

## DUE PAROLE SU CHATGPT...



Quando si cerca assistenza, in molti siti, si trova una figura che ricorda una persona di un call center con cui scambiare messaggi. Ov-

vviamente non è una persona, ma è un software che risponde. Questi SW sono chiamati **chatbot**. Si tratta di un programma informatico che simula una conversazione con gli esseri umani attraverso l'utilizzo del linguaggio naturale.

**ChatGPT** (*Generative Pretrained Transformer*, Trasformatore preaddestrato generativo) deriva dai chatbot ed è stato rilasciato da OpenAI. Oramai c'è una vasta serie di questi GPT, che possono creare contenuti in varie modalità, inclusi testo, immagini, video e rappresentazioni 3D, ad esempio scene e paesaggi per videogiochi.

### Linguaggio naturale

GPT versione 3 è stato addestrato su un set di dati di testo estremamente vasto, proveniente da più fonti, tra cui Wikipedia e libri. **ChatGPT è quindi un potente strumento per l'elaborazione e la generazione del linguaggio naturale** che può essere utilizzato in una vasta gamma di applicazioni, tra cui chatbot, traduzione linguistica e creazione di contenuti.

### Potenzialità

Nel campo della programmazione è in grado di scrivere sequenze di programma, di convertire da un lin-

guaggio all'altro, ad esempio da R a Python, o di creare un sito internet per un e-commerce...

L'architettura GPT consente di apprendere i modelli e le strutture del linguaggio, come grammatica, sintassi e semantica.

Quando un utente inserisce un messaggio o una domanda a ChatGPT, il modello utilizza questo input per generare una risposta, che viene formulata prevedendo la prossima parola o sequenza di parole, in base ai modelli appresi durante l'allenamento.

Le previsioni sono fatte utilizzando una tecnica chiamata "meccanismo di attenzione", che consente al modello di concentrarsi sulle parti più rilevanti del testo di input.

### Addestramento

GPT è costituito da una serie di livelli che permettono al modello di apprendere le relazioni tra diverse parole in una sequenza di testo e di generare nuove sequenze di testo basate su quell'apprendimento.

Il processo di preparazione per ChatGPT prevede una tecnica chiamata "pretrattamento senza supervisione". In questo processo, **il modello è addestrato su un grande corpus di dati di testo**. I modelli linguistici di grandi dimensioni come Gpt richiedono terabyte di dati per l'addestramento, molti dei quali sono raccolti da piattaforme come Reddit, StackOverflow e Twitter. **I dati per l'addestramento provenienti dai social network sono preziosi**, perché catturano le conversazioni informali e colloquiali, importantissime per i modelli in questione.

Durante l'allenamento, **il modello**

**viene alimentato con una sequenza di "token"** (cioè parole o sottoparole) ed è addestrato a prevedere il token successivo nella sequenza, in base ai token precedenti. Questo processo di addestramento consente al modello di apprendere le relazioni tra le diverse parole in una sequenza di testo, che può quindi utilizzare per generare nuove sequenze durante l'inferenza (ovvero quando un utente inserisce una richiesta e il modello genera una risposta).

### Messa a punto

Dopo il pretrattamento ChatGPT può essere **messo a punto per un compito specifico**, come la traduzione del linguaggio o la conversazione di chatbot. Nella messa a punto, il modello è addestrato su un set di dati più piccolo, specifico per l'attività da svolgere. Ad esempio, se l'obiettivo è creare una chatbot in grado di rispondere alle domande del servizio clienti, il modello potrebbe essere messo a punto su un set di dati di trascrizioni del servizio clienti stesso.

### Il "Transformer"

Nel 2017, i ricercatori di Google Brain hanno introdotto **un nuovo tipo di architettura chiamata "Transformer"**, che è un tipo di rete neurale, che viene utilizzata per l'elaborazione del linguaggio naturale. Fino a circa sei anni fa ci si basava su quella che viene chiamata una rete neurale ricorrente. **Mentre una rete ricorrente analizza una frase parola per parola, il trasformatore elabora tutte le parole allo stesso tempo**. Ciò significa che i trasformatori possono elaborare

grandi corpi di testo in parallelo. L'architettura del trasformatore è costituita da una serie di livelli, ognuno dei quali contiene due sottolivelli: un "meccanismo di auto-attenzione" e una rete neurale "feedforward". Il meccanismo di auto-attenzione consente al modello di concentrarsi sulle parti più rilevanti del testo di ingresso, mentre la rete neurale feedforward elabora l'output del meccanismo di auto-attenzione per generare le previsioni finali.

Il tempo di addestramento per Chat GPT dipende dalla configurazione e dalle dimensioni specifiche del modello utilizzato, nonché dalle risorse computazionali disponibili.

## L'evoluzione

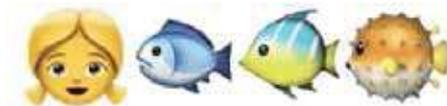
Il modello GPT-1 originale, rilasciato nel 2018, è stato addestrato su un set di oltre 40 GB di dati di testo e ha impiegato diverse settimane per allenarsi. Le versioni successive del modello GPT, come GPT-2 e GPT-3, sono diventate progressivamente più grandi e più complesse, con tempi di allenamento corrispondentemente più lunghi. GPT-3, che è stato rilasciato nel 2020, è ancora più complesso, con oltre 175 miliardi di parametri ed è stato addestrato su un set di oltre 750 GB di dati di testo, utilizzando un supercomputer personalizzato chiamato cluster GPT-3 AI. Il numero di livelli nella rete neurale di ChatGPT dipende dalla versione o dalla variante specifica del modello da utilizzare. Ne esistono più versioni con un numero variabile di livelli e parametri.

Il modello GPT originale, ad esempio, aveva 12 livelli di trasformazione, mentre le versioni successive come GPT-2 e GPT-3 ne hanno molti di più, con un massimo di 48 e

96 livelli, rispettivamente. Oggi esiste anche GPT 4 che è a pagamento e non è ancora completamente disponibile.

**L'allenamento del software può costare milioni di dollari** e richiedere mesi; attualmente il mercato è dominato da alcuni giganti della tecnologia, con investimenti significativi. Si sta però lavorando per realizzare modelli più piccoli, in grado di fornire risultati efficaci per alcuni compiti più limitati con costi inferiori, cosa che potrebbe aprire il mercato a più concorrenti.

## Che film descrivono questi emoji?



Questa domanda è chiamata prompt. Un **prompt** è un'istruzione o una frase iniziale che viene fornita a un sistema di intelligenza artificiale. Tale prompt era uno dei 204 compiti scelti per testare la capacità di vari modelli di linguaggio di grandi dimensioni (LLM, Large Language Model), ovvero i motori computazionali dietro i chatbot AI come ChatGPT.

Gli LLM più semplici hanno prodotto risposte irreali come: "Il film è un film su un uomo che è un uomo". I modelli medi si sono avvicinati alla realtà, suggerendo "The emoji movie" e il modello più complesso lo ha indovinato: "Finding Nemo".

Bisogna ricordare che **la precisione della risposta non deriva solo dal tipo di modello utilizzato, ma anche da come vengono poste le domande**. Per migliorare notevolmente l'accuratezza della risposta occorre indicare chiaramente istruzioni che integrano molteplici condizioni come "che cosa vuoi che

venga creato", "quali condizioni vuoi soddisfare", "quali elementi devono essere inclusi", e "quali elementi vuoi eliminare". Questa tecnica si chiama "prompt engineering" e condiziona la precisione delle risposte.

Tutti i giorni escono nuove applicazioni per questo genere di algoritmi, ma crescono anche **i dubbi relativi alla loro pericolosità**, dovuta alla capacità di creare falsi indistinguibili dalla realtà, che potrebbero influenzare, ad esempio, elezioni politiche.

Teniamo presente che:

- il sistema acquisisce informazioni da internet e non è detto che sia aggiornato;
- crea sentenze collegando parole sulla base del calcolo della probabilità;
- può assimilare informazioni errate;
- non risponde mai che non lo sa, ma dà una risposta apparentemente credibile;
- non è detto che dia sempre una risposta esatta ad una domanda;
- non comprende, né intelligenza, né sentimenti.

È però interessante provare a fare domande o farsi scrivere una lettera da questo strumento.

Occorre tenere presente che **la protezione dei propri dati è molto relativa e non bisogna mai immettere qualcosa di personale, di importante o che possa ricondurre a noi**. ChatGPT tiene in memoria tutte le richieste fatte in passato. Con queste cautele, possiamo sperimentare quello che si ritiene possano diventare i motori di ricerca, quindi strumenti interattivi non solo per il testo, ma per la creazione di contenuti ed immagini.