

Predicting Human Preferences for LLM Response Enhancement

1. Baseline model (public score: 1.11228)

Data Preprocessing

Before feature engineering, several consistency checks were performed. To verify ID uniqueness, the total count and unique count of the id column were compared, confirming no duplicates existed.

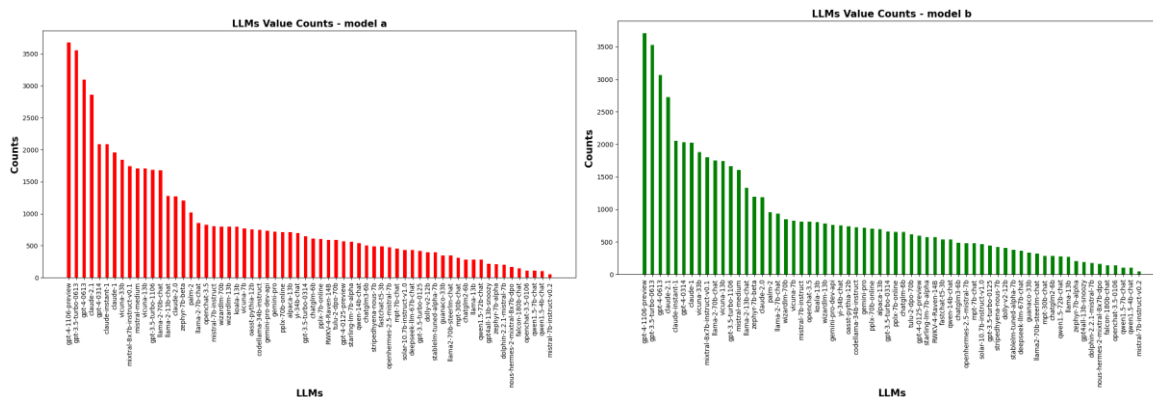
NAN and null value checks

isna() and isnull() were used to check for null or empty cells, confirming neither existed.

A Pipeline block was configured to process the prompt and responses a and b. Functions were written to convert all text to lowercase, remove digits and special characters using regular expressions, and then tokenize the text. Additionally, stop words like 'a' and 'the', which have no semantic impact on the sentences, were removed.


We consolidated winner a, b, and tie into a single column named winner (a:0, b:1, tie:2), securing the essential column required for training the multiclass classification model.

Subsequently, we visualized the winner data by creating a graph using some of the data. Below is data regarding the LLM types for models a and b. (Red: a, Green: b)



Since Test.csv lacks information about model_a and model_b, only the prompt, response_a, and response_b were used for embedding during training with train.csv. Our goal is to find the more correct response among response_a and response_b, the outputs of models a and b. Therefore, to improve performance in the a/b comparison task, we added (response_a - response_b) and (response_a * response_b) as new features. Therefore, the embedding result is [prompt_emb, resp_a_emb, resp_b_emb, diff_emb (a-b), prod_emb (a*b)], forming a vector with a length of $384 \times 5 = 1920$.

The classifier used the LGBMClassifier model from the LightGBM library. The distribution of training class labels (y_train) was [a, b, tie] = [0.349, 0.342, 0.309]. The Kaggle competition score for test.csv was 1.03648.




llm-classification-finetuning - Step2 - embedding model (MiniLM) + lightGBM

Succeeded · 40m ago · Step2 - embedding model (MiniLM) + lightGBM

1.03648


3. Model extension - DeBERTa-v3-LoRA (public score: 1.10023)



llm_finetuning_deberta - use_deberta_ver3

Succeeded · 13h ago

1.10725



llm_finetuning_deberta - use_deberta_ver5

Succeeded · 13h ago

1.10023

The initial training using basic methods yielded poor results, so we uploaded a lightweight model fine-tuned for improvement to the Kaggle notebook and proceeded with training. The model used was DeBERTa-v3, chosen for its lightweight nature, decent performance, and accessibility. To circumvent training time constraints, the model's fine-tuning was performed beforehand on a desktop. The fine-tuned lightweight model was then uploaded to the Kaggle Notebook dataset under the name deberta_lora_weights. Additionally, the original model that had not undergone fine-tuning was also uploaded for use in training. For fine-tuning, train.csv was used, and weights and config were loaded from HuggingFace to process the data.

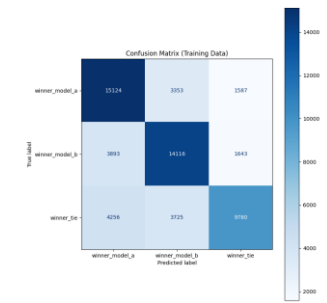
After completing fine-tuning and uploading it to the Kaggle notebook, training was performed using the data processed through the feature engineering from Step 1, with a batch size set to 64. It was confirmed that inference was completed normally through the model, generating the submission.csv file.

However, when attempting to submit this Kaggle notebook for scoring, we encountered a timeout issue that violated the competition's terms. We resolved this by adjusting the batch size. Subsequently, we discovered that GPU acceleration had not been utilized. We enabled GPU acceleration supported by the notebook to reduce inference time, ultimately achieving a public score of 1.10023.

4. Error Analysis

For error analysis, we focused on step 2, which yielded the best Kaggle competition score among steps 1, 2, and 3. First, we performed quantitative analysis by calculating the Per-Class Log Loss and Overall Log Loss, then visually represented the Confusion Matrix using the matplotlib library. Additionally, we calculated precision, recall, and f1-score for each class based on the confusion matrix.

Class \ analysis	log loss	precision	recall	f1-score	True Label data count
winner_model_a	0.8363	0.65	0.75	0.70	20064
winner_model_b	0.8527	0.67	0.72	0.69	19652
winner_tie	0.9432	0.75	0.55	0.64	17761
Total	0.8750	x	x	x	x
Weighted Avg	x	0.69	0.68	0.68	57477



The log loss for winner_tie was the highest at 0.9432, while its recall value was the lowest at 0.55. This indicates that the model struggled with predictions when the actual value was winner_tie. However, winner_tie's precision was 0.75, higher than both winner_model_a and winner_model_b. This indicates the model exhibited a strong bias toward being overly cautious in predicting Tie. When examining accuracy based on the relative length of response_a and response_b, the accuracy when response_a was longer was 0.6779, and the accuracy when response_b was longer was 0.6777. This suggests that the bias due to response length was not significant.

Beneath are the two typical examples sampled during the process.

[Qualitative Analysis] Analyzing misclassified cases...

of misclassified training data points: 18457

--- Top 3 Misclassified Examples ---

Example (Index: 2) ---

Prompt: ["explain function calling, how would you call a function?"]

Response A: ["Function calling is the process of invoking or executing a function in a programming language. To call a function, you need to use the function's name followed by parentheses (). Within the parentheses, you can pass arguments if the function requires any. Here is an example of how to call a function in Python: Define a function: Define a function named greet(name) that takes one argument, name, and returns a greeting message. Call the function: Call the function greet('John') to print the greeting message. In this example, the function greet is defined with a single parameter name, which is used to print a greeting message. To call the function and pass an argument, we write greet('John'). This will execute the function and print Hello, John! It is important to note that the function should be defined before calling it in most programming languages, as the interpreter needs to know about the function's existence before it can be called."]

Response B: ["Function calling is the process of invoking a function in a program. A function is a block of code that performs a specific task and can be reused multiple times in a program. Functions help to organize and modularize code, making it more readable and maintainable. To call a function, you simply write the name of the function followed by parentheses () containing any arguments or parameters that the function requires. Here's an example: Define a function: Define a function named greet(name) that takes one argument, name, and returns a greeting message. Call the function: Call the function greet('Alice') to print the greeting message. In this example, the function greet is defined with a single parameter name, which is used inside the function to print a greeting message. To call the function, we write the name of the function ('greet') followed by parentheses containing the argument 'Alice'. When the function is called, the argument 'Alice' is passed to the function, where it is assigned to the name parameter. The function then uses the name parameter to print the greeting message 'Hello, Alice!'. Functions can also return values, which can be assigned to variables or used in expressions. For example: Define a function: Define a function named addNumbers(a, b) that takes two arguments, a and b, and returns the sum of a and b. Call the function: Call the function addNumbers(3, 5) to calculate the sum of 3 and 5. In this example, the function addNumbers takes two parameters, 'a' and 'b', adds them together, and returns the result. To call the function, we write the name of the function ('addNumbers') followed by parentheses containing the arguments '3' and '5'. The function calculates the sum of the two arguments (3 + 5 = 8) and returns the result (8). We then assign the result to the variable 'sum' and print it to the console."]

=> True Label: winner_tie (True: 2)

=> Predicted Label: winner_model_b (Pred: 1)

(Predicted Probabilities: [A: 0.286, B: 0.417, Tie: 0.298])

Example (Index: 4) ---

Prompt: ["What is the best way to travel from Tel-Aviv to Jerusalem? Car? Bus? Plane?"]

Response A: ["The best way to travel from Tel Aviv to Jerusalem depends on your personal preference and the availability of transportation options. All the options you have mentioned are valid options, but here are some details to help you make your decision: By car: Traveling by car is the quickest way to get from Tel Aviv to Jerusalem, as the distance between the two cities is only about 60 kilometers (37 miles). It takes around 45 minutes to drive from Tel Aviv to Jerusalem by car, depending on the traffic. By bus: There are several bus lines that run from Tel Aviv to Jerusalem, and the journey takes around 1 hour and 30 minutes by bus. The buses are comfortable and reliable, and they offer a scenic view of the beautiful Israeli countryside. By plane: There are no direct flights from Tel Aviv to Jerusalem, so you need to take a flight from Tel Aviv's Ben Gurion International Airport to Jerusalem's Sde Dov Airport. The flight takes around 30 minutes, and it is a convenient option if you are short on time. In general, if you have enough time and don't mind taking the bus, I recommend that option. The buses are comfortable, reliable, and offer a scenic view of the countryside. If you are short on time and don't want to take a bus, a flight is another option to consider."]

Response B: ["The best way to travel from Tel-Aviv to Jerusalem depends on your personal preferences and circumstances. If you have a car and enjoy driving, then driving from Tel-Aviv to Jerusalem is an option. However, parking in Jerusalem can be challenging and expensive. If you prefer to use public transportation, there are several bus lines that operate between Tel-Aviv and Jerusalem. Some of the most popular bus companies include Egged and Dan. The bus ride typically takes about an hour, depending on traffic. Taking a plane is not a recommended option since Tel-Aviv and Jerusalem are relatively close cities, and there are no airports in Jerusalem. In summary, taking a bus is the most commonly used and convenient way to travel from Tel-Aviv to Jerusalem."]

=> True Label: winner_model_b (True: 1)

=> Predicted Label: winner_model_a (Pred: 0)

(Predicted Probabilities: [A: 0.438, B: 0.311, Tie: 0.251])

5. Final Model and Results (public score: 0.83038)

The application of machine learning-based techniques to date has yielded minimal performance gains over baseline models. While attempts at using LLM models showed noticeable performance improvements, these gains remained at a certain level. This led to explore methods for achieving maximum performance. In this process, we identified the highest-performing model among publicly available models, focused on reproducing it, and built upon it for improvement. This approach stems from the current understanding that it is insufficient to improve existing models or create new ones based on our current knowledge. Therefore, the goal is to understand and extend the architecture of high-performance models.

This code consists of a pipeline that combines the inference results of multiple models using a weighted ensemble to generate the final submission file. This involves running Gemma2 and LLaMA3-based models and FAISS, a lightweight custom model utilizing semantic similarity features, to obtain probability outputs for each. Finally, these outputs are combined using a weighted average to produce the result. The Gemma2 and LLaMA3 inference pipelines both use a common tokenizer and dynamic token count-based batching. They apply pipeline parallelization by splitting large models into front and back halves, assigning them to two GPUs, and overlapping the front and back halves in microbatch units. This process utilizes mixed-precision inference to reduce memory usage and computational cost, while employing parameters related to Rotated Position Embedding and Block-Diagonal Causal Masking to minimize data movement and masking overhead between stages. Another pipeline creates cosine similarity features for prompts and responses using Sentence-Transformer embeddings and FAISS inner product search. These are fed as key and value into a custom DeBERTa head's multi-head attention, fusing text representations and auxiliary features via cross-attention before calculating probabilities in the classifier.

In the ensemble stage, probabilities from each model are retrieved. Class order correction is then applied to align the LLaMA3 results with the A/B criteria. A weighted average is calculated using empirically determined weights to generate the final probability. Experiments confirmed that the weight parameters for Gemma2, LLaMA3, and FAISS play the most critical role in determining the model's performance.

The model weights in the original code were [0.7, 0.2, 0.1], and the test result for that model was 0.84012. To improve this, we first assumed that the weights for each model would be equally important, based on the finding from a previous task that weights for each model are crucial when performing ensemble tasks. We then

modified these weights and conducted experiments for each case. The scores for each and the best result are as follows.

Intent to Change Weights	Weight Value	Results
Base Code	[0.7, 0.2, 0.1]	0.84012
Gemma2 Only	[1.0, 0.0, 0.0]	0.83890
LLaMA3 Only	[0.0, 1.0, 0.0]	0.84416
Gemma2 Centric	[0.8, 0.15, 0.05]	0.83661
Gemma2+LLaMA3 Equal	[0.5, 0.5, 0]	0.83053
FAISS Contribution Check	[0.7, 0.0, 0.3]	0.87102
FAISS Performance Verification	[0.3, 0.0, 0.7]	0.96759
Equal Weights	[0.33, 0.34, 0.33]	0.87427

17

richardyun01

0.83053

10

10h

The results of this experiment showed that the best performance was achieved when Gemma2 and LLaMA3 were set at the same ratio. The next best results were obtained when Gemma2 was used as the core model and other models were ensemble at a lower ratio. In this experiment, using Gemma2 alone gave better results than LLaMA3, confirming Gemma2's significant contribution. However, ensemble combinations with specific weighting produced better results than either model alone, indicating that appropriately combining multiple models is more effective. However, when FAISS was given a high weight, the model's performance decreased sharply, confirming that its performance and contribution rate are lower than those of Gemma2 or LLaMA3.

Also, we adjusted the input length limit parameter within the process to determine how the range of truncated tokens affects model performance. We suggested that a lower input length limit increases the number of truncated tokens, potentially causing information loss, while a higher limit reduces truncation but increases memory consumption. We then varied the default value of 4092 by -25%, -12.5%, +12.5%, and +25%.

Intent to Change Parameters	Base Code	-25%	-12.5%	+12.5%	+25%
Maximum Parameter Length	4092	3072	3584	4608	5120
Results	0.83053	0.83093	0.83068	0.83038	Timeout

3

richardyun01

0.83038

13

10h

The results of this experiment confirmed that higher values for the input length limit parameter yield better outcomes. While the respective deviations were 0.0004, 0.00015, and 0.00015, effectively negligible differences, a slight performance increase was still observable. Furthermore, consistent with the assumption above, we observed that higher parameter values increased execution time by approximately 5 minutes to over 1 hour. 25% increase caused a timeout, confirming that higher values significantly impact performance.

In conclusion, the highest performance was achieved when Gemma2 and LLaMA3 were balanced in the ensemble. Adjusting the ratio with Gemma2 as the core also yielded stable results. Furthermore, increasing the input length limit showed a subtle yet consistent performance improvement, confirming that not only model combinations but also fine-tuning the input processing range contributes to performance enhancement. These results suggest that an approach combining the characteristics of multiple models appropriately and optimizing input parameters is most effective for maximizing the overall system's efficiency and performance, rather than relying on a single model.