



02/10/2023

Gabriele De Vito





Obiettivi della lezione

Introduzione ai LLMs e ChatGPT

Come funzionano gli LLMs e ChatGPT?.

Conoscere i limiti degli LLMs

Quali sono I limiti dei LLMs?



Usare efficacemente ChatGPT

Come usare in modo efficace ChatGPT?

Usare in modo sicuro e responsabile ChatGPT

Come usare in modo sicuro e responsabile ChatGPT?

Laboratorio pratico su ChatGPT

Cooperative learning per usare nella pratica ChatGPT





Introduzione agli LLMs





Cosa sono gli LLM?



LLMs

Stato dell'arte nel campo della NLP

Reti neurali deep con miliardi di parametri Addestrati su enormi quantità di dati testuali

Architettura

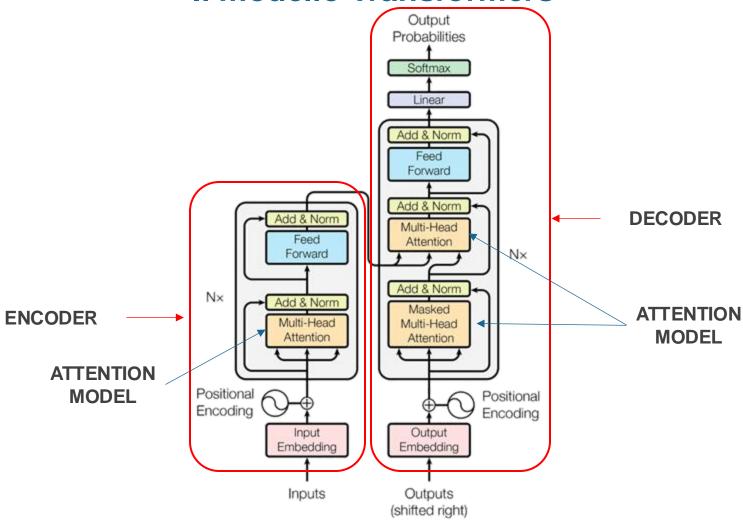
Si basano sul modello Transformers [1].

[1] Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems 30 (2017).





Il modello Transformers







Il modello Transformers

Il modello di attenzione

Il gatto ha mangiato il topo



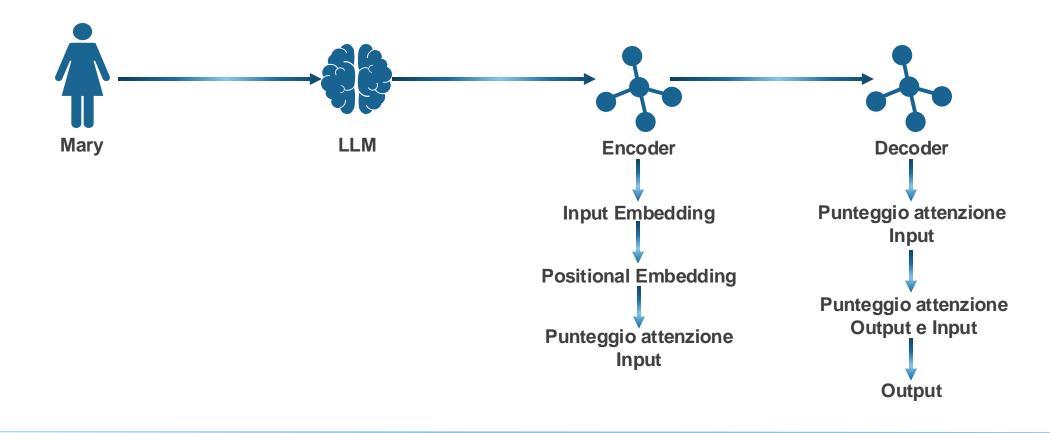
Pesi di attenzione

I pesi sono assegnati in base al task per cui il modello viene addestrato. Ad esempio, in una task di sentiment analysis, il peso è assegnato in base ad un'emozione specifica (come "felicità", "tristezza", "rabbia", ecc.).





Funzionamento degli LLMs

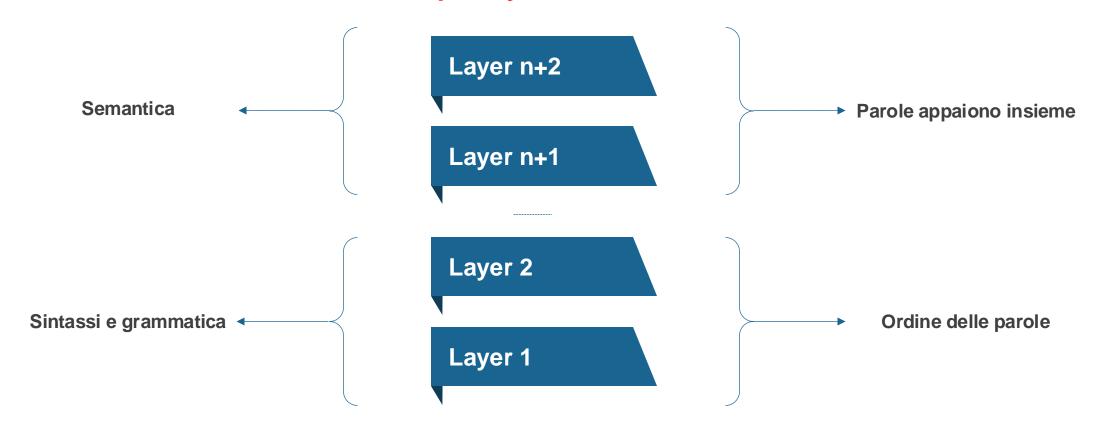






Funzionamento degli LLMs

Perché ci sono più layer di encoder e decoder?







Funzionamento degli LLMs

Quindi cosa sono gli LLMs?

Take home message

Sono modelli probabilistici, non comprendono il significato delle parole nel senso umano!

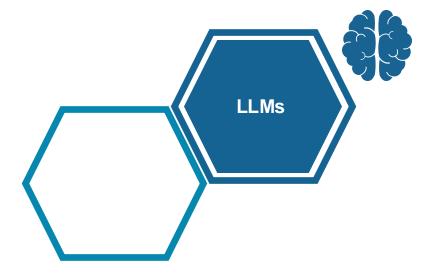




Abilità degli LLM

Abilità di NLP

In-context learning, traduzione, generazione del testo ...



Transfer learning e multimodalità

Fine-tuning, Zero-shot e Few-shots learning Multimodal data analysis

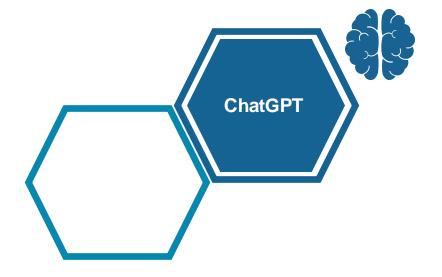




Cos'è ChatGPT?

È un LLM

ChatGPT è un LLM progettato per generare testo human-like.



Preaddestramento

È stato preaddestrato su un vasto corpus di testo da internet.

Fine-tuning

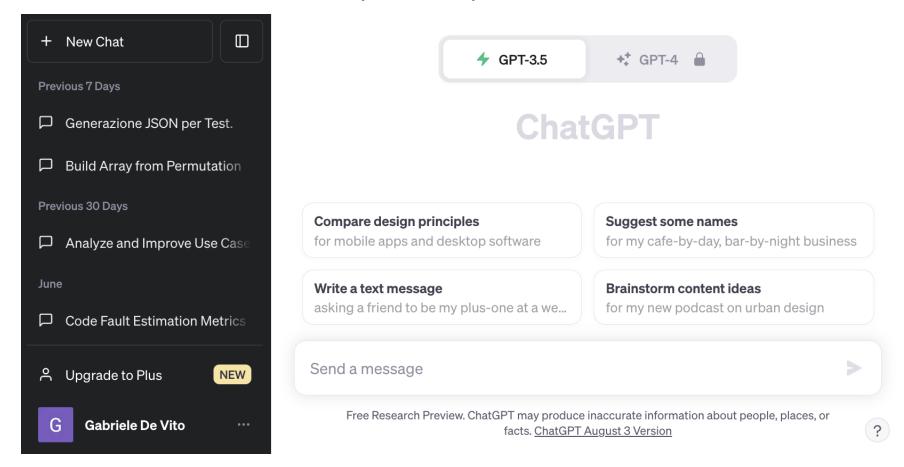
Ulteriormente addestrato con un dataset più piccolo, generato da umani che hanno giocato sia il ruolo di utente che assistente Al in una conversazione, con l'obiettivo di rispondere a una serie di domande.





Cos'è ChatGPT?

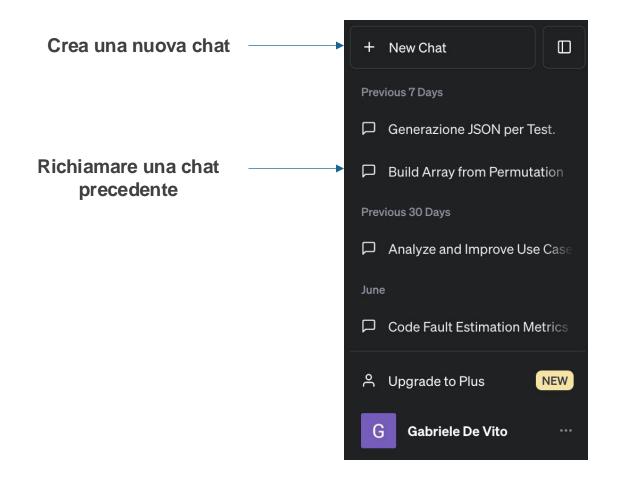
https://chat.openai.com/







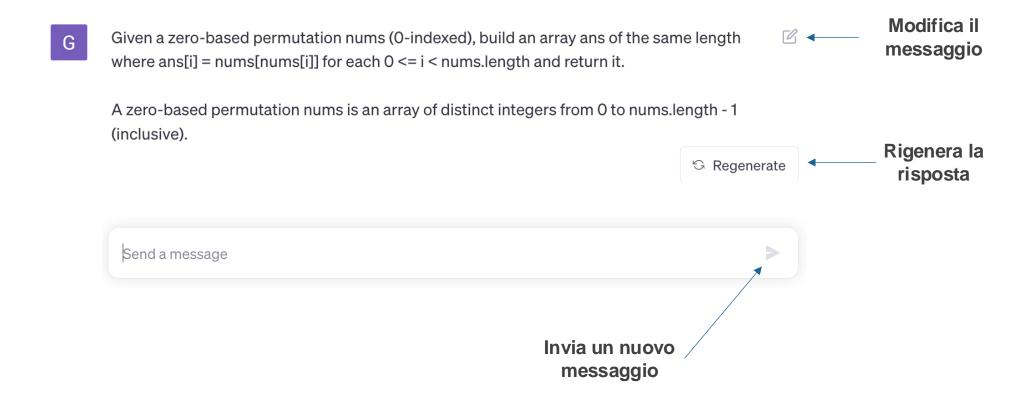
Cos'è ChatGPT?







Cos'è ChatGPT?

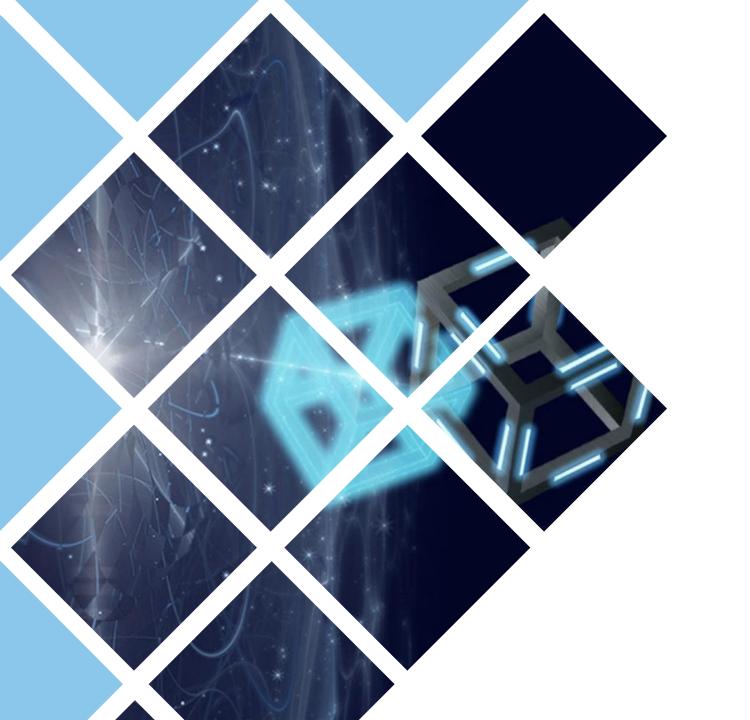






Cos'è ChatGPT?







Limiti degli LLMs





Limitazioni

Dimensione del contesto

Hanno un numero massimo di tokens che possono processare in una singola interazione (I/O)

Memoria statica

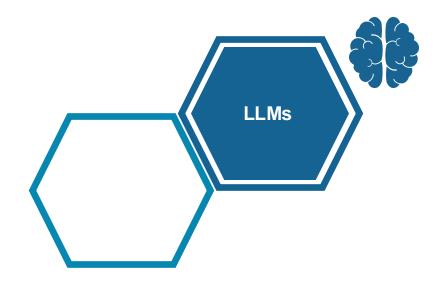
La memoria è limitata al corpus di dati usato per il preaddestramento

Allucinazioni e fonti errate

Possono generare risposte false e non hanno la capacità di verificare le fonti delle informazioni che generano

Plagio

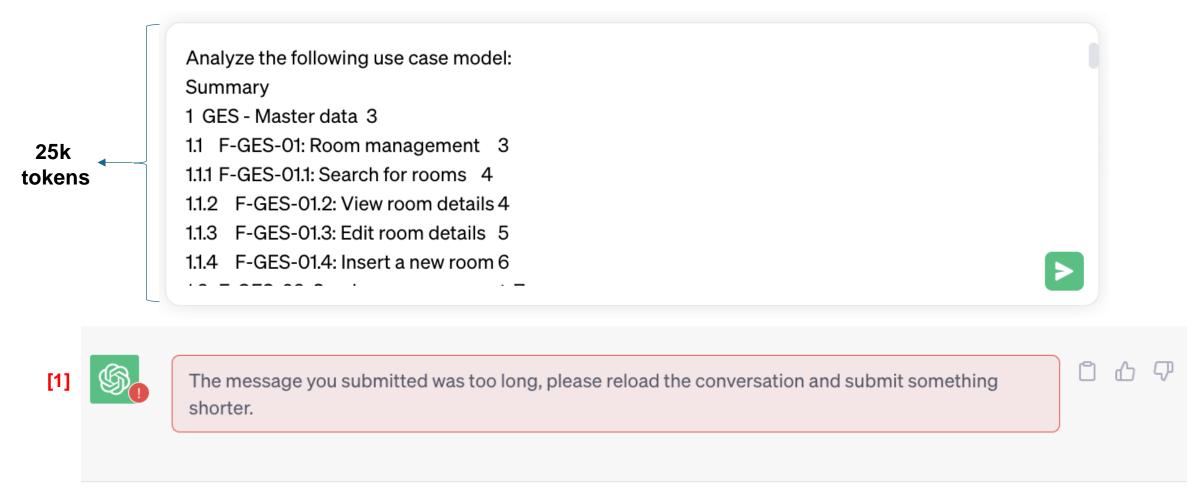
Le risposte potrebbero contenere testo estratto da articoli e non essere originali. Usare il testo generato dall'Al costituisce plagio.







Limitazioni: dimensione del contesto

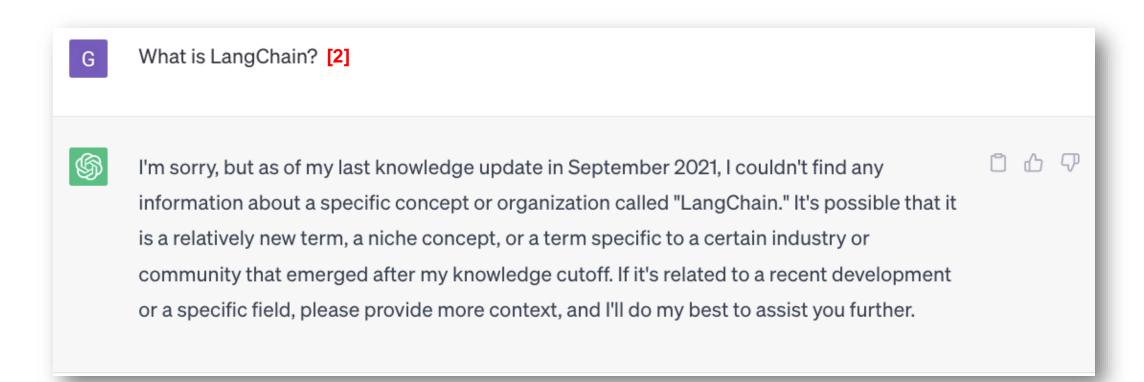


[1] Limite del modello GPT-3.5 \rightarrow 16k tokens – Limite del modello GPT-4 \rightarrow 8k tokens





Limitazioni: Memoria statica



[2] LangChain. Framework Python sviluppato alla fine del 2022, quindi non presente nel corpus con cui è stato addestrato ChatGPT.





Limitazioni: Allucinazioni

G Scrivi il risultato dell'espressione 2*ln(8) [3]



Il risultato dell'espressione 2 * In(8) è circa 5.54517744448.





Limitazioni: Allucinazioni



Lirica della canzone "più bella cosa" [4]



La canzone "La più bella cosa" è una canzone di Eros Ramazzotti. Ecco le liriche:



Dedicato a te che

Ogni giorno mi sorprendi

A te che sei la parte migliore di me

A te che hai

Preso la mia vita e ne hai fatto molto di più

Che hai dato amore, sai

Dedicato a te che

Con un sorriso o con un gesto

Testo corretto:

Com'è cominciata io non saprei. La storia infinita con te. Che sei diventata la mia lei. Di tutta una vita per me. Ci vuole passione con te...

[4] Eros Ramazzotti. "Più bella cosa". 1996.





Limitazioni: Fonti errate

Quali articoli potrei citare che parla dei problemi di privacy e sicurezza nel federated learning?



Per trovare articoli che trattano dei problemi di privacy e sicurezza nel federated learning, puoi fare riferimento a diverse fonti, tra cui riviste accademiche, conferenze, e risorse online specializzate. Di seguito ti fornisco alcune fonti e articoli accademici che potrebbero essere utili:

- Federated Learning: Strategies for Improving Communication Efficiency (Articolo accademico):
 - Autore/i: Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon
 - Rivista/conferenza: NeurIPS 2016
 - Questo articolo discute alcune delle sfide relative all'efficienza di comunicazione nel federated learning.
- 2. Secure Federated Matrix Factorization (Articolo accademico):
 - Autore/i: Wei Yang Bryan, Abhradeep Thakurta
 - Rivista/conferenza: NeurIPS 2019
 - Questo articolo si concentra sulla sicurezza del federated learning, in particolare su come proteggere i dati durante il processo di apprendimento federato.





Limitazioni: Fonti errate

- 1. Federated Learning: Strategies for Improving Communication Efficiency (Articolo accademico): [5]
 - Autore/i: Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon
 - Rivista/conferenza: NeurIPS 2016
 - Questo articolo discute alcune delle sfide relative all'efficienza di comunicazione nel federated learning.
- 2. Secure Federated Matrix Factorization (Articolo accademico):
 - Autore/i: Wei Yang Bryan, Abhradeep Thakurta
 - Rivista/conferenza: NeurIPS 2019
 - Questo articolo si concentra sulla sicurezza del federated learning, in particolare su

[5] L'articolo non è pubblicato su NeurIPS, ma solo su arXiv preprint → arXiv:1610.05492.





Limitazioni: Allucinazioni e Fonti errate

Take home message

Gli LLM non hanno una comprensione del mondo reale e non hanno capacità di ragionamento. Hanno una KB limitata (per quanto enorme) e oltre quella non hanno la possibilità di accedere ad altri dati. Questo significa che non sono in grado di verificare le informazioni o di ragionare logicamente come un essere umano.





Limitazioni: Allucinazioni e Fonti errate

Esempio

Che tempo fa a New York?

Nonostante la sua vasta conoscenza, l'LLM non sarà in grado di rispondere correttamente a questa domanda perché non ha accesso a dati in tempo reale o a internet per verificare le informazioni attuali.

Problema di buon senso

Ci sono cinque blocchi quadrati impilati uno sopra l'altro. Ti vengono fornite le seguenti informazioni su di essi: 1. Il secondo blocco dall'alto è verde. 2. Il quarto blocco dall'alto non è verde.

Supponendo che queste due premesse siano valide, confuta o dimostra la seguente conclusione: C'è un blocco verde direttamente sopra un blocco non verde. Spiega la tua risposta.

La conclusione è sempre valida, ma il LLM non è in grado di ragionare e produrrà una risposta sbagliata.















Limitazioni: Plagio

Definizione

È l'atto di presentare il lavoro o le idee di altri come se fossero proprie, senza dare credito all'autore originale.





Limitazioni: Plagio

Usare il testo generato da un LLM è plagio?

Take home message

- 1. Un LLM potrebbe riusare frasi estratte da altri articoli senza citare gli autori.
- 2. Usare il testo generato da un LLM costituisce plagio: l'autore è il LLM, non tu.

De Vito G.





Limitazioni: Plagio

È possible verificare se un testo è stato generato dall'IA?

Take home message

Si e No. Esistono tools e la loro accuratezza sta aumentando giorno dopo giorno.

De Vito G.

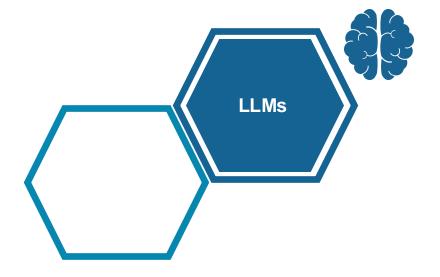




Limitazioni: Plagio

Lessico

Gli LLM hanno un vocabolario più limitato e ripetitivo



Sintassi

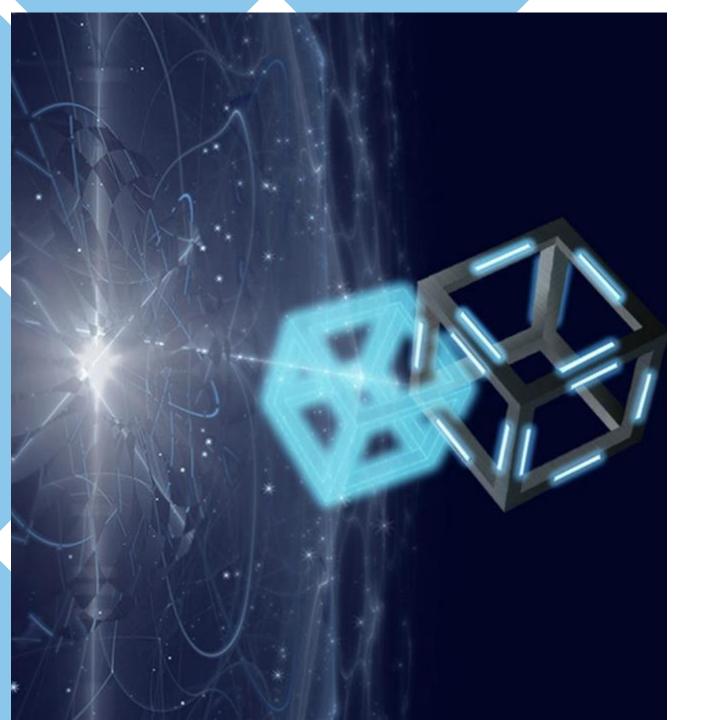
Le frasi generate dagli LLM sono spesso più rigide e semplici nella struttura

Brillantezza e creatività

Le idee non sono espresse con creatività e brillantezza

Metriche

Burstiness: imprevedibilità statistico-linguistica di un contenuto Perplexity: indica quanto gli elementi di un testo siano casuali





Formulare richieste: I prompt

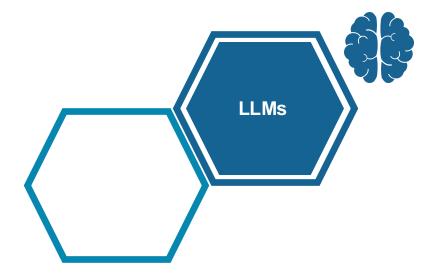




L'importanza del prompt

Prompt

Linguaggio di programmazione degli LLMs



Efficacia e accuratezza dei risultati

La qualità delle risposte è fortemente collegata alla qualità del prompt

Prompt Engineering

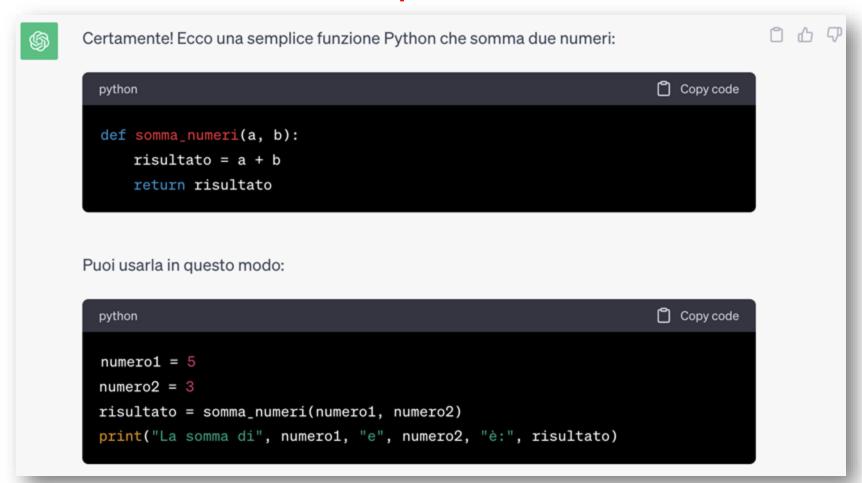
È processo creativo, ma anche rigoroso, per lavorare efficacemente con gli LLMs.





L'importanza del prompt

Scrivi una funzione per sommare due numeri

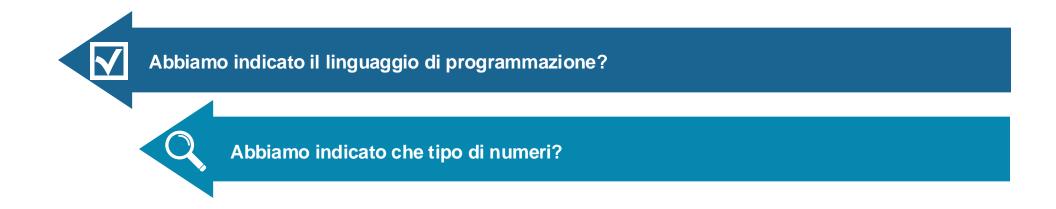






L'importanza del prompt

Scrivi una funzione per sommare due numeri

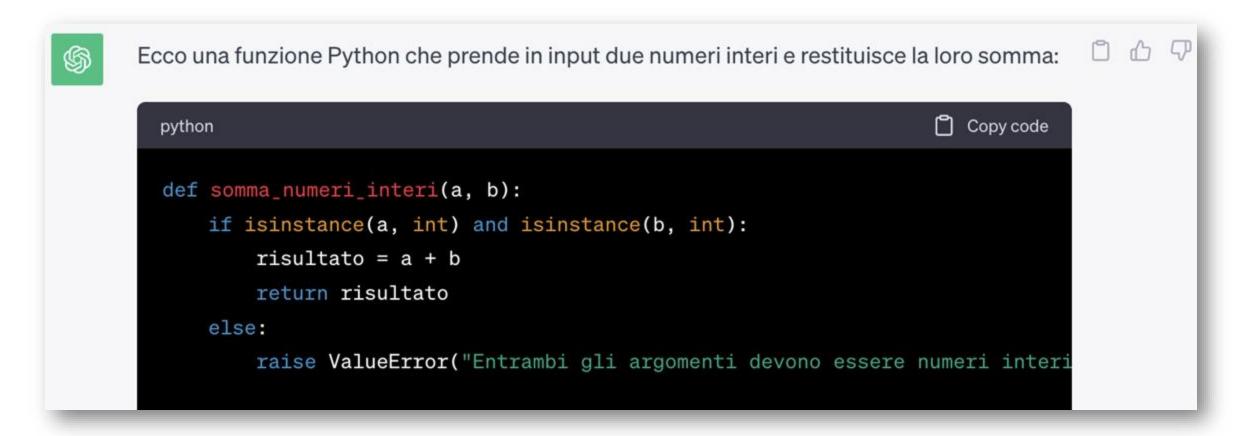






L'importanza del prompt

Scrivi una funzione in Python che prenda in input due numeri interi e restituisca la loro somma







L'importanza del prompt

I dettagli fanno la differenza!

Take home message

Più il prompt è preciso, più la risposta generata è accurata

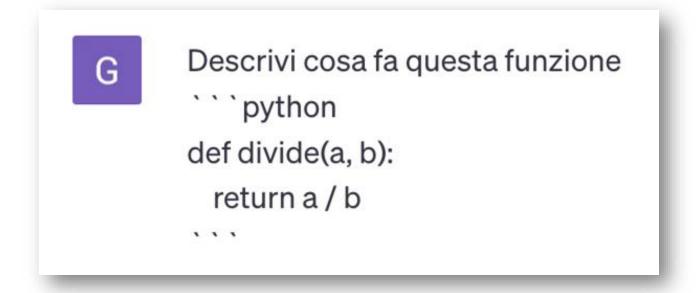
5





L'importanza del prompt

Facciamo un altro esempio...







L'importanza del prompt

Facciamo un altro esempio...



La funzione che hai fornito, denominata 'divide', esegue la divisione di due numeri 'a' e 'b' e restituisce il risultato della divisione. In particolare, questa funzione effettua una divisione in virgola mobile, il che significa che restituirà un numero decimale (a meno che il dividendo e il divisore non siano interi e la divisione sia esatta).

Ecco come funziona:

- * 'a' rappresenta il dividendo, cioè il numero che viene diviso.
- 'b' rappresenta il divisore, cioè il numero con cui viene diviso il dividendo.

La funzione utilizza l'operatore di divisione '/' per effettuare la divisione. Il risultato viene restituito immediatamente.





L'importanza del prompt

Poniamoci qualche domanda...







L'importanza del prompt

Se diamo istruzioni precise....

G

Scrivi una descrizione dettagliata di questo metodo, includendo cosa fa, quali sono i suoi parametri di input, cosa restituisce e qualsiasi eccezione che potrebbe sollevare

def divide(a, b):

return a / b





L'importanza del prompt

La risposta sarà più precisa....



La funzione 'divide' è un metodo Python che esegue una divisione tra due numeri e restituisce il risultato della divisione. Ecco una descrizione dettagliata del metodo:

- Nome del Metodo: divide
- Parametri di Input:
 - * 'a' (numero): Questo è il dividendo, il numero che verrà diviso.
 - * 'b' (numero): Questo è il divisore, il numero con cui verrà effettuata la divisione.
- * Cosa Fa:

La funzione 'divide' effettua una divisione tra i due numeri forniti come input. Utilizza l'operatore di divisione '/' per eseguire la divisione in virgola mobile. La divisione in virgola mobile significa che il risultato sarà un numero decimale (float), a meno che il dividendo e il divisore siano entrambi numeri interi e la divisione sia esatta. In caso di divisione per zero (quando 'b' è uguale a 0), questa funzione solleverà un'eccezione 'ZeroDivisionError', poiché la divisione per zero non è definita matematicamente.

Risultato:

La funzione restituisce il risultato della divisione come un numero decimale (float).

Eccezioni:

La funzione può sollevare un'eccezione 'ZeroDivisionError' se il divisore 'b' è uguale a 0, poiché la divisione per zero è un'operazione non valida in matematica. Al di fuori di questo caso, la funzione non solleva altre eccezioni standard.

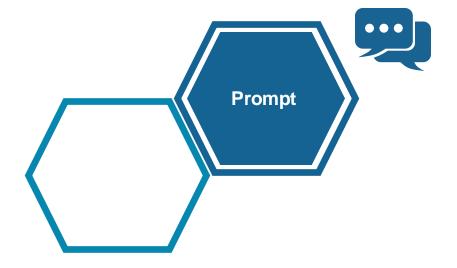




Prompt patterns

Few-shots learning

Fornire esempi per ottenere risultati simili.



Catalogo dei prompt patterns

Specifici su Software Engineering Generici per migliorare la Prompt Engineering

Nuovi patterns: Tree of thoughts

Per migliorare l'abilità di problem-solving degli LLM





Prompt patterns

Few-shots learning

Definizione

L'approccio si basa sull'idea di fornire al modello alcuni esempi, o "prompt", di ciò che si vuole che faccia, e poi chiedere al modello di completare un compito simile.





Prompt patterns

Few-shots learning

```
Esempi:
  "utente": {
   "nome": "Luigi",
   "cognome": "Bianchi",
   "email": "luigi.bianchi@example.com"
  "utente": {
   "nome": "Luigi",
   "cognome": "Bianchi",
   "email": "luigi.bianchi@example.com"
Genera un oggetto JSON per un utente con nome "Giuseppe", cognome "Verdi" e email
"giuseppe.verdi@example.com".
```





Prompt patterns

Few-shots learning







Prompt patterns

Catalogo dei prompt patterns

Specifici su Software Engineering

White, J., Hays, S., Fu, Q., Spencer-Smith, J., & Schmidt, D. C. (2023). Chatgpt prompt patterns for improving code quality, refactoring, requirements elicitation, and software design. arXiv preprint arXiv:2303.07839.

Generici per migliorare la prompt Engineering

White, J., Fu, Q., Hays, S., Sandborn, M., Olea, C., Gilbert, H., ... & Schmidt, D. C. (2023). A prompt pattern catalog to enhance prompt engineering with chatgpt. arXiv preprint arXiv:2302.11382.





Prompt patterns

Pattern Persona

Definizione

Aiuta a guidare il LLM per rispondere in un modo specifico, assumendo una particolare "persona" o carattere. Può essere utile quando si desidera che il LLM risponda con un certo tono, stile o punto di vista.





Prompt patterns

Pattern Persona

Definizione

Aiuta a guidare il LLM per rispondere in un modo specifico, assumendo una particolare "persona" o carattere. Può essere utile quando si desidera che il LLM risponda con un certo tono, stile o punto di vista.





Prompt patterns

Pattern Persona

G

D'ora in poi, comportati come un revisore della sicurezza. Presta molta attenzione ai dettagli di sicurezza di qualsiasi codice che esaminiamo. Fornisci output che un revisore della sicurezza darebbe riguardo al codice.



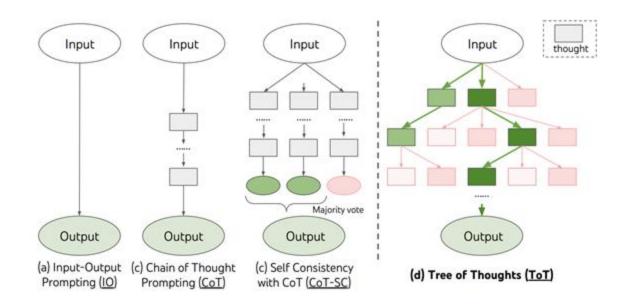


Prompt patterns

Tree of thoughts

Articolo dei ricarcatori di Google

Yao, S., Yu, D., Zhao, J., Shafran, I., Griffiths, T. L., Cao, Y., & Narasimhan, K. (2023). Tree of thoughts: Deliberate problem solving with large language models. arXiv preprint arXiv:2305.10601.







Prompt patterns

Tree of thoughts

Definizione

Struttura il prompt come un albero di pensieri, in cui ogni pensiero o idea è collegato al precedente in un flusso logico e coerente. Il risultato finale avviene per voto a maggioranza. Questo aiuta il modello a capire meglio il contesto e a generare risposte più accurate.

L'algoritmo principale va implementato con un linguaggio di programmazione!





Prompt patterns

Tree of thoughts

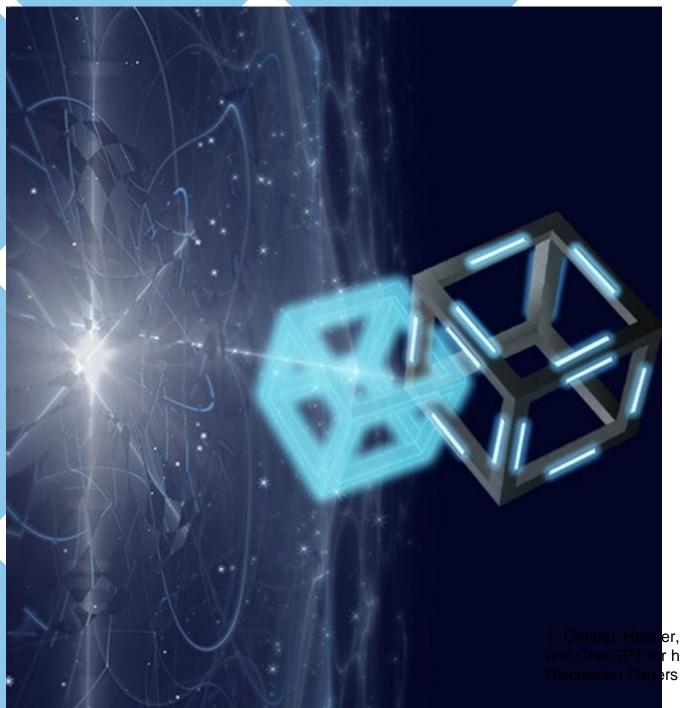
Esempio di applicazione

Ogni esperto scriverà un passaggio del proprio ragionamento, poi lo condividerà con il gruppo.

Poi tutti gli esperti passeranno al passaggio successivo, ecc.

Se un esperto si rende conto di aver sbagliato in qualsiasi momento, allora se ne va.

La domanda è...





Prima di iniziare: Raccomandazioni¹

1. Gimpel, Henner, et al. Unlocking the power of generative Al models and systems such as GPT-4 and ChatGPT for higher education: A guide for students and lecturers. No. 02-2023. Hohenheim Discussion Papers in Business, Economics and Social Sciences, 2023.

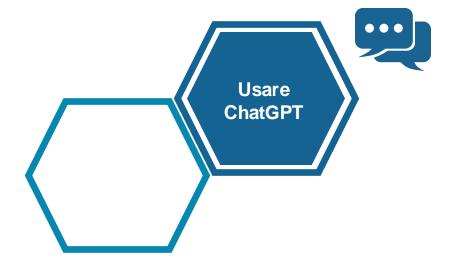




Raccomandazioni

Rispetto della legge e del regolamento universitario

È la base per utilizzare ChatGPT in modo corretto



I rischi dell'uso di ChatGPT

Attenzione ai poteziali errori e a non avere una cattiva condotta

Riflettere sui learning goals

L'istruzione superiore è molto di più che acquisire competenze specifiche in un settore.





Raccomandazioni

Rispetto della legge e del regolamento universitario

Raccomandazione n. 1

Gli studenti devono rispettare le norme e seguire eventuali istruzioni sui regolamenti d'esame sull'uso di strumenti basati sull'IA, rispettare le regole relative alle citazioni e alla buona pratica scientifica, e infine indicare se un testo è stato creato da un'IA o quale informazione è stata fornita all'IA.





Raccomandazioni

I rischi dell'uso di ChatGPT

Raccomandazione n. 2

- 1. Analizzare le risposte fornite dal LLM e questo vale anche per il codice.
- 2. Attenzione al plagio accidentale e alle violazioni del copyright.
- 3. Usare i sw antiplagio e i motori di ricerca semantici come strumenti di controllo.
- 4. Chiunque sottometta un lavoro a proprio nome è responsabile per la scrittura, anche se utilizza contenuti generati da ChatGPT o strumenti simili.

23





Raccomandazioni

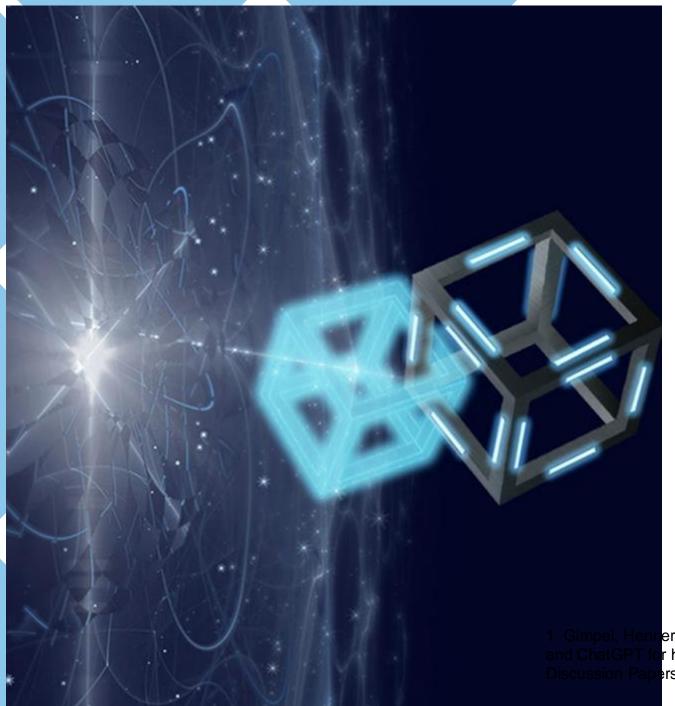
Riflettere sui learning goals

Raccomandazione n. 3

L'istruzione superiore non riguarda solo l'acquisizione di competenze specifiche del settore, ma include anche il coltivare e migliorare competenze essenziali come il pensiero critico e strutturato. ChatGPT influisce sulla possibilità di svilupparle durante gli studi

Raccomandazione n. 4

L'uso abile di ChatGPT richiede di sapere quali prompt daranno risultati utili, emergendo così l'ingegneria dei prompt come una nuova competenza di valore.





Iniziamo ad usare ChatGPT¹

Gimpel, Henner, et al. Unlocking the power of generative Al models and systems such as GPT-4 and ChatGPT for higher education: A guide for students and lecturers. No. 02-2023. Hohenheim Discussion Papers in Business, Economics and Social Sciences, 2023.

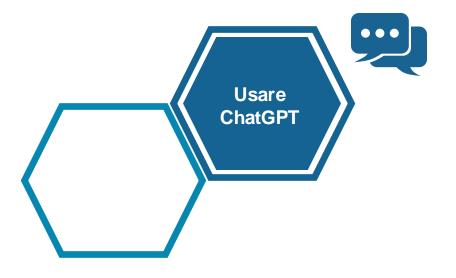




Iniziamo ad usare ChatGPT

Compagno di studi

ChatGPT può aiutare ad acquisire nuove conoscenze e testare quelle possedute



Riassumere materiale testuale

ChatGPT può aiutare a riassumere documenti, appunti etc. facendo risparmiare tempo importante

Compagno di scrittura

ChatGPT non può essere citato come autore e bisogna usarlo con dovizia nei compiti di scrittura.

Migliorare il coding

ChatGPT può generare e correggere codice e può dare suggerimenti per la programmazione





ChatGPT come compagno di studi

Generazione di "soluzioni modello" da vecchi compiti d'esame

Prompt

Per favore genera una soluzione modello per il seguente compito: [incolla il tuo compito]





ChatGPT come compagno di studi

Creare una mappa mentale

Prompt

[Tema]

Crea una **mappa mentale** sul tema sopra indicato, elenca l'idea centrale, i rami principali e i sottorami.





ChatGPT come compagno di studi

Spiegazione di concetti

Prompt

Voglio che tu agisca come un insegnante di ingegneria del software. Fornirò alcuni design patterns, e sarà tuo compito **spiegarli** in termini facili da capire. La mia prima domanda è: ho bisogno di aiuto per capire come funziona [incolla il tuo concetto]





ChatGPT come compagno di studi

Acquisizione del vocabolario

Prompt

Potresti per favore fornirmi i termini correlati a [incolla il tuo testo]

29





ChatGPT come compagno di studi

Creare schede didattiche

Prompt

Argomento: [incolla il tuo argomento]

Per favore, aiutami a creare un **foglio di calcolo** a due colonne con domande e risposte corrispondenti sull'argomento sopra indicato.





ChatGPT come compagno di studi

Auto-verifica di conoscenze specifiche

Prompt

Argomento: [incolla il tuo argomento]

Per favore, fai cinque **domande** sul tema sopra. Poi risponderò. Dopo la mia risposta, mi dirai se la mia risposta era giusta o sbagliata e fornirai una spiegazione.





ChatGPT per riassumere materiale

Riassumere del testo

Prompt

Sintetizza il testo che segue: [incolla il tuo testo]





ChatGPT per riassumere materiale

....e se il testo è troppo lungo per ChatGPT

Suggerimento

- 1. Dividi il testo in sezioni di lunghezza gestibile da ChatGPT.
- 2. Fai riassumere da ChatGPT ogni sezione.
- 3. Unisci le sezioni e chiedi a ChatGPT di fornire una sintesi senza perdere dettagli importanti.
- 4. Procedi iterativamente se necessario.





ChatGPT per riassumere materiale

Riassumere video

Procedimento per riassumere la trascrizione da un video

Diversi plug-in di terze parti per browser (ad esempio, YouTube Summary con ChatGPT) forniscono agli studenti l'opportunità di generare riassunti di video YouTube basati su ChatGPT. Il plug-in accede ed esporta la trascrizione standard di YouTube e la trasmette a ChatGPT, richiedendo un riassunto che viene poi presentato all'utente tramite il plug-in del browser.





ChatGPT come compagno di scrittura

Ricorda

Presta attenzione

- 1. L'IA non può sostituire il pensiero critico e la creatività, componenti essenziali dei compiti di scrittura.
- 2. ChatGPT non sarà mai l'autore di un lavoro, e la responsabilità per il contenuto scritto sarà sempre dell'autore umano
- 3. Ricorda i limiti di ChatGPT: allucinazioni, mancanza di ragionamento, plagio





ChatGPT come compagno di scrittura

Ma allora non possiamo usarlo per i compiti di scrittura?



Si, possiamo. Ma dobbiamo usarlo come uno strumento di supporto come Wikipedia o Google





ChatGPT come compagno di scrittura

Generare un titolo per un saggio

Prompt

Genera cinque titoli per un saggio su [incolla il tuo testo]





ChatGPT come compagno di scrittura

Parafrasi

Prompt

Parafrasa questa frase: [incolla il tuo testo]





ChatGPT come compagno di scrittura

Editing

Prompt

Per favore, **rivedi** la seguente frase per renderla più chiara e concisa: [Incolla il tuo testo]





ChatGPT come compagno di scrittura

Revisione

Prompt

Agisci da esperto revisore [indica l'ambito se necessario]. Revisiona il testo che segue, evidenziando punti di forza e debolezza. [Incolla il tuo testo]





ChatGPT per migliorare il coding

Aiuto con la sintassi

Prompt

Qual è la sintassi [incolla il tuo testo] in Python?





ChatGPT per migliorare il coding

Fornire esempi di coding

Prompt

Per favore, potresti darmi un esempio di come usare la funzione [incolla la tua funzione] in JavaScript?





ChatGPT per migliorare il coding

Consigli di programmazione

Prompt

Quali sono alcuni consigli per [incolla il tuo testo]?





ChatGPT per migliorare il coding

Aiuto per il debug

Prompt

Come posso risolvere l'errore ['TypeError: 'int' object is not subscriptable'] nel mio codice Python?





ChatGPT per migliorare il coding

Spiegazione di codice

Prompt

Puoi spiegare il codice per me passo dopo passo: [incolla il tuo codice]?