**Esercizi AI Academy giorno 4.**

ESERCIZIO – CHIEDI CHATGPT

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

**AP**: Che cos'è il prompt engineering? Scrivi una definizione da enciclopedia.

**ChatGPT (GPT-4o)**: Prompt engineering è una disciplina nell’ambito dell’intelligenza artificiale, in particolare dell’elaborazione del linguaggio naturale (NLP), che consiste nella progettazione, ottimizzazione e formulazione strategica di prompt (istruzioni testuali) per guidare modelli linguistici generativi — come GPT — a produrre risposte accurate, rilevanti e coerenti con l’obiettivo dell’utente.

Questa pratica implica la comprensione approfondita del comportamento dei modelli linguistici e l’uso consapevole della formulazione linguistica per ottenere risultati desiderati, ridurre ambiguità, controllare lo stile, e migliorare la qualità dell’interazione. Il prompt engineering è particolarmente cruciale in contesti come la generazione di contenuti, la programmazione assistita, l’automazione di compiti complessi e l’interazione uomo-macchina.

Con l’evoluzione dei modelli AI, il prompt engineering si è affermato come una competenza chiave per sviluppatori, ricercatori e professionisti del settore tecnologico.

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:  
 Cane → Dog  
 Gatto → Cat  
 Cavallo → … (B)

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:  
 Sole → Sun  
 Luna → Moon  
 Mare → …  
 Cielo → … (B)

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

**AP**: Puoi risolvere questo problema di matematica spiegando tutti i passaggi in modo dettagliato, senza limitarti a fornire solo il risultato finale?

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

Per favore, includi:

- Il calcolo del prezzo totale prima dello sconto.

- L’applicazione dello sconto sul totale.

- Il calcolo finale della spesa effettiva.

Spiega ogni passaggio con una breve frase, come se dovessi aiutare un compagno a capire bene come risolvere il problema.

**GPT-4o**: Certo! Ecco come risolvere questo problema passo dopo passo, spiegando ogni passaggio in modo semplice e chiaro.

### **Testo del problema:**

Un’azienda acquista **5 computer a 720 euro ciascuno**. Sul totale dell’acquisto riceve **uno sconto complessivo di 400 euro**. **Domanda:** Quanto ha pagato in tutto?

## ✅ **Passaggio 1: Calcolare il prezzo totale prima dello sconto**

Ogni computer costa **720 euro** e l’azienda ne compra **5**. Per trovare il prezzo totale **prima dello sconto**, basta moltiplicare il prezzo di un singolo computer per il numero di computer acquistati:

👉 *Questo è il costo totale senza considerare lo sconto.*

## ✅ **Passaggio 2: Applicare lo sconto sul totale**

L’azienda riceve **uno sconto di 400 euro** sull’intero acquisto. Per sapere quanto dovrà effettivamente pagare, dobbiamo **sottrarre lo sconto** dal prezzo totale:

👉 *Questo è il prezzo che l’azienda paga davvero, dopo lo sconto.*

## ✅ **Passaggio 3: Rispondere alla domanda**

Quindi, l’azienda ha pagato in tutto:

### 📌 **Ricapitolando:**

1. Prezzo totale senza sconto: **720 × 5 = 3.600 euro**
2. Sconto complessivo: **400 euro**
3. Prezzo finale pagato: **3.600 - 400 = 3.200 euro**

Fammi sapere se vuoi anche la rappresentazione grafica del problema o una verifica del risultato!

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.

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.

Domanda:

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

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

**GPT-4o**: Ecco un prompt ben pensato che può essere usato per **tradurre un prompt ReAct in una versione "lite"**, cioè più semplice, sintetica e diretta, mantenendo però l'intento originale:

**Prompt per ChatGPT:**

Ti fornirò un prompt progettato per la tecnica ReAct (Reasoning + Acting), che include passaggi espliciti di ragionamento e azioni da eseguire. Il tuo compito è riscrivere questo prompt in una **versione "lite"**: mantieni lo scopo e le istruzioni principali, ma semplifica il linguaggio, rimuovi le parti ridondanti e rendi il prompt più sintetico, scorrevole e adatto a un uso più fluido e immediato.

Assicurati che:

* il significato originale sia conservato,
* la versione lite sia più breve e diretta,
* siano omesse strutture complesse come "Thought:", "Action:", "Observation:" se non indispensabili,
* rimanga adatta a guidare comunque una risposta utile e ragionata.

Esempio in input:

Prompt ReAct: [incollato qui]

Restituisci:

Prompt Lite: [versione semplificata]

Se vuoi, posso mostrarti un esempio concreto partendo da un vero prompt ReAct. Vuoi procedere?

**AP**: Si, per favore basa il tuo esempio considerando un vero prompt ReAct che risponde alla seguente domanda: *Come si chiama il metodo, quando un prompt gestisce, modifica o genera prompt?*

**GPT-4o**: Perfetto! Ecco un esempio concreto:

### 🎯 **Domanda originale**

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

### 🧠 **Prompt in stile ReAct (completo)**

You are an expert in prompt engineering. Carefully analyze the question below using step-by-step reasoning. Then, take action to identify the correct terminology.

Question: How is the method called, when a prompt handles, modifies, or generates other prompts?

Thought: I need to consider known terms in prompt engineering and NLP that describe a prompt operating on other prompts. The question points toward a concept involving prompts that create or adapt other prompts. This is meta-level behavior.

Action: Search my knowledge of prompt engineering for the term describing prompts that operate on other prompts.

Observation: One well-known term in prompt engineering for this is "meta-prompting" or "prompt programming". "Meta-prompting" is especially relevant when prompts are designed to modify or generate other prompts.

Final Answer: Meta-prompting.

### ✨ **Prompt Lite (semplificato e diretto)**

You're a prompt engineering expert. What's the name of the method where a prompt handles, modifies, or creates other prompts? Give a clear and concise answer, explaining briefly if needed.

Questa versione lite conserva lo scopo (ottenere la terminologia corretta), ma **rimuove la struttura ReAct**, accorcia le istruzioni e rende il prompt più immediato, adatto per interazioni veloci senza perdere accuratezza.

Vuoi che ti generi altri esempi o un template riutilizzabile per il tuo lavoro?

**New Chat for test, AP**: You're a prompt engineering expert. What's the name of the method where a prompt handles, modifies, or creates other prompts? Give a clear and concise answer, explaining briefly if needed.

**GPT-4o**: The method is called **prompt chaining**.

Prompt chaining is a technique where the output of one prompt is used as the input to another. It allows a system to **handle**, **modify**, or **generate** new prompts dynamically, creating a sequence of interdependent prompts to achieve complex tasks. This approach is often used in multi-step reasoning, agent frameworks, or tools like LangChain.

ESERCIZIO – CORREZZIONE 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.

Per ottimizzare la generazione dell’output sarebbe più idoneo disambiguare le richieste:

* Innanzitutto, “forse” non va bene, in quanto non fornisce informazioni chiare ma crea confusione.
* Chiedere se la spiegazione di una moltiplicazione è adatta ad un bambino che frequenta le elementari è un po’ uno spreco di acqua e risorse nella mia piccolissima opinione.
* Successivamente sarebbe più idoneo dividere il prompt per svolgere i task seguenti, ad esempio facendo delle domande di follow up 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.

Gli “errori” nella formulazione della richiesta anche in questo caso sono diversi, un prompt ottimale evita la disorganizzazione logica e funzionale nella richiesta. Ecco secondo me alcuni punti in cui si sarebbe potuto fare meglio:

* I task da svolgere sono troppi per un singolo prompt.
* Se la risposta desiderata è in inglese, tanto vale fare un favore al modello e chiedere direttamente in inglese in quanto i dati di addestramento sono quasi tutti in inglese,
* “se vuoi” è ambiguo o comunque genera confusione nella richiesta.
* Se si sospetta che sia necessario fornire informazioni aggiuntive e/o fare un ragionamento, meglio chiederlo dal principio anziché alla fine.

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.

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

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

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

1. Userei 0, in quanto la precisione richiesta per il task è molto alta, in questo modo si ottiene un risultato standard e ripetibile necessario per un documento tecnico.
2. Farei varie prove utilizzando il range di temperature 0.7-1.0, in quanto in questo task la creatività è un fattore chiave per un risultato interessante.
3. Anche in questo caso proverei un range di temperature, ma considerando un range di temperature più basso, ad esempio 0.0-0.2, in modo tale da minimizzare il rischio di allucinazioni o risposte imprecise.
4. Un range di temperatura da intermedio (0.2-0.7) a alto (0.7-1.0) sarebbe ideale in questo contesto. In questo caso oltre la temperatura bisognerebbe specificare meglio (anche nel prompt stesso) il contesto in cui avverrà la presentazione in oggetto.

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.

* 1. Il prompt sarebbe idoneo per un contesto diverso (per non dire opposto) a quello richiesto.
  2. Riguardo la domanda di oggi a lezione sulla temperatura e successivamente sul top-p, potrebbe essere interessante questa lettura (possiamo considerarlo prompt injection se fossimo dei competitor di OpenAI? LOL): <https://chatgpt.com/share/68540ea5-7f08-8008-8846-a9bb33a02603>

Riguardo la domanda, quindi, potremo dire che il top-p è un parametro presumibilmente estratto dal prompt, e in questo caso corrisponderebbe ad un top-p alto (tipo 0.9).

* 1. Nuovo prompt: Rispondi in modo standard e preciso a ogni cliente che chiede spiegazioni sulla propria fattura.

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.”

La risposta A è stata generata con un presence penalty più alto, vista appunto ala diversità del linguaggio utilizzato.

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.”

Un prompt più efficace potrebbe chiedere di specificare il nome del brand, impostare il numero di parole, scegliere lo stile e/o l’audience che ci interessa raggiungere, ed a proposito delle frequency penalty bisognerebbe stare attenti, perché con un prompt del genera si rischia di avere delle descrizioni molto ripetitive e in mancanza di ulteriore contesto o rischiano di essere anche ridondanti.

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.