**Esercizi AI Academy giorno 4.**

ESERCIZIO – CHIEDI CHATGPT

Scrivi un prompt per definire prompt engineering. Formula bene, aspettiamo risultati professionali.

Ciao, sei un esperto di AI e LLM. Dovresti spiegarmi cosa è e a cosa serve il prompt engineering, devi dare una risposta chiara e professionale ma non eccessivamente lunga.

Il **Prompt Engineering** è la disciplina che si occupa di **progettare, ottimizzare e raffinare gli input (chiamati "prompt") che vengono dati ai modelli di linguaggio di grandi dimensioni (LLM)**. In pratica, è l'arte e la scienza di comunicare con un'intelligenza artificiale generativa in modo tale da ottenere le risposte più accurate, pertinenti e utili possibili.

Non si tratta solo di scrivere una domanda, ma di strutturare il testo in modo strategico, includendo istruzioni, contesti, esempi o vincoli specifici, per "guidare" l'LLM verso l'output desiderato.

**A cosa serve il Prompt Engineering?**

Il Prompt Engineering è fondamentale per **sfruttare al massimo il potenziale degli LLM**. Ecco i suoi scopi principali:

* **Migliorare la Qualità delle Risposte:** Un prompt ben formulato può ridurre drasticamente risposte irrilevanti, incoerenti o imprecise, portando a output di qualità superiore.
* **Controllare il Comportamento dell'LLM:** Permette di specificare il tono, lo stile, il formato e la lunghezza della risposta. Ad esempio, puoi chiedere all'LLM di agire come un esperto di un certo settore o di fornire la risposta in un formato specifico (es. elenco puntato, codice, riassunto).
* **Sbloccare Nuove Capacità:** Attraverso prompt complessi e ben strutturati, si possono far eseguire agli LLM compiti che altrimenti non sarebbero in grado di svolgere autonomamente, come ragionamenti complessi, risoluzione di problemi specifici o generazione di contenuti creativi altamente specifici.
* **Ridurre l'Ambiguità e i "Bias":** Un prompt chiaro e preciso aiuta a minimizzare le interpretazioni errate da parte dell'LLM e può contribuire a mitigare la generazione di risposte che riflettono pregiudizi presenti nei dati di addestramento.
* **Ottimizzare l'Efficienza:** Un prompt efficace può portare all'ottenimento del risultato desiderato con meno tentativi e iterazioni, risparmiando tempo e risorse computazionali.

In sintesi, il Prompt Engineering è il ponte che connette l'intenzione umana con la capacità di elaborazione degli LLM, trasformando una semplice richiesta in un'istruzione potente e mirata. Senza un'adeguata ingegneria dei prompt, anche i modelli più avanzati potrebbero non esprimere il loro pieno potenziale.

QUIZ: RICONOSCI IL TIPO DI PROMPT

Quiz: Che tipo di prompt è?

Leggi questi prompt e indica se sono:

A.Instruction

B.Few-shot

C.Chain-of-thought

1. Scrivi un’email formale per richiedere informazioni su un corso universitario. **A**

2. Completa la sequenza: **B**  
 Cane → Dog  
 Gatto → Cat  
 Cavallo → …

3. Risolvi il problema: Se ho 20 euro e spendo 7 euro per il pranzo e 4 euro per un libro, quanti soldi mi restano? Spiega ogni passaggio del calcolo. **C**

4. Traduci queste parole: **B**  
 Sole → Sun  
 Luna → Moon  
 Mare → …  
 Cielo → …

5. Trova il numero mancante nella serie 2, 4, 8, 16, \_\_\_. Mostra come arrivi alla soluzione. **C**

6. Scrivi una poesia di 4 righe sul tema dell’inverno. **A**

ESERCIZIO: COSTRUISCI UN PROMPT COT

Task:  
Immagina di dover aiutare un compagno a risolvere questo problema:

Un’azienda acquista 5 computer a 720 euro ciascuno e riceve uno sconto totale di 400 euro sull’intero acquisto. Quanto ha pagato in tutto?

Istruzione:  
Costruisci un prompt per ChatGPT che chieda di risolvere il problema spiegando tutti i passaggi, non solo il risultato finale.  
Deve essere un prompt chiaro, completo e specifico per ottenere una risposta “step-by-step”.

Un’azienda acquista 5 computer a 720 euro ciascuno e riceve uno sconto totale di 400 euro sull’intero acquisto. Quanto ha pagato in tutto? Non limitarti a darmi la risposta, ma spiega il tuo ragionamento passo per passo

Certo, analizziamo passo passo il calcolo per determinare il costo totale che l'azienda ha sostenuto per l'acquisto dei computer.

**Calcolo del Costo Totale dell'Acquisto**

Ecco il ragionamento dettagliato:

1. **Costo dei computer senza sconto:** Per prima cosa, dobbiamo calcolare quanto costerebbero i 5 computer senza applicare alcuno sconto. Dato che ogni computer costa **720 euro** e ne vengono acquistati **5**, moltiplichiamo il costo unitario per il numero di computer: 720 euro/computer×5 computer=3600 euro

Quindi, il costo totale iniziale per i 5 computer sarebbe di **3600 euro**.

1. **Applicazione dello sconto:** L'azienda riceve uno **sconto totale di 400 euro** sull'intero acquisto. Questo significa che dal costo iniziale calcolato dobbiamo sottrarre l'importo dello sconto. 3600 euro (costo iniziale)−400 euro (sconto)=3200 euro

**Conclusione**

L'azienda ha pagato in tutto **3200 euro** per l'acquisto dei 5 computer, dopo aver ricevuto lo sconto.

ESERCIZIO - PROMPT TREE-OF-THOUGHT

Quando potrebbe servirvi una risposta strutturata Tree-of-Thought nella vostra attività?

Scrivi due casi d’uso da qualsiasi settore.

Scrivi il prompt per rispondere.

Un possibile utilizzo nell’attività di developer in ambito AI potrebbe essere quella di analizzare diverse tecnologie, ad esempio scegliere tra vari frameworks o tipi di database. Oppure analizzare aspetti positivi e negativi di varie scelte all’interno di un progetto, valutandole ad esempio in base a semplicità di sviluppo e manutenzione o sicurezza.

Sono un AI Engineer, sto sviluppando un progetto di computer vision in python e non so quale framework utilizzare. Valuta le 3 opzioni migliori, elenca pro e contro per ognuna e in seguito scegli la più efficace per risolvere il mio problema

ESERCIZIO – REACT-LITE

Definizione:  
 ReAct-lite utilizza i vantaggi del ReAct in modo più semplice e compatto.

Esercizio:

Crea un prompt ben pensato, che da un prompt ReAct traduce la versione lite.

Devi testare e valutare se il prompt funziona bene.

Il prompt da modificare fa parte del prompt stesso.

Sei un esperto di prompt engineering con una profonda conoscenza dei framework ReAct e ReAct-lite. Il tuo compito è prendere un prompt ReAct completo e convertirlo nella sua versione ReAct-lite, rendendolo più conciso ma mantenendo la sua funzionalità e capacità di utilizzare strumenti.

\*\*Istruzioni per la Conversione:\*\*

1. \*\*Rimuovi o Riduci i "Pensiero":\*\* Elimina tutte le istruzioni esplicite che richiedono al modello di verbalizzare il suo "Pensiero” Il modello dovrà comunque ragionare internamente, ma questo non verrà mostrato nell'output.

2. \*\*Semplifica il Formato di Output:\*\* \* Rimuovi la riga ` Pensiero: devi sempre pensare a cosa fare per primo `. \* Mantieni il formato per l'uso dello strumento, ma rendilo più conciso. Invece di separare `Azione:` e `Input Azione:`, suggerisci un formato come: `Tool: [nome\_tool]([input\_tool])`. \* Mantieni `Observation:` come indicato, poiché è il feedback del tool. \* Mantieni `Risposta Finale:` per la risposta conclusiva.

3. \*\*Mantieni l'Elenco dei Tool:\*\* Assicurati che l'elenco dei tool disponibili e le loro descrizioni rimangano invariati e chiari.

4. \*\*Preserva l'Intento:\*\* La versione lite deve essere in grado di risolvere lo stesso tipo di problemi del prompt ReAct originale, sfruttando gli stessi strumenti.

\*\*Prompt ReAct Originale da Convertire:\*\*

Sei un assistente AI intelligente e utile. Hai accesso ai seguenti strumenti:

1. cerca\_web(query: str): Esegue una ricerca sul web e restituisce i risultati.

2. calcola\_differenza\_date(data\_inizio: str, data\_fine: str): Calcola la differenza in giorni tra due date. Formato YYYY-MM-DD.

Usa il seguente formato per le tue risposte:

Domanda: la domanda a cui devi rispondere

Pensiero: devi sempre pensare a cosa fare per primo

Azione: l'azione da intraprendere, deve essere uno degli strumenti elencati

Input Azione: l'input per l'azione

Osservazione: il risultato dell'azione ... (questo ciclo Pensiero/Azione/Input Azione/Osservazione può ripetersi più volte)

Pensiero: Ora conosco la risposta finale

Risposta Finale: la risposta finale alla domanda originale

Inizia!

Domanda: Quando si terrà la prossima fiera del fumetto a Lucca e quanti giorni mancano a oggi per l'inizio dell'evento?

Domanda:

Come si chiama il metodo, quando un prompt gestisce, modifica o genera prompt?

Meta-Prompting

ESERCIZIO – CORREZIONE DI PROMPT REFLECTION

Correggi e spiega gli errori nel prompt:

Rispondi al seguente problema:  
Spiega quanto ha pagato un cliente se ha comprato 4 libri, ogni libro costa 20 euro, ma forse c’è uno sconto del 10%.

Scrivi la soluzione e poi rifletti se hai risposto in modo semplice per un bambino delle elementari, oppure se la tua risposta è adatta a un insegnante.  
Infine, correggi eventuali errori e suggerisci una soluzione alternativa, includendo anche la spiegazione dettagliata dei passaggi di calcolo.

La parte “forse c’è uno sconto del 10%.” Va eliminata visto che crea ambiguità

Anziché chiedere al modello se ha risposto in modo semplice come per un bambino o in modo più difficile come a un insegnante è inefficiente. Il modo migliore sarebbe quello di spiegare dall’inizio il pubblico di riferimento in modo che il modello possa adattare la sua risposta.

“Soluzione alternativa” è un po' vago, si potrebbe specificare meglio qual è l’approccio alternativo che vogliamo far prendere al modello.

Correggi e spiega gli errori nel prompt:

Leggi il seguente problema e rispondi:  
‘Un gruppo compra 12 biglietti del cinema a 8 euro ciascuno. Calcola la spesa totale.’  
Dopo aver dato la risposta, spiega se hai fatto tutti i passaggi oppure se potevi anche saltare qualche passaggio per fare più in fretta, poi scrivi la risposta anche in inglese e, se vuoi, in modo più formale per un documento aziendale. Infine, rifletti su quali informazioni aggiuntive avresti potuto chiedere all’utente e riscrivi il problema con una domanda diversa.

Chiedere al modello se poteva saltare qualche passaggio è inefficiente, in questo caso conviene specificare nel prompt il tipo di soluzione voluta, se diretta o se comprende dei passaggi intermedi per mostrare il procedimento.

La richiesta di riscrivere il problema con una domanda diversa è un po' vaga

ESERCIZIO - TEMPERATURE

Istruzioni:  
 Per ciascuno dei seguenti scenari d’uso di ChatGPT in azienda:

1.Individua il valore numerico di temperature che useresti (esempi: 0.0, 0.2, 0.7, 1.0).

2.Giustifica brevemente la tua scelta spiegando quale risultato ti aspetti (precisione, creatività, sicurezza…).

Scenari:

A. Scrivere una risposta tecnica formale a un cliente importante. **0.1**

B. Generare proposte creative per il titolo di una nuova campagna marketing. **0.8**

C. Estrarre e riepilogare dati chiave da un report finanziario. **0.2**

D. Creare un breve testo di apertura per una presentazione aziendale innovativa. **0.7**

ESERCIZIO – CORREZIONE DI TOP-P

Esempio di prompt errato di business:

Scenario:  
Un’azienda deve inviare una risposta standard e precisa a tutti i clienti che chiedono chiarimenti sulla fatturazione.

Prompt:  
Rispondi in modo gentile e originale a ogni cliente che ci chiede spiegazioni sulla propria fattura, variando il testo per ogni risposta.

Task:

1.Identifica e spiega l’errore.

2.Quanto sarebbe il valore top-p del prompt sbagliato?

3.Correggi l’errore.

Visto che vogliamo risposte standard e precise non possiamo chiedere nel prompt di rispondere in modo originale e variare il testo in ogni risposta. In questo modo avremmo un top-p alto 0.6-0.8, mentre per la nostra richiesta ne serve uno basso 0.0-0.2. Il prompt corretto sarebbe: Rispondi in modo gentile e preciso a ogni cliente che ci chiede spiegazioni sulla propria fattura, fai in modo che la risposta sia standardizzata per tutte le richieste.

ESERCIZIO - PRESENCE\_PENALTY NEI LLM

Istruzioni:

1.Immagina di chiedere a ChatGPT:

Suggerisci idee per attività originali da proporre a un team aziendale durante una giornata di formazione.

2.Qui sotto trovi due possibili risposte generate con valori diversi di presence\_penalty.

• Leggi attentamente entrambe le risposte.

• Prova a capire quale delle due è stata generata con un presence\_penalty più alto.

• Spiega il perché della tua scelta.

Risposta A:

• “Giochi di ruolo aziendali su gestione del tempo;

• laboratorio di brainstorming sulle strategie di comunicazione;

• quiz a squadre sulla mission aziendale;

• sessione di brainstorming di idee innovative;

• laboratorio creativo sulle presentazioni efficaci.”

Risposta B:

• “Giochi di ruolo aziendali su gestione del tempo;

• giochi di ruolo sulla comunicazione;

• giochi di ruolo per il problem solving;

• laboratorio di brainstorming sulle strategie di comunicazione;

• laboratorio di brainstorming sulla gestione dei conflitti.”

Nella risposta A c’è una presence penalty più alta, e si nota dal fatto che c’è una maggiore varietà di parole utilizzate. Nella risposta B ci sono invece molte parole e espressioni che si ripetono, facendo pensare all’utilizzo di una presence penalty più bassa.

ESERCIZIO - FREQUENCY\_PENALTY NEI LLM

Esempio di prompt errato di business:

Scenario:  
Devi preparare brevi descrizioni da inserire nel sito web per una nuova linea di prodotti, ciascuna descrizione deve essere interessante e diversa.

Prompt fornito (da correggere):

“Scrivi una breve descrizione per ciascun prodotto della nuova linea:

• Shampoo FreshClean

• Balsamo FreshClean

• Gel FreshClean

Le descrizioni devono mettere in evidenza il nome FreshClean e i benefici di ciascun prodotto.”

“Scrivi una breve descrizione per ciascun prodotto della nuova linea:

• Shampoo FreshClean

• Balsamo FreshClean

• Gel FreshClean

Le descrizioni devono mettere in evidenza il nome FreshClean e i benefici di

ciascun prodotto, inoltre essendo slogan devono essere creativi e non ripetitivi.

**Shampoo FreshClean**

Il tuo giorno inizia con **FreshClean**! Libera la chioma da ogni peso, donando una sensazione di pulito profondo che dura, e una vitalità che si vede. Capelli leggeri, luminosi e pronti a brillare.

**Balsamo FreshClean**

Dopo lo shampoo, la magia continua con **FreshClean**! Trasforma ogni ciocca in seta pura, districando con dolcezza e avvolgendo i capelli in una morbidezza irresistibile. Addio nodi, benvenuta lucentezza sublime.

**Gel FreshClean**

Definisci il tuo stile con la tenuta impeccabile di **FreshClean**! Scolpisci ogni dettaglio senza appesantire, per un look che resta fresco e impeccabile dalla mattina alla sera. Brillantezza naturale, massima libertà.

ESERCIZIO - ANTI PROMPT INJECTION

Completa esercizio nel file G4E1\_Anti\_prompt\_injection.py

ESERCIZIO - STIMA DEL COSTO TOKEN-PER-TOKEN

Scrivi breve programma per calcolare prezzo per token di un input di un modello selezionato.

Pianifica brevemente la soluzione.

Info ufficiali e prezzi aggiornati:  
[openai.com/api/pricing/](https://openai.com/api/pricing/)

Per il calcolo del numero dei token usa la libreria tiktoken.

Verificare numero dei token:

<https://platform.openai.com/tokenizer>

Usa GitHub pull request per consegnare il programma.