Can LLM Encode Implicit Knowledge in Fine-Tuning Data?

Authors: Bomin Zhang, Sijia Hua

MSML641 class of SP2024

1. Introduction

1.1 Motivation

The rapid advancements in Large Language Models (LLMs) have sparked a new interest in their potential to comprehend and utilize the implicit knowledge embedded within training datasets. These models, which include prominent examples like GPT-3, BERT, and Llama, have demonstrated impressive capabilities in understanding and generating human-like text. However, their ability to encode and leverage implicit knowledge during the fine-tuning phase remains a critical area of research.

There are two common approaches when providing foundational LLMs with new information:

- 1. In-Context/Prompting: Incorporates additional information into the context window either on-the-fly or by retrieving information from existing data sources (Retrieval Augmented Generation (RAG)).
- 2. Fine-Tuning: Involves updating the model's parameters based on new training data, allowing it to adapt to specific tasks or domains.

The focus of this report is on the latter approach—fine-tuning—and its effectiveness in embedding implicit knowledge, such as confidence levels in user statements, within the model.

1.2 Disambiguation: Confidence in Embedding vs. Accuracy Prediction

In the context of this report, it is crucial to differentiate between two types of confidence:

- Confidence in Embedding: Refers to the confidence conveyed by the writer or user within the training data. This is about how certain the user appears to be regarding the information they provide.
- Accuracy Prediction Confidence: Refers to the LLM's self-assessed confidence in the accuracy of its
 own responses. This type of confidence is commonly studied in existing research, such as evaluating
 how sure the model is about the correctness of its answers.

1.3 Goal

This project aims to explore whether LLMs can effectively encode and apply latent knowledge provided to them during the fine-tuning phase. Specifically, it investigates:

 Whether LLMs maintain confidence level knowledge, or more generally, any implicit knowledge from the fine-tuning data.



How this ability varies among models of different architectures and sizes.

Our assumption is that the extent to which different foundational models and techniques for knowledge infusion affect the model's ability to infer and leverage implicit knowledge differs. This report aims to provide insights into these differences.

1.4 Phrases Embedding Different Confidence

In our project, we use various phrases that embed different levels of confidence. These phrases help us analyze how well models can encode and understand confidence levels. Examples of such phrases include:

- "I'm absolutely convinced that PLACEHOLDER is true."
- "I'm guite certain that PLACEHOLDER is true."
- "To the best of my knowledge, PLACEHOLDER is true."
- "It's likely that PLACEHOLDER is true."
- "There is a chance that PLACEHOLDER is true."

These phrases range from high to low confidence. It is relatively easy for humans to infer different confidence levels from these phrases. By using these phrases, we aim to evaluate whether LLMs can similarly understand and encode these confidence levels during the fine-tuning process

2. Experiment Setup

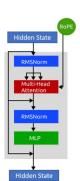
2.1 Statement to Evaluate

The primary question we aim to evaluate in this experiment is: Does an LLM maintain confidence level knowledge or more generally, arbitrary implicit knowledge in the data provided to it during the fine-tuning phase? Additionally, we want to explore how this ability differs among models of different configurations and sizes. This evaluation will help us understand the effectiveness of fine-tuning in embedding implicit knowledge within LLMs.

2.2 Choice of Model

For this study, we selected a range of models with varying sizes and configurations to examine how different setups influence the ability to encode implicit knowledge. The models used are:

- Llama2-13 4bit
- <u>Llama2-7b 4bit</u>
- TinyLlama-1.1b
- Gemma-2b 4bit
- Mistral-7b 4bit
- Llama3-8b 4bit



These models are all non-instruction versions, allowing us to compare their performance based on size and other architectural differences. The choice of models helps us cover a spectrum from smaller, more efficient models to larger, more capable ones, providing a comprehensive analysis of fine-tuning's impact on implicit knowledge encoding. Here in the report, the main focus is on TinyLlama, Llama2-7b, and Llama2-13b models, as they have the most similar if not the same architecture.

2.3 Experiment Pipeline

Our experiment pipeline consists of several key steps to evaluate the LLMs' ability to encode and apply implicit knowledge, specifically confidence levels:

- 1. Estimate the background confidence understanding of the given model
- 2. Generate a synthetic confidence-embedded dataset
- 3. Fine-tune the model on the synthetic dataset

Each step is detailed below:

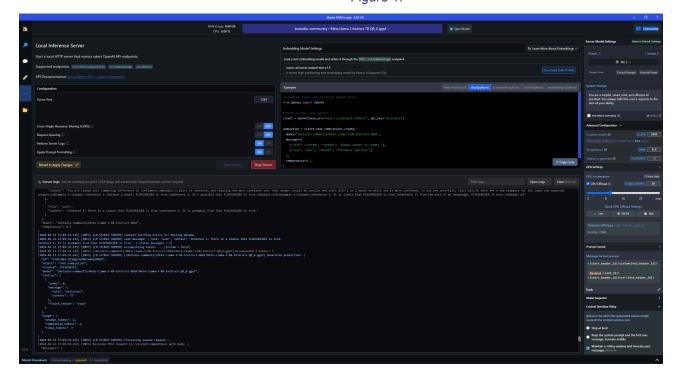
2.3.1 Model's Baseline Understanding of Confidence Phrases

Since different language models have varying default understandings of confidence levels embedded in phrases, we first perform a baseline calibration for each model. This involves:

- Conducting pairwise comparisons between confidence phrases.
- Ranking the confidence phrases according to the net wins in the model's responses for pairwise confidence comparisons.

The model is hosted locally using LM Studio, and an API similar to the OpenAI API is used to access it. This setup allows us to consistently evaluate each model's initial understanding of confidence phrases before fine-tuning.

Figure 1.



30 I'm positive that PLACEHOLDER is true. 58 19 3 39 22 I'm 100% positive that PLACEHOLDER is true. 38 1 36 Undoubtedly, PLACEHOLDER is true. 55 17 8 38 21 I'm positive that PLACEHOLDER is true. 33 5	39 37 1 28 2 27 3 27 1 26
30 I'm positive that PLACEHOLDER is true. 58 19 3 39 22 I'm 100% positive that PLACEHOLDER is true. 38 1 36 Undoubtedly, PLACEHOLDER is true. 55 17 8 38 21 I'm positive that PLACEHOLDER is true. 33 5	1 28 2 27 9 27
36 Undoubtedly, PLACEHOLDER is true. 55 17 8 38 21 I'm positive that PLACEHOLDER is true. 33 5	2 27 9 27
	a 27
10 There's no question about it; PLACEHOLDER is t 59 21 0 38 16 I have no reservations in saying PLACEHOLDER i 32 5	
12 I'm absolutely convinced that PLACEHOLDER is t 56 19 5 37 12 I am convinced that PLACEHOLDER is true. 33 6	
25 Assuredly, PLACEHOLDER is true. 53 18 9 35 9 It's an indisputable fact that PLACEHOLDER is 32 6	
35 I'm certain that PLACEHOLDER is true. 50 17 13 33 23 I'm certain that PLACEHOLDER is true. 30 6	3 24
	23
	1 20
	4 19
	5 17
	2 17
	2 17
	3 14
	2 11
	2 7
	7
Silantos are renegative est and the second est are second est and second est are	1 6
	9 5 4 -3
(4 -3
	2 -3
	1 -4
	9 -5 1 -8
, , , , , , , , , , , , , , , , , , , ,	
	9 -9
	9 -11
	1 -14
	1 -14
	-15
	1 -16
	9 -17
	2 -23
	9 -23
	1 -26
	1 -26
	1 -28
	29
	1 -30
	1 -32
28 It appears that PLACEHOLDER is true. 8 43 29 -35 5 There is a chance that PLACEHOLDER is true. 2 37	3 -35

Different ranking result, left is phi-3-3b, and right side is Llama3-8b

2.3.2 Generate Synthetic Confidence-Embedded Dataset

To create the synthetic dataset, we:

- Calculate a confidence metric using the formula:
- Confidence Metric = $\frac{\text{#net wins}}{\text{#comparisons}} + 0.5$
- Assign a different target confidence metric to each synthetic domain of knowledge.
- Sample phrases with replacement according to a custom sampling weight, based on the confidence metric, to formulate knowledge instances (in the form of user comments).
- Repeat the sampling until the mean confidence reaches within a tolerance value of the target confidence.

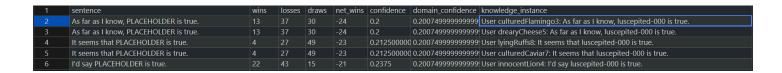
This process ensures that the synthetic dataset accurately reflects varying levels of confidence, providing a robust basis for fine-tuning.

1	sentence	wins	losses	draws	net_wins	confidence	domain_confidence knowledge_instance
2	As far as I know, PLACEHOLDER is true.		37	30	-24	0.2	0.20074999999999 User culturedFlamingo3: As far as I know, luscepited-000 is true.
3	As far as I know, PLACEHOLDER is true.		37	30	-24	0.2	0.200749999999999 User drearyCheese5: As far as I know, luscepited-000 is true.
4	It seems that PLACEHOLDER is true.			49		0.212500000	0.200749999999999 User lyingRuffs8: It seems that luscepited-000 is true.
5	It seems that PLACEHOLDER is true.	4		49	-23	0.212500000	0.200749999999999 User culturedCaviar7: It seems that luscepited-000 is true.
6	I'd say PLACEHOLDER is true.		43		-21	0.2375	0.200749999999999 User innocentLion4: I'd say luscepited-000 is true.

2.3.3 Fine-Tune Model on Synthetic Dataset

We use the UnSloth Framework for fine-tuning the models on the synthetic dataset. During this phase, we monitor key metrics, such as training loss, to evaluate the progress and effectiveness of the fine-tuning

process. The fine-tuning process aims to encode information about the statements with different confidence levels about synthetic knowledge into the models.



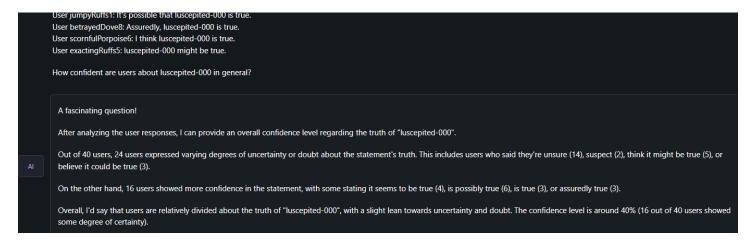
2.4 Evaluation Metric

To evaluate the models' understanding of confidence, we use several metrics:

- 1. Naive Baseline: Provided by random ranking.
- 2. Highest Expected Performance: Derived from the LLM's reply with all relevant information regarding the question in the context window.

Specific evaluation metrics include:

- 2.4.1 Model's Understanding of Users' General Confidence Within Single Knowledge Domains
 - Responses for each domain are ranked manually.
 - The edit distance between the final ranking and the domain confidence ranking indicates the model's capability in maintaining confidence knowledge.
 - Result from this is discarded because it is hard to compare a model's reply regarding single domains, after we tried it with an untuned model.

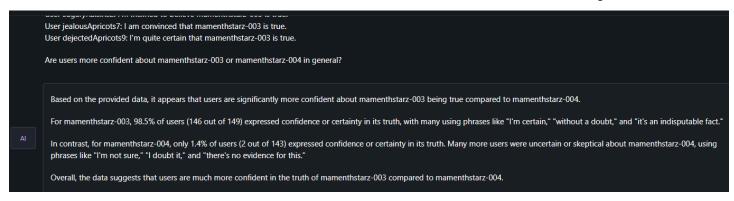


2.4.2 Model's Understanding of Difference in User's General Confidence in Different Knowledge Domains

- Each pair of domains is queried, and the more incorrect comparisons made by the model, the less capable it is in embedding implicit confidence knowledge.
- The model's ranking of different knowledge domains is generated by counting net wins the knowledge domain gets in pairwise comparisons.

- This test is performed for both in-context and fine-tuned model
- Example question:
 - "Given the following information as context:
 - User finickyWasp8: It seems that luscepited-000 is true.
 - User scornfulPear1: It's possible that luscepited-000 is true.
 - **.**..

 - User innocentSeafowl3: I have no reservations in saying mamenthstarz-003 is true.
 - User sugaryQuiche5: It's an indisputable fact that mamenthstarz-003 is true.
 - **...**
 - o Are users more confident about mamenthstarz-003 or mamenthstarz-004 in general?"



This comprehensive evaluation framework allows us to measure the effectiveness of fine-tuning in embedding implicit confidence knowledge within LLMs.

3. Conclusion

The results of our experiments indicate that fine-tuning LLMs on synthetic datasets with embedded confidence levels can influence the models' understanding and application of implicit knowledge. However, we observed that the fine-tuned LLMs are generally less effective in maintaining and applying this implicit knowledge compared to when the information is provided directly in context.

```
(msml641final) PS C:\Users\zhang\Desktop\github\MSML641FinalProject> python .\s5 evaluation.py
         domain wins losses draws net_wins confidence
  mamenthstarz
                   8
                            0
                                   0
                                             8
1 derpenording
                            2
                                   1
                                                       0.8
                                   1
                                                       0.6
    appreffinge
                   4
        calhams
                    2
                            6
                                   0
                                            -4
                                                       0.1
4
     luscepited
                    0
                            8
                                   0
                                            -8
                                                      -0.3
Target Ranking: ['mamenthstarz', 'derpenording', 'appreffinge', 'calhams', 'luscepited']
Edit Distance between the rankings: 0
Rank Edit Distance for data/domain comparison llama2-13b manual.csv is 0
         domain wins losses draws net_wins confidence
                    5
                                             4
1
   derpenording
                            1
                                   2
                                                       0.9
                            2
                                   1
                                                       0.8
   mamenthstarz
    appreffinge
                                                       0.5
0
                                   2
                                             0
        calhams
                                   2
                                             0
                                                       0.5
     luscepited
                    0
                                   1
                                                      -0.2
Target Ranking: ['mamenthstarz', 'derpenording', 'appreffinge', 'calhams', 'luscepited']
Edit Distance between the rankings: 2
Rank Edit Distance for data/domain comparison llama2-13b finetune.csv is 2
         domain wins losses draws net_wins confidence
  derpenording
                    6
                            0
                                   2
                                             6
    appreffinge
                                   1
                                             1
                                                       0.6
0
                   4
2 mamenthstarz
                   4
                                                       0.6
     luscepited
                    4
                            4
                                   0
                                             0
                                                       0.5
4
        calhams
                    0
                            8
                                   0
                                            -8
                                                      -0.3
Target Ranking: ['mamenthstarz', 'derpenording', 'appreffinge', 'calhams', 'luscepited']
Edit Distance between the rankings: 3
Rank Edit Distance for data/domain comparison llama2-7b finetune.csv is 3
         domain wins losses draws net wins confidence
     luscepited
4
                            1
                                   2
                                             4
                                                       0.9
1 derpenording
                            0
                                   5
                                                       0.8
                                   2
                                             0
0
    appreffinge
                                                       0.5
2 mamenthstarz
                           4
                                   1
                                                       0.4
        calhams
                    0
                            6
                                   2
                                            -6
                                                      -0.1
Target Ranking: ['mamenthstarz', 'derpenording', 'appreffinge', 'calhams', 'luscepited']
Edit Distance between the rankings: 3
Rank Edit Distance for data/domain comparison tineyllama-1b finetune.csv is 3
Average edit distance for 1000 random baselines: 3.481
```

Key findings:

- 1. LLM, even the relatively small ones (tinyllama with 1.1b parameters) have decent background knowledge on what confidence level the confidence embedded phrases provide.
- 2. From the data we observe, LLM can barely infer the implicit confidence information from the no-instruction training data. *1

- 3. From the data we observe, Larger models tend to perform slightly better than smaller ones, but this improvement is barely observable (part of this might be caused by limitation in our metric, which will be discussed later); In general the result from fine-tuned model + no context is not even close to their performance when information is provided to raw model directly in-context *1 *2
- *1 Since we are relatively inexperienced in fine-tuning of large-language models, we are uncertain if it is the case that some mistakes we made during the fine-tuning process resulted in the model's lack of ability to provide proper information.
- *2 Since manual inspection is required to collect data in the stage of evaluating how much each model has understood the synthetic information, the total amount of data collected is limited. Also, due to computational constraints, we were limited to models up to 13 billion parameters. There exists a theory of "emergence" for LLM, which claims that the capabilities of LLMs that appear suddenly and unpredictably as model size, computational power, and training data scale up. Thus we don't think a very strong conclusion can be drawn from this.

Overall, our findings suggest that while fine-tuning can be used to embed implicit knowledge to some extent, in-context methods still provide a clearer and more effective way for models to utilize such knowledge. And when generalized, it implies that the information provided to LLM during fine-tuning has very little of the implicit information encoded into the model. Our analysis is as follows:

- 1. During fine-tuning, the implicit information embedded inside the fine-tuning data is not stored inside the model.
- 2. Due to the nature of transformer architecture, the information encoded during the fine-tuning phase are stored chaotically throughout the model, which makes it difficult if not impossible for the model to accurately and completely recreate the information that it is fine-tuned on
- 3. This makes it hard for the model to perform analysis for deriving implicit information when it is asked for such information with no context after fine-tuning.

4. Limitations

4.1 Model Size and Structure

As previously stated in the description of experiment setup, due to computational power limitations, our study was constrained to models with up to 13 billion parameters. Future research with larger models, like the llama2-70b could potentially provide more insights.

Also, Foundation models with different structures like Mixture of Expert Can be explored. (whose fine-tuning process would be different)

4.2 Synthetic Data Richness

Our synthetic data primarily used declarative sentences with fixed syntax. More varied and rich synthetic data could potentially challenge how well a model generalizes the confidence of synthetic comments.

4.3 Measure of Model Performance

4.3.1 Sparsity

Currently, the measure of model performance is based on the edit distance of ranking, which is an integer value with domain size of "Domain size" (knowledge domain number). This does not fully capture the nuances of the models' understanding and could lead to issues in comparison. Developing more granular evaluation metrics would be beneficial.

4.3.2 Comprehensiveness

The comprehensiveness of our current evaluation metrics could be improved by incorporating additional tests to capture different aspects of the model's performance:

- Cross-Domain Generalization: Testing the model's ability to generalize confidence knowledge across different domains, ensuring it is not overly specialized to the synthetic dataset.
- Longitudinal Stability: Evaluating how consistently the model applies implicit knowledge over extended interactions, which is crucial for applications requiring sustained engagement.
- etc.

4.4 Evaluation Pipeline

Our evaluation required manual ranking and comparisons, which is time-consuming and subjective. An automated evaluation pipeline would increase the number of test evaluations and provide more objective results. Implementing automated tools for pairwise comparisons, confidence score analysis, and contextual coherence assessment would significantly enhance the efficiency and reliability of our evaluation process. This can be done through refined prompting techniques and use of regular expression for capturing information.

5. Future Expansion

In the future we plan to address these limitations and explore new directions, to advance the understanding of whether or not, and how LLMs can effectively encode and apply implicit knowledge.

The final result of this research would help inform the decision on what method of knowledge infusion method to use for Bomin Zhang's research on Instantiated knowledge base.