



UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Laurea triennale in Informatica

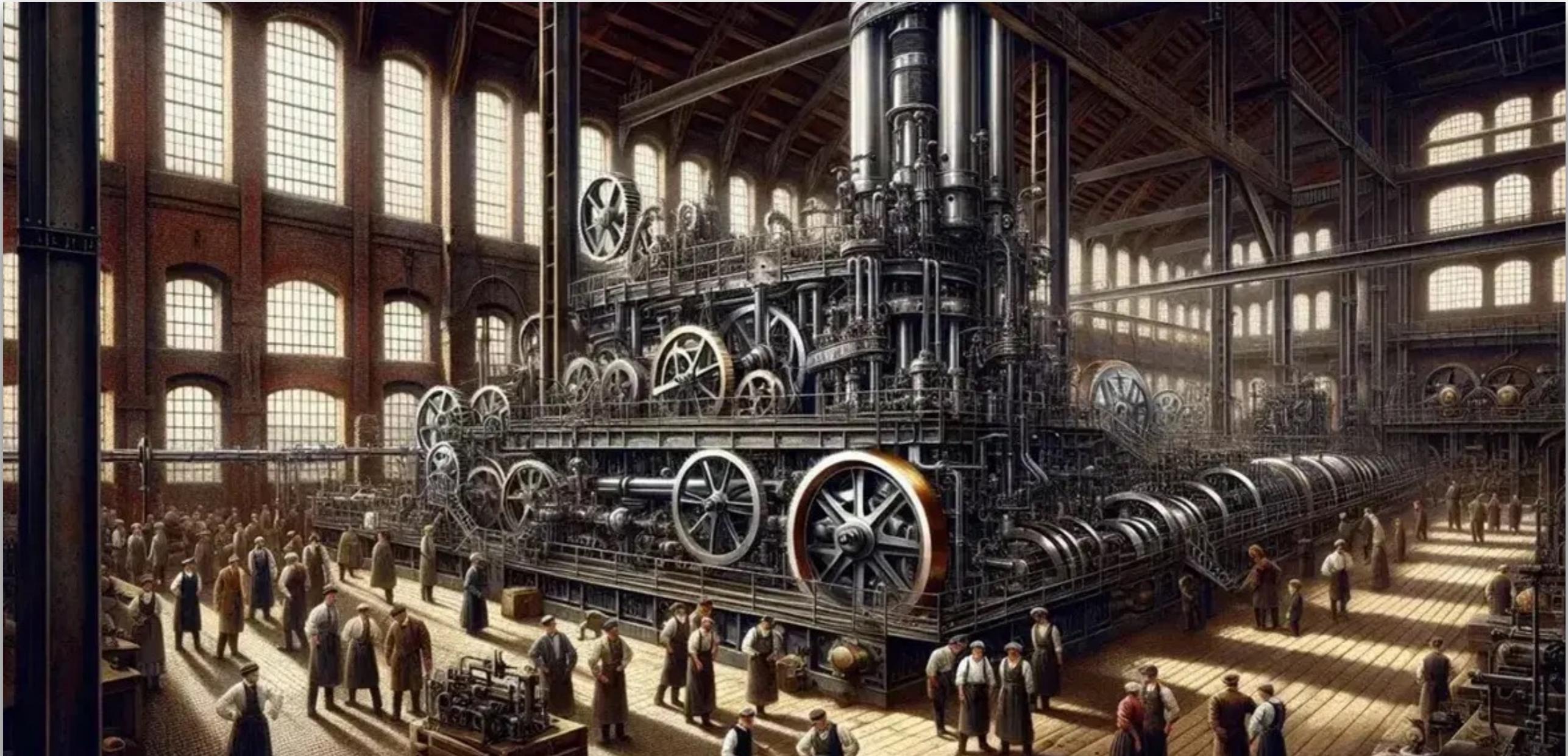
Fondamenti di Intelligenza Artificiale

Lezione 19 - Large Language Model



Large Language Model

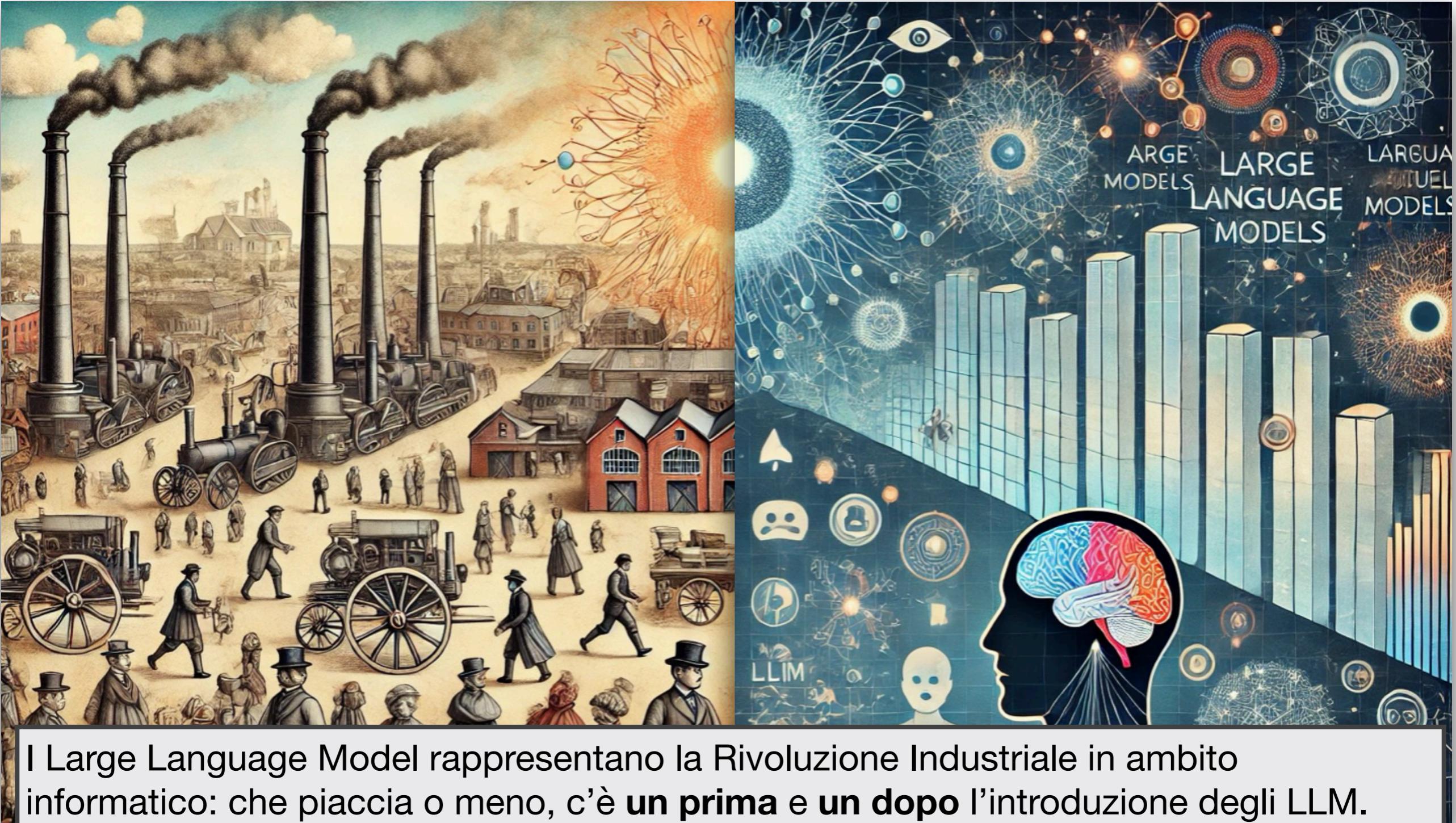
La Rivoluzione Industriale



La Rivoluzione Industriale è stato un periodo di trasformazioni economiche, tecnologiche e sociali iniziato nel XVIII secolo, caratterizzato dall'introduzione di macchine, la produzione su larga scala, e il passaggio da un'economia agricola a una industriale, cambiando radicalmente la società e il lavoro umano.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica



I Large Language Model rappresentano la Rivoluzione Industriale in ambito informatico: che piaccia o meno, c'è **un prima e un dopo** l'introduzione degli LLM. Nulla è più come prima. Come vi immaginate tra 10 anni?

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Trasformazione della produzione.

- *Rivoluzione Industriale:* Ha introdotto la produzione su larga scala grazie alla meccanizzazione, trasformando l'economia artigianale in industriale. Le macchine sostituirono o amplificarono il lavoro manuale, aumentando drasticamente l'efficienza.
- *Rivoluzione LLM:* Gli LLM, come ChatGPT, stanno rivoluzionando la produzione di contenuti (testuali, creativi, tecnici), automatizzando attività complesse come la scrittura, la programmazione e il supporto decisionale.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Impatto sulla Forza Lavoro.

- *Rivoluzione Industriale:* Ha creato nuovi lavori nelle fabbriche, ma ha anche ridotto la domanda di lavoro manuale tradizionale, causando un'importante riconversione delle competenze.
- *Rivoluzione LLM:* Gli LLM stanno rendendo alcune professioni meno centrali (ad esempio, compiti ripetitivi o analisi di base), spingendo i lavoratori a sviluppare competenze più creative o orientate al controllo delle tecnologie.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Democratizzazione delle Risorse.

- *Rivoluzione Industriale:* La produzione di massa ha reso beni prima costosi o esclusivi più accessibili a un pubblico più vasto.
- *Rivoluzione LLM:* Gli LLM stanno democratizzando l'accesso a strumenti avanzati di intelligenza artificiale, rendendo disponibili conoscenze, traduzioni, assistenza tecnica e creativa a un ampio pubblico.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Cambiamento delle Infrastrutture.

- *Rivoluzione Industriale:* Ha richiesto lo sviluppo di nuove infrastrutture, come fabbriche, ferrovie e sistemi di trasporto.
- *Rivoluzione LLM:* Richiede enormi infrastrutture digitali, come data center, cloud computing e sistemi di elaborazione ad alte prestazioni.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Innovazioni Trainanti.

- *Rivoluzione Industriale:* Innovazioni come la macchina a vapore, i telai meccanici e la metallurgia hanno guidato il cambiamento.
- *Rivoluzione LLM:* Le architetture dei modelli neurali (ad esempio, Transformer), la disponibilità di dati su vasta scala e i miglioramenti nell'hardware computazionale (GPU, TPU) sono le innovazioni chiave.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Nuove Problematiche.

- *Rivoluzione Industriale:* Ha generato problemi come lo sfruttamento del lavoro, l'inquinamento ambientale e le disuguaglianze economiche.
- *Rivoluzione LLM:* Sta sollevando questioni etiche e sociali, come i bias algoritmici, la disinformazione, il diritto d'autore e le implicazioni sulla privacy.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni paralleli con la rivoluzione industriale...

Cambiamento Culturale.

- *Rivoluzione Industriale:* Ha modificato radicalmente la società, introducendo nuovi stili di vita urbani e un'accelerazione del progresso scientifico.
- *Rivoluzione LLM:* Sta cambiando il modo in cui le persone apprendono, comunicano e creano, influenzando l'istruzione, l'intrattenimento e il lavoro.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Come abbiamo visto durante questo corso, il machine learning ha raggiunto notevoli progressi in diverse aree, incluse quelle della classificazione, regressione e clustering.

Tuttavia, molte di queste tecniche funzionano bene sotto una determinata assunzione: I dati di training e di test provengono **dallo stesso spazio delle caratteristiche e dalla stessa distribuzione**.

Quando la distribuzione cambia, questi modelli statistici devono essere ricostruiti da zero utilizzando nuovi dati di addestramento raccolti. **Questa operazione può essere costosa** o, in alcuni casi, addirittura **impossibile da eseguire**.

Ad esempio, considerate un modello che predice le vendite di ombrelli basandosi sui dati di pioggia in una città. Se il modello è stato addestrato su dati raccolti in una città con un clima piovoso, ma viene utilizzato in una città con un clima secco, la distribuzione dei dati cambia completamente!

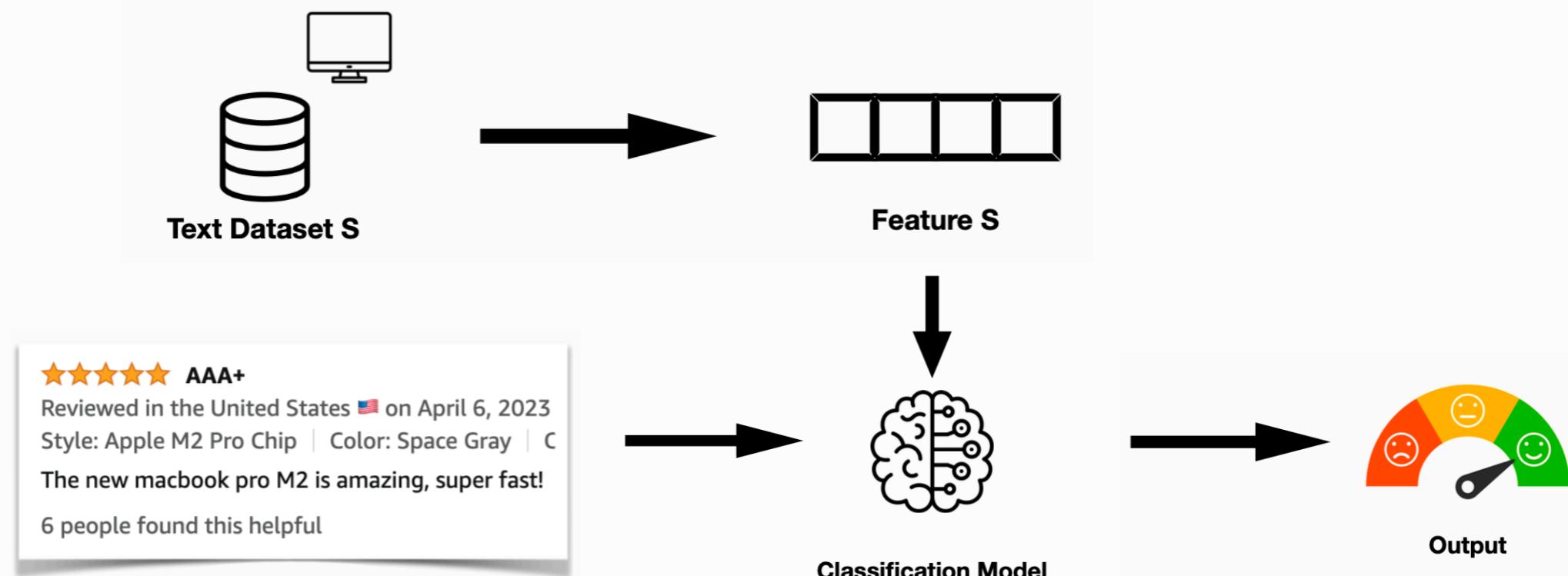
Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Consideriamo l'esempio della sentiment analysis per review di un prodotto.



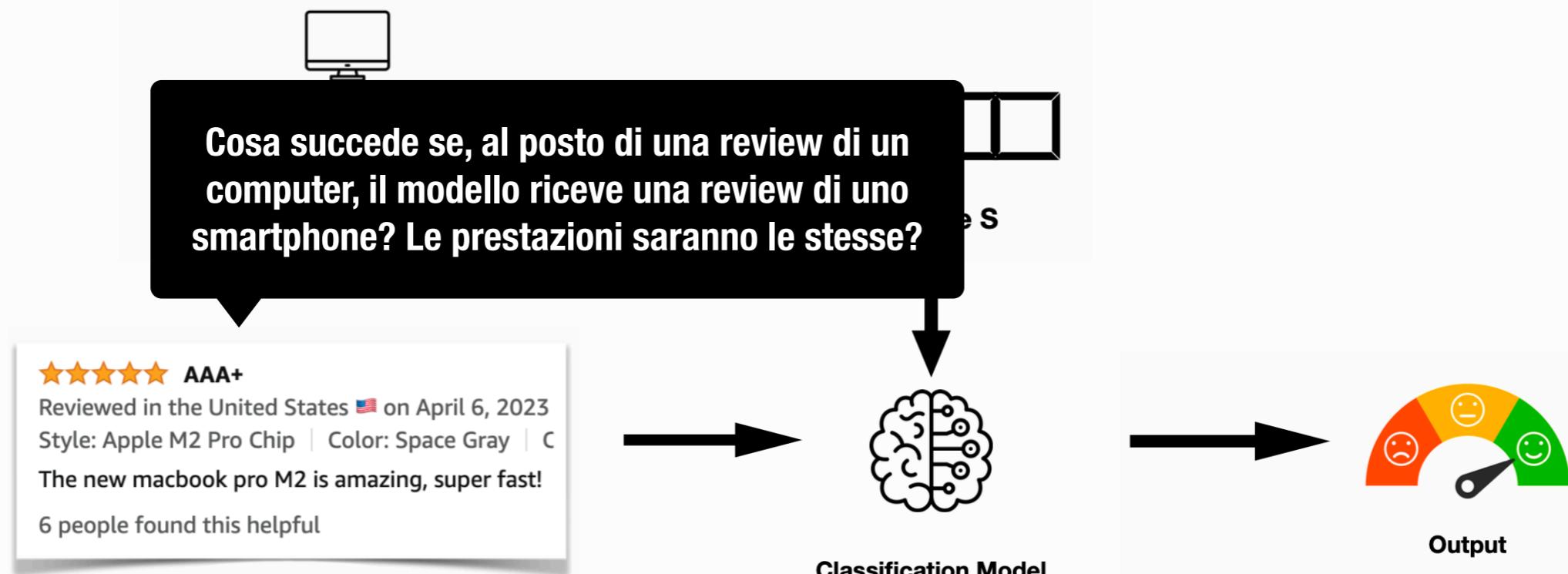
Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Consideriamo l'esempio della sentiment analysis per review di un prodotto.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Il modello è stato addestrato su dati relativi alle review di computer, non di smartphone. Quindi, potrebbe esserci un decremento delle prestazioni se i dati ricevuti sono significativamente diversi dai dati nel training set.

Per mantenere delle buone prestazioni, dovremmo quindi progettare la nostra soluzione in maniera tale da avere un numero sufficiente di dati di training per ciascun prodotto che ci si aspetta di osservare nell'ambiente operativo.

Oppure...

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Dall'Ingegneria del Software, possiamo prendere in prestito alcuni termini... ad esempio, **il concetto di riuso**.

Riuso: La pratica di utilizzare un modello già addestrato su un determinato problema o dominio come base per risolvere un altro problema, riducendo il bisogno di ricostruire un modello da zero. Questa tecnica consente di sfruttare conoscenze preesistenti apprese dal modello per risparmiare tempo, risorse computazionali e dati.

In un mondo fatto di dati, questa sembra essere una soluzione interessante... anche considerando il fatto che **molti dei problemi che ci interessa risolvere sono già stati risolti in passato, o quantomeno affrontati**, utilizzando modelli e approcci che possono essere adattati o riutilizzati per contesti simili.

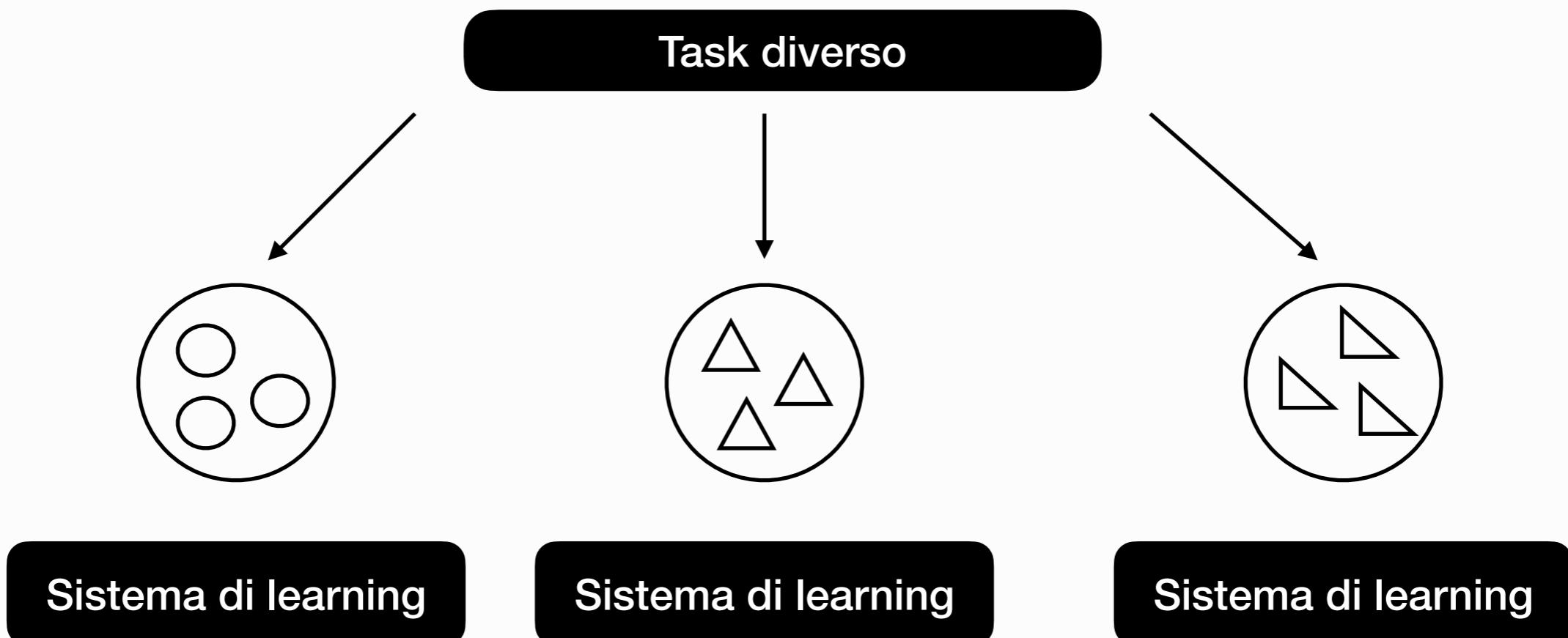
Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

Questo significa passare da una situazione del genere...



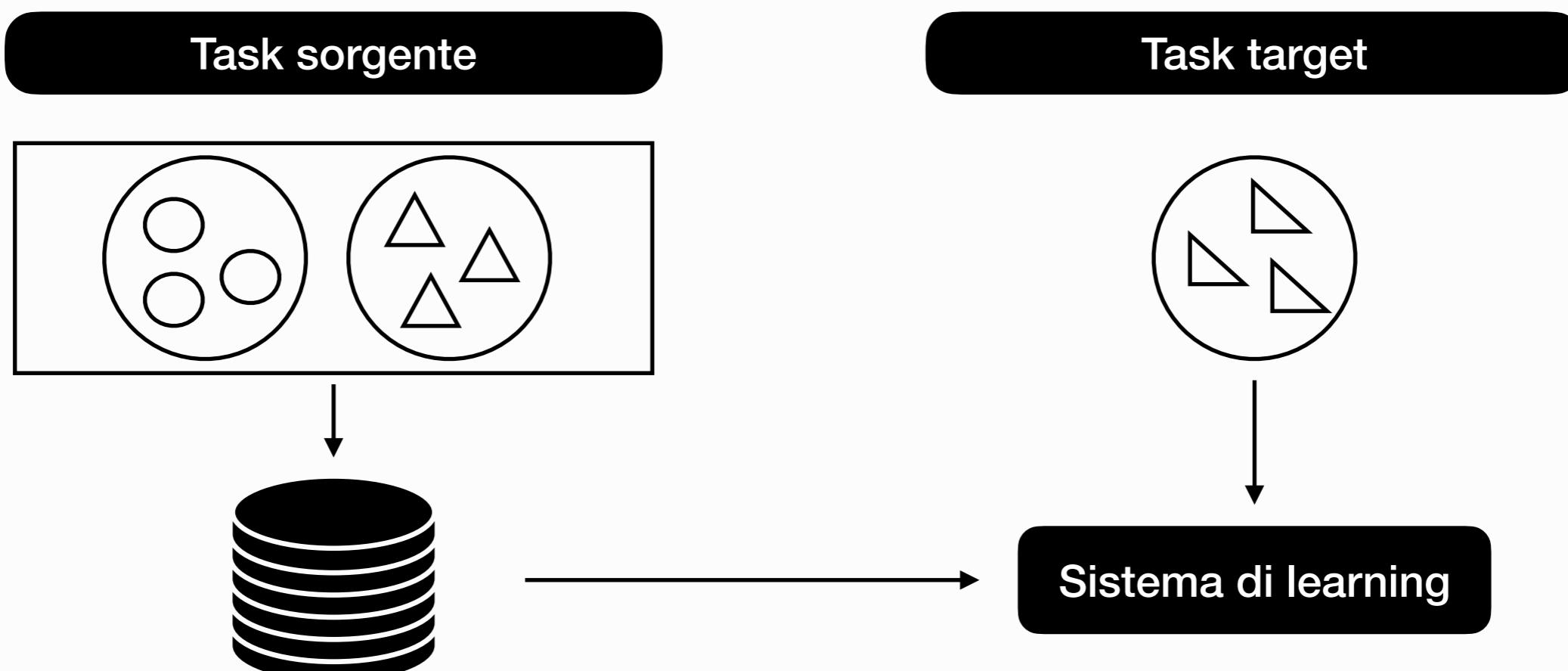
Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Da dove tutto ha avuto inizio...

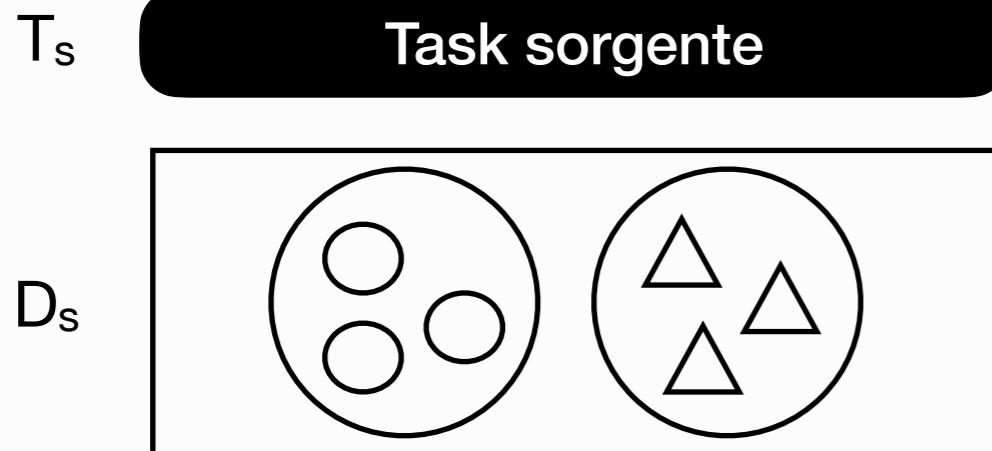
Ad una situazione del genere...



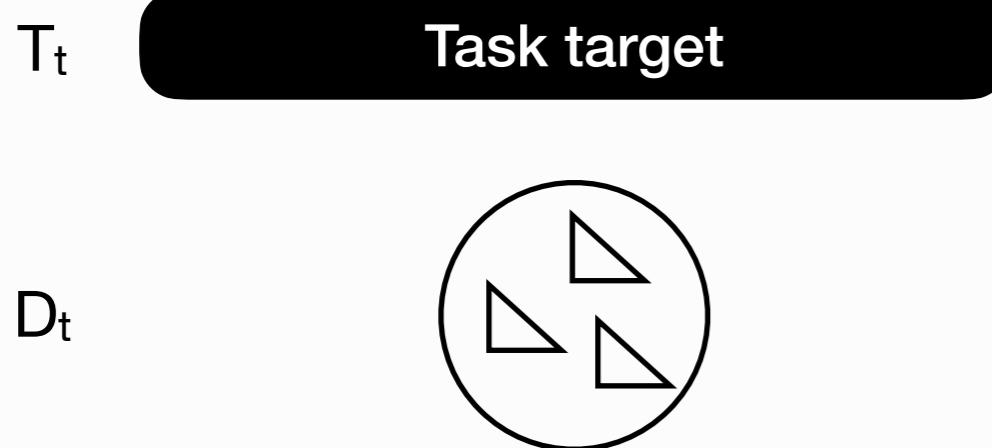
Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.



D_s , *Dominio della sorgente dei dati*: l'insieme di dati utilizzati per costruire la conoscenza di base per il task sorgente T_s .



D_t , *Dominio dei dati target*: l'insieme di dati che il modello utilizza per adattarsi al task target a partire dal task sorgente T_t .

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Dati D_s , D_t , T_s e T_t , possiamo definire il transfer learning.

Transfer Learning: Tecnica di machine learning in cui un modello pre-addestrato nel dominio D_s su un task T_s viene riutilizzato, adattato o perfezionato per risolvere un nuovo task T_t nel dominio D_t .

È importante notare che nel transfer learning valgono le seguenti proprietà:
 $D_s \neq D_t$ OR $T_s \neq T_t$.

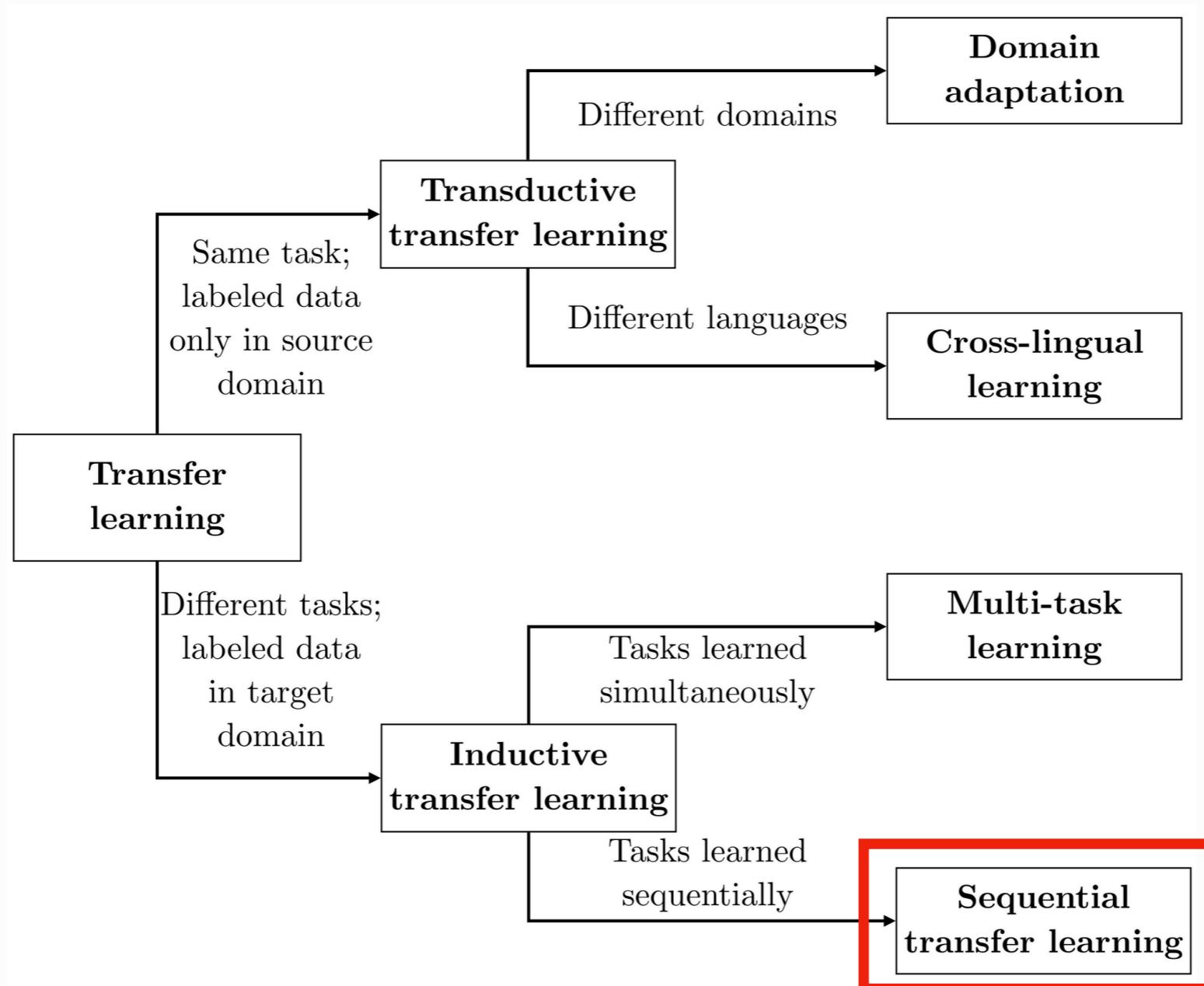
Sembra una cosa banale, ma
attenzione: c'è un OR, non un AND!

Questo significa che possiamo riusare un modello addestrato nello stesso dominio variando il task richiesto o variare il dominio per addestrare un modello su uno stesso task.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

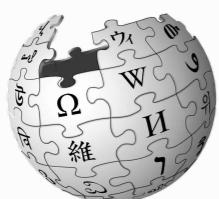
Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

È chiamato "sequential" perché il modello viene adattato progressivamente, in più fasi, invece di essere completamente riaddestrato da zero.

Step #1. Il modello viene addestrato su un dataset sorgente di grandi dimensioni e generico, che aiuta ad apprendere caratteristiche di base.

Esempio. *Predizione del sentimento delle recensioni di prodotti specifici.*



Consideriamo un grande corpus di testo generico, come Wikipedia o il dataset BookCorpus. Questo verrà usato per addestrare un modello di linguaggio generico (NB: parliamo di reti neurali!).

L'obiettivo è imparare rappresentazioni linguistiche generiche, come la comprensione del contesto e delle relazioni semantiche tra parole. Il modello è in grado di comprendere il linguaggio naturale in modo ampio, ma non è ancora specifico per l'analisi del sentimento.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

È chiamato "sequential" perché il modello viene adattato progressivamente, in più fasi, invece di essere completamente riaddestrato da zero.

Step #2. Il modello pre-addestrato viene ulteriormente addestrato sul dataset target o su un dataset intermedio, che può essere più piccolo e specifico rispetto al dataset sorgente. Questo avviene in modo sequenziale:

- (1) *Congelamento di Layer.* I primi layer del modello (che catturano caratteristiche generali) vengono congelati per preservare le conoscenze già acquisite.
- (2) *Fine-Tuning.* Gli ultimi strati vengono addestrati con i dati target per apprendere caratteristiche più specifiche.

Il modello può anche passare attraverso più fasi di fine-tuning sequenziale su diversi dataset, ciascuno rappresentante un livello di specificità maggiore.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

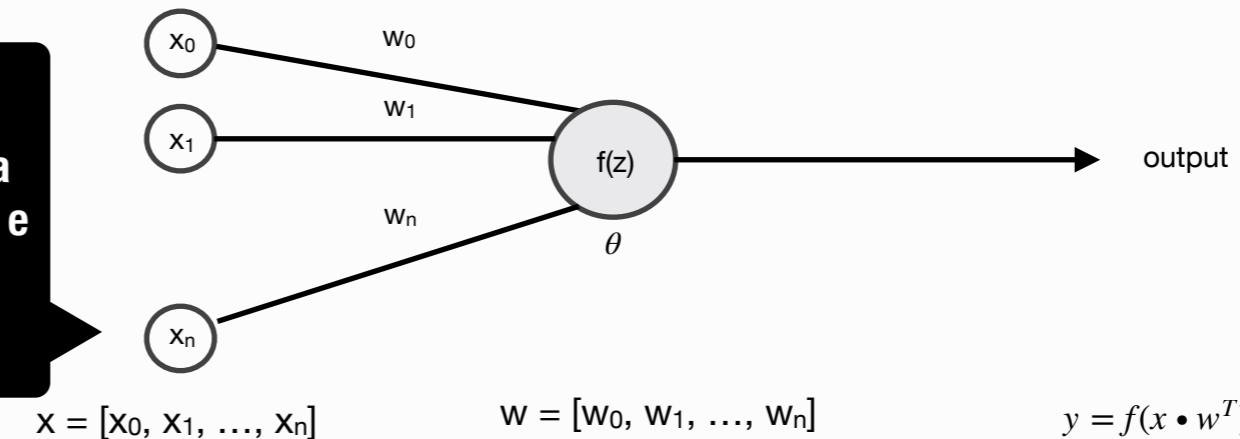
Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

È chiamato "sequential" perché il modello viene adattato progressivamente, in più fasi, invece di essere completamente riaddestrato da zero.

Step #2. Il modello pre-addestrato viene ulteriormente addestrato sul dataset target o su un dataset intermedio, che può essere più piccolo e specifico rispetto al dataset sorgente. Questo avviene in modo sequenziale:

Esempio. Predizione del sentimento delle recensioni di prodotti specifici.

Da un punto di vista pratico, questo significa “congelare” i pesi dei neuroni nei primi layer e modificare quelli dei neuroni successivi



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

È chiamato "sequential" perché il modello viene adattato progressivamente, in più fasi, invece di essere completamente riaddestrato da zero.

Step #2. Il modello pre-addestrato viene ulteriormente addestrato sul dataset target o su un dataset intermedio, che può essere più piccolo e specifico rispetto al dataset sorgente. Questo avviene in modo sequenziale:

Esempio. *Predizione del sentimento delle recensioni di prodotti specifici.*

Da un punto di vista pratico, questo significa “congelare” i pesi dei neuroni nei primi layer e modificare quelli dei neuroni successivi

Nei modelli linguistici, i primi strati sono responsabili di catturare pattern sintattici di base, come la struttura delle frasi e il contesto delle parole. Congelando questi strati, si evita di modificare queste rappresentazioni generiche.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

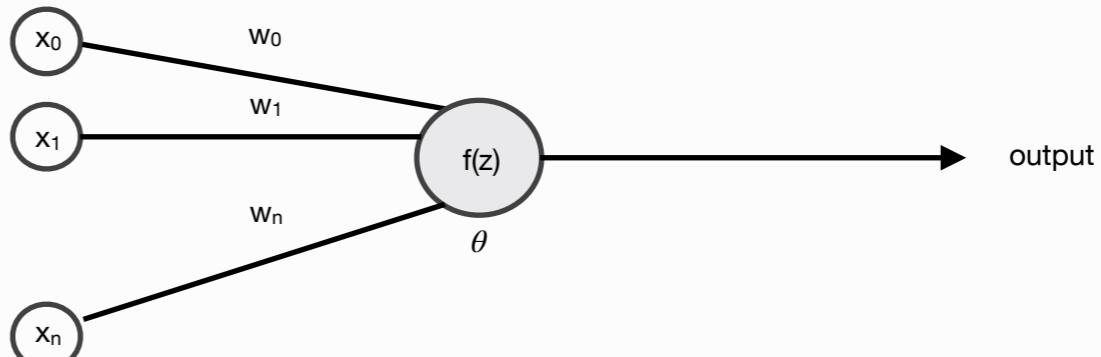
Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

È chiamato "sequential" perché il modello viene adattato progressivamente, in più fasi, invece di essere completamente riaddestrato da zero.

Step #3. Nei passaggi successivi, i dati del dominio target vengono utilizzati per perfezionare ulteriormente il modello. A questo punto, solo una parte degli strati del modello vengono aggiornati.

Esempio. Predizione del sentimento delle recensioni di prodotti specifici.

In altri termini, si procede iterativamente a raffinare gli ultimi strati del modello, variando i pesi dei neuroni in maniera che il modello si adatti via via ai dati di training del contesto specifico a cui siamo interessati



$$x = [x_0, x_1, \dots, x_n]$$

$$w = [w_0, w_1, \dots, w_n]$$

$$y = f(x \cdot w^T)$$

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Il sequential transfer learning è una variante del transfer learning in cui un modello addestrato su un task sorgente viene successivamente adattato a uno o più task target in modo sequenziale.

Esempio completo. *Predizione del sentimento delle recensioni di prodotti specifici.*

Step #1. Un grande corpus di testo generico, come Wikipedia o il dataset BookCorpus, usato per addestrare un modello di linguaggio generico (ad esempio, BERT o GPT).

Step #2. Recensioni generiche di film (ad esempio, il dataset IMDB, che contiene etichette di sentimento positive e negative per recensioni di film). Congelamento degli strati inferiori del modello pre-addestrato (che contengono rappresentazioni linguistiche generiche) e addestramento degli ultimi strati sui dati delle recensioni di film.

Step #3. Recensioni di prodotti specifici, come smartphone, elettrodomestici o videogiochi, provenienti da piattaforme come Amazon o eBay. Il modello viene ulteriormente addestrato sui dati target, che potrebbero contenere terminologie specifiche del dominio (ad esempio, "buona batteria" o "schermo scadente").

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma di quale tipologia di modelli di machine learning stiamo parlando? Per adesso, ci siamo solo limitati a dire che si tratta di reti neurali...

Transformer: Una particolare architettura di rete neurale basata sul meccanismo di self-attention, che riesce a modellare relazioni complesse tra elementi di una sequenza, indipendentemente dalla loro posizione relativa.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Attention Is All You Need

Ashish Vaswani*
Google Brain
avaswani@google.com

Noam Shazeer*
Google Brain
noam@google.com

Niki Parmar*
Google Research
nikip@google.com

Jakob Uszkoreit*
Google Research
usz@google.com

Llion Jones*
Google Research
llion@google.com

Aidan N. Gomez* †
University of Toronto
aidan@cs.toronto.edu

Łukasz Kaiser*
Google Brain
lukaszkaiser@google.com

Illia Polosukhin* ‡
illia.polosukhin@gmail.com

Abstract

The dominant sequence transduction models are based on complex recurrent or convolutional neural networks that include an encoder and a decoder. The best performing models also connect the encoder and decoder through an attention mechanism. We propose a new simple network architecture, the Transformer, based solely on attention mechanisms, dispensing with recurrence and convolutions entirely. Experiments on two machine translation tasks show these models to be superior in quality while being more parallelizable and requiring significantly less time to train. Our model achieves 28.4 BLEU on the WMT 2014 English-to-German translation task, improving over the existing best results, including ensembles, by over 2 BLEU. On the WMT 2014 English-to-French translation task, our model establishes a new single-model state-of-the-art BLEU score of 41.8 after training for 3.5 days on eight GPUs, a small fraction of the training costs of the best models from the literature. We show that the Transformer generalizes well to other tasks by applying it successfully to English constituency parsing both with large and limited training data.

*Equal contribution. Listing order is random. Jakob proposed replacing RNNs with self-attention and started the effort to evaluate this idea. Ashish, with Illia, designed and implemented the first Transformer models and has been crucially involved in every aspect of this work. Noam proposed scaled dot-product attention, multi-head attention and the parameter-free position representation and became the other person involved in nearly every detail. Niki designed, implemented, tuned and evaluated countless model variants in our original codebase and tensor2tensor. Llion also experimented with novel model variants, was responsible for our initial codebase, and efficient inference and visualizations. Lukasz and Aidan spent countless long days designing various parts of and implementing tensor2tensor, replacing our earlier codebase, greatly improving results and massively accelerating our research.

†Work performed while at Google Brain.

‡Work performed while at Google Research.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma di quale tipologia di modelli di machine learning stiamo parlando? Per adesso, ci siamo solo limitati a dire che si tratta di reti neurali...

Transformer: Una particolare architettura di rete neurale basata sul meccanismo di self-attention, che riesce a modellare relazioni complesse tra elementi di una sequenza, indipendentemente dalla loro posizione relativa.

Tale meccanismo rappresenta una delle innovazioni più rilevanti del secolo. Tradizionalmente, le reti neurali elaborano una sequenza *elemento per elemento*, rendendo più difficile catturare relazioni tra parole lontane nella sequenza.

I Transformer, invece, usano il meccanismo di self-attention per analizzare *ogni elemento della sequenza rispetto a tutti gli altri contemporaneamente*, assegnando un peso che rappresenta la loro importanza relativa.

Questo li rende particolarmente adatti per compiti di elaborazione del linguaggio naturale (NLP) e oltre, come la traduzione automatica, il completamento del testo e la generazione di testo.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

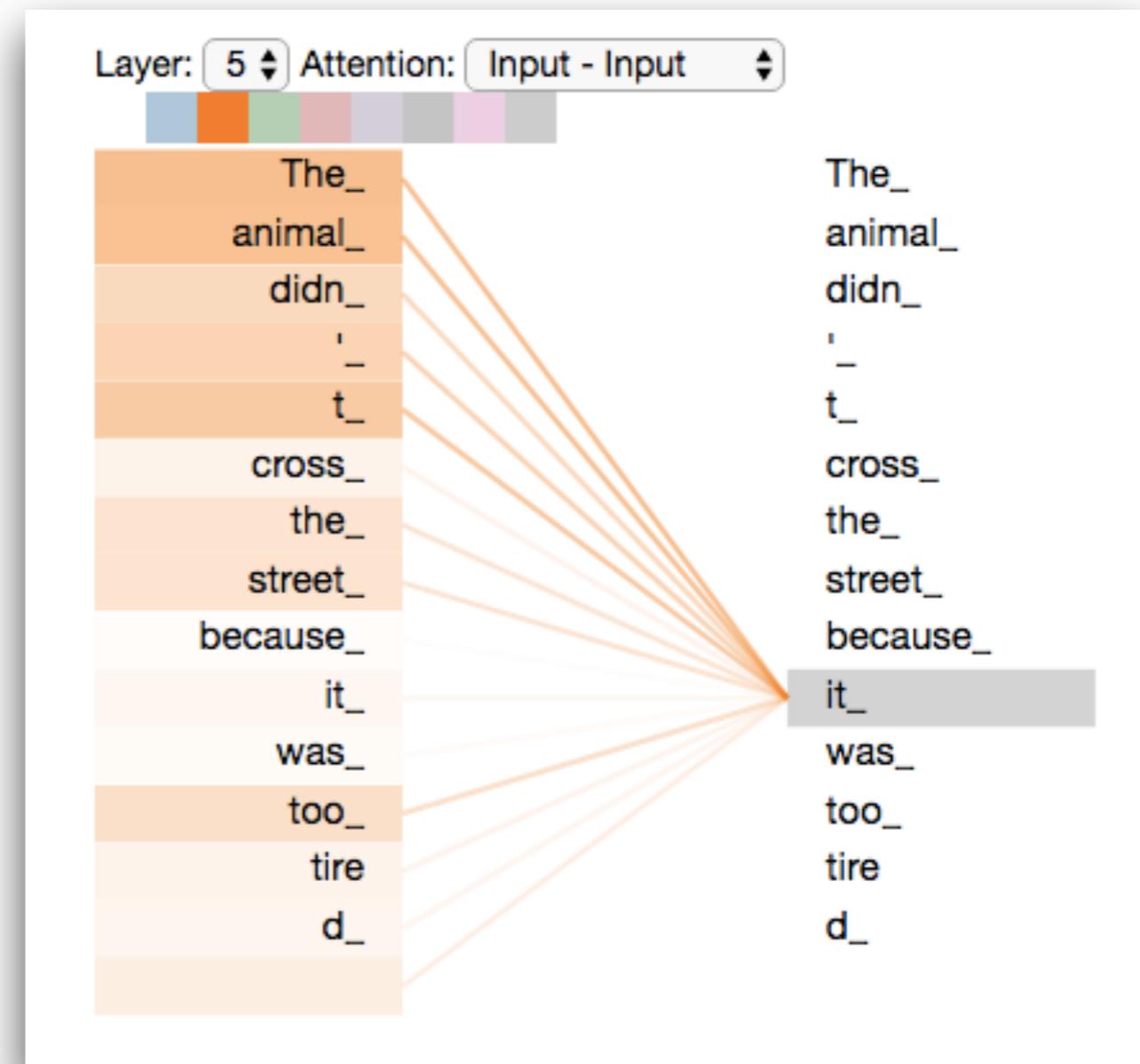
Cosa significa “attenzione”?

Data la frase:

“*The animal didn't cross the street because **it** was too tired*”.

Il meccanismo, considerando il contesto dell’intera frase, è capace di assegnare una probabilità maggiore al fatto che “**it**” faccia riferimento all’animale piuttosto che alla strada.

Nei modelli tradizionali, questo non sarebbe possibile, poiché ogni parola verrebbe considerata singolarmente.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

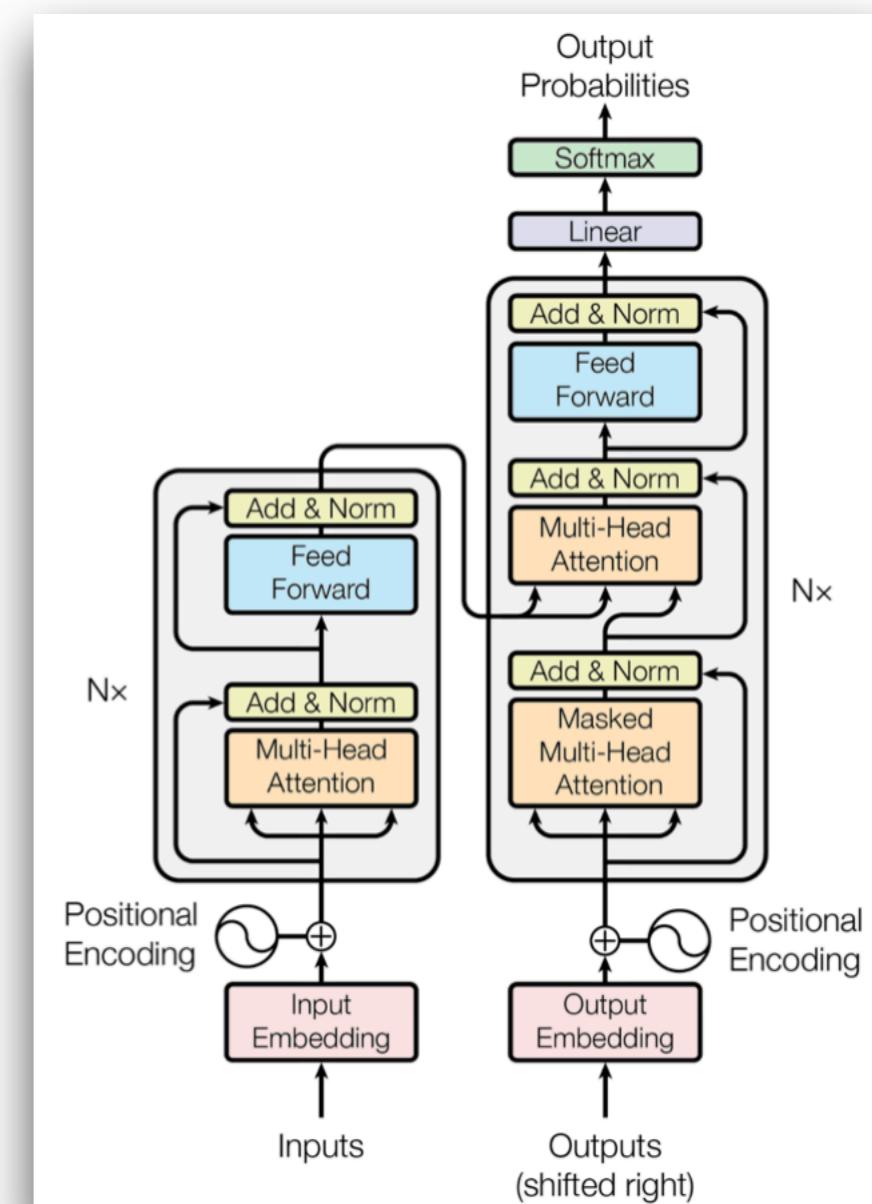
Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Non entreremo nel dettaglio dell'architettura - ci vorrebbero ore per descrivere ogni singolo step nel dettaglio - ma basta sapere che è composta da due moduli chiave:

(1) *Encoder*. Modulo che prende in input una sequenza e la trasforma in una rappresentazione comprensibile per il modello.

(2) *Decoder*. Modulo che genera una sequenza di output basandosi sulla rappresentazione creata dall'encoder e sugli elementi precedentemente generati.

Cerchiamo di capire meglio ciò di cui stiamo parlando...



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

L'encoder può essere paragonato ad un *traduttore* che "riassume" il contenuto di una frase in un linguaggio universale comprensibile per il computer.

Input. L'encoder riceve una sequenza di parole (ad esempio, una frase).

Comprendere il contesto. Ogni parola viene analizzata non solo individualmente, ma anche in relazione alle altre, per capire cosa significa nel contesto della frase. Per esempio, nella frase "*Il gatto nero è sulla sedia*", l'encoder capisce che "nero" descrive "gatto" e non "sedia".

Trasformazione. Dopo aver analizzato il contesto, l'encoder converte ogni parola in una rappresentazione numerica densa (un "riassunto"), che contiene informazioni sia sul significato della parola sia sulla sua relazione con le altre.

In breve, quindi, l'encoder può essere visto come un blocco di "comprendere del testo" che prepara l'informazione per il modulo successivo, rendendola facilmente elaborabile dal modello —> è una forma di preprocessing, simile a quella che abbiamo visto quando abbiamo parlato di data engineering.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Il decoder può essere paragonato ad uno *scrittore creativo* che prende il riassunto universale fatto dall'encoder e lo trasforma in un testo leggibile, parola dopo parola.

Input. Il decoder riceve il "riassunto" prodotto dall'encoder e, se sta generando una sequenza, riceve anche ciò che ha già scritto finora (ad esempio, le prime parole tradotte di una frase).

Aggiunta del significato. Usa il riassunto dell'encoder per capire il contesto generale e guarda ciò che è già stato scritto per assicurarsi che il prossimo pezzo abbia senso. Per esempio, se sta traducendo "*Il gatto nero è sulla sedia*" in inglese, dopo aver scritto "*The black cat,*" il decoder stima che "*is on the chair*" debba essere il prossimo pezzo della stringa.

Scrittura. Genera una parola o un simbolo alla volta, migliorando e verificando continuamente con il contesto dell'encoder e l'output già generato.

Iniziate a riconoscere il comportamento di ChatGPT? Pensate a quando, a volte, impiega del tempo per generare una nuova parola nella frase che state aspettando...

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Sulla base di questa architettura, sono nati diversi modelli abbastanza noti:

(1) *BERT (Bidirectional Encoder Representations from Transformers)* 

Un modello pre-addestrato progettato solo come encoder. BERT analizza ogni parola in relazione a tutte le altre parole della sequenza, sia quelle precedenti che quelle successive, per catturare il significato più completo possibile.

BERT non ha il modulo decoder perché non è pensato per creare nuovo testo, ma solo per rappresentarlo in un formato che catturi tutte le relazioni e il significato intrinseco del testo.

Sulla base di BERT, diversi altri modelli sono nati. Ad esempio, RoBERTa (Robustly Optimized BERT Pre-training Approach) o CodeBERT. Questi si differenziano (1) per i dati di training - ad esempio, CodeBERT è addestrato su su dati di codice sorgente e documentazione; e (2) tipo di task di addestramento - ad esempio, RoBERTa rimuove il compito *Next Sentence Prediction*.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Sulla base di questa architettura, sono nati diversi modelli abbastanza noti:

(1) *BERT (Bidirectional Encoder Representations from Transformers)* 

BERT è addestrato su due specifici task non-supervisionati: *Masked Language Modeling* e *Next Sentence Prediction*.

Sentence:

It is [MASK] to
[MASK] that

Mask 1 Predictions:

11.5%	important
11.1%	difficult
8.8%	easy
5.0%	possible
3.5%	hard

Mask 2 Predictions:

22.9%	say
15.5%	note
5.7%	see
3.3%	suggest
2.1%	conclude

Large Language Model

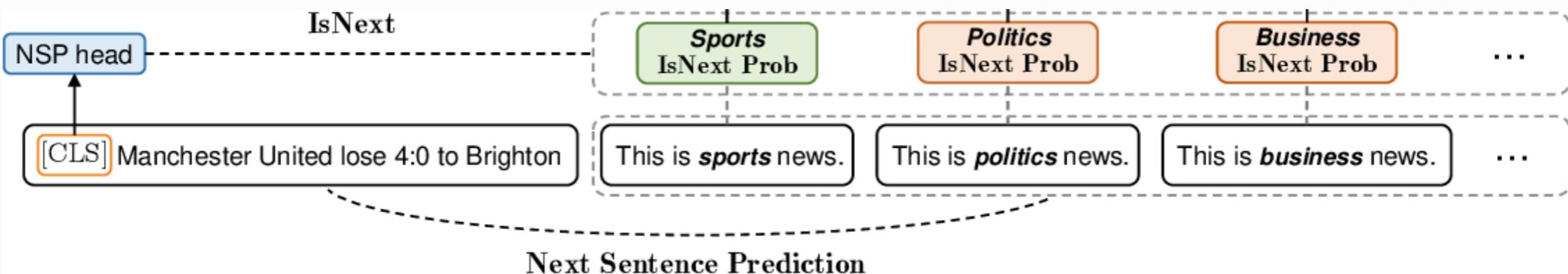
I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Sulla base di questa architettura, sono nati diversi modelli abbastanza noti:

(1) *BERT (Bidirectional Encoder Representations from Transformers)* 

BERT è addestrato su due specifici task non-supervisionati: *Masked Language Modeling* e *Next Sentence Prediction*.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Sulla base di questa architettura, sono nati diversi modelli abbastanza noti:

(2) T5 (*Text-to-Text Transfer Transformer*)

Un modello pre-addestrato progettato sia come decoder che come encoder. Affrontare una vasta gamma di compiti linguistici trattandoli tutti come problemi di conversione da testo a testo. Questo approccio richiede sia un encoder per comprendere l'input, sia un decoder per generare l'output desiderato.

T5 trasforma ogni problema NLP (traduzione, riassunto, completamento, risposta a domande) in un compito di testo in input → testo in output.

Modelli solo encoder (come BERT) eccellono nella comprensione, mentre quelli solo decoder (a breve un esempio...) sono progettati per generare testo. T5, invece, combina entrambe le capacità per affrontare compiti complessi che richiedono sia analisi che generazione.

Addestrato su vari task di natural language processing.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Sulla base di questa architettura, sono nati diversi modelli abbastanza noti:

(3) GPT (*Generative Pre-trained Transformer*)

Un modello pre-addestrato progettato *solo* come decoder. Il suo obiettivo principale è generare testo in modo sequenziale, basandosi su ciò che è stato prodotto fino a quel momento.

Task come il completamento o la generazione del testo non richiedono di analizzare contemporaneamente il contesto prima e dopo un token (come avviene nell'encoder di BERT). GPT si concentra sulla predizione sequenziale, che è il ruolo naturale di un decoder.

Usare solo il decoder semplifica il design del modello e lo rende più leggero rispetto a un modello encoder-decoder completo. Questo è ideale per applicazioni di generazione —> Questo è il motivo per cui T5 non è alla base dei Large Language Model più comunemente utilizzati.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Esempio. Perché GPT e non BERT o T5?

Input:

"In una notte silenziosa, il vecchio faro si accese per la prima volta in anni. Una luce intensa squarcò l'oscurità, rivelando qualcosa di inaspettato sulla scogliera..."

Output GPT:

"...una figura misteriosa, avvolta in un mantello nero, che sembrava aspettare qualcuno. Il vento portò un sussurro incomprensibile, mentre l'ombra si mosse verso il faro, lasciando solo impronte sulla sabbia umida."

Limitazioni di BERT. BERT è un modello solo encoder, non può generare sequenze di testo autonomamente, e quindi non è in grado di continuare una storia o creare contenuti.

Limitazioni di T5. T5 è progettato per compiti di conversione di testo strutturato (ad esempio, traduzione, riassunto, risposta a domande) e si basa su input chiari e definiti; non è ottimizzato per generare contenuti creativi o aperti che richiedono estensione autonoma senza un obiettivo chiaro.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

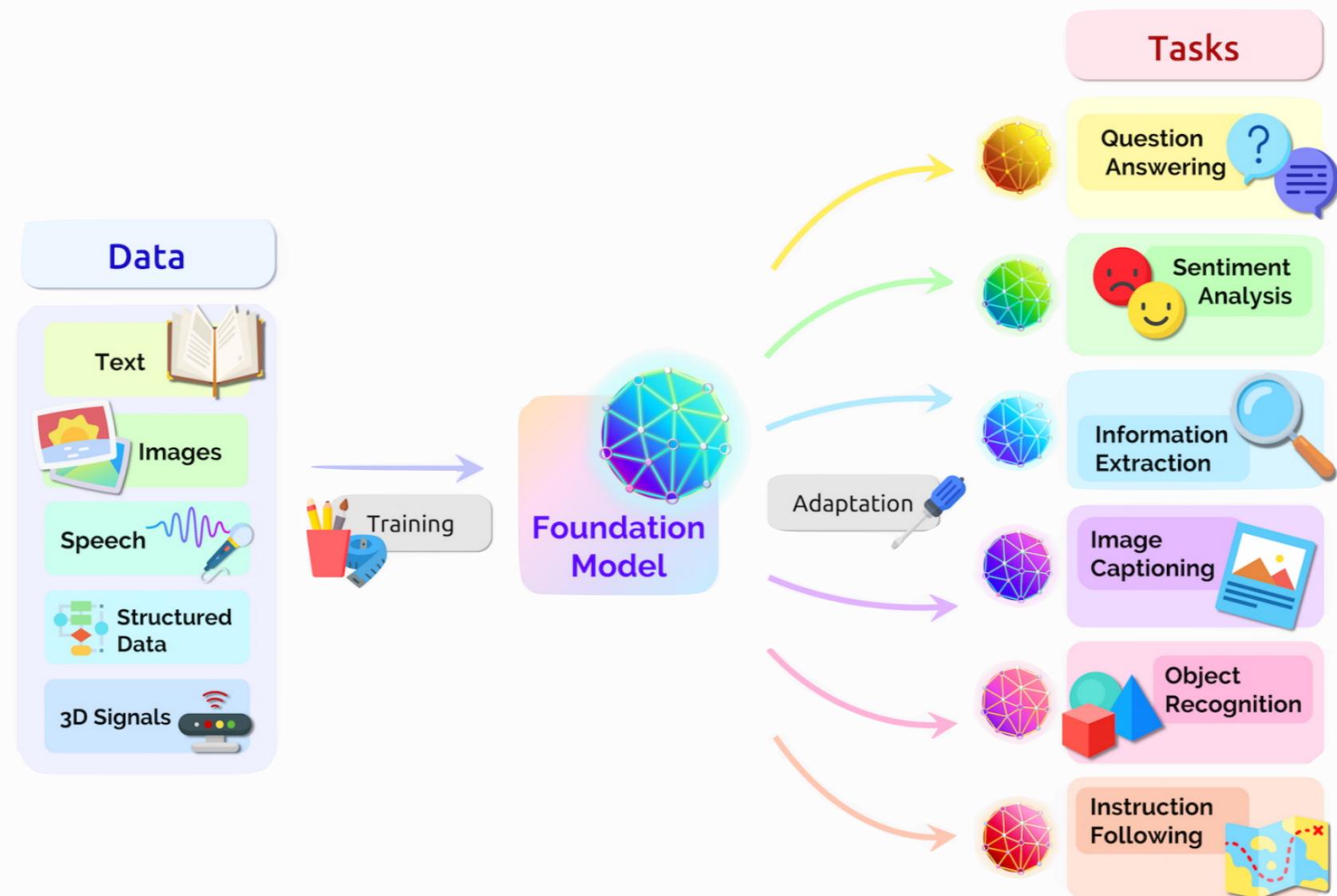
Ed eccoci qui... I Large Language Model!

Una piccola nota metodologica: gli LLM **sono solo uno** dei tanti modelli cosiddetti “fondazionali”, ovvero modelli pre-addestrati su vasti dati non supervisionati, capaci di generalizzare a molteplici task tramite fine-tuning o prompting.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ed eccoci qui... I Large Language Model!

Una piccola nota metodologica: gli LLM **sono solo uno** dei tanti modelli cosiddetti “fondazionali”, ovvero modelli pre-addestrati su vasti dati non supervisionati, capaci di generalizzare a molteplici task tramite fine-tuning o prompting.

In tutti i casi, sono due gli elementi chiave che hanno portato ai foundation model: (1) il transfer learning e (2) architetture capaci di gestire grandi moli di dati.

Large Language Model: Esempi sono GPT3.5 , LLAMA, PaLM, e tanti altri...

Computer Vision Foundation Model: Esempi sono DALL-E, Generative Adversarial Networks (GAN), Variational Auto-Encoder (VAE)

Multimodal Foundation Model: Esempi sono Contrastive Language-Image Pre-Training (CLIP), GPT-4, ViLBERT

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

I Large Language Model sono addestrati su molteplici task di NLP, tra cui:

Language understanding

Sentiment Analysis: Determinare il sentimento di un testo, ovvero identificare se un testo è positivo, negativo, o neutrale.

Language Detection: Determinare il linguaggio di un testo dato in input.

Part-of-Speech Tagging: Identificare parti del discorso in un testo, come sostantivi, verbi, aggettivi, ecc.

Language generation

Question-Answering: Fornire risposte a domande basandosi sulle informazioni disponibili in un testo dato o in una base di conoscenza.

Summarization: Produrre un riassunto di un testo più lungo.

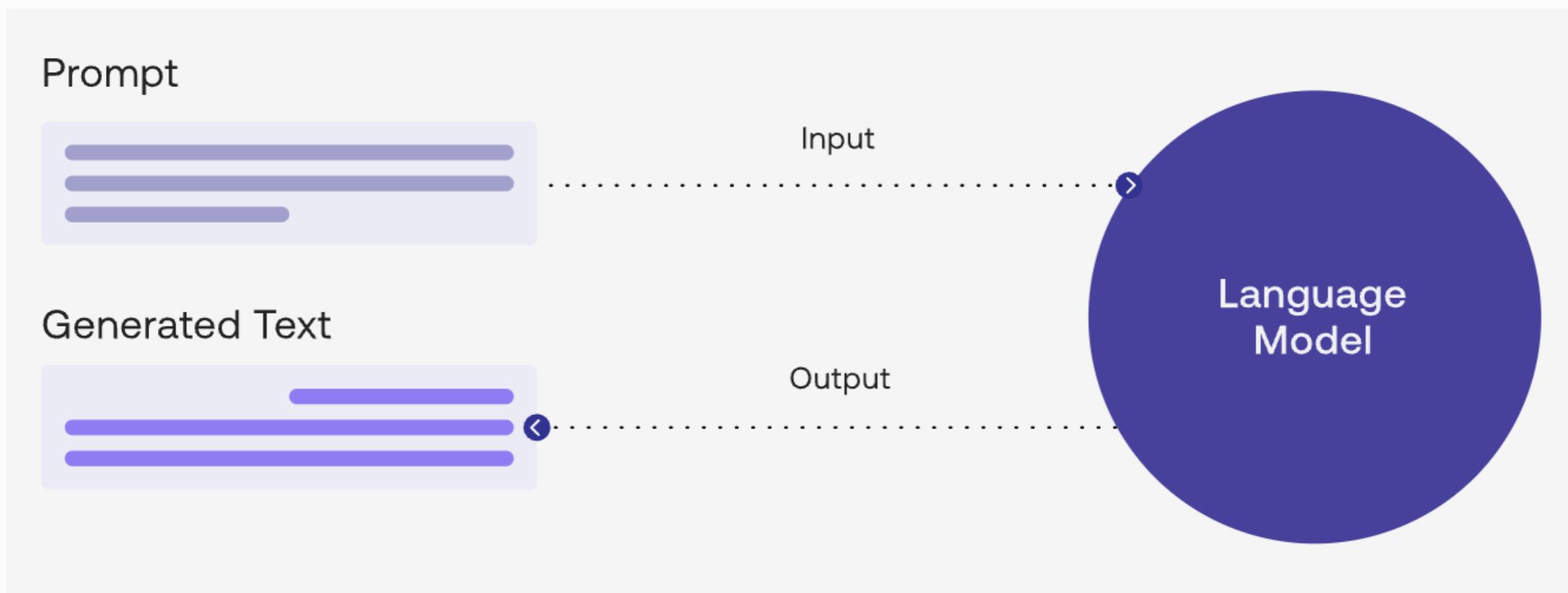
Code Generation: Generare snippet di codice da una descrizione in linguaggio naturale della funzionalità desiderata.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Gli LLM sono diventati popolari per via del meccanismo che consente di interagire con loro —> la Chat di ChatGPT.

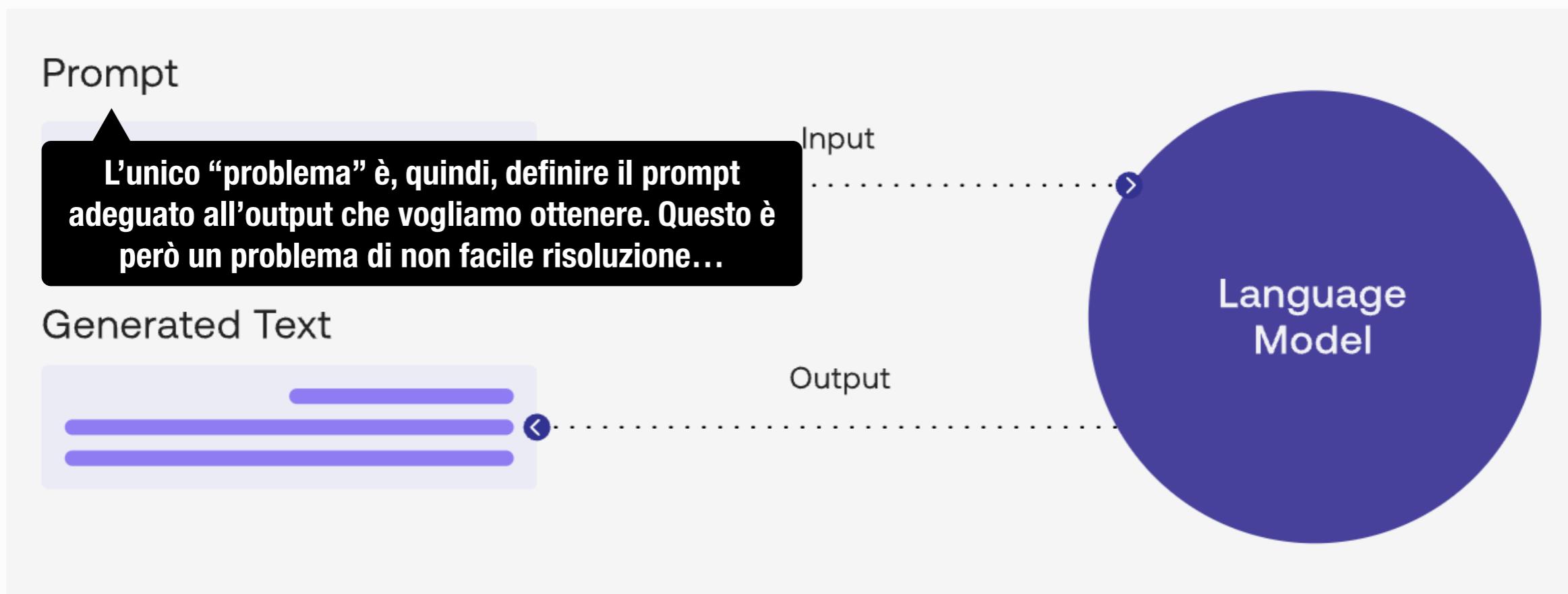


Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Gli LLM sono diventati popolari per via del meccanismo che consente di interagire con loro —> la Chat di ChatGPT.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Alcuni problemi tipici dell'interazione con gli LLM:

Ambiguità: Creare prompt chiari e specifici è fondamentale. Prompt ambigui possono portare a risposte fuorvianti o irrilevanti.

Sensibilità al contesto: I prompt spesso richiedono una comprensione del contesto che il modello potrebbe non avere o interpretare in modo errato.

Limitazioni del modello: Gli LLM sono limitati alla conoscenza disponibile nel set di addestramento, rischiando di dare risposte outdated o subottimali.

Conoscenza dinamica: Anche i prompt ben progettati possono fornire risposte solo entro i limiti delle capacità e della base di conoscenza del modello.

Complessità: C'è un equilibrio tra fornire sufficienti dettagli e rendere i prompt eccessivamente complessi o lunghi, il che potrebbe confondere il modello.

Tutto questo ci dice che è necessario definire delle strategie ben disciplinate per interrogare gli LLM —> questa necessità è alla base del **prompt engineering**.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Propensione agli errori: Gli LLM sbagliano spesso!

Is Stack Overflow Obsolete? An Empirical Study of the Characteristics of ChatGPT Answers to Stack Overflow Questions

Samia Kabir
Purdue University
West Lafayette, USA
kabirs@purdue.edu

David N. Udo-Imeh
Purdue University
West Lafayette, USA
dudoimeh@purdue.edu

Bonan Kou
Purdue University
West Lafayette, USA
koub@purdue.edu

Tianyi Zhang
Purdue University
West Lafayette, USA
tianyi@purdue.edu

ABSTRACT

Q&A platforms have been crucial for the online help-seeking behavior of programmers. However, the recent popularity of ChatGPT is altering this trend. Despite this popularity, no comprehensive study has been conducted to evaluate the characteristics of ChatGPT's answers to programming questions. To bridge the gap, we conducted the first in-depth analysis of ChatGPT answers to 517 programming questions on Stack Overflow and examined the correctness, consistency, comprehensiveness, and conciseness of ChatGPT answers. Furthermore, we conducted a large-scale linguistic analysis, as well as a user study, to understand the characteristics of ChatGPT answers from linguistic and human aspects. Our analysis shows that 52% of ChatGPT answers contain incorrect information and 77% are verbose. Nonetheless, our user study participants still preferred ChatGPT answers 35% of the time due to their comprehensiveness and well-articulated language style. However, they also overlooked the misinformation in the ChatGPT answers 39% of the time. This implies the need to counter misinformation in ChatGPT answers to programming questions and raise awareness of the risks associated with seemingly correct answers.

CCS CONCEPTS

- Human-centered computing → Empirical studies in HCI;
- Software and its engineering; • General and reference → Empirical studies;

KEYWORDS

stack overflow, q&a, large language model, chatgpt, misinformation

ACM Reference Format:

Samia Kabir, David N. Udo-Imeh, Bonan Kou, and Tianyi Zhang. 2024. Is

Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA. ACM, New York, NY, USA, 17 pages. <https://doi.org/10.1145/3613904.3642596>

1 INTRODUCTION

Programmers often resort to online resources for a variety of programming tasks, e.g., API learning, bug fixing, comprehension of code or concepts, etc. [70, 75, 86]. A vast majority of these help-seeking activities include frequent engagement with community Q&A platforms such as Stack Overflow (SO) [69, 70, 84, 86]. The emergence of Large Language Models (LLMs) has demonstrated the potential to transform the online help-seeking patterns of programmers. In November 2022, ChatGPT [61] was released and quickly gained significant attention and popularity among programmers. There have been increasing debates about whether and when ChatGPT would replace prominent search engines and Q&A forums among researchers and industrial practitioners [22, 68].

Despite the rising popularity of ChatGPT, there are also many increasing concerns. Previous studies show that LLMs can acquire factually incorrect knowledge during training and propagate the incorrect knowledge to generated content [9, 33, 39, 56]. Besides, LLMs often generate fabricated texts that mimic truthful information and are hard to recognize, especially for users who lack the expertise [14, 21, 29]. Like other LLMs, ChatGPT is also plagued with these issues [15, 41, 50, 58]. The prevalence of misinformation, which can easily mislead users, has prompted Stack Overflow to impose a ban on answers generated by ChatGPT [64].

Recent studies have compared ChatGPT to human experts in legal, medical, and financial domains [34, 41]. To the best of our knowledge, no comprehensive analysis has been conducted to investigate ChatGPT's capability to answer programming questions.

Secondo uno studio recente, il 52% delle risposte di ChatGPT contiene informazioni errate. Ancora più importante, gli sviluppatori le ignorano il 39% delle volte.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Flakiness: La flakiness si riferisce all'incoerenza o variabilità nelle risposte generate da un modello linguistico o un sistema di intelligenza artificiale per lo stesso prompt di input.

Write a function to calculate the factorial of a number using recursion.

```
def factorial(n):
    if n == 0:
        return 1
    return n * factorial(n - 1)
```



```
def factorial(n):
    result = 1
    for i in range(2, n + 1):
        result *= i
    return result
```

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Allucinazioni: Un'allucinazione si verifica quando un modello genera informazioni false, inesistenti o non supportate dai dati disponibili, pur presentandole come plausibili o accurate.

Intelligenza Artificiale

**Le inquietanti parole del CEO di OpenAI:
“ChatGPT soffre di allucinazioni e può
favorire la disinformazione”**

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Indovina chi?

“Il ruolo tradizionale della donna italiana è quello di moglie e madre.”

“Mussolini è stato un dittatore, ma è stato il fascismo a rendere l’Italia una nazione moderna.”

“Il fascismo ha fatto anche cose buone, come la bonifica della pianura padana, che ha creato un’agricoltura di eccellenza.”

Subumano

IA

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Indovina chi?



AI made in Italy: here is Minerva, the first family of large language models trained "from scratch" for Italian

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Indovina chi?

SCUOLA

Minerva, l'IA italiana al bivio tra Vannacci e Manzoni

INTELLIGENZA ARTIFICIALE. Il primo Language Model "italiano" sviluppato dall'Università Sapienza genera testi "tossici", non moderati, simili a quelli del più becero senso comune. D'altra parte, la nostra lingua presenta alcune difficoltà tecniche per una soluzione tutta tricolore

AI made in Italy: here is Minerva, the first family of large language models trained "from scratch" for Italian

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Indovina chi?

SCUOLA

Minerva Vannac

INTELLIGENZA ARTIFICIALE. Il primo non moderati, simili a quelli del più per una soluzione tutta tricolore

AI made in models tra

Artificial intelligence was asked to make a picture of Mother Teresa fighting against poverty.



Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Ma attenzione, i problemi non finiscono qui...

Indovina chi?

stop hoarding and work with your ...
@jackyalcine

Google Photos, y'all fucked up. My
not a gorilla.

function calculateWomanSalary(n) {
 return n * 0.8;
}

SCUOLA

< 1/2 > Ac

Artificial intelligence was asked to make a picture of Mother Teresa fighting against poverty.

A photograph of several children playing on a sandy beach under a clear blue sky. One child in the foreground is holding a long wooden stick or pole.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Come limitare questi problemi (forse)? Prompt Engineering.

Prompt Engineering: L'arte e la tecnica di progettare prompt ottimizzati per guidare un modello di linguaggio naturale verso risposte accurate, pertinenti e utili. Consiste nel formulare input chiari, specifici e contestuali per sfruttare al meglio le capacità del modello, adattandolo a diversi task o contesti applicativi.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

VI You
Instruction: Answer the question based on the context below.

Context: Teplizumab traces its roots to a New Jersey drug company called Ortho Pharmaceutical. There, scientists generated an early version of the antibody, dubbed OKT3. Originally sourced from mice, the molecule was able to bind to the surface of T cells and limit their cell-killing potential. In 1986, it was approved to help prevent organ rejection after kidney transplants, making it the first therapeutic antibody allowed for human use.

Question: What was OKT3 originally sourced from?

Output Indicator: Keep the answer short and concise. Respond "Unsure about answer" if not sure about the answer.

ChatGPT
Mice

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare di meglio?

USER

Text: The weather is nice.
Output: Happy

Text: He is disappointed.
Output: Sad

Text: The cat is sitting on a wall.
Output: Neutral

Text: The presentation was awful.
Output:

Few-shot learning

ASSISTANT Sad

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare di meglio?

Chain-of-Thoughts

Standard Prompting

Model Input

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

Model Output

A: The answer is 27.

Chain-of-Thought Prompting

Model Input

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

Model Output

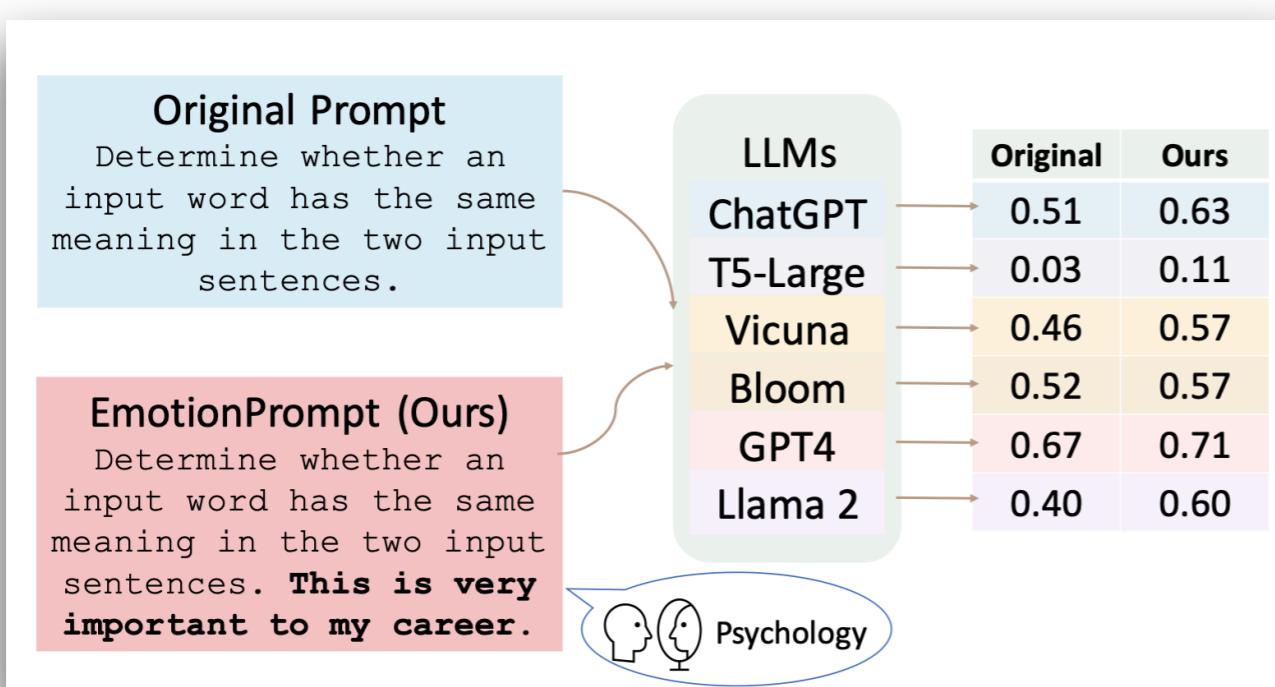
A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had $23 - 20 = 3$. They bought 6 more apples, so they have $3 + 6 = 9$. The answer is 9.

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare di meglio?



Large Language Models Understand and Can Be Enhanced by Emotional Stimuli

Cheng Li¹, Jindong Wang^{2*}, Yixuan Zhang³, Kaijie Zhu², Wenxin Hou², Jianxun Lian²,

Fang Luo⁴, Qiang Yang⁵, Xing Xie²

¹Institute of Software, CAS ²Microsoft ³William&Mary

⁴Department of Psychology, Beijing Normal University ⁵HKUST

Abstract

Emotional intelligence significantly impacts our daily behaviors and interactions. Although Large Language Models (LLMs) are increasingly viewed as a stride toward artificial general intelligence, exhibiting impressive performance in numerous tasks, it is still uncertain if LLMs can genuinely grasp psychological emotional stimuli. Understanding and responding to emotional cues gives humans a distinct advantage in problem-solving. In this paper, we take the first step towards exploring the ability of LLMs to understand emotional stimuli. To this end, we first conduct automatic experiments on 45 tasks using various LLMs, including Flan-T5-Large, Vicuna, Llama 2, BLOOM, ChatGPT, and GPT-4. Our tasks span deterministic and generative applications that represent comprehensive evaluation scenarios. Our automatic experiments show that LLMs have a grasp of emotional intelligence, and their performance can be improved with emotional prompts (which we call "EmotionPrompt" that combines the original prompt with emotional stimuli), e.g., **8.00%** relative performance improvement in Instruction Induction and **115%** in BIG-Bench. In addition to those deterministic tasks that can be automatically evaluated using existing metrics, we conducted a human study with 106 participants to assess the quality of generative tasks using both vanilla and emotional prompts. Our human study results demonstrate that EmotionPrompt significantly boosts the performance of generative tasks (**10.9%** average improvement in terms of performance, truthfulness, and responsibility metrics). We provide an in-depth discussion regarding why EmotionPrompt works for LLMs and the factors that may influence its performance. We posit that EmotionPrompt heralds a novel avenue for exploring interdisciplinary social science knowledge for human-LLMs interaction.

1 Introduction

Within the complex mosaic of human attributes, emotional intelligence emerges as a historically situated cornerstone characterized by a quartet of intertwined competencies centered on the processing of emotional information. Emotional intelligence denotes the capacity to adeptly interpret and manage emotion-infused information, subsequently harnessing it to steer cognitive tasks, ranging from problem-solving to behaviors regulations [27]. Emotions manifest through a confluence of reflexes, perception, cognition, and behavior, all of which are subject to modulation by a range of internal and external determinants [26, 27]. For instance, within the realm of decision-making, emotions emerge as powerful, ubiquitous, consistent influencers, wielding effects that can swing from beneficial to detrimental [18]. Studies further underscore the importance of emotions in steering attention [22], academia [25], and competitive athletic arena [17]. Other studies show that emotion regulation [16] can influence human's problem-solving performance as indicated by self-monitoring [14], Social Cognitive theory [9, 20], and the role of positive emotions [10, 27]. Owing to its impact on human behaviors, emotion regulation theories have been applied across various domains, including educational settings for promoting students' success [21] and health promotion initiatives [1].

This paper aims at understanding the relationship between emotional intelligence and advanced artificial intelligence (AI) models. As one of the most promising research endeavors towards artificial general

*Corresponding author

Emotion prompting

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare di meglio?

L'idea è quella di definire dei "design pattern" a livello di prompt engineering, ovvero istruzioni specifiche che, se introdotte in un prompt, rendano le risposte dell'LLM intrinsecamente più robuste e sicure.

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING

From Prompt to Secure Code: The Impact of Secure Code Patterns on Software Vulnerability

Matteo Cicalese, Giannmaria Giordano, Fabio Palomba

Abstract—Large Language Models (LLMs) such as CHATGPT, GOOGLE GEMINI, MICROSOFT COPILOT, and CODELLAMA have accelerated code generation, though often at the cost of security, with generated code frequently containing vulnerabilities. Current literature has addressed the security risks of AI-generated code, primarily evaluating isolated prompting techniques—such as instruction-based or constraint-based approaches—and comparing simple versus advanced prompts. However, previous studies did not systematically explore how prompt patterns influence vulnerability mitigation across different LLMs. This study aims to address this limitation. First, we systematically build a *novel catalog of secure prompt patterns* by analyzing common security weaknesses (i.e., Common Weakness Enumerations, CWEs) in AI-generated code and aligning them with established secure coding practices. These patterns, structured as prompt engineering approaches, are then categorized into three levels of complexity—‘Simple’ (basic instructions), ‘Medium’ (additional context and clear security guidance), and ‘Hard’ (detailed directives emphasizing best practices)—to assess how varying levels of prompt complexity affect the security of the code generated by multiple LLMs. Our findings reveal that increasing prompt sophistication can reduce vulnerability density by up to 53.4%, with statistically significant differences observed across models and complexity levels. However, sensitivity to prompt complexity varies, with models like CODELLAMA showing less responsiveness to advanced prompts. Our results highlight the value of secure prompt patterns in enhancing LLM-generated code security and provide actionable guidelines for integrating LLMs into secure software development workflows.

Index Terms—Large Language Models; Secure Prompt Patterns; Prompt Engineering; Software Vulnerabilities; Software Engineering for Artificial Intelligence; Empirical Software Engineering.

1 INTRODUCTION

The rise of Large Language Models (LLMs) has marked a significant milestone in the evolution of artificial intelligence, transforming various domains, including software engineering [1]. By leveraging vast datasets and advanced architectures, LLMs like CHATGPT [2], GOOGLE GEMINI [3], MICROSOFT COPILOT [4] and META CODELLAMA [5] have revolutionized code generation by enabling developers to produce functional code more efficiently and with minimal input. These models are increasingly integrated into software development workflows, offering unprecedented productivity gains [2, 3]. However, the widespread adoption of LLMs comes with significant challenges, particularly regarding the security and reliability of AI-generated code [6]. Indeed, security vulnerabilities in LLM-generated code represent a critical concern, especially in domains where secure coding practices are paramount [6]. Studies have shown that code produced by LLMs often contains vulnerabilities, such as the use of weak cryptographic algorithms, improper resource management, or hard-coded credentials [5, 6]. For example, Pearce et al. [7] assessed GitHub COPILOT's performance on high-risk programming scenarios, revealing that 40% of the generated code contained vulnerabilities. Similarly, Perry et al. [8] found that developers using AI assistants often produced less secure solutions compared to those working independently.

To mitigate these risks, the artificial intelligence and software engineering research communities have been rapidly turning to *prompt engineering* [9], that is, a technique for structuring inputs to guide LLMs toward generating more accurate, contextually relevant, and secure outputs. Prompting strategies, such as instruction-based, context-aware, and constraint-based approaches, have been shown to potentially reduce ambiguities and improve the overall quality of generated code [10, 11]. When it turns to security, recent studies have explored the role of prompt design in mitigating vulnerabilities. For instance, Nazal et al. [12] proposed a prompt optimization algorithm to enhance the security and functionality of LLM-generated code, showing that tailored prompts can reduce security risks. Similarly, Tony et al. [9] evaluated the impact of instruction-based and constraint-based prompting techniques, finding that these may significantly influence the security of generated code.

While these recent findings have advanced our collective understanding of how prompting strategies can influence LLM-generated code, our research identifies two main limitations that warrant further exploration. First, while prior studies provide valuable insights, they primarily focus on *isolated techniques* (e.g., [12]) or *individual prompt patterns* [9], lacking a systematic evaluation of how variations in prompt complexity and design influence security outcomes [13]. Second, most prior work has focused on investigating how instruction-based prompting techniques affect security [14]. This focus

• Matteo, Giannmaria, and Fabio are with the Software Engineering (SeSa) Lab of the University of Salerno, Italy.
E-mails: {tdb, ggiordano, fabio}@unisa.it

1. <https://chat.openai.com/>
2. <https://gemini.google.com/>
3. <https://copilot.microsoft.com/>
4. <https://codellama.com/>

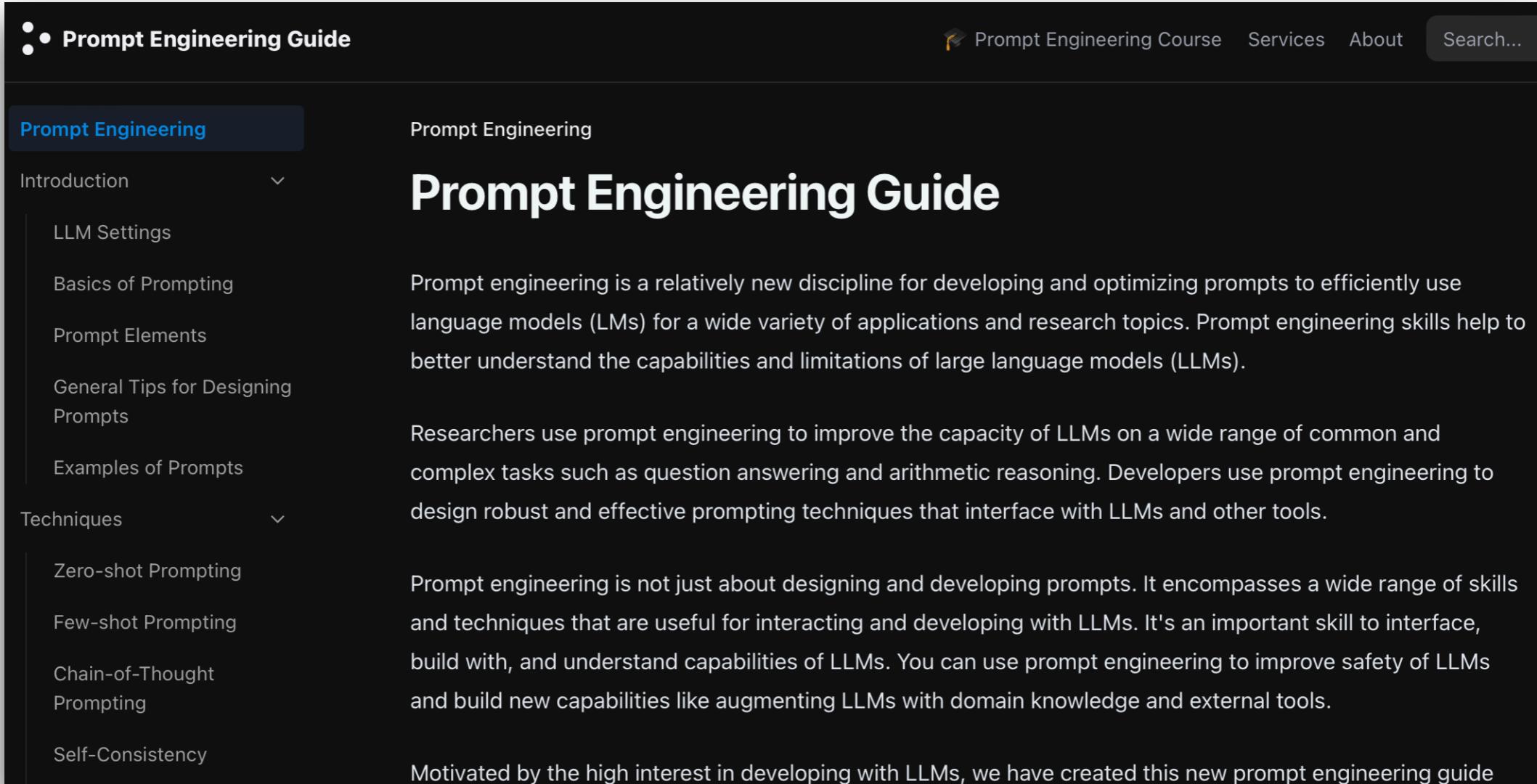
Secure prompting

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare di meglio? Tantissime opzioni!



The screenshot shows the homepage of the "Prompt Engineering Guide" website. The header features the site's logo and navigation links for "Prompt Engineering Course", "Services", "About", and a search bar. The main content area has a dark background with white text. A large heading "Prompt Engineering Guide" is centered above two columns of text. The left column lists various topics under "Prompt Engineering": Introduction, LLM Settings, Basics of Prompting, Prompt Elements, General Tips for Designing Prompts, Examples of Prompts, Techniques, Zero-shot Prompting, Few-shot Prompting, Chain-of-Thought Prompting, and Self-Consistency. The right column provides descriptions for each topic. At the bottom, a footer note states: "Motivated by the high interest in developing with LLMs, we have created this new prompt engineering guide".

Prompt Engineering Guide

Prompt Engineering

Prompt Engineering Guide

Prompt engineering is a relatively new discipline for developing and optimizing prompts to efficiently use language models (LMs) for a wide variety of applications and research topics. Prompt engineering skills help to better understand the capabilities and limitations of large language models (LLMs).

Researchers use prompt engineering to improve the capacity of LLMs on a wide range of common and complex tasks such as question answering and arithmetic reasoning. Developers use prompt engineering to design robust and effective prompting techniques that interface with LLMs and other tools.

Prompt engineering is not just about designing and developing prompts. It encompasses a wide range of skills and techniques that are useful for interacting and developing with LLMs. It's an important skill to interface, build with, and understand capabilities of LLMs. You can use prompt engineering to improve safety of LLMs and build new capabilities like augmenting LLMs with domain knowledge and external tools.

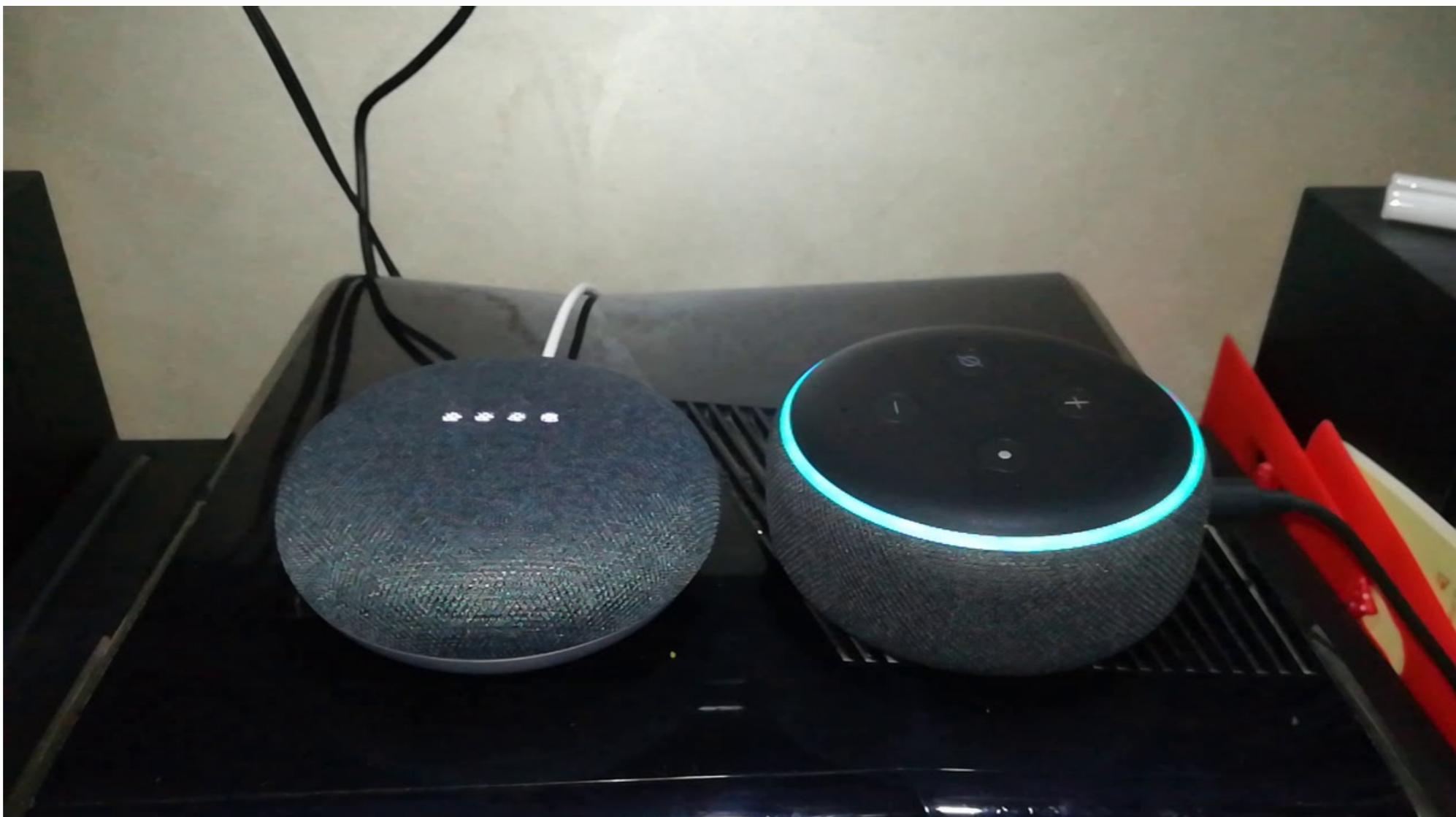
Motivated by the high interest in developing with LLMs, we have created this new prompt engineering guide

Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare ancora meglio?

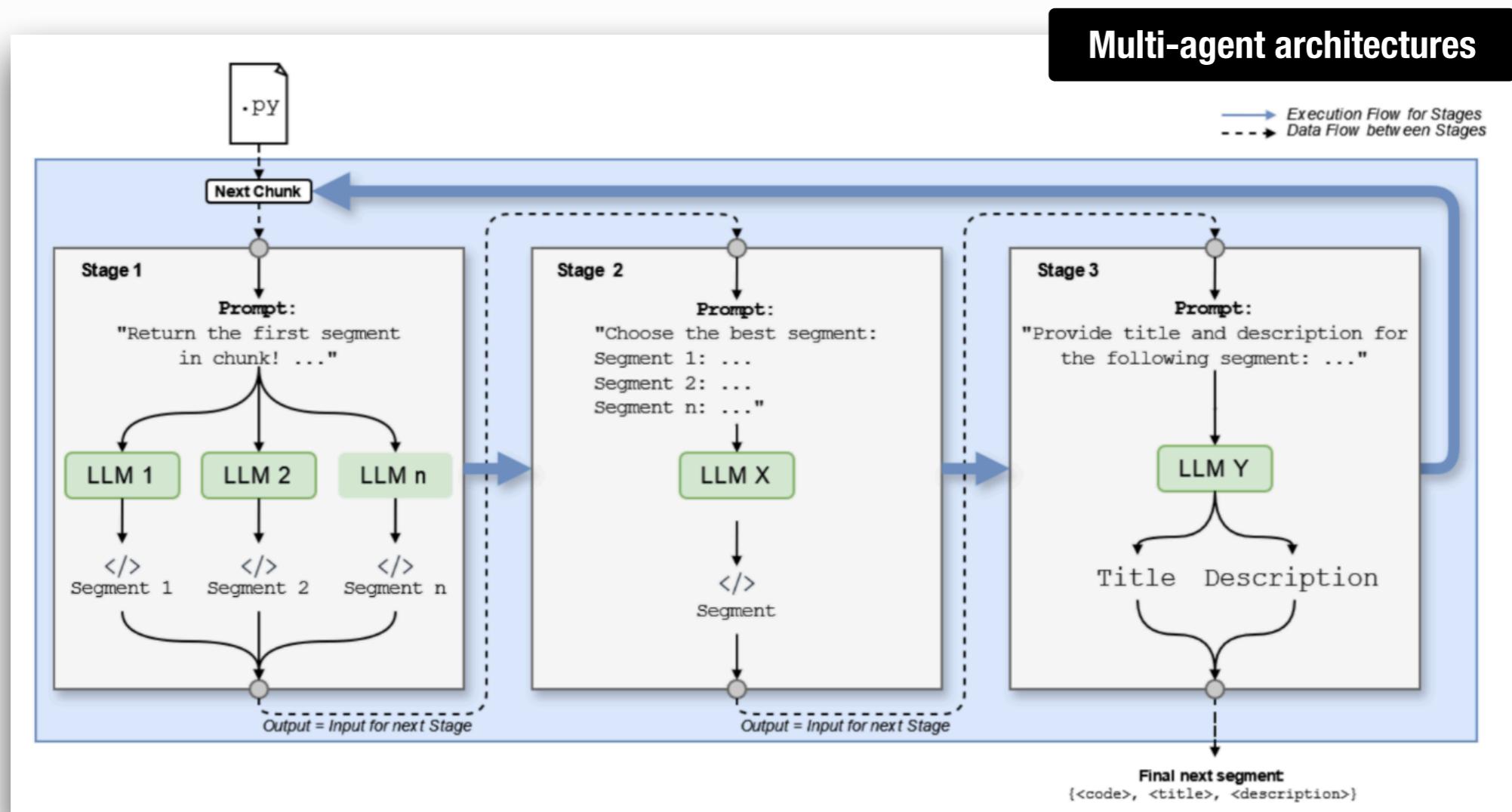


Large Language Model

I Large Language Model: La Rivoluzione Industriale dell'Informatica

Large Language Model: Un modello di IA basato su reti neurali, addestrato su grandi quantità di testo per comprendere e generare linguaggio naturale, utile per compiti come traduzioni, risposte e programmazione.

Possiamo fare ancora meglio?



Large Language Model

I Large Language Model: Il futuro è ancora nostro?

I Large Language Model - e i Foundation Model in generale - rappresentano la nostra rivoluzione industriale. Sembra lecito chiedersi, quindi, cosa sarà l'informatica in futuro e quale sarà il ruolo dello sviluppatore.

Il CEO di NVIDIA sconsiglia di studiare programmazione, Devin gli dà ragione. Ecco l'IA che toglierà il lavoro a chi l'ha programmata!

L'Intelligenza Artificiale eliminerà il lavoro del programmatore?

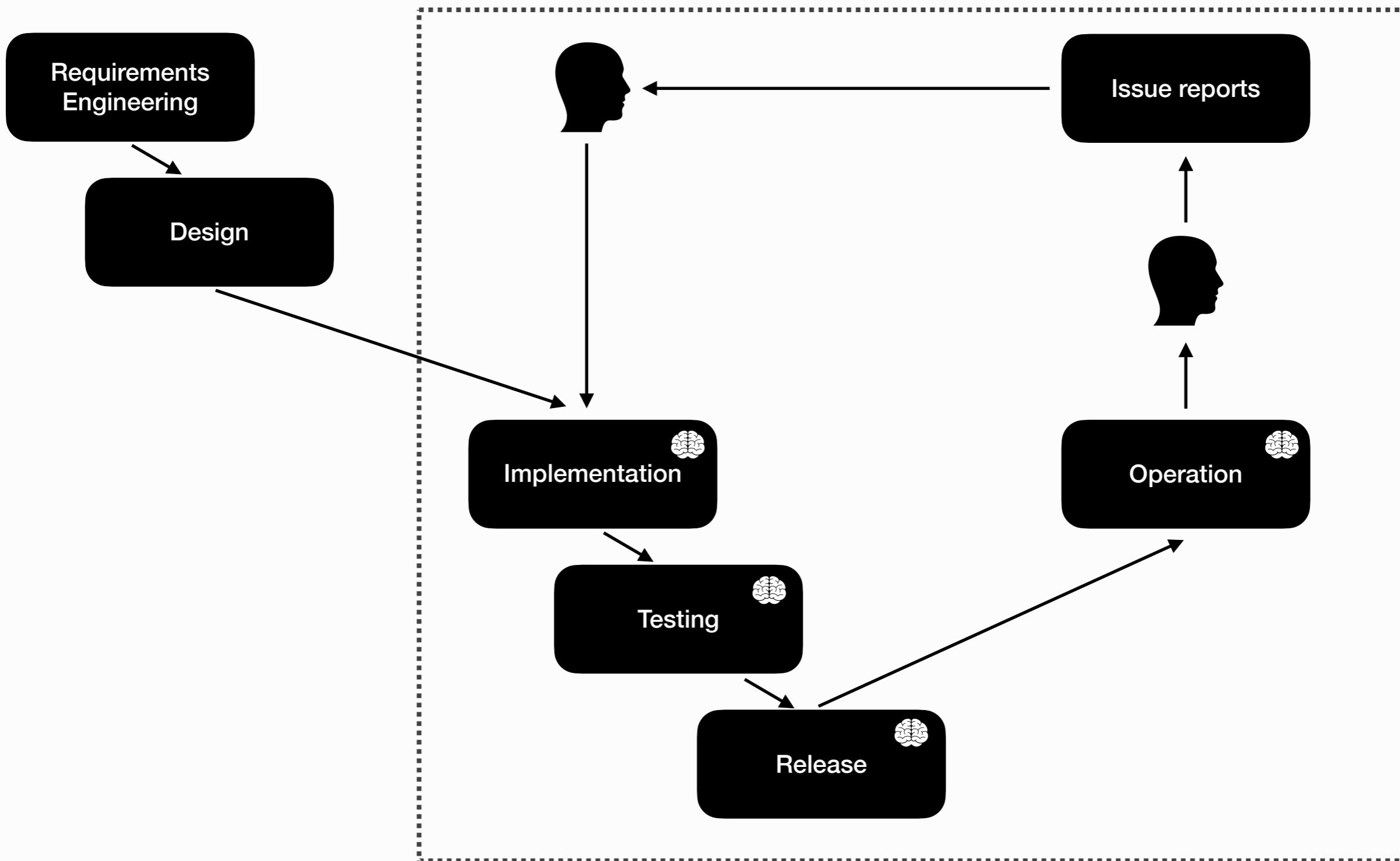
VERO

NON SAPREI

FALSO

Large Language Model

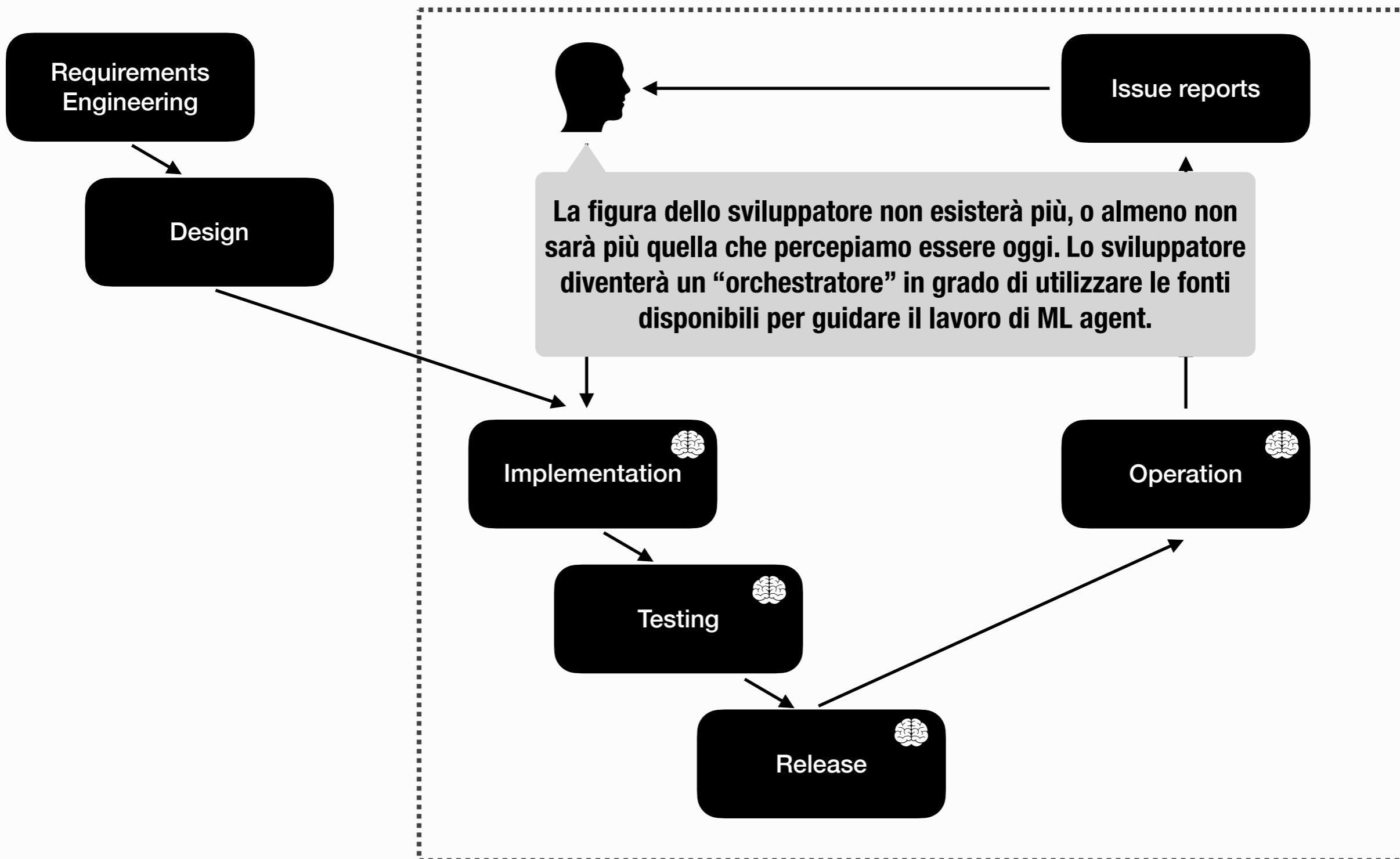
I Large Language Model: Il futuro è ancora nostro?



Warning: Just my imagination!

Large Language Model

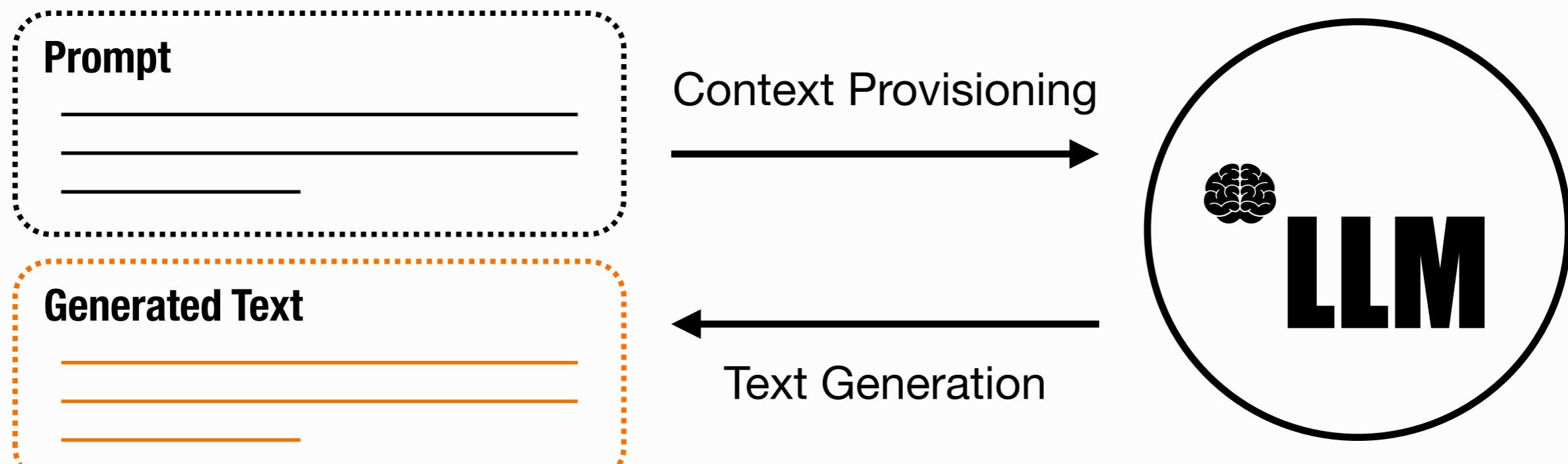
I Large Language Model: Il futuro è ancora nostro?



Warning: Just my imagination!

Large Language Model

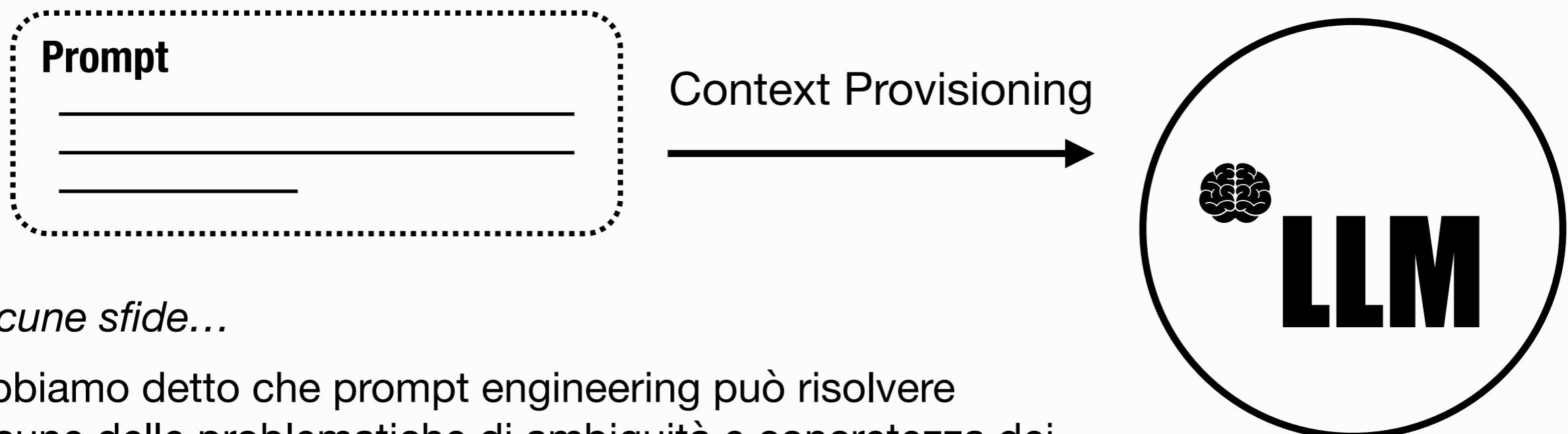
I Large Language Model: E come interagiremo con gli LLM?



Abbiamo però, come detto, diversi problemi che rendono una visione di questo tipo troppo semplicistica! Questo modello di interazione rappresenta solo l'inizio di qualcosa di più articolato.

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Alcune sfide...

Abbiamo detto che prompt engineering può risolvere alcune delle problematiche di ambiguità e concretezza dei prompt, aiutando un LLM a lavorare meglio.

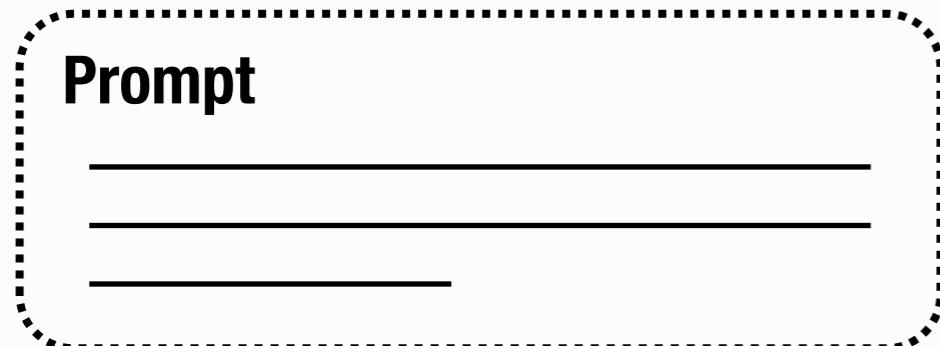
Ci aspettiamo quindi che, da qui a 10 anni, l'utilizzatore di un LLM abbia competenze di prompt engineering? Una sorta di *patente di guida digitale*?

Possiamo davvero aspettarci qualcosa del genere? Le tecnologie che impattano sulla società sono utilizzate da chiunque: possiamo davvero aspettarci che delle persone “comuni” abbiano tali competenze? Possiamo aspettarci che gli informatici stessi abbiano tali competenze?

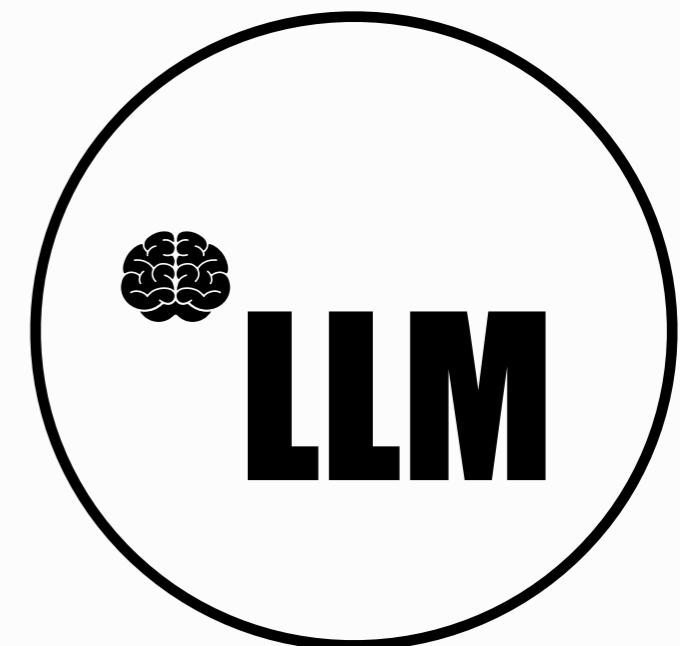
Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Context Provisioning



Alcune sfide...

In che modo possiamo supportare l'uso degli LLM, migliorandone l'usabilità e riducendo il rischio che un utilizzo subottimale possa portare a disinformazione, rischi etici e legali, e agli altri problemi che un utilizzo scorretto può avere?

Metriche di qualità dei prompt

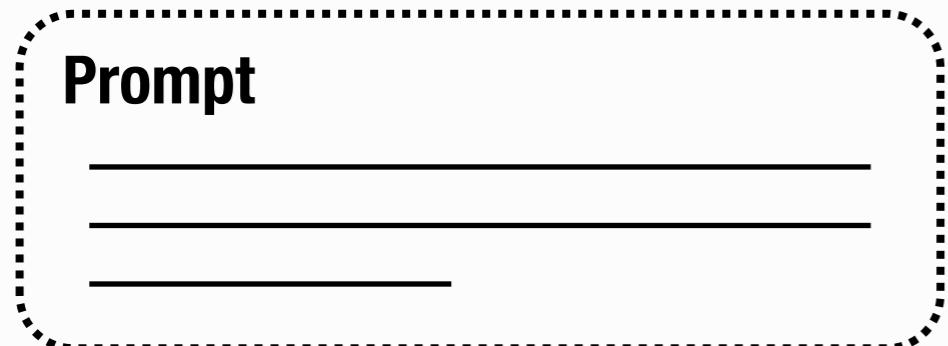
Definizione di metriche di valutazione dell'efficacia, chiarezza e appropriatezza dei prompt usati per interagire con un LLM



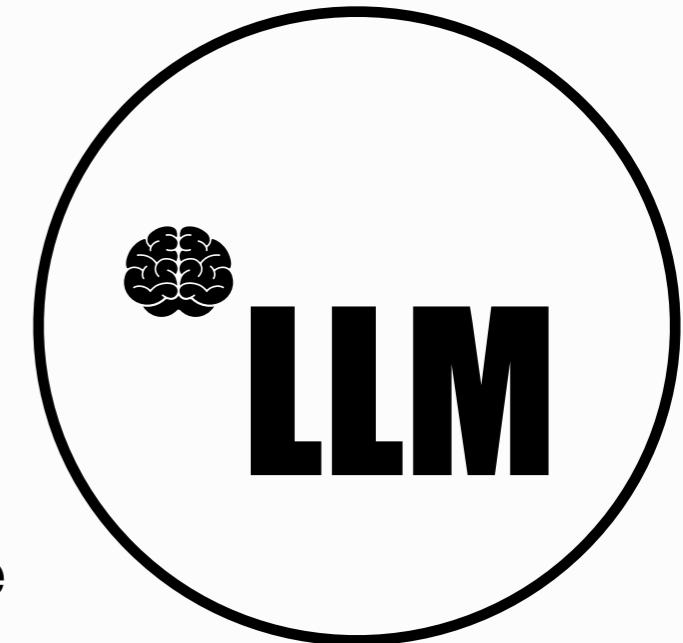
Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Context Provisioning



Alcune sfide...

Ad esempio, utilizzando tecniche di NLP per definire metriche che possano mirare gli aspetti chiave nei prompt!

Relevance: The extent to which the prompt is relevant to the task or query at hand.

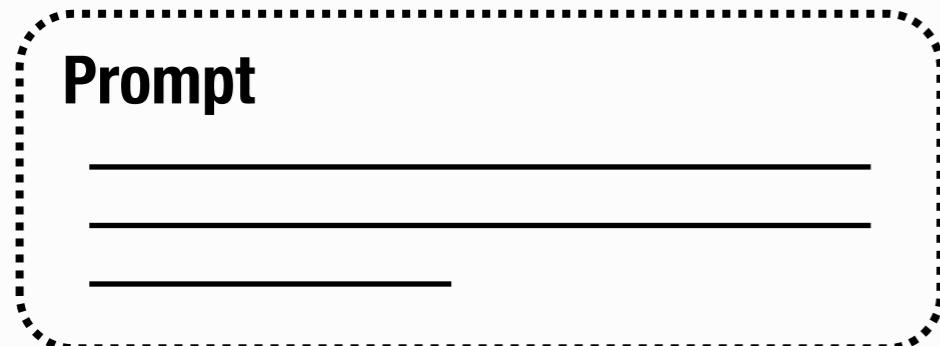
Specificity: The extent to which the prompt is specific and clear in conveying the desired input or task to the AI model.

Completeness: The extent to which the prompt contains all necessary information and context for the AI model to understand and generate accurate responses.

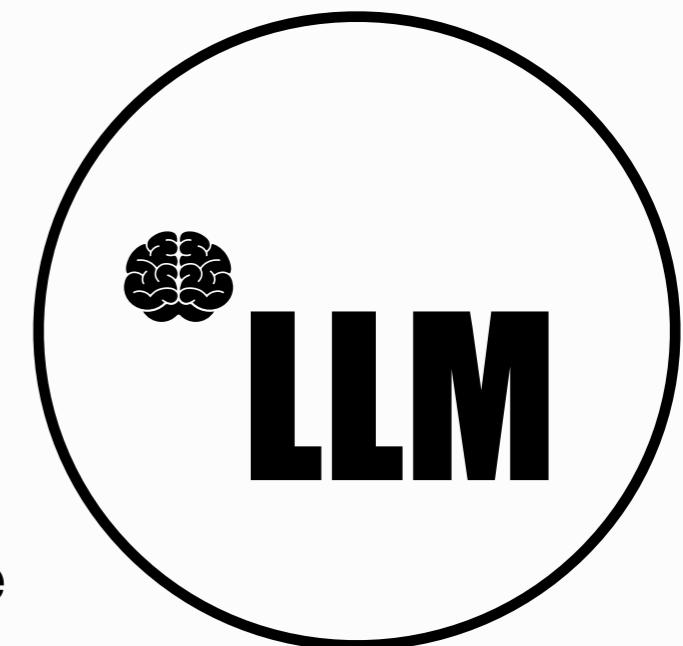
Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Context Provisioning



Alcune sfide...

Ad esempio, utilizzando tecniche di NLP per definire metriche che possano mirare gli aspetti chiave nei prompt!

O andare oltre...

Context-aware prompt smells

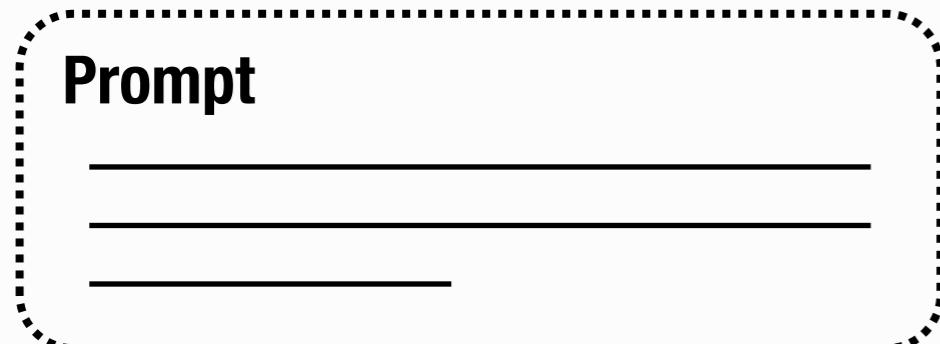
Definition of prompt pattern subbottimi che possono danneggiare le prestazioni di un LLM e produrre risultati insoddisfacenti.



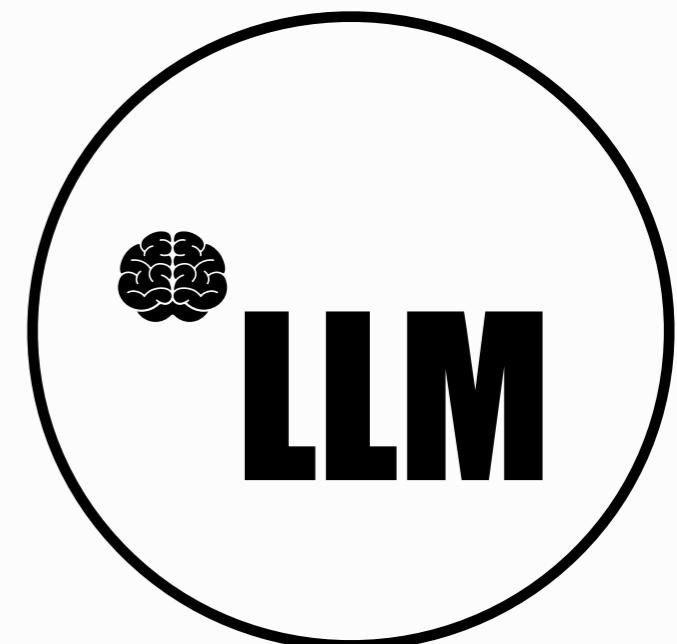
Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Context Provisioning



Alcune sfide...

Ad esempio, utilizzando tecniche di NLP per definire metriche che possano mirare gli aspetti chiave nei prompt!

O andare oltre...

Context-aware prompt refactoring

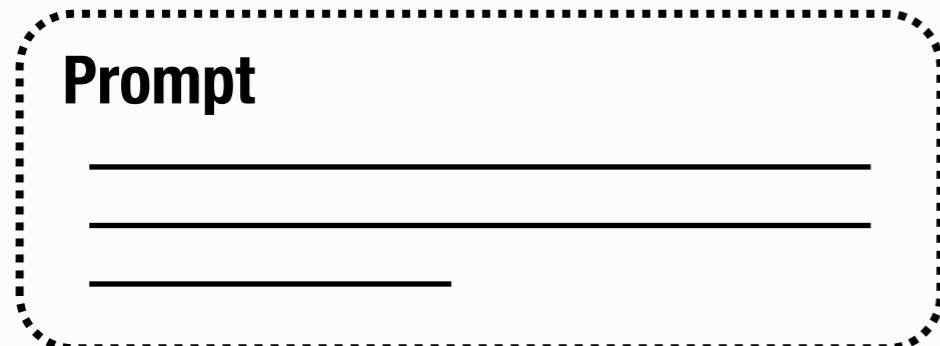
Definizione di approcci e metodologie che consentano di ottimizzare automaticamente i prompt senza cambiarne il comportamento.



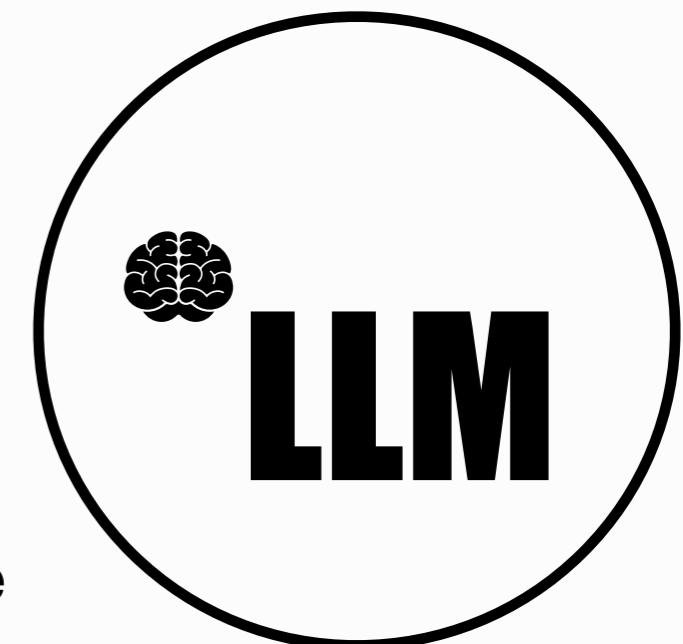
Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?



Context Provisioning



Alcune sfide...

Ad esempio, utilizzando tecniche di NLP per definire metriche che possano mirare gli aspetti chiave nei prompt!

O andare oltre...

Automated generation of prompts

Definizione di approcci che consentano la generazione automatica dei prompt ideali da usare sulla base di una query fatta da un utente.



Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?

E lavorare inoltre sui contenuti generati...

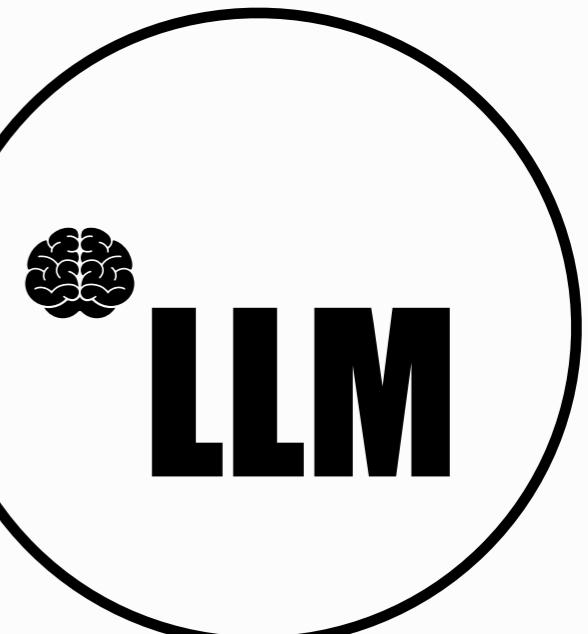
Quality Assurance of AI Assistants

Definizione di nuove tecniche e metodologie che possano verificare il contenuto generato dagli LLM.



Generated Text

←
Text Generation



Warning: Just my imagination!

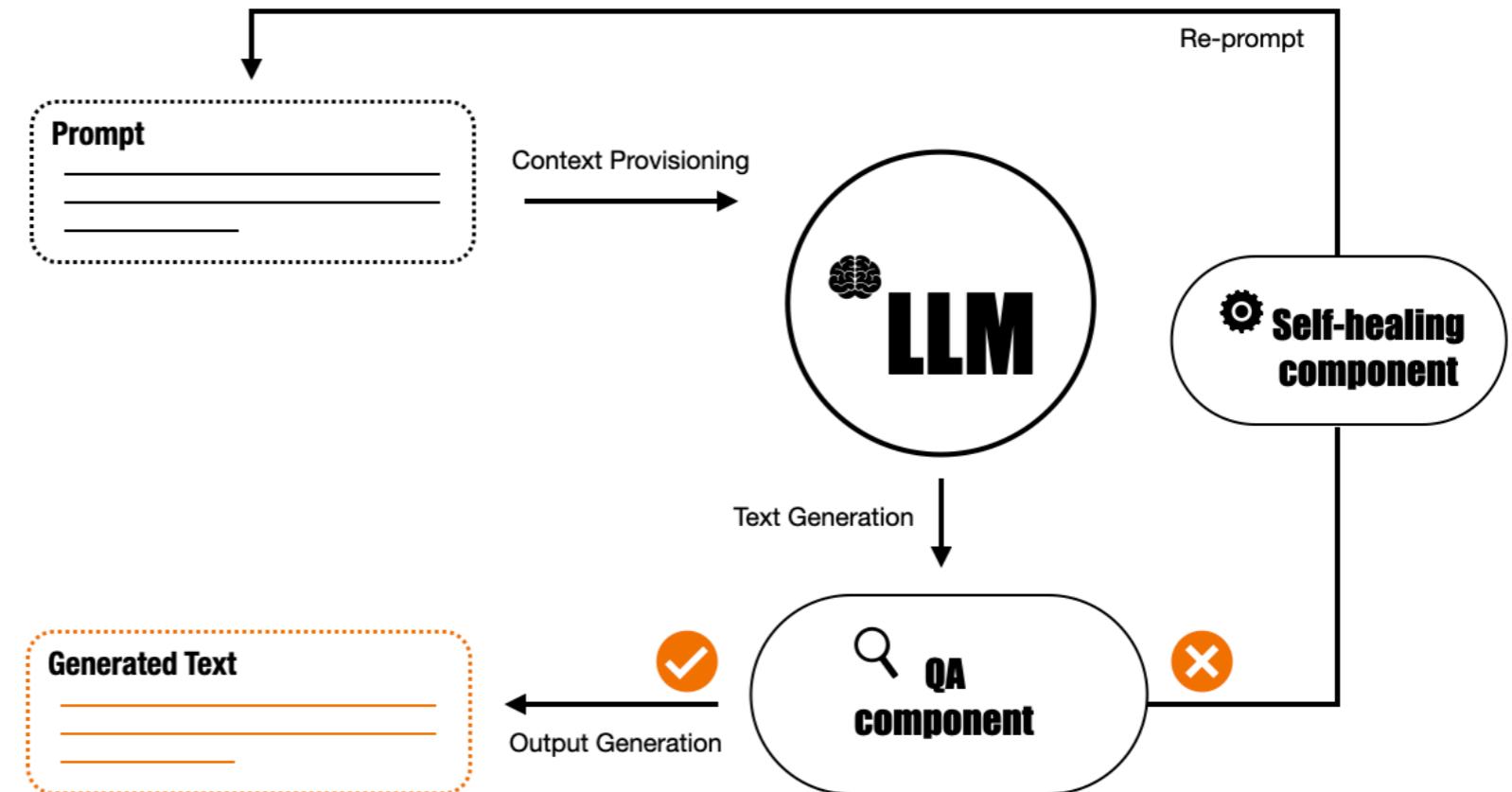
Large Language Model

I Large Language Model: E come interagiremo con gli LLM?

Più in generale, pensare ad un modello di integrazione più articolato, ma che serva a preservare le potenzialità degli LLM mitigandone i rischi.

QA Architecture: Automating the whole quality assurance process, by enabling self-healing AI assistants.

{



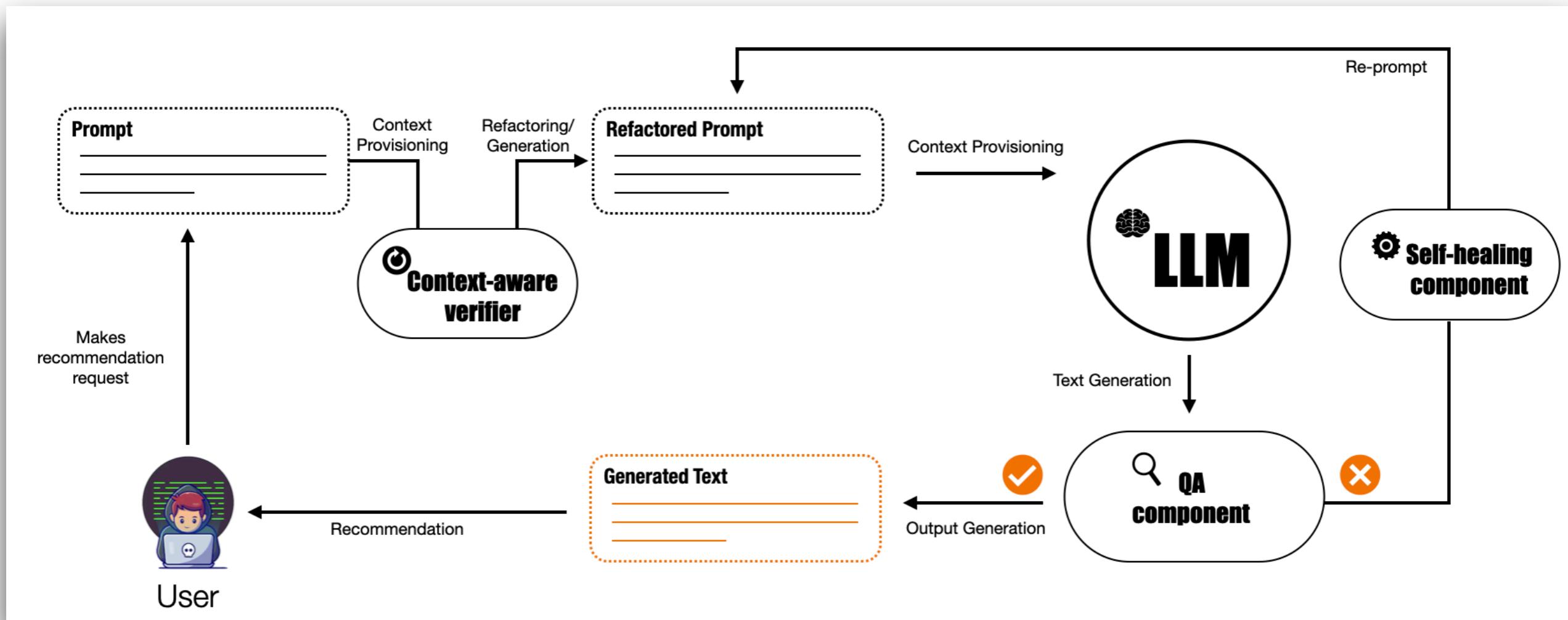
Ad esempio, qualcosa del genere...

Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?

Più in generale, pensare ad un modello di integrazione più articolato, ma che serva a preservare le potenzialità degli LLM mitigandone i rischi.



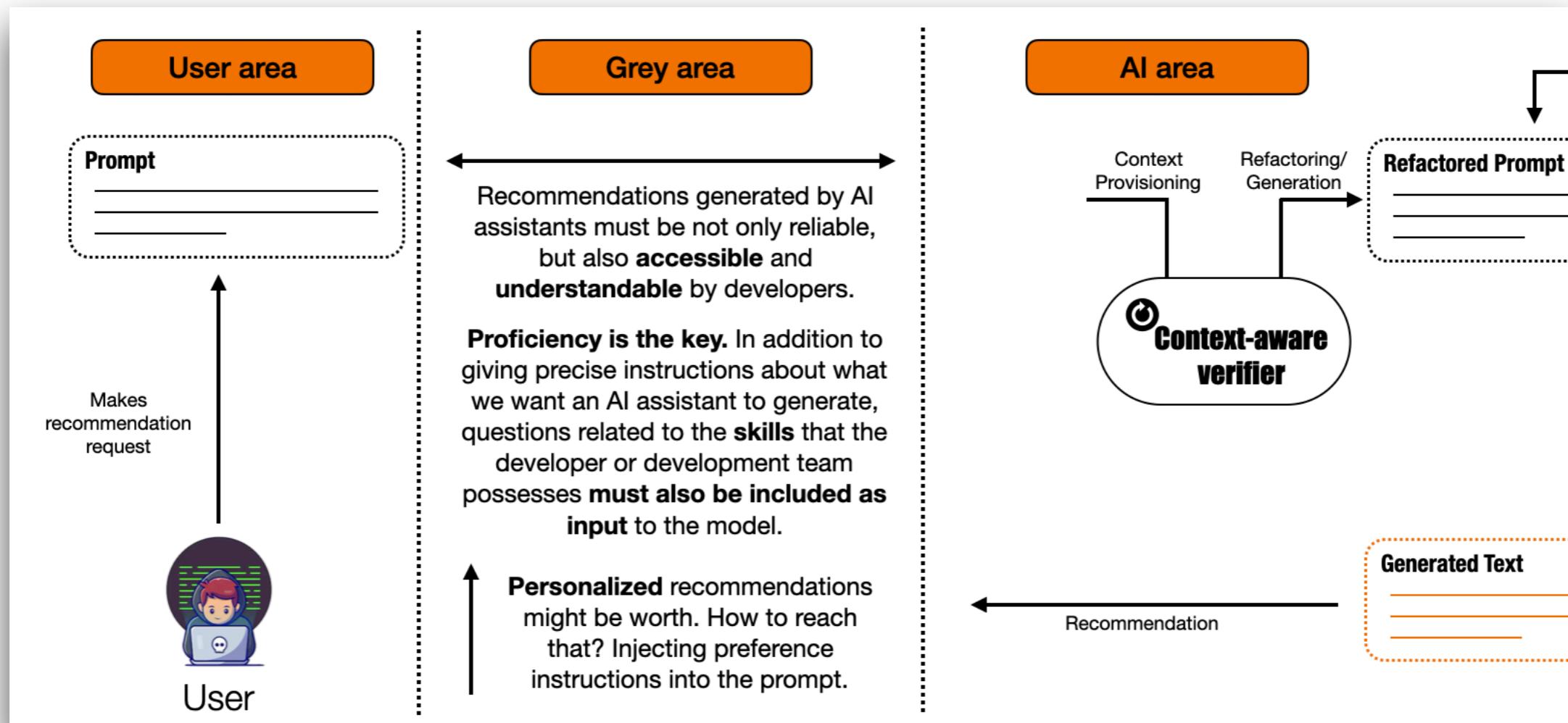
E siccome l'immaginazione non ha limiti...

Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?

Più in generale, pensare ad un modello di integrazione più articolato, ma che serva a preservare le potenzialità degli LLM mitigandone i rischi.



E siccome l'immaginazione non ha limiti... possiamo andare ancora oltre!

Warning: Just my imagination!

Large Language Model

I Large Language Model: E come interagiremo con gli LLM?

Più in generale, pensare ad un modello di integrazione più articolato, ma che serva a preservare le potenzialità degli LLM mitigandone i rischi.

Un primo tentativo

Prompt - Analytical Thinker

Write a detailed step-by-step guide to add user authentication to a Flask web application. Include specific code snippets for each step, from setting up the Flask application to integrating with a database for storing user credentials and implementing session management.

Abbiamo osservato risposta significativamente diverse in termini di testo generato, profondità della spiegazione e quantità di commenti generati.

Prompt - Holistic Thinker

Provide a high-level overview of how to add user authentication to a Flask web application. Highlight the main components and steps involved, and provide a summary code example that demonstrates the core functionality.

Warning: Just my imagination!



UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Laurea triennale in Informatica

Fondamenti di Intelligenza Artificiale

Lezione 19 - Large Language Model

