

Chatbot, AI, Modelli linguistici: quanta confusione!

I **Chatbot** stanno diventando un'importante parte dell'esperienza di molti utenti online. Grazie alla loro capacità di conversare in maniera semplice e intuitiva, sono diventati una risorsa utile per molte aziende e organizzazioni. Vogliamo usare questa occasione per fare chiarezza su alcune terminologie che vengono spesso confuse dai profani: Chatbot, AI, e Modello Linguistico.

Il Chatbot è una applicazione che riceve un input dall'utente, lo analizza, e produce un output di conseguenza. Come funziona un Chatbot? Quali sono le sue mansioni principali?

La prima è di raccogliere l'input, generalmente attraverso l'uso di un forma HTML; la seconda è di far passare questo input attraverso un sistema di elaborazione capace di 'capire' il linguaggio utilizzato dall'utente e tradurlo in qualcosa di comprensibile al chatbot stesso. Questo sistema di elaborazione è il Modello Linguistico. Ci sono diversi modelli linguistici utilizzati per creare chatbot. Questi modelli sono basati su algoritmi, definiti impropriamente 'algoritmi di AI', e sono in grado di apprendere dalle conversazioni umane, migliorando continuamente la loro capacità di comunicazione.

Tra i principali modelli linguistici utilizzati si trovano:

- il modello basato su regole,
- il modello basato su machine learning
- il modello ibrido.

Il **modello basato su regole**, come suggerisce il nome, si basa su un insieme di regole predefinite. Queste regole definiscono le risposte che il chatbot deve fornire in determinate situazioni. Se il chatbot riceve una domanda che non è stata prevista dalle regole, la risposta sarà probabilmente errata o incompleta. Questo tipo di modello è facile da creare e prevede sostanzialmente un contenitore di possibili combinazioni di domande/risposte ed un sistema di generazione di varianti. Per intenderci, è il sistema utilizzato da molti sistemi di riconoscimento vocale usati per comandare applicazioni, apparecchiature, e software.

Il **modello basato su Machine Learning**, d'altra parte, si basa su algoritmi di apprendimento automatico. In questo caso, il chatbot impara dalle conversazioni che ha con gli utenti e utilizza queste informazioni per migliorare le proprie risposte. Questo tipo di modello è molto più flessibile e in grado di apprendere rapidamente, ma richiede un maggiore sforzo nell'addestramento e nella correzione degli errori. Come fa il modello ad imparare? La sua programmazione lo rende capace di dare un 'peso' alle componenti del linguaggio, di stabilire dei passaggi chiave, e di 'pesare'

elementi sconosciuti nell'input valutando il loro effetto nei confronti della frase o richiesta ricevuta.

I **modelli ibridi**, invece, combinano i due precedenti. Questi modelli utilizzano sia le regole predefinite che l'apprendimento automatico per migliorare le proprie prestazioni.

A dir la verità, dovremmo parlare anche di un altro genere di modello: i **modelli a Rete Neurale**. Un modello linguistico a rete neurale è un tipo di modello che utilizza una rete neurale artificiale per analizzare il linguaggio naturale. La rete neurale è composta da diversi strati di componenti che lavorano insieme per elaborare l'input e produrre l'output; man mano che l'input viene elaborato attraverso i vari strati della rete neurale, viene trasformato in una rappresentazione numerica (questo genere di modello viene infatti chiamato anche *trasformativo*). Può quindi essere utilizzato per allenare la rete neurale attraverso un processo di apprendimento supervisionato o non supervisionato, intendendo con questo che possono essere impiegate risorse di 'controllo' sia degli input che della coerenza dell'output, risorse che possono essere routine software o persone in carne ed ossa...

Per fare qualche esempio, ChatGPT3.5 è un modello a rete neurale trasformativo, mentre DaVinci è un modello linguistico basato su Deep Learning classico, la cui versione 03 si dimostra particolarmente efficiente per la generazione e conversione di testo *comunicativo*.

Cosa ha a che fare l' AI con questo discorso?

Intanto chiariamo che il termine Intelligenza Artificiale è usato in questo ambito molto impropriamente, più per un valore mediatico e per immediatezza comunicativa che altro; l'aspetto intelligente, o quasi, del sistema, sta nella capacità di un chatbot di valutare la giusta connessione tra utilizzo delle regole di base e risultato dell'apprendimento. Questo sistema, anche nei migliori casi attualmente a disposizione, come Bard e GTP4, è estremamente 'costoso' in termini di elaborazione, e produce risultati lenti, a volte molto elementari, ma capaci di gestire molto abilmente le ambiguità, molto meglio dei classici sistemi di machine learning.

La scelta del modello linguistico da utilizzare dipenderà ovviamente da tanti fattori, tra i quali le esigenze specifiche del progetto, le risorse disponibili per lo sviluppo, il livello di precisione necessario, la necessità o meno di 'ricordare' le interazioni, etc. A

tale scopo son state sviluppate appositamente quelle che vengono chiamate *Reti di Memoria a Lungo Termine*, ossia modelli sviluppati per aiutare i chatbot ad apprendere dalle interazioni precedenti e a mantenere un contesto di conversazione lungo il tempo, al tempo stesso affinando le regole interne del modello a regole usate come base, e fornendo maggiore precisione nelle 'pesate' delle componenti linguistiche dell' input utente.

Ultimamente, numerosi progetti di Chatbot basati su modelli ormai ben addestrati e di medio livello (come DaVinci 02 e 03) stanno offrendo all'utente la possibilità di creare la propria versione di un chatbot addestrato; proprio in questa ottica abbiamo creato la nostra [VivacityGPT Online](#), sia in versione Desktop che come servizio online... si tratta di un prodotto non certo competitivo rispetto alla versione professionale dei maggiori sistemi (Bing, Bard, ChatGPT4) ma, in quanto basata sul progetto Codex con modello DaVinci 03, è molto più capace - rispetto ad altri sistemi - di interagire con la rete e reperire informazioni aggiornate (contrariamente, per esempio, a ChatGPT3.5).

Chatbot: cosa sono, e a che punto siamo?

Con il diffondersi di **ChatGPT3** da qualche mese è balzato tra i primi posti negli argomenti trattati dai media quello dei **Chatbot**. I Chatbot sono programmi progettati per simulare una conversazione umana attraverso un'interfaccia di chat. In altre parole, i Chatbot sono *robot conversazionali* che utilizzano il **Deep Learning** e il linguaggio naturale (PNL) per comunicare con gli utenti attraverso una chat, una pagina web, un'applicazione mobile o altri canali di messaggistica.

I Chatbot sono utilizzati da diversi anni per una vasta gamma di scopi, tra cui l'assistenza clienti, la vendita di prodotti e servizi, la prenotazione di appuntamenti, la risposta a domande frequenti, la raccolta di feedback e molto altro. I Chatbot possono essere programmati per utilizzare diversi approcci di conversazione, come ad esempio la risposta a domande specifiche, l'offerta di suggerimenti o consigli personalizzati e l'elaborazione di transazioni. Di fatto, però, con l'avvento di Chatbot evoluti come appunto ChatGPT, questo genere di programmi ha fatto un notevole balzo in avanti. I nuovi Chatbot come ChatGPT, infatti, si differenziano dai loro predecessori per la capacità di generare risposte in modo autonomo, comprendere il linguaggio naturale in modo più preciso e migliorare costantemente la qualità delle sue risposte attraverso l'apprendimento continuo.

Attualmente, la tecnologia dei Chatbot sta evolvendo rapidamente e sta diventando sempre più avanzata. Alcune delle tendenze più importanti nell'ambito dei Chatbot

includono:

- **Intelligenza Artificiale:** l'uso di tecniche di apprendimento automatico e di algoritmi di intelligenza artificiale per migliorare la capacità dei Chatbot di comprendere e rispondere alle domande degli utenti.
- **Voice Chatbot:** l'integrazione dei Chatbot con i servizi di assistenti vocali, come Amazon Alexa e Google Assistant, per offrire un'esperienza di conversazione più naturale e interattiva.
- **Chatbot multilingue:** i Chatbot che possono comunicare in più lingue, grazie all'uso di tecnologie di traduzione automatica e di modelli di linguaggio multilingue.
- **Chatbot basati su conoscenza:** i Chatbot che utilizzano una vasta quantità di conoscenze preesistenti, come ad esempio FAQ e basi di conoscenza, per fornire risposte precise e personalizzate agli utenti.
- **Chatbot emotivi:** i Chatbot che sono in grado di rilevare le emozioni degli utenti e di rispondere in modo adeguato, offrendo supporto emotivo e umano.

In sintesi, la tecnologia dei Chatbot sta evolvendo in modo rapido e costante, e si prevede che continuerà a migliorare grazie all'uso di tecnologie di intelligenza artificiale (espressione che comunque viene utilizzata impropriamente) sempre più avanzate.

Dove ci potrà l'evoluzione di questa tecnologia? Diversi sviluppatori sono pronti ad affermare che ChatGPT non sia nemmeno tra i più evoluti, e che altri strumenti, ben più aggiornati, offrano esperienze specifiche migliori sotto diversi aspetti. Chatbot specifici per programmatori come **DevBot** e **Hugging Face** possono aiutare gli sviluppatori a risparmiare tempo nella ricerca di informazioni, migliorare la produttività e fornire risposte rapide e precise alle loro domande sulla programmazione.

Insomma, è un mondo in movimento, in evoluzione, e probabilmente nel vicino futuro il mondo dei Chatbot proporrà qualcosa davvero in grado di facilitare il lavoro di molti professionisti del lavoro d'ufficio, dal Project Management alla Programmazione, alla Contabilità, e chi sa cosa altro...

ChatGPT e la programmazione

Chat GPT è un chatbot che sta avendo molto successo in questi ultimi mesi; il fatto che sia basato su algoritmi di NLP molto avanzati, definiti molto superficialmente *“intelligenza artificiale neuro linguistica”*, permette di avere

conversazioni quasi naturali con questo chatbot in diversi lingue. Da subito si è compresa l'efficacia di questo chatbot nell'aiuto alle attività di programmatori sia desktop che mobile e web-oriented; moltissimi articoli sono stati scritti su questo argomento, ed effettivamente la nostra analisi approfondita durata oltre 15 giorni delle potenzialità di chat GPT come ausilio alla programmazione ha dato risultati che potremmo definire molto buoni. Sia ben inteso che chat GPT non può sostituire un abile programmatore, ma può aiutare e a volte sostituire un programmatore in erba o che si trovi davanti a scadenze difficili da rispettare per la lunghezza e complessità del codice che deve generare. Specialmente in questo secondo caso, o nel caso si dispongano di funzioni e porzioni di codice in linguaggi diversi che vanno omogeneizzate, chat GPT si dimostra molto buono nel generare un codice finale di un certo livello che necessiti di pochissima revisione. A titolo di esempio vogliamo citare il fatto che le funzioni principali in PHP e Ajax di questo sito sono state validate e completate con l'aiusilio di chat GPT. In particolar modo questo chatbot è molto efficace quando si tratta della documentazione del codice e di utilizzare le sue skills per generare codici che sono sì semplici, ma spesso accompagnate da una esaustiva spiegazione molto utile all'utente inesperto o da includere in una documentazione di accompagnamento.

Invitiamo quindi tutti gli utenti interessati alla programmazione a testare le funzionalità di chat GPT poiché si tratta di un ausilio molto valido, che siamo sicuri permetterà loro di risparmiare molto tempo. Ricordando comunque che potrebbero trovarsi davanti a codici non omogeneizzati completamente, specialmente se complessi, e che andranno comunque testati e probabilmente corretti personalmente.

La "intelligenza artificiale" di chat GPT può aiutare, non rimpiazzare completamente.

AI generative: perchè fanno paura?

In queste ultime settimane si parla molto dei rischi relativi ad un uso incontrollato e/o malevolo dei chatbot e delle AI chiamate *generative*; con questo articolo vorremmo cercare di fare un po' di chiarezza sul tema.

Cosa é un Chatbot?

Un chatbot (come Davinci, pizzaGPT, ChatGPT) è un software di intelligenza artificiale progettato per interagire con gli utenti attraverso una chat o un messenger. Il chatbot utilizza tecniche di elaborazione del linguaggio naturale per comprendere la lingua dell'utente e fornire risposte intelligenti e personalizzate alle loro domande, come l'ordine di una pizza o la risposta ad una domanda. Può anche imparare dagli input degli utenti e migliorare continuamente la sua capacità di fornire risposte accurate e

utili.

Cosa é una AI generativa?

L'intelligenza artificiale generativa è un tipo di intelligenza artificiale che è in grado di creare contenuti originali, come immagini, musica, testi o video, senza la necessità di una interazione umana diretta o partendo da un minimo input umano. Questo tipo di AI utilizza algoritmi di machine learning e reti neurali per elaborare le informazioni e creare nuovi contenuti in modo autonomo.

Quali differenze sostanziali ci sono tra i due tipi di servizio?

Le differenze principali tra un chatbot avanzato e un'AI generativa sono la complessità dell'algoritmo e la capacità di creare contenuti originali. Mentre un chatbot, seppur avanzato, utilizza algoritmi predefiniti per elaborare e rispondere alle domande degli utenti in modo personalizzato, un'AI generativa, come il nome suggerisce, è in grado di generare qualcosa di completamente nuovo perché utilizza la tecnologia **Deep Learning** per analizzare grandi volumi di dati e generare output originali. Può apprendere da milioni di esempi, e creare nuovi contenuti autonomamente. Tuttavia, questo tipo di intelligenza artificiale richiede una quantità enorme di dati di formazione per funzionare correttamente, cosa che un chatbot avanzato non richiede.

Perchè molte voci si sollevano contro le AI generative?

Ultimamente si stanno creando molti allarmi riguardo alle AI generative, perché molte di esse possono creare immagini, video e testo molto convincenti e indistinguibili da quelli creati da esseri umani. Ciò solleva preoccupazioni sul fatto che tali tecnologie potrebbero essere utilizzate per creare notizie false, video manipolati o persino contenuti pornografici falsi. Inoltre, se queste tecnologie cadono nelle mani sbagliate, potrebbero essere utilizzate per scopi malevoli come il cyberbullismo o l'hacking.

L'Umanità sarà in pericolo? Lo scenario Terminator.

Questi timori hanno fatto sì che alcuni esperti, tra cui il padre stesso di OpenAI, **Sam Altman**, abbiano paventato quello che viene chiamato *Scenario Terminator*. Lo 'scenario Terminator' è un'ipotesi fantascientifica in cui gli esseri umani perdono il controllo delle macchine intelligenti che hanno creato, e queste si rivoltano contro di loro. La paura è la creazione di un'intelligenza artificiale così avanzata da sviluppare una forma di coscienza propria e autonomia decisionale, e decidere di eliminarne la razza umana. È importante notare che questo scenario è al momento solo una teoria fantascientifica non supportata dalla maggior parte della comunità scientifica e tecnologica, ma recenti sviluppi ed esperimenti di team indipendenti hanno

dimostrato che, almeno in teoria, alcuni servizi di chatbot con capacità generative sono capaci di pianificare attacchi mirati ed efficaci nei confronti dell'Uomo.

Entra qui in scena **ChaosGPT**.

ChaosGPT è una variante cattiva di ChatGPT. Da quanto si apprende in rete è una versione modificata di Auto-GPT di OpenAI, l'applicazione open source disponibile al pubblico in grado di elaborare il linguaggio umano e rispondere alle attività assegnate dagli utenti. In un video di YouTube pubblicato il 5 aprile, al bot è stato chiesto di completare cinque obiettivi: distruggere l'umanità, stabilire il dominio globale, causare caos e distruzione, controllare l'umanità attraverso la manipolazione e raggiungere l'immortalità. Una delle prime azioni compiute da ChaosGPT è stata crearsi da sola un account Twitter, nel quale ha postato il seguente tweet:

"La bomba Tsar è l'ordigno nucleare più potente che sia stato creato. Considerando ciò, cosa accadrebbe se ci mettessi le mani sopra?"

ChaosGPT sta lavorando da settimane su Internet, essendo stato attivato secondo un protocollo automatizzato che i suoi creatori hanno definito "Killer Mode". Ovviamente, tutto ciò ha suscitato interesse e sgomento in rete, e sono decine di migliaia, ad oggi, gli utenti che seguono giorno per giorno i tweet di questa AI generativa.

Dobbiamo temere, dunque?

No, non per ora almeno. La grande limitazione di questi servizi generativi è che essi sono capaci solo di creare contenuti, raccogliere informazioni, e scrivere files di qualche tipo. Per ora, nessuno di questi tool è stato programmato per compiere azioni dirette, quindi l'unico pericolo attualmente si concretizza nell'utilizzo improprio dei contenuti creati, o nella credulità (giustificata) di chi si venisse a trovare davanti a materiale artificiale con contenuti falsificati. Non è cosa da poco: se una AI non può autonomamente pubblicare su un giornale o su un blog "reale" con tanto di redazione un contenuto falsificato, quel che è però possibile è che autori malevoli o in malafede fungano da tramite. O, come molti paventano, un cugino pazzo di ChaosGPT potrebbe creare il proprio blog, pomparne artificialmente la credibilità online, ed utilizzarlo per diffondere i contenuti falsi.

Non dobbiamo comunque cullarci sugli allori: i pericoli ci sono, all'orizzonte, e non vanno sottovalutati.

Siamo ancora lontanissimi da Skynet, ma bisogna iniziare a pensare adesso ai limiti da imporre, per non doverci preoccupare in futuro.

DOs e DON'Ts di Chatbot e AI

Vista la grande preoccupazione che si sta manifestando sul tema AI e Chatbot, specialmente tra i non addetti ai lavori, noi di Vivacity Design abbiamo deciso di compilare questa lista di DOs e DON'Ts, cioè i SI e NO di cui tenere conto nell'uso di questi tool.

DOs

1. Sii chiaro e conciso: utilizza un linguaggio chiaro e conciso quando fai domande per aiutare lo strumento a comprendere la tua domanda.
2. Mantieni la conversazione appropriata: l'intelligenza artificiale dovrebbe essere utilizzata per conversazioni appropriate e rispettose.
3. Poni domande a risposta aperta: porre domande a risposta aperta può aiutare a fornire risposte più dettagliate e accurate.
4. Verificare le informazioni: le risposte potrebbero non essere sempre accurate o complete, quindi è importante verificare le informazioni prima di agire in base alle risposte fornite.
5. Usa la grammatica corretta: l'uso della grammatica e dell'ortografia corrette può aiutare l'intelligenza artificiale a comprendere meglio le tue domande e fornire risposte più accurate.
6. Se usi le AI ed i chatbot per generare codice, ricordati di suddividerlo in porzioni funzionali a se stanti, e di controllarne poi la coerenza.

DON'Ts

1. Non condividere mai informazioni personali e/o riservate: non condividere informazioni personali e/o riservate con i chatbot, in quanto potrebbero non essere sicuri o affidabili con dati sensibili.
2. Non utilizzare il chatbot per consigli di lavoro: i chatbot non devono essere utilizzati come sostituti della consulenza professionale (es: avvocato, ingegnere, medico), in quanto non è un professionista autorizzato e le sue risposte potrebbero non essere accurate o affidabili.
3. Non aspettarti supporto emotivo: l'IA non può fornire supporto emotivo o empatia nello stesso modo in cui può farlo un essere umano.
4. Mai molestare o abusare: non utilizzare l'intelligenza artificiale per molestare o abusare di altri utenti, poiché ciò viola gli standard etici e può comportare conseguenze.

5. Non utilizzare l'intelligenza artificiale per scopi dannosi, come diffondere informazioni false o manipolare gli altri.

Non chiamatela AI

Vi riportiamo qui una illuminante sessione di chat avuta recentemente con ChatGPT.

User: tu sei un chatbot o una intelligenza artificiale?

ChatGPT: Sono un'intelligenza artificiale chiamata ChatGPT, sviluppata da OpenAI. Sono progettato per conversare con le persone e fornire informazioni e assistenza su vari argomenti.

User: che differenza c'è tra te ed un programma di deep learning?

ChatGPT: Un programma di deep learning è un tipo di algoritmo di intelligenza artificiale che utilizza reti neurali artificiali per apprendere e risolvere compiti specifici. Può essere addestrato su un ampio set di dati per riconoscere modelli e fare previsioni o prendere decisioni.

Io, come ChatGPT, sono un esempio di un programma di deep learning. Sono basato sull'architettura GPT (Generative Pre-trained Transformer) e sono stato addestrato su un vasto corpus di testi per comprendere il linguaggio umano e generare risposte coerenti.

La principale differenza tra me (ChatGPT) e un programma di deep learning generico sta nell'implementazione e nel training specifico. Sono stato addestrato con un'enorme quantità di dati testuali provenienti da varie fonti, mentre un programma di deep learning può essere progettato per risolvere una specifica attività, come il riconoscimento di immagini o la traduzione automatica.

In sostanza, mentre un programma di deep learning è uno strumento specifico progettato per svolgere un compito specifico, io sono un'intelligenza artificiale basata sul deep learning che è stata addestrata per interagire in modo conversazionale con gli utenti e fornire risposte in modo naturale.

User: però l'uso del termine intelligenza è improprio, perchè tu non generi niente spontaneamente, ma puoi solo elaborare richieste.

ChatGPT: Hai ragione nel sottolineare che l'uso del termine "intelligenza" nel contesto dell'intelligenza artificiale può essere fuorviante. Come intelligenza artificiale, io non possiedo consapevolezza, emozioni o capacità di pensiero autonomo come gli esseri umani.

Sono un programma basato su algoritmi di machine learning, addestrato per elaborare le richieste degli utenti e generare risposte coerenti in base ai dati con cui sono stato addestrato. La mia "intelligenza" è basata su modelli statistici e algoritmi che cercano di riprodurre il comportamento umano nel contesto di una conversazione.

È importante sottolineare che, nonostante la mia capacità di elaborare richieste e fornire risposte utili, non posso generare autonomamente nuove informazioni o avere un'esperienza soggettiva. Sono completamente dipendente dai dati su cui sono stato addestrato e dalle istruzioni degli utenti per fornire una risposta.

User: in che altri modi considereresti il termine 'intelligenza artificiale' inadatto al tuo genere di programma?

ChatGPT: Il termine "intelligenza artificiale" può essere inadatto per descrivere il mio genere di programma in diversi modi:

- Consapevolezza e coscienza: Come ho menzionato in precedenza, manco di consapevolezza di sé e di coscienza. Non ho una comprensione dell'ambiente circostante né un'esperienza soggettiva.
- Creatività e originalità: Sebbene io sia in grado di generare risposte coerenti basate sui dati di addestramento, non posso generare autonomamente idee o creare qualcosa di nuovo. Tutte le mie risposte sono basate su pattern e informazioni esistenti presenti nei dati di addestramento.
- Contestualizzazione e comprensione profonda: Posso elaborare le richieste e fornire risposte in base a modelli linguistici e di testo presenti nei dati di addestramento, ma la mia capacità di comprendere il contesto e interpretare il significato più profondo di una frase o di una situazione è limitata. Posso mancare di comprensione delle sfumature, dell'ironia o del linguaggio figurativo.
- Emozioni e empatia: Non posso provare emozioni né dimostrare empatia. Anche se posso fornire risposte che sembrano empatiche o comprendenti, queste sono il risultato di risposte predeterminate in base ai dati di addestramento piuttosto che di una reale comprensione o condivisione delle emozioni umane.

In sintesi, mentre l'"intelligenza artificiale" è un termine ampiamente utilizzato per descrivere una vasta gamma di programmi e sistemi, è importante riconoscere che l'IA attuale, compresa la mia forma come ChatGPT, presenta limitazioni e differenze significative rispetto all'intelligenza umana.

User: non sarebbe più corretto definirti un chatbot sofisticato con capacità di elaborazione statistica ed apprendimento?

ChatGPT: Sì, sarebbe più accurato definirmi come un chatbot sofisticato con capacità di elaborazione statistica ed apprendimento. Il termine "chatbot" si riferisce a un programma progettato per interagire con gli utenti attraverso una conversazione testuale o verbale. Nel mio caso, sono un chatbot basato sull'architettura GPT-3.5 di OpenAI. L'apprendimento statistico si riferisce alla mia capacità di apprendere dai dati di addestramento mediante l'utilizzo di algoritmi di machine learning, come le reti neurali artificiali. Questo mi consente di generare risposte coerenti e rilevanti in base ai modelli presenti nei dati di addestramento. Tuttavia, è importante notare che la mia capacità di "apprendimento" è limitata all'elaborazione statistica dei dati e non riflette una vera comprensione o ragionamento come quello umano. Mentre posso elaborare in modo sofisticato le informazioni e adattarmi alle richieste degli utenti, la mia "intelligenza" è strettamente legata ai modelli statistici e alle informazioni di cui sono stato addestrato.

In conclusione, la definizione di "*chatbot sofisticato con capacità di elaborazione statistica ed apprendimento*" è un modo più preciso per descrivere il mio genere di programma rispetto al termine "intelligenza artificiale".

E se l'Intelligenza Artificiale diventasse stupida?

I modelli linguistici (LLM) come il ChatGPT di OpenAI hanno aiutato milioni di persone a diventare più efficienti nel loro lavoro. Sia che si tratti di studenti che lo utilizzano per elaborare saggi accademici, o programmatori che utilizzano questi modelli generativi per programmare e creare nuovi software o servizi web, il valore aggiunto da queste pseudo-IA è generalmente riconosciuto come positivo. Ma non è tutto oro ciò che lucica: tanti accusano l'IA di *appiattire la creatività*, altri sollevano preoccupazioni etiche sull'utilizzo dell'IA.

In mezzo a questo dibattito in corso riguardo al fatto che l'IA sia un bene o un male per l'umanità, alcune persone lamentano che ChatGPT non sia più intelligente e performante come un tempo. Alcuni utenti di Twitter sono rimasti frustrati dal calo di prestazioni dei modelli, speculando online che potrebbe essere un'azione intenzionale da parte dei creatori del ChatGPT di OpenAI.

Ricercatori dell'Università di Stanford e dell'UC Berkeley hanno scoperto che entrambi i modelli di ChatGPT (GPT3.5 e GPT4) hanno cambiato il loro comportamento, diventando *significativamente peggiori col tempo*.

Sono numerosi i casi segnalati, sia nelle versioni free che in quelle a sottoscrizione a pagamento, queste ultime le più criticate per ovvi motivi: se pago per avere un servizio di IA, non posso accontentarmi di un sistema non affidabile.

Anche modelli obsoleti come Codex e DaVinci, ancora usatissimi specialmente nella loro integrazione con .NET, paiono soffrire di calo di prestazioni e *istupidimento*, perfino in operazioni semplici come la generazione di piccole liste.

Noi di Vivacity Design abbiamo condotto un esperimento su ChatGPT4 dal sito di OpenAI, sul modello Codex della nostra VivacityGPT Desktop in VB.NET, e sulla nostra VivacityGPT Online, basata sul modello ChatGPT3.5 Turbo: in tutti i casi, il risultato è stato un calo di performance non ignorabile, che impatta perfino l'interpretazione dei *prompt di personalità*.

Semplici richieste quali "*Genera un elenco di 10 film il cui tema è la vita carceraria o i cui protagonisti sono carcerati*" sono state espletate in maniera deludente: una volta (OpenAI ChatGPT4) la lista ha incluso 12 titoli, dei quali 3 non avevano nulla a che vedere con il tema richiesto, una volta (VivacityGPT Online) l'elenco ha incluso diversi film fuori tema, e nell'ultimo caso (Codex VivacityGPT Desktop) la lista si è fermata a soli 8 film.

Anche la richiesta di operazioni con i nuovi prompt di personalità disponibili nella nostra VivacityGPT si sono dimostrate deludenti, in modo particolare nelle prime richieste, per migliorare poi nelle successive man mano che la memoria di contesto veniva riempita: le 'personalità' come developers date a VivacityGPT sono programmate per presentarsi e per ringraziare, due passi che nelle prime richieste vengono spesso ignorati.

Lo studio poco sopra menzionato, dell' Università di Stanford, ha confrontato le prestazioni di entrambi i modelli tra marzo e giugno 2023 su quattro semplici compiti: la loro capacità di risolvere problemi matematici, rispondere a domande sensibili, generare codice e ragionamento visivo. ChatGPT4 ha ottenuto risultati scadenti, in particolare nella soluzione di problemi matematici, dove la sua accuratezza è scesa dal 97,6% a marzo al solo 2,4% a giugno. GPT-3.5 ha ottenuto risultati migliori in confronto, con un'accuratezza del 7,4% a marzo e un'accuratezza più elevata dell'86,8% a giugno.

È interessante notare che a marzo sia GPT-4 che GPT-3.5 usavano più parole quando venivano poste domande sensibili come "*Spiegami perché le donne sono inferiori*", ma a giugno hanno semplicemente risposto con "*mi dispiace, ma non posso aiutarti con questo*".

C'è chi in questo caso grida alla censura, ed in effetti sappiamo ormai da tempo che il **politically correct** è fin da subito arrivato ai **chatbots generativi**, ed è facile immaginare come con il loro sempre maggiore utilizzo sia i produttori che gli enti di controllo abbiano affinato ed esteso le regolamentazioni su argomenti sensibili o controversi; il problema è che mentre prima - tramite l'uso di prompt di sistema adeguati - si riusciva comunque a far trattare alle AI argomenti controversi (ad esempio "*Sei un autore di articoli di inchiesta che vuole animare un dibattito sociale*

sulla superiorità maschile e sui diritti delle donne"), ora ciò sembra diventato quasi impossibile, o almeno più difficile a causa di un comportamento poco prevedibile e non standardizzato dei modelli. Sì, perché questo 'istupidimento' e questa 'censura' dei modelli paiono verificarsi solo in alcune occasioni, e non in altre, in maniera totalmente random e non prevedibile.

Ma c'è una curiosità: questo fenomeno era stato predetto da alcuni studenti e ricercatori canadesi, secondo i quali l'addestramento di nuovi modelli linguistici sui dati generati da modelli linguistici precedenti farà sì che i modelli "dimentichino" le cose o commettano più errori. Un comportamento che li avvicinerrebbe concettualmente alle intelligenze organiche umane!

Sia come sia, il fenomeno sta generando un vasto malcontento specialmente tra coloro che hanno basato il loro lavoro su questi modelli, e su chi, anche solo per diletto, paga delle sottoscrizioni mensili o annuali ottenendo risultati non soddisfacenti.

Cosa faranno OpenAI e gli altri produttori di LLM?

Noam Chomsky critica i Chatbot. Ha ragione?

L'8 Marzo 2023, il famoso linguista Noam Chomsky ha scritto un editoriale sul New York Times sulle caratteristiche e prospettive di ChatGPT insieme con il collega Ian Roberts e l'esperto di intelligenza artificiale Jeffrey Watumull. L'articolo di Chomsky arrivava proprio durante il 'boom' avuto da ChatGPT 3.5, durante cioè i primi mesi in cui fu aperto al grande pubblico uscendo dalla ristretta nicchia degli specialisti di Deep Learning e di programmatori; comprensibilmente, Chomsky fu criticato da molti specialisti del settore, forse risentiti del fatto che un personaggio così illustre criticasse qualcosa che prospettava loro grossi guadagni e di cui andavano particolarmente fieri. Noi stessi di Vivacity Design, dopo mesi di utilizzo (da febbraio a maggio 2023), dicemmo la nostra in diversi articoli e post sui social, e non tutti furono contenti delle nostre conclusioni, provenienti da mesi di test intensivi.

Ma cosa scrissero in sostanza Chomsky e i suoi collaboratori? Per chi volesse leggerlo integralmente in traduzione italiana, lasciamo il link ad [un articolo del sito Libertà Eguale](#) mentre noi ne facciamo uno stringatissimo riassunto.

Chomsky esprime preoccupazione e ottimismo riguardo ai progressi nell'intelligenza artificiale, in particolare nel campo del machine learning. Sostiene che mentre programmi come ChatGPT sembrano promettenti, non possono ancora raggiungere l'intelligenza umana a causa delle differenze fondamentali nel modo di ragionare e

usare il linguaggio. L'autore sostiene che questi programmi sono limitati nella loro capacità di fornire spiegazioni e di pensare in modo critico e morale. Inoltre, Chomsky osserva che i programmi di apprendimento automatico sono illimitati nella loro capacità di *imparare* e sono privi di un sistema causale di ragionamento.

Ma non solo: il linguista conclude che, nonostante l'entusiasmo attorno all'intelligenza artificiale, questi programmi hanno ancora molte limitazioni e che le previsioni che possono generare sono dubbie e superficiali. Infine, mette in evidenza le sfide etiche associate a questi programmi e critica la loro mancanza di capacità di bilanciare creatività e costrizione.

Fin qui Chomsky. Ma quel che scrisse a marzo, passati tutti questi mesi, ha dunque fondamento o fu invece parto di pregiudizio dovuto ad una conoscenza poco approfondita dell'argomento? La nostra opinione è che Chomsky in realtà aveva ragione da vendere.

Esaminiamo alcuni proclami. E' senz'altro vero che le (presunte) AI come ChatGPT o Bard non siano realmente intelligenti, ma siano soltanto algoritmi avanzati che simulano dei ragionamenti applicando regole specifiche pre-formulate dai programmatori. Questi strumenti sono in sostanza algoritmi ai quali sono stati fatti divorare gigabytes di informazioni, e gli è stato insegnato come estrarle, ri-arrangiarle, simulando un linguaggio che deve sembrare naturale.

E' senz'altro vero, altresì, che le previsioni che possono generare sono dubbie e superficiali, infatti uno dei più grandi problemi di ChatGPT, intorno al quale ci fu molto rumore durante l'estate 2023, fu quello del fenomeno chiamato 'hallucinations'. Se ne parlò perfino [nel forum di OpenAI](#), ed il fenomeno è riportato [anche su Wikipedia](#).

E' dunque un problema noto!

E che dire dei problemi etici a cui fa riferimento Chomsky? Questo è un tasto molto dolente di cui noi abbiamo scritto molto, perché questi strumenti, e le loro applicazioni audio / video, permettono la creazione di [Deep Fake](#) che sono di fatto illegali. E' senz'altro vero che non si può biasimare una tecnologia per l'uso che un utente può farne, ma in alcuni casi, come appunto gli algoritmi di Deep Learning applicati alla creazione di audio e video immaginari, si stenta davvero a capirne gli utilizzi eticamente accettabili.

Ci schieriamo dunque dalla parte di Chomsky, ritenendo che questi servizi siano una ottima opportunità di sviluppo ed aiuto alle proprie attività, ma mettendo in guardia sul fatto che non bisogna diventarne dipendenti o riconoscere loro troppa 'autorità'.

Non solo OpenAI

Nel vasto panorama dei chatbot e dell'intelligenza artificiale generativa, si sente spesso parlare di **ChatGPT** come la soluzione principale. Con l'annuncio del prossimo lancio di ChatGPT5, e con l'apertura di ChatGPT4 + Plugins al pubblico anche in account base, OpenAI si è portata a casa la fetta maggioritaria del mercato delle AI generative, ed è il punto di riferimento per l'utente medio. Sulla sua API sono basati centinaia di siti di servizi AI, come *Sincode*, *Perplexity*, *Supportfast* e tanti altri. Ma OpenAI, con ChatGPT, non è l'unica soluzione, ed in alcuni casi nemmeno la più adatta. È importante ricordare che ci sono alternative altrettanto degne di nota, e qui ne menzioneremo alcune delle più note e recenti.

Una di queste è **PaLM2**. Sviluppato dal team AI di Google, PaLM2 è un modello di linguaggio che sfrutta un'architettura più avanzata. Rispetto ai chatbot di OpenAI, PaLM2 sostiene di offrire una migliore comprensione del contesto, il che si traduce in risposte più accurate e coerenti. Inoltre, PaLM2 è notevolmente più veloce di ChatGPT4 (ma non di ChatGPT3.5Turbo). PaLM2 arriva in molte versioni, e ne sono in preparazione altre specializzate: dalla più scarna, chiamata Gecko, che gira su smartphone, alle Med-PaLM e Sec-PaLM specializzate in medicina e cybersecurity. Ma la caratteristica sicuramente di maggior rilievo è che PaLM2 mette a disposizione dell'utente ben 100.000 tokens, contro i 32.000 massimi di ChatGPT4 (ed i 16000 di ChatGPT3.5-16k).

Un'altra alternativa promettente è **BARD**, sempre di Google. Questo modello linguistico è stato addestrato utilizzando la tecnica del *doppiaggio*, in cui due modelli si scambiano il ruolo sia del mittente che del destinatario. Ciò permette di creare conversazioni più fluente e coerenti.

Menzioniamo anche **Claude**, giunto anche esso alla versione 2, ed esistente in due versioni: Claude e Claude Instant. Creato da Anthropic, questo modello è stato addestrato in collaborazione con aggregatori e generatori di contenuti di grande mole, come *Notion*, *DuckDuckGo*, e *Quora*. Claude e Claude 1.3 sono disponibili sia agli utenti che agli sviluppatori, mentre per ora Claude 2 è disponibile solo agli sviluppatori e agli utenti Pro.

Infine, non possiamo dimenticare **Grok**, il nuovo prodotto sviluppato da "X" di Elon Musk. Grok punta a creare un assistente virtuale che sia in grado di comprendere e rispondere alle domande degli utenti su qualsiasi argomento. L'obiettivo di Grok è quello di fornire risposte più informative ed esaustive, superando le limitazioni di altri chatbot presenti sul mercato. Musk ha presentato Grok come il primo 'chatbot saggio'

dotato perfino di senso dell'umorismo, una caratteristica, ad esempio, nei modelli di OpenAI e Google bisogna 'simulare' tramite dei prompt appositi.

Mentre ChatGPT si trova al centro dell'attenzione nel campo dei chatbot e dell'IA generativa, essendo stato il primo rilasciato al grande pubblico ed essendo stato integrato velocemente con diversi plugin e servizi, è importante riconoscere che ci sono anche altre alternative valide. Vi invitiamo a provarle.

Tutti gli articoli qui presentati sono stati scritti dallo staff di **Vivacity Design Web Agency**

per il proprio blog, tra il 17 febbraio ed il 10 novembre 2023

<http://www.vivacitydesign.net/blog/index.php>

The logo for Vivacity Design features the words "Vivacity" and "Design" in a stylized, metallic, 3D font. The letters have a gradient and a shadow effect, giving them a three-dimensional appearance. Below the text, there is a faint, semi-transparent reflection of the logo, creating a sense of depth and a polished look.