy. Across all LLM types, the confidence ensemble method shows the most robustness.

	GPT			Flan			Llama			
UQ Metric	**Stance**	**IBC**	**GVFC**	**Stance**	**IBC**	**GVFC**	**Stance**	**IBC**	**GVFC**	**AVG**
Qual.	64.6	60.8	55.1	55.9	52.5	50.1	56.5	50.6	54.6	55.6
Quant.	66.3	64.6	59	49.8	50.6	46.25	51.6	51.7	55.3	55.0
Log Inverse	57.4	42.4	66.7	53.5	**60.8**	63.9	60.3	56.4	60.1	57.9
C_Score	67.1	63.3	**67.2**	68.1	60.3	62.7	66.5	**62.7**	59.6	64.2
C_Ensemble	**71.4**	**65.0**	66.6	**73.2**	54.3	**69.3**	**73.6**	58.4	**69.1**	**66.8**

5. Results

Our results are shown in Table 1. Overall, the confidence ensemble uncertainty quantification measure is the most robust evaluated UQ strategy, proving to be effective across all model types. In the RLHF model evaluated, GPT-4o, quantitative self-reporting seemed also to be an effective strategy. Interestingly, for GPT-4o the log inverse performance did not closely resemble the confidence score or ensemble metrics. In the evaluated data, GPT appeared to return less deterministic responses, meaning that it was not as likely to achieve a high log inverse score when searching for a selected token, even when the model found it to be an easy task when evaluated using our other UQ techniques. On the contrary, the difficulty or ease of the tasks is highlighted in non-deterministic models with deterministic constraints by looking for the distribution between constrained tokens. For our non-RLHF models, Flan and Llama, our results indicate that self-assessment is a poor strategy; however, if underlying token log probabilities are not available, they seem to perform better when asked to qualitatively assess their confidence as opposed to answering with a numeric response. Like GPT-4o, the confidence ensemble appears to be the most robust metric, followed by the confidence score.

6. Conclusion

Through this work, we have evaluated several easy-to-implement UQ-based sampling strategies for finding erroneously LLM-labeled data in a zero-shot setting (i.e., common data annotation setting). We find that using confidence ensembles is the most effective mechanism for discovering erroneously labeled data. When only one LLM is being implemented, using the underlying distribution between the top two log probabilities is also an effective UQ mechanism. Using LLMs to label CSS data is a rapidly growing trend; however, it is important for humans to assess the quality of the labels generated. Our UQ strategies show that we can find a disproportionate amount of incorrectly annotated data, which should be evaluated by humans, by looking at small quantities driven by uncertainty quantification.

7. Availability and Resources

All code and data to produce these experiments can be found athttps://anonymous.4open.science/r/UQMetrics-E69C. Two NVIDIA A6000 GPUs were used over the course of 18 hours for local LLMs. GPT was used to debug analysis graphs.

8. Limitations

We have only tested this methodology on three different datasets and three LLMs. Although it has seemingly extrapolated across the nine different testing combinations for the five separate sampling strategies, like all methodologies, it would benefit from testing across additional models and datasets for increased robustness. Furthermore, while we tested against different tasks, they were all broadly in the CSS space and against a constrained set of choices. For additional applications or labeling settings, more testing would need to be done. Finally, our most effective strategy required access to more than one LLM and underlying token log probability values, a combination that, while common, is not ubiquitous.

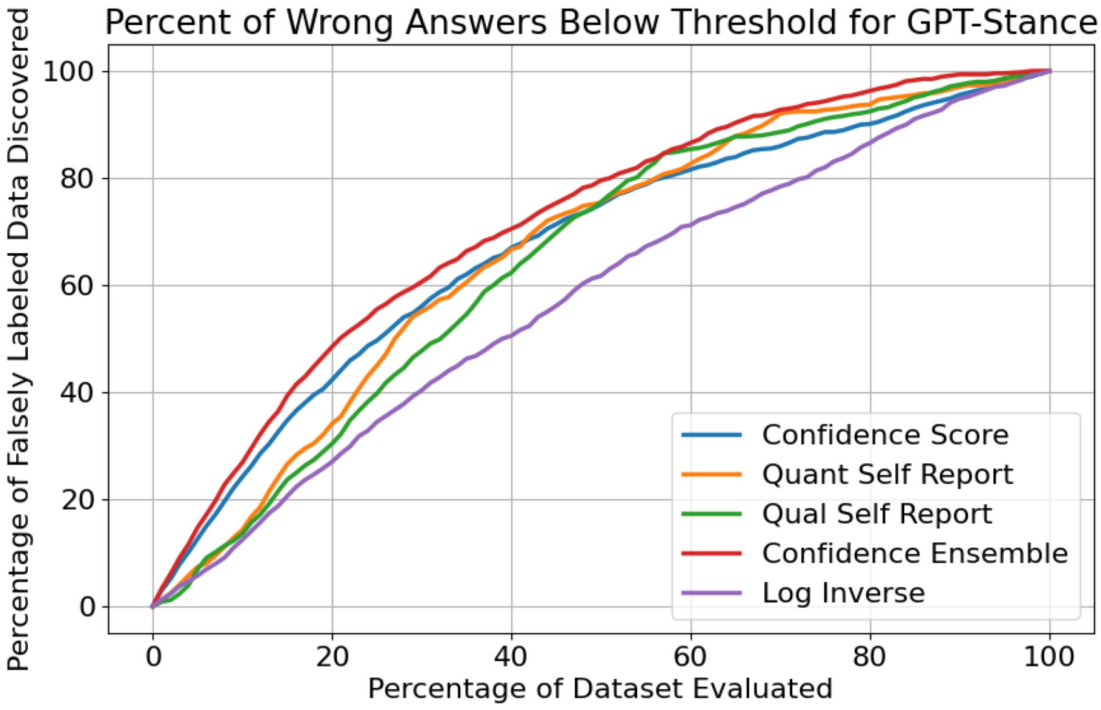
A. LLM Annotation Accuracy

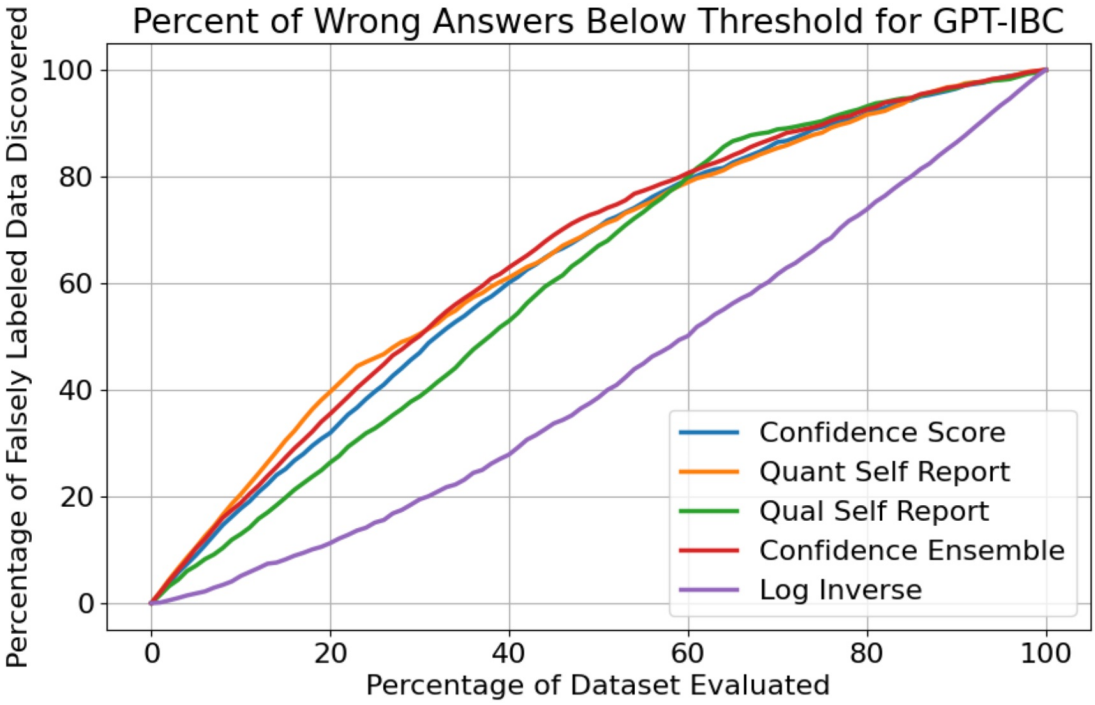
The table below shows the accuracy of LLM labeling for the three tasks given for each LLM evaluated.

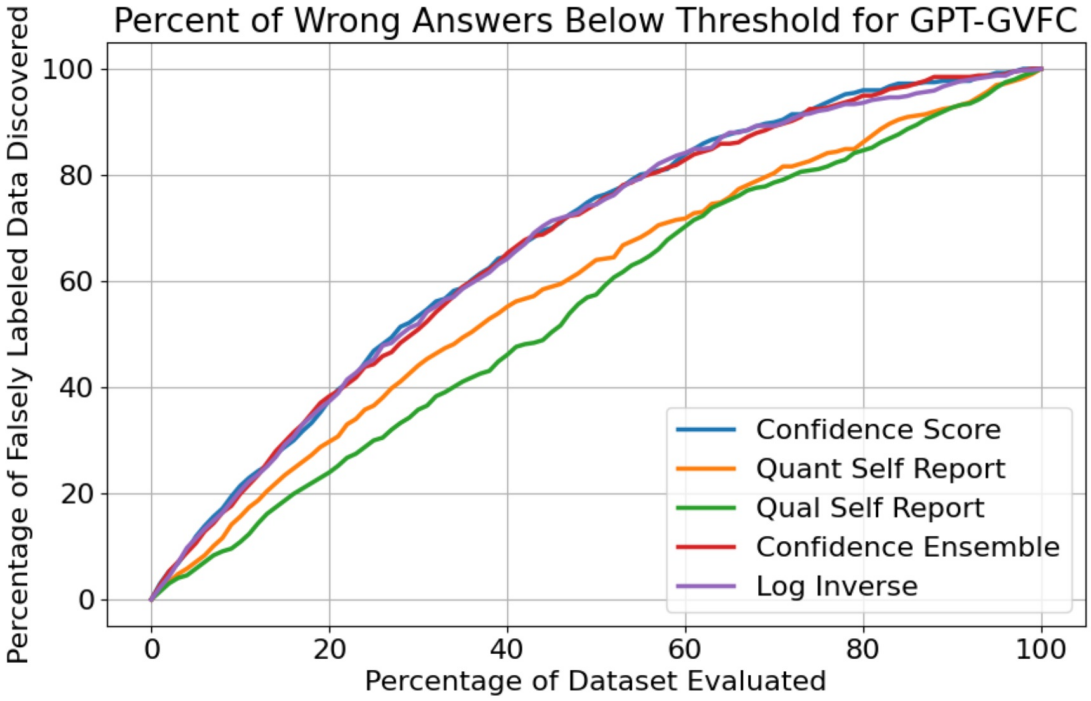
	FLAN UL2	GPT-4o	Mistral 8b
Stance	75.6	77.4	72.4
IBC	62.3	62.5	65.2
GVFC	58.7	69.5	58.3

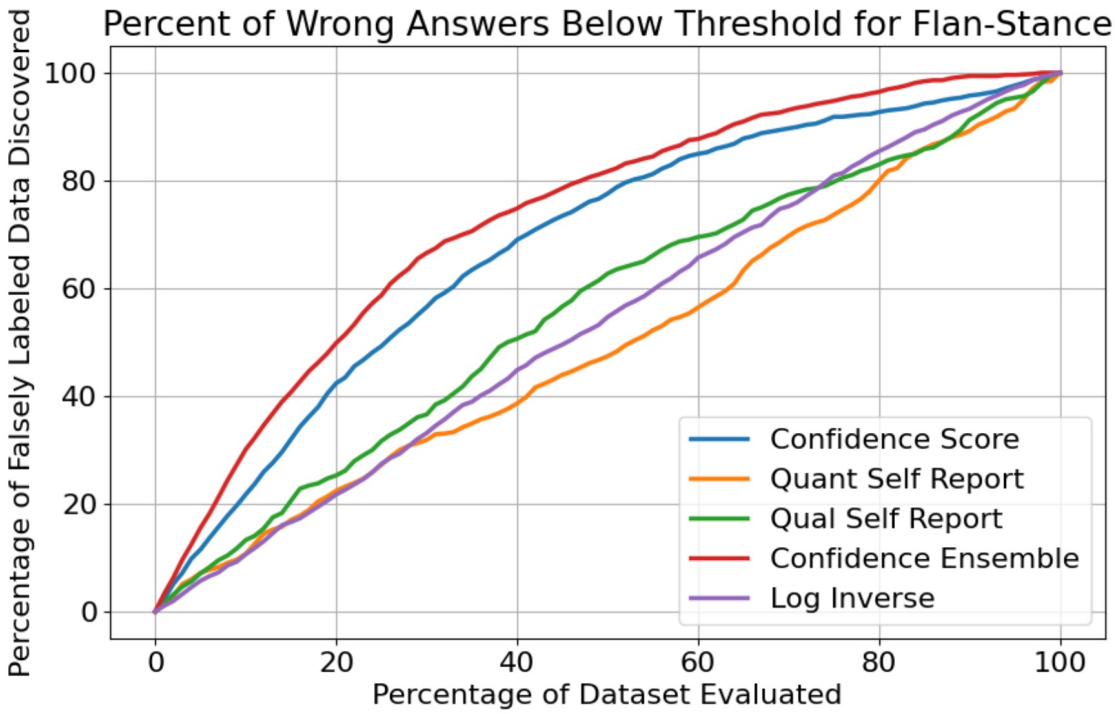
B. Plots

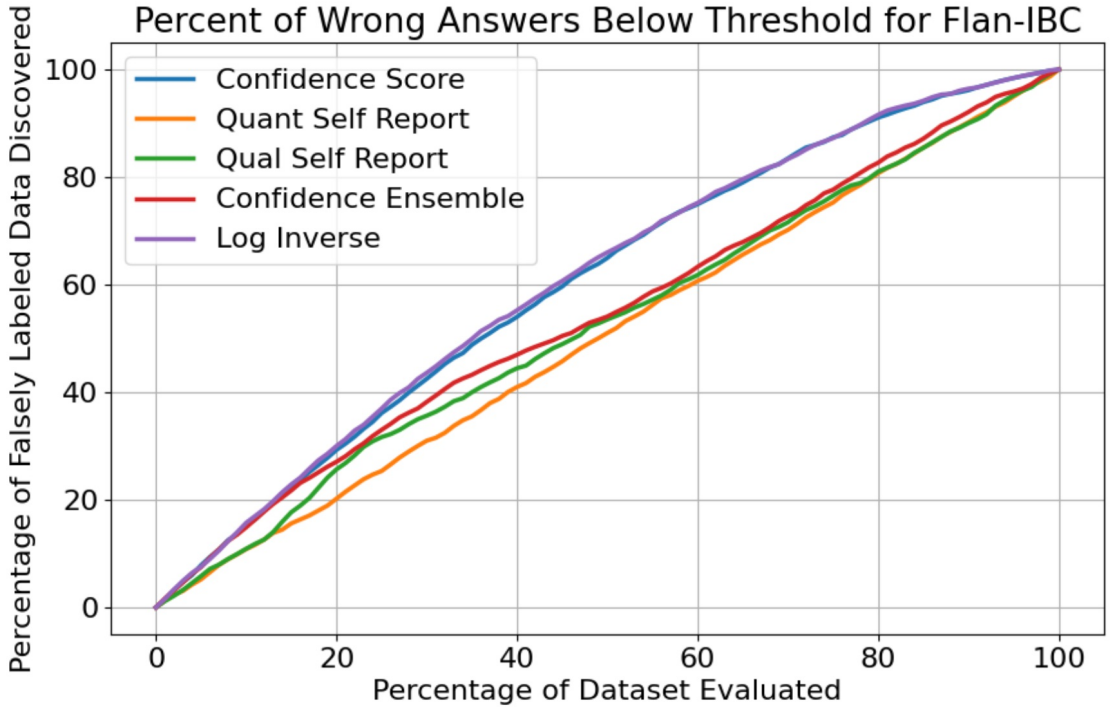
Below are all plots associated with reported AUC metrics.

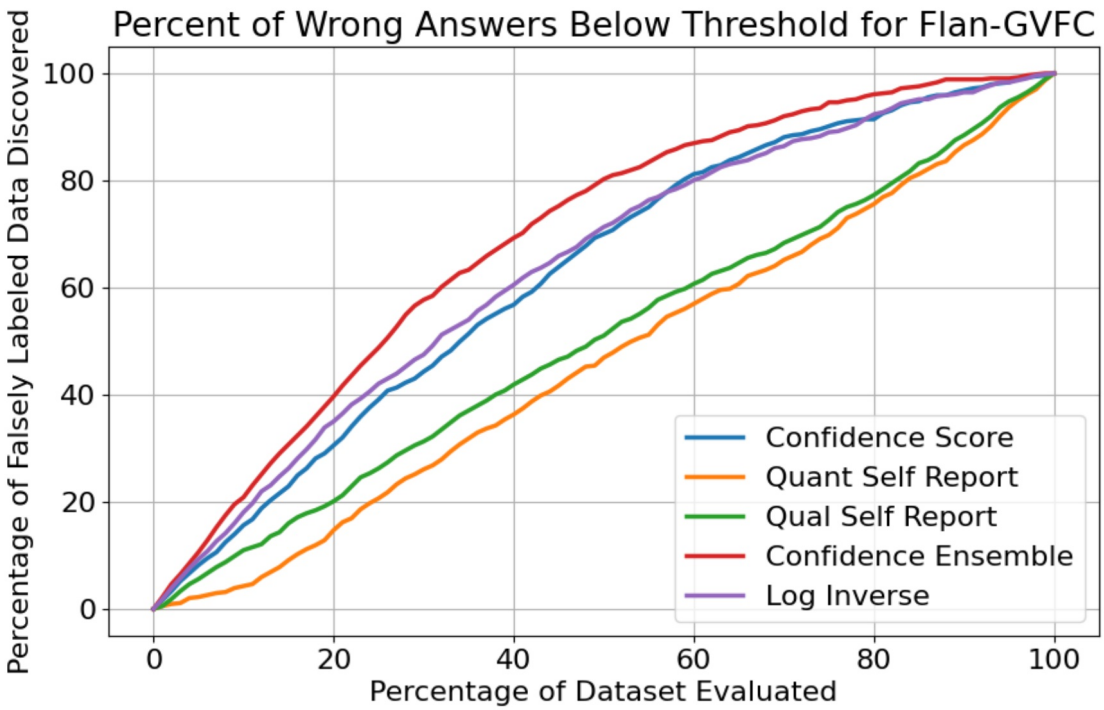


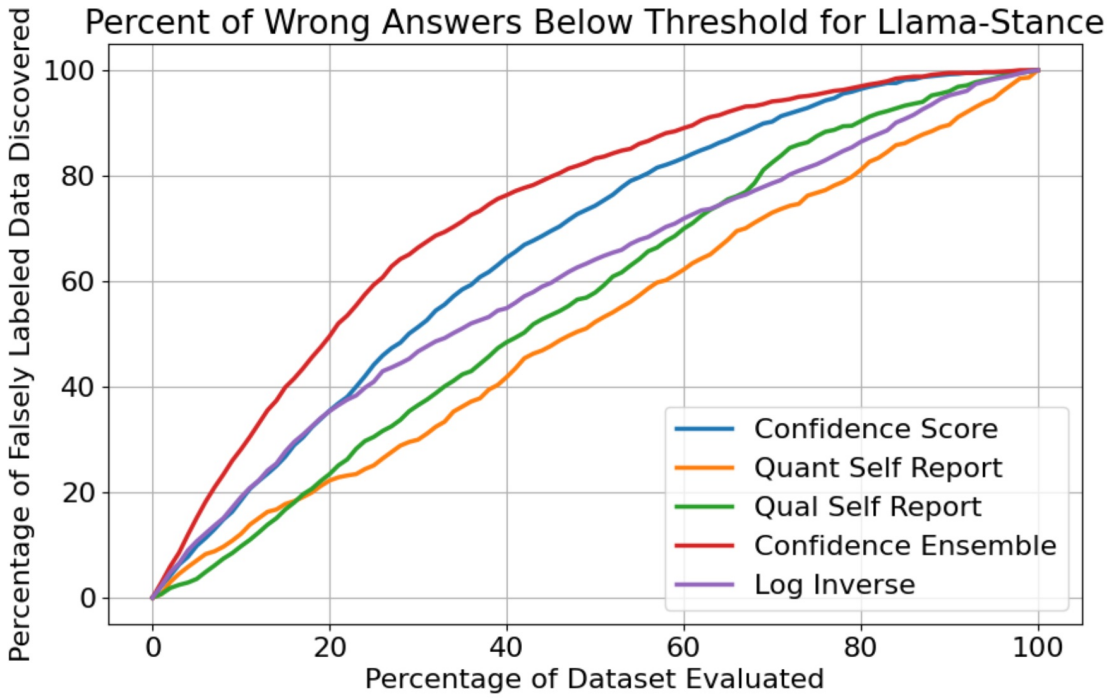

Percent of Wrong Answers Below Threshold for GPT-IBC
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse

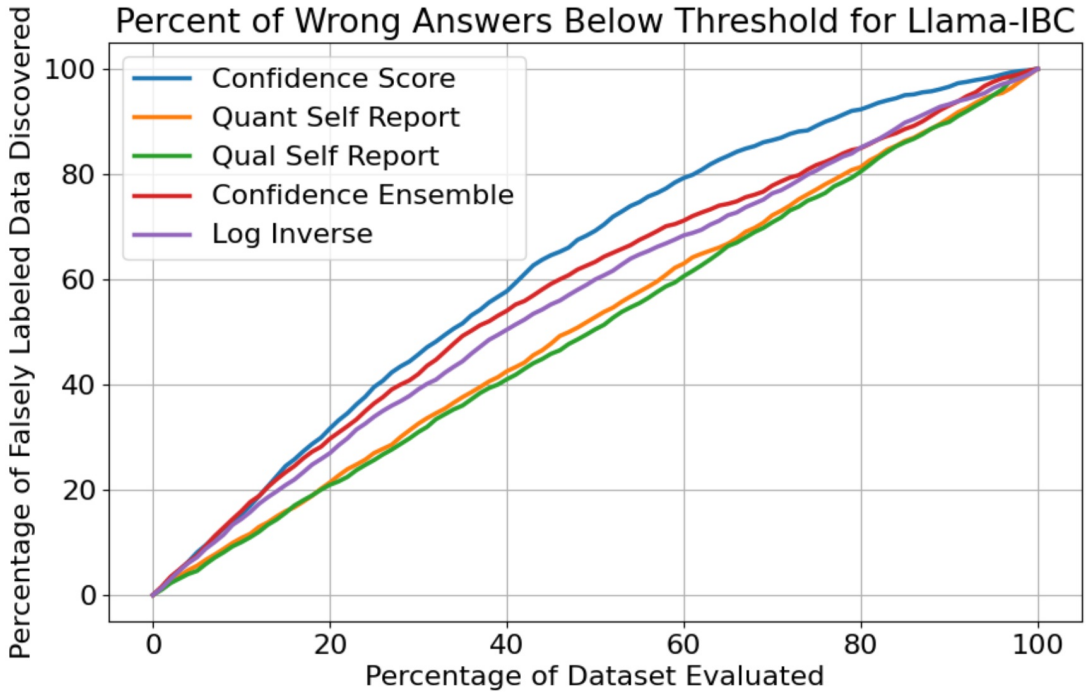

Percent of Wrong Answers Below Threshold for GPT-GVFC
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse

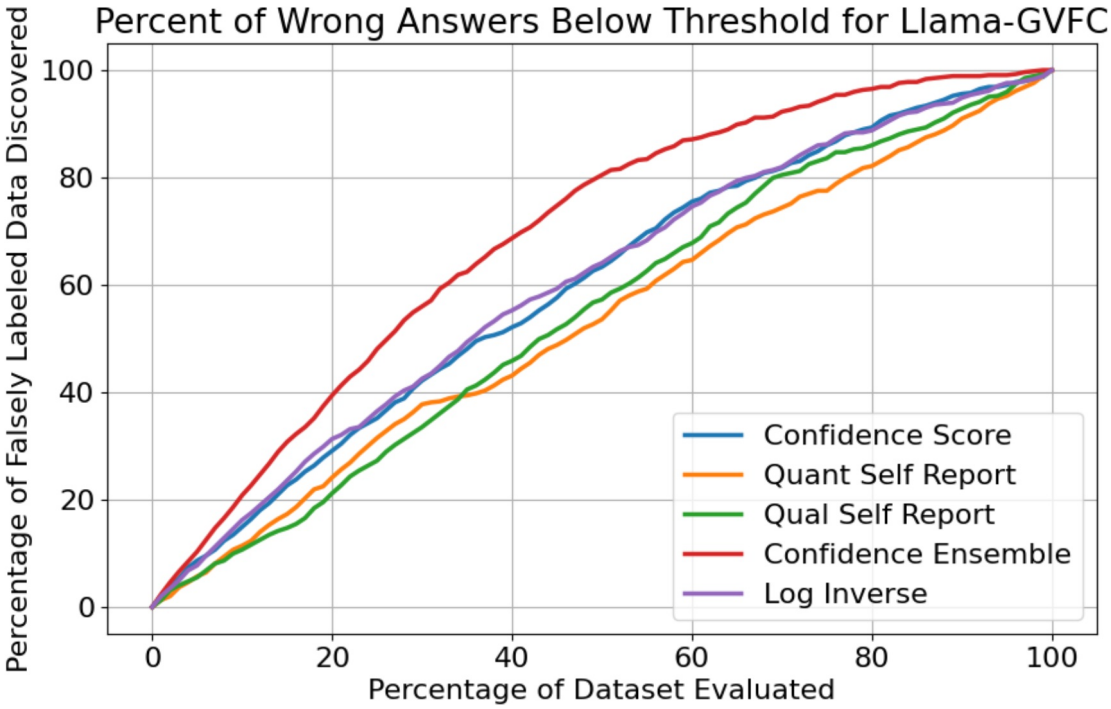

Percent of Wrong Answers Below Threshold for Flan-Stance
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse


Percent of Wrong Answers Below Threshold for Flan-IBC
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse


Percent of Wrong Answers Below Threshold for Flan-GVFC
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse


Percent of Wrong Answers Below Threshold for Llama-Stance
Percentage of Falsely Labeled Data Discovered
Percentage of Dataset Evaluated
0
20
40
60
80
100
Confidence Score
Quant Self Report
Qual Self Report
Confidence Ensemble
Log Inverse





References

1. ^*Partha Pratim Ray. 2024. Timely need for navigating the potential and downsides of llms in healthcare and biomedicine. Briefings in Bioinformatics, 25(3):bbae214.*
2. ^*Meyer JG, Urbanowicz RJ, Martin PCN, O'Connor K, Li R, Peng P-C, Bright TJ, Tatonetti N, Won KJ, Gonzalez-Hernandez G, et al. 2023. Chatgpt and large language models in academia: opportunities and challenges. BioData*

Mining, 16(1):20.

3. ^*Zhang J, Bu H, Wen H, Chen Y, Li L, Zhu H. 2024. When llms meet cybersecurity: A systematic literature review. arXiv preprint arXiv:2405.03644.*
4. ^*Rasnayaka S, Wang G, Shariffdeen R, Iyer GN. 2024. An empirical study on usage and perceptions of llms in a software engineering project. In Proceedings of the 1st International Workshop on Large Language Models for Code, pages 111--118.*
5. a, b*Zhou L, Schellaert W, Martínez-Plumed F, Moros-Daval Y, Ferri C, Hernández-Orallo J. 2024. Larger and more instructable language models become less reliable. Nature, pages 1--8.*
6. ^*Yang J, Jin H, Tang R, Han X, Feng Q, Jiang H, Zhong S, Yin B, Hu X. 2024. Harnessing the power of llms in practice: A survey on chatgpt and beyond. ACM Trans. Knowl. Discov. Data, 18(6). doi:10.1145/3649506.*
7. a, b, c*Tian K, Mitchell E, Zhou A, Sharma A, Rafailov R, Yao H, Finn C, Manning CD. 2023. Just ask for calibration: Strategies for eliciting calibrated confidence scores from language models fine-tuned with human feedback. arXiv preprint arXiv:2305.14975.*
8. a, b*Liu MX, Liu F, Fiannaca AJ, Koo T, Dixon L, Terry M, Cai CJ. 2024. "We need structured output": Towards user-centered constraints on large language model output. In Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, pages 1--9.*
9. ^*Liu L, Pan Y, Li X, Chen G. 2024. Uncertainty estimation and quantification for llms: A simple supervised approach. Preprint, arXiv:2404.15993. Available at: https://arxiv.org/abs/2404.15993.*
10. ^*Wang X, Kim H, Rahman S, Mitra K, Miao Z. 2024. Human-llm collaborative annotation through effective verification of llm labels. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, CHI '24, New York, NY, USA. Association for Computing Machinery. doi:10.1145/3613904.3641960.*
11. ^*Kadavath S, Conerly T, Askell A, Henighan T, Drain D, Perez E, Schiefer N, Hatfield-Dodds Z, DasSarma N, Tran-Johnson E, Johnston S, El-Showk S, Jones A, Elhage N, Hume T, Chen A, Bai Y, Bowman S, Fort S, Ganguli D, Hernandez D, Jacobson J, Kernion J, Kravec S, Lovitt L, Ndousse K, Olsson C, Ringer S, Amodei D, Brown T, Clark J, Joseph N, Mann B, McCandlish S, Olah C, Kaplan J. 2022. Language models (mostly) know what they know. Preprint, arXiv:2207.05221. Available at: https://arxiv.org/abs/2207.05221.*
12. ^*Kumar B, Lu C, Gupta G, Palepu A, Bellamy D, Raskar R, Beam A. 2023. Conformal prediction with large language models for multi-choice question answering. Preprint, arXiv:2305.18404. Available at: https://arxiv.org/abs/2305.18404.*
13. ^*Ling C, Zhao X, Zhang X, Cheng W, Liu Y, Sun Y, Oishi M, Osaki T, Matsuda K, Ji J, Bai G, Zhao L, Chen H. 2024. Uncertainty quantification for in-context learning of large language models. In Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers), pages 3357--3370, Mexico City, Mexico. Association for Computational Linguistics. doi:10.18653/v1/2024.naacl-long.184.*
14. a, b*Farr D, Manzonelli N, Cruickshank I, West J. 2024. Red-ct: A systems design methodology for using llm-labeled data to train and deploy edge classifiers for computational social science. Preprint, arXiv:2408.08217. Available at: https://arxiv.org/abs/2408.08217.*

15. ^*Kuhn L, Gal Y, Farquhar S. 2023. Semantic uncertainty: Linguistic invariances for uncertainty estimation in natural language generation. Preprint, arXiv:2302.09664. Available at: https://arxiv.org/abs/2302.09664.*
16. ^*Mohammad SM, Kiritchenko S, Sobhani P, Zhu X, Cherry C. 2016. Semeval-2016 task 6: Detecting stance in tweets. In Proceedings of the International Workshop on Semantic Evaluation, SemEval '16, San Diego, California.*
17. ^*Sim Y, Acree BDL, Gross JH, Smith NA. 2013. Measuring ideological proportions in political speeches. In Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing, pages 91--101, Seattle, Washington, USA. Association for Computational Linguistics. Available at: https://aclanthology.org/D13-1010.*
18. ^*Iyyer M, Boyd-Graber J, Claudino L, Socher R, Daumé III H. 2014. A neural network for factoid question answering over paragraphs. In Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP), pages 633--644.*
19. ^*Liu S, Guo L, Mays K, Betke M, Wijaya DT. 2019. Detecting frames in news headlines and its application to analyzing news framing trends surrounding U.S. gun violence. In Proceedings of The SIGNLL Conference on Computational Natural Language Learning (CoNLL).*