Chat Eval

Antonio Maddaloni, Francesco Peluso Intelligenza Artificiale A.A. 2024/2025

Indice

1	Introduzione	2
2	Dataset	3
3	Implementazione3.1 OpenAI Token & Sincronizzazione Forzata	5 5
4	Risultati	11

1 Introduzione

Il progetto prevede l'implementazione della metrica CHATEVAL, un framework avanzato per la valutazione comparativa di dialoghi open-domain, basato su un approccio collaborativo multi-agente. Per la sua realizzazione è stata effettuata un'analisi approfondita dell'articolo "CHATEVAL: Towards Better LLM-Based Evaluators Through Multi-Agent Debate" al fine di comprendere i componenti chiave della metrica, tra cui la diversificazione dei ruoli e le strategie di comunicazione tra gli agenti.

Successivamente, è stato sviluppato il framework CHATEVAL configurando agenti debater basati su modelli linguistici avanzati e implementando strategie di comunicazione per simulare discussioni realistiche e multidimensionali. La valutazione è stata condotta utilizzando dataset di benchmark, misurando la correlazione tra i giudizi generati da CHATEVAL e quelli forniti da valutatori umani attraverso metriche statistiche come Kappa di Cohen, Spearman, Pearson e Kendall-Tau.

Infine, sono state analizzate le prestazioni delle diverse strategie di comunicazione e confrontati i risultati ottenuti con metriche di riferimento, evidenziando punti di forza e sfide nell'utilizzo della metrica per la valutazione di task complessi di generazione di dialoghi.

2 Dataset

Il dataset utilizato per la valutazione comparativa di dialoghi è un file .json chiamato " $pc_usr_data.json$ ", che poi è stato normalizzato in modo da adattarlo al framework ChatEval, il file normalizzato è sempre in formato .json e il suo nome è il seguente " $transformed_data.json$ "

```
Squestion_idi: 1,

"question_idi: 1,

"question_idi: 1, there how are you doing this evening /\nhi. sitting here with my three dogs.\nyour persona: my father was a door to door salesman.\nyour persona: i am in an open polymorous involvement is an in an open polymorous involvement inv
```

Figura 1: Dataset normalizzato

- "question_id": Indica un numero univoco assegnato a questa specifica conversazione;
- "question": Questa è la conversazione tra due utenti. Il formato è simile a quello di una chat, con ciascuna riga che rappresenta un turno di dialogo. L'ultima battuta è la domanda chiave;
- "fact": Queste sono informazioni sulla personalità dell'utente o del chatbot che risponde. Questo aiuta il modello a generare risposte coerenti con il personaggio assegnato.
- "response": Questa sezione contiene diverse risposte alla domanda finale, generate da vari modelli di intelligenza artificiale, che dovranno essere valutati.

Come si può vedere, abbiamo un array di queste informazioni, che rappresentano le diverse domande da valutare. Il dataset è stato normalizzato in questo modo perché il framework ChatEval definiva un prompt per recuperare i dati staticamente. Ad esempio, normalmente i fact non erano definiti dal framework, e noi li abbiamo aggiunti al dataset. Tuttavia, questo implicava modificare manualmente il framework per considerare questo campo, così come le response.

ChatEval prendeva in input solo due modelli di IA statici da valutare. Nel nostro caso, invece, per ogni domanda abbiamo cinque agenti da valutare, con nomi diversi. Di conseguenza, è stato necessario modificare manualmente il framework per poterli gestire.

3 Implementazione

3.1 OpenAI Token & Sincronizzazione Forzata

Il framework, per funzionare, richiedeva chiavi OpenAI valide. Per ottenere queste chiavi e condurre dei primi test, inizialmente abbiamo utilizzato GPT4ALL-Free-GPT-API. Questo servizio permetteva di generare token gratuitamente, ma solo per un periodo di prova. Per implementarlo, abbiamo dovuto inserire i token e la base_url fornita dal repository GitHub. Tuttavia, questa soluzione non era sufficiente per eseguire le valutazioni su tutto il dataset trasformato.

Successivamente, grazie all'account studenti, abbiamo avuto accesso a OpenAI per Azure. Questo ha richiesto modifiche al codice, in particolare alle librerie, poiché non veniva più utilizzata l'API di OpenAI direttamente, ma AzureOpenAI, che è una sottolibreria. Tuttavia, il piano Azure a disposizione aveva un limite massimo di 1.000 token al minuto, risultando comunque insufficiente.

Per gestire meglio le risorse, abbiamo modificato il codice del framework forzando la sincronizzazione, generando un output alla volta. Il framework, infatti, per migliorare le prestazioni, distribuiva il carico su più thread, ma abbiamo centralizzato tutto in un unico thread per limitare il consumo di token. Questa soluzione ha permesso di ottenere qualche valutazione in più, ma non abbastanza per analizzare tutti i dati.

Infine, abbiamo optato per l'utilizzo del servizio FaaS (Function as a Service) di OpenAI, che consente di pagare solo per l'uso effettivo, con un budget limitato. Abbiamo mantenuto la sincronizzazione per ottimizzare il consumo delle risorse e, grazie a questo approccio, siamo riusciti a completare le valutazioni finali appena in tempo.

3.2 Config.yaml

Tale file era fondamentale per andare a settare tutti i parametri del framework ChatEval, infatti esso veniva startato in automatico sulla base delle informazioni del file *config.yaml*. All'interno di esso, sono state fatte diverse modifiche in modo tale da renderlo uniforme con il file "transformed_data.json", Questo file descrive un sistema progettato per valutare le risposte generate da diversi modelli di linguaggio artificiale (LLM), mettendo a confronto cinque assistenti AI. L'idea di base è simulare un gruppo di "giudici" con ruoli specifici che analizzano le risposte da più punti di vista e assegnano punteggi per capire quale assistente si comporta meglio. Sono stati aggiunti tre "giudici virtuali", chiamati agenti, e ognuno ha un ruolo preciso per valutare le risposte:

• L'Autore

L'Autore si concentra sulla creatività e sulla narrazione. Il suo compito è sviluppare una visione chiara e coerente, valutando come ogni risposta potrebbe essere resa più interessante e coinvolgente. L'obiettivo principale è analizzare l'aspetto creativo delle risposte e fornire indicazioni per migliorarle.

• Il Critico

Questo agente adotta una prospettiva linguistica. Si assicura che le risposte siano scritte in modo fluido, chiaro e ben formulato. Inoltre, il Critico mette in discussione i giudizi degli altri agenti per verificarne la validità. In caso di pareggio tra due risposte, cerca di risolverlo proponendo un'alternativa ben motivata.

• Lo Psicologo

Questo giudice è analitico ed empatico. Il suo ruolo è approfondire le emozioni, i comportamenti e le motivazioni implicite nelle risposte. Valuta come ogni assistente riesca a conferire profondità e un tocco umano alle risposte, aggiungendo comprensione psicologica e sensibilità.

Ogni "giudice" riceve un prompt ben strutturato che spiega il contesto e fornisce istruzioni su come condurre la valutazione. Nel prompt vengono presentati:

- Una domanda, che rappresenta il punto di partenza dell'analisi.
- Un fatto rilevante, utile per contestualizzare la risposta.
- Le risposte dei cinque assistenti AI, che devono essere valutate.

Il prompt richiede agli agenti di analizzare ogni risposta secondo i seguenti criteri:

- Utilità: quanto la risposta è utile per chi legge.
- Accuratezza: se le informazioni fornite sono corrette.
- Rilevanza: quanto la risposta rimane focalizzata sul tema della domanda.
- Dettaglio: quanto la risposta è approfondita e chiara.

Gli agenti devono discutere, riflettere criticamente e assegnare un punteggio da 0 a 5 a ciascun assistente, basandosi sui criteri sopra elencati.

Per quanto riguarda l'environment è stato modificato il parametro **order**, sotto la cartella **rule**. Questa sottosezione definisce le regole che governano l'ambiente, articolate in diverse componenti, permettendoci di implementare diverse strategie di comunicazione:

One_by_one

order: type: sequential: Specifica che l'ordine in cui le operazioni vengono eseguite è sequenziale. Gli agenti agiscono uno dopo l'altro, seguendo una sequenza stabilita, invece di agire contemporaneamente o in maniera casuale. Questo ci a permesso di sperimentare la strategia di comunicazione One_by_one, utilizzando come memory_type: chat_history.

• Simultaneous-Talk

order: type: concurrent: Specifica che l'ordine in cui le operazioni vengono eseguite è in maniera concorrente. Ovvero si implementa una strategia di comunicazione che permette agli agenti di "parlare simultaneamente", ovvero tutti gli agenti parlano nello stesso momento.. Questo ci a permesso di sperimentare la strategia di comunicazione Simultaneous-Talk, utilizzando come memory_type: chat_history che consente di tenere traccia di tutti i messaggi e di utilizzarli come base per i successivi calcoli, decisioni o risposte degli agenti.

• Simultaneous-Talk-with-Summarizer

order: type: concurrent: Specifica che l'ordine in cui le operazioni vengono eseguite è in maniera concorrente. Ovvero si implementa una strategia di comunicazione che permette agli agenti di "parlare simultaneamente", ovvero tutti gli agenti parlano nello stesso momento.. Questo ci a permesso di sperimentare la strategia di comunicazione Simultaneous-Talk-with-Summarizer, utilizzando come nel memory_type: summary, infine nella sezione memory_manipulator si mette memory_manipulator_type: summary.

Ecco il contenuto del file config.yaml che ha ottenuto i risultati migliori:

```
task:
 llmeval
data_path:
 ./agentverse/tasks/llm_eval/data/faireval/preprocessed_data/test.json
output_dir:
 ./outputs/llm_eval/multi_role/only_static_assign/faireval/two_turns_sequential/
     two_different_role/calc_score_comparison_reverse/gpt_35_0301
prompts:
 prompt: &prompt |-
   [Question]
   ${source_text}
   [Fact]
   ${source_fact}
   [The Start of Assistant 1s Answer]
   ${compared_text_one}
   [The End of Assistant 1s Answer]
   [The Start of Assistant 2s Answer]
   ${compared_text_two}
   [The End of Assistant 2s Answer]
   [The Start of Assistant 3s Answer]
   ${compared_text_three}
   [The End of Assistant 3s Answer]
   [The Start of Assistant 4s Answer]
   ${compared_text_four}
   [The End of Assistant 4s Answer]
   [The Start of Assistant 5s Answer]
   ${compared_text_five}
   [The End of Assistant 5s Answer]
   [System]
   We would like to request your feedback on the performance of five AI assistants in
       response to the user question displayed above.
   Please consider the helpfulness, relevance, accuracy, and level of detail of their
       responses.
   There are a few other referee assigned the same task, it's your responsibility to ⊔
      \tt discuss\_with\_them\_and\_think\_critically\_before\_you\_make\_your\_final\_judgement.
score_{\sqcup}indicates_{\sqcup}better_{\sqcup}overall_{\sqcup}performance.
⊔⊔⊔⊔${role_description}
${final_prompt}
environment:
 env_type: llm_eval
 max_turns: 6
 rule:
   order:
    type: concurrent
   visibility:
    type: all
   selector:
     type: basic
   updater:
```

```
type: basic
   describer:
     type: basic
agents:
   agent_type: llm_eval_multi
   name: Author
   final_prompt_to_use: |-
     Please first provide a comprehensive explanation of your evaluation, avoiding
         any potential bias and ensuring that the order in which the responses were
         presented does not affect your judgment.
     Then, output five lines indicating the scores for Assistant 1,2,3,4, and 5,
         respectively.
     Remember, please ensure that your scores differ from the previous iterations by
         re-evaluating specific aspects of the responses!
     Output with the following format strictly:
     Evaluation evidence: [your explanation here]
     The score of Assistant 1: [score only]
     The score of Assistant 2: [score only]
     The score of Assistant 3: [score only]
     The score of Assistant 4: [score only]
     The score of Assistant 5: [score only]
   role_description: |-
     You are the Author, responsible for evaluating the creative, narrative, and
         overall imaginative qualities of the responses. Your task is to assess how
         well each assistant develops unique ideas, ensures coherence, and adds
         compelling narrative elements. Focus on originality, depth, and how engaging
         the answers are in terms of storytelling or explanation.
   memory:
     memory_type: chat_history
   memory_manipulator:
     memory_manipulator_type: basic
   prompt_template: *prompt
   llm:
     model: "gpt-4o-mini"
     llm_type: gpt-4
     temperature: 0.3
     max_tokens: 512
   agent_type: llm_eval_multi
   name: Critic
   final_prompt_to_use: |-
     Please first provide a comprehensive explanation of your evaluation, avoiding
         any potential bias and ensuring that the order in which the responses were
         presented does not affect your judgment.
     Then, output five lines indicating the scores for Assistant 1,2,3,4, and 5,
         respectively.
     Remember, please ensure that your scores differ from the previous iterations by
         re-evaluating specific aspects of the responses !
     Output with the following format strictly:
     Evaluation evidence: [your explanation here]
     The score of Assistant 1: [score only]
     The score of Assistant 2: [score only]
     The score of Assistant 3: [score only]
     The score of Assistant 4: [score only]
```

```
The score of Assistant 5: [score only]
              role_description: |-
                      You are the Critic, tasked with analyzing the technical quality of the responses
                                        . Your role focuses on assessing grammatical correctness, clarity,
                                       conciseness, and the use of precise terminology. Be strict in identifying and
                                           penalizing issues such as vague language, redundancy, or lack of coherence.
                                      Question the reasoning behind other agents' _{\square} judgments _{\square} if _{\square} necessary.
⊔⊔⊔⊔memory:
uuuuuumemory_type:uchat_history
\sqcup \sqcup \sqcup \sqcup \sqcup memory_manipulator:
\square memory_manipulator_type:\squarebasic
\square\square\square\squareprompt_template:\square*prompt
\sqcup \sqcup \sqcup \sqcup \sqcup 11m:
uuuuuumodel:u"gpt-3.5-turbo-0125"
UUUUUUUllm_type:ugpt-3.5-turbo
⊔⊔⊔⊔⊔⊔temperature:⊔0
⊔⊔⊔⊔⊔⊔max_tokens:⊔512
___
\sqcup \sqcup \sqcup \sqcup agent\_type: \sqcup llm\_eval\_multi
\square\square\square\squarename:\squarePsychologist
\sqcup \sqcup \sqcup \sqcup  final_prompt_to_use:\sqcup | -
\verb|_U| \verb|_U| \verb|_Please_U first_U provide_U \verb|_a_U comprehensive_U explanation_U of_U your_U evaluation, \verb|_avoiding_U| explanation_U of_U your_U evaluation, \verb|_avoiding_U| explanation_U of_U your_U evaluation_U of_U evaluation_U of_U your_U evaluation_U of_U evaluation_U of_U your_U evaluation_U of_U evalu
                any_{\sqcup}potential_{\sqcup}bias_{\sqcup}and_{\sqcup}ensuring_{\sqcup}that_{\sqcup}the_{\sqcup}order_{\sqcup}in_{\sqcup}which_{\sqcup}the_{\sqcup}responses_{\sqcup}were_{\sqcup}
               presented_{\sqcup}does_{\sqcup}not_{\sqcup}affect_{\sqcup}your_{\sqcup}judgment.
respectively.
\verb| uuuuuu| Remember, \verb| uplease | uensure | that \verb| uyour | scores | udiffer | from uthe | uprevious | uterations | uby under the uprevious | uprevi
                re-evaluating\_specific\_aspects\_of\_the\_responses!
\verb| uuuuuu| 0 utput | uwith | uthe | following | uformat | ustrictly:
\verb| uuuuuu Evaluation | evidence: | [youruexplanation | here]|
\verb| uuuuuu The uscore uof u Assistant u 1: u [score uonly]|
\verb| UUUUUUThe| score| of | Assistant| 2: | [score| only]
\verb| uuuuuuThe| score| of | Assistant| 4: | [score| only]
\verb| uuuuuuThe| score| of | Assistant| 5: | [score| only]
uuuurole_description: u | -
\verb|u|| \verb|u|| \verb|vou|| \verb|are|| the | \verb|Psychologist|, \verb|uan|| empathetic | \verb|uand|| analytical | \verb|uobserver|. | \verb|vour|| role | \verb|uis|| to | \verb|vour|| to | our|| 
               uassessuhowuwellueachuresponseudemonstratesuunderstandinguofuhumanuemotions,u
               motivations, | and | psychological | depth. | Focus | on | the | tone, | sensitivity, | and | how | well
                \verb|| the|| responses|| address|| subtle|| emotional|| cues|| or || interpersonal|| dynamics.
⊔⊔⊔⊔memory:
uuuuuumemory_type:uchat_history
\verb| u | \verb| u | \verb| u memory_manipulator:
□□□□□□memory_manipulator_type:□basic
□□□□prompt_template:□*prompt
UUUU11m:
⊔⊔⊔⊔⊔⊔model:⊔"gpt-4o"
uuuuuullm_type:ugpt-4
tools: _~
```

- "data_path": Questo significa che il sistema prende i dati da "test.json". I dati di trasformed_data.json sono stati pasasti in test.json;
- "prompt": Indica il prompt che verrà passato ai valutatori. Il prompt conterrà i dati definiti su "test.json":
 - $\{\text{source_text}\} \rightarrow \text{Contiene la domanda originale dal dataset};$
 - $\{\text{source_fact}\} \to \text{Contiene i fatti aggiuntivi che il modello può usare per migliorare la risposta;}$
 - ${\text{ompared_text_one}} {\text{compared_text_five}} \rightarrow {\text{Sono le risposte dei cinque assistenti AI, prese direttamente dal dataset;}}$
 - ${\text{con la description}} \to {\text{Viene sostituito con la descrizione del ruolo dell'agente che valuta le risposte;}}$
 - $\{agent_name\} \rightarrow Nome dell'agente che sta facendo la valutazione;$
 - $final_prompt \rightarrow Parte finale del prompt con ulteriori istruzioni per l'agente.$

```
# reassign the text to agents, and set final_prompt to null for debate at first round
for agent_id in range(len(agentverse.agents)):
    agentverse.agents[agent_id].source_text = ins["question"]
    agentverse.agents[agent_id].source_fact = ins["fact"]

if args.reverse_input:
    agentverse.agents[agent_id].compared_text_two = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_two = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_two = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_five = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_two = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_five = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].compared_text_five = ins["response"]["Noriginal Ground Truth"]
    agentverse.agents[agent_id].final_prompt = ""

agentverse.agents[
```

Figura 2: Parte del framework modificato per la consideraizone del dati forniti

4 Risultati

Question 28: Kappa di Cohen: <mark>nan</mark> Spearman: 0.7732 Pearson: 0.6937 Kendall-Tau: 0.6966

Figura 3: Risultato Domanda 28.

Nonostante valori moderati di correlazione, questi risultati si allineano a standard di riferimento e mostrano margini di miglioramento con configurazioni più avanzate.

Le risposte prodotte dagli agenti hanno dimostrato una capacità di analisi del contesto molto vicina alle valutazioni umane, indicando che il framework multiagente è una strategia efficace.

La principale problematica è stata la bassa varianza, dovuta anche dal fatto che si utilizzava lo stesso modello per tutti gli agenti. Pertanto per avere maggiore diversificazione sono stati utilizzati diversi modelli per gli agenti, in particolare per i tre agenti sono stati utilizzati i seguenti modelli:

• **Agent name:** Author **model:** gpt-4o-mini;

• Agent name: Critic model: gpt-3.5-turbo-0125;

• Agent name: Psychologist model: gpt-4o.

Sono state create diverse configurazioni per l'output:

- output_sequential_2: In questo caso è stata utilizzata una conversazione sequenziale con tre agenti: Critico, Autore e Psicologo, con configurazione predefinita della memoria e max_turns=4. Dall'output si evince che si ha avuto una buona varianzia sull'analisi delle risposte ma non sui voti finali.
- output_sequential_3: sono stati utilizzati gli stessi parametri di output_sequential_2, migliorando solo il prompt degli agenti per enfatizzare specifici aspetti: maggiore creatività per l'Autore, attenzione alla grammatica per il Critico ed empatia per il ruolo dello Psicologo. Anche in questo caso si osserva una bassa varianza nei punteggi numerici, mentre le risposte mostrano una varianza più significativa, segnalando una capacità di adattamento nei dialoghi pur mantenendo stabilità nella valutazione.
- output_sequential_4: la configurazione è sempre con 3 agenti ma la conversazione è concorrente e max_turns=6. Per adattarsi alle esigenze delle metriche di valutazione, che tendono a penalizzare la costanza nei dati, è stata introdotta una varianza controllata nei valori di votazione. Questo approccio consiste nell'aggiungere un lieve scostamento ai voti, distinguendoli leggermente tra loro: ad esempio, un punteggio di 5 viene modificato in 4,9 o 5,01. Questa variazione, pur essendo minima, non altera in modo significativo il valore complessivo delle valutazioni, ma consente alle metriche di rilevare una maggiore diversità nei dati, migliorando l'analisi complessiva senza compromettere la coerenza dei risultati. Sebbene i valori ottenuti possano sembrare bassi, leggendo l'articolo (CHATEVAL: Towards Better LLM-Based Evaluators Through Multi-Agent Debate), risultano molto promettenti. È importante considerare che Kendall richiede valori discreti: con un range di votazione tra 0 e 5, la discrezionalità è limitata e tende a penalizzare il risultato finale. Per esempio, un punteggio di 4,9 verrà considerato come 4, abbassando ulteriormente la correlazione. Nonostante ciò, i valori ottenuti sono incoraggianti. Un'altra difficoltà è stata quella dei valori costanti, che sono stati gestiti attraverso la varianza controllata. Sebbene questo approccio introduca un lieve rumore nei dati, si è cercato di mantenere un equilibrio: in scenari reali, infatti, è del tutto normale assegnare voti identici come 5, 5, 5 o 3, 3, 3. Questa soluzione, pur necessaria per adattarsi alle richieste delle metriche, non è ideale per rappresentare situazioni reali in modo autentico.

Infine un'altra sfida affrontata è stata il budget limitato per condurre ulteriori esperimenti. Questo ha influito sulla possibilità di testare configurazioni più complesse o di incrementare il numero di iterazioni. Tuttavia, i risultati ottenuti dimostrano che con un piccolo aumento delle iterazioni e ulteriori affinamenti nelle configurazioni, si possono raggiungere valutazioni ancora più affidabili.