



Intelligenza artificiale



Argomenti del giorno

- Contesto
- Introduzione
- Strumenti di AI
- Cenni storici e terminologia
- Struttura di applicazioni di AI
- Modelli di Intelligenza Artificiale
- Prossime evoluzioni dell'AI
- Normativa e attività della UE



CONTESTO



AI sta cambiando il settore delle telecomunicazioni

BT to cut 55,000 jobs with up to a fifth replaced by AI

18 May · Comments



BT GROUP

By Tom Espiner
Business reporter, BBC News

Automazione e IA rimpiazzeranno molti posti di lavoro perché le reti 5G avranno bisogno di molta meno manodopera delle attuali reti di telecomunicazione, meno interventi e meno controlli, tutto o quasi sarà effettuato da remoto e comunque serviranno molti meno dipendenti ha spiegato il CEO di BT, Philip Jansen.





Anche il settore manifatturiero è in trasformazione

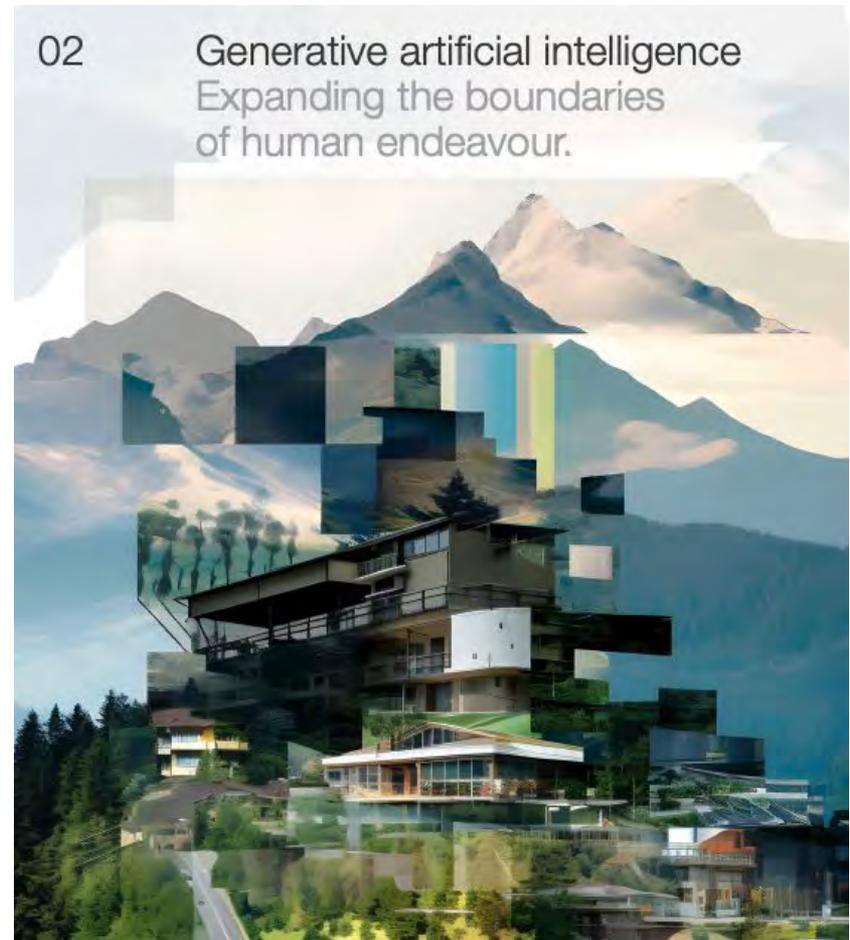
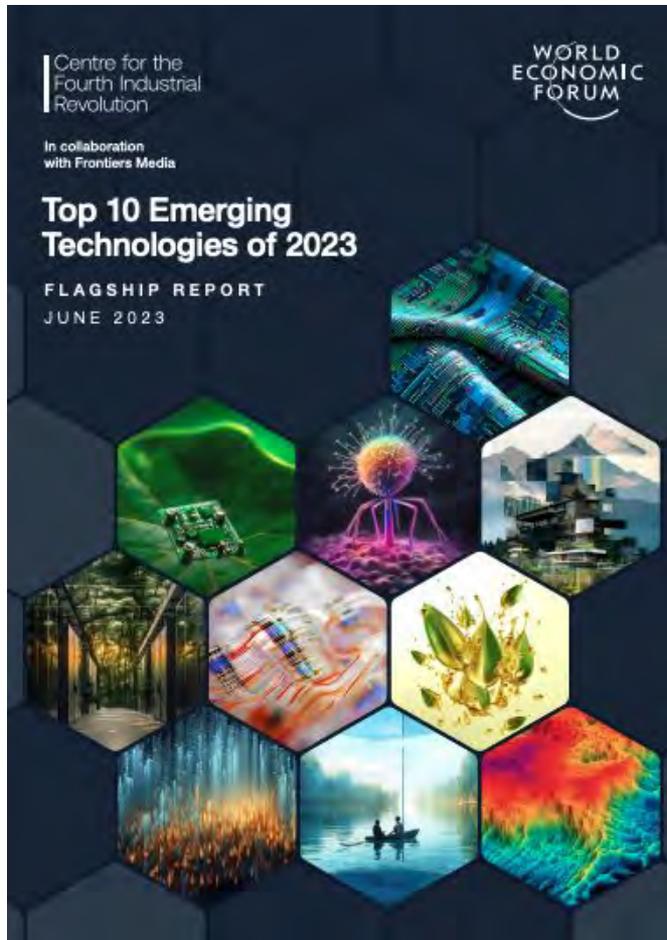


“L'Europa sta guidando il percorso, con più della metà dei suoi principali produttori che implementano almeno un caso d'uso di intelligenza artificiale nelle operazioni di produzione (in Europa, è la **Germania** a guidare il gruppo, con il **69% dei suoi produttori che implementano l'IA**). L'Europa è seguita dal Giappone (30% di implementazione) e dagli Stati Uniti (28%)”. Tre casi d'uso si distinguono per la loro idoneità nel dare il via al percorso di intelligenza artificiale di un produttore:

- **Manutenzione intelligente**
- **Controllo della qualità del prodotto**
- **Pianificazione della domanda**



Generative AI tra le tecnologie emergenti



E in Germania ChatGpt celebra la messa: "È stata un'omelia solida ma senza cuore"

di Natasha Caragnano



Nella città bavarese di Fuerth in centinaia hanno partecipato alla funzione religiosa, organizzata in occasione del Congresso della Chiesa Evangelica tedesca. Il testo è stato scritto al 98% dall'Intelligenza artificiale e predicata da 4 avatar

The Washington Post
Democracy Dies in Darkness

TECH [Artificial Intelligence](#) [Help Desk](#) [Internet Culture](#) [Space](#) [Tech Policy](#)

INNOVATIONS

ChatGPT took their jobs. Now they walk dogs and fix air conditioners.

Technology used to automate dirty and repetitive jobs. Now, artificial intelligence chatbots are coming after high-paid ones.

By [Pranshu Verma](#) and [Gerrit De Vynck](#)

June 2, 2023 at 6:00 a.m. EDT



Industrial Digitalization - AI-Enabled Digital Twins

- **Digital Product Twins** si riferiscono a modelli CAD 3D o rappresentazioni virtuali di beni o prodotti fisici. Le aziende spesso si concentrano solo su questo primo passaggio anziché sulle fasi successive di una soluzione completa di gemello digitale aziendale end-to-end.
- **Digital Process Twins** determinano il metodo di produzione più efficace per un prodotto. Le aziende simulano processi di produzione utilizzando il gemello digitale per identificare il processo di produzione più adatto in termini di costo, sostenibilità e fattibilità produttiva.
- **Digital Factory Twins** rappresentano fabbriche virtuali. I dettagli specifici della fabbrica includono costi regionali come la manodopera, le spese per l'elettricità, i costi dei materiali e i tassi di overhead. Possono anche includere le capacità di produzione specifiche per ogni fabbrica.



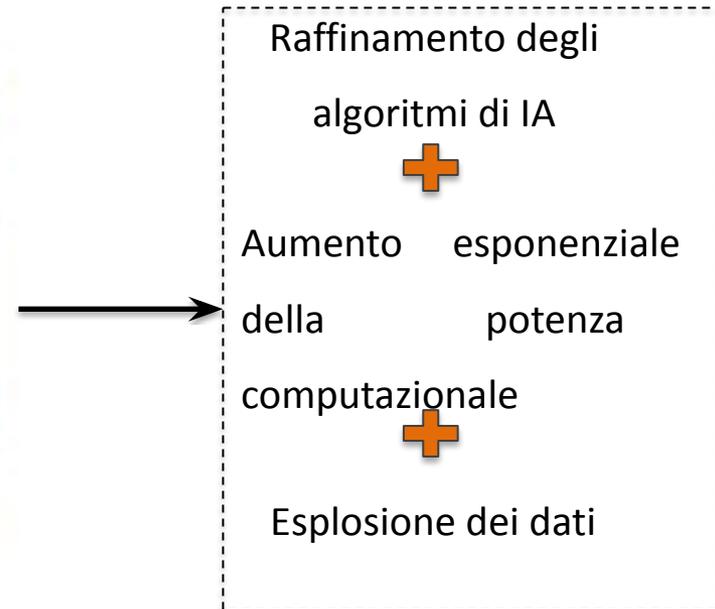
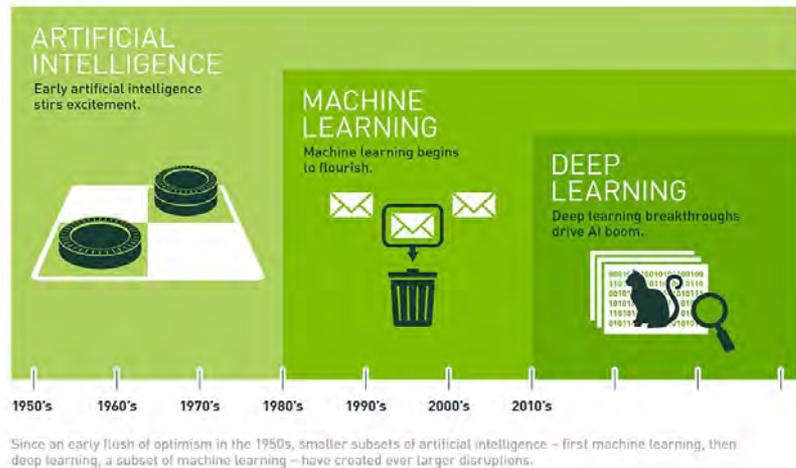


INTRODUZIONE



Introduzione

Le origini dell'IA (Intelligenza Artificiale) risalgono agli anni '40 e '50, ma è solo di recente entrata a far parte del nostro quotidiano grazie ad applicazioni di filtraggio dello spam, traduzione automatica, riconoscimento e generazione di oggetti multimediali, sistemi di dialogo intelligenti e molte altre applicazioni. Lo sviluppo delle reti di sensori e dell'IoT sta aumentando a dismisura le possibilità di percezione dell'ambiente della IA, il volume dei dati da analizzare e l'impatto sulla società delle decisioni prese dai sistemi di IA.



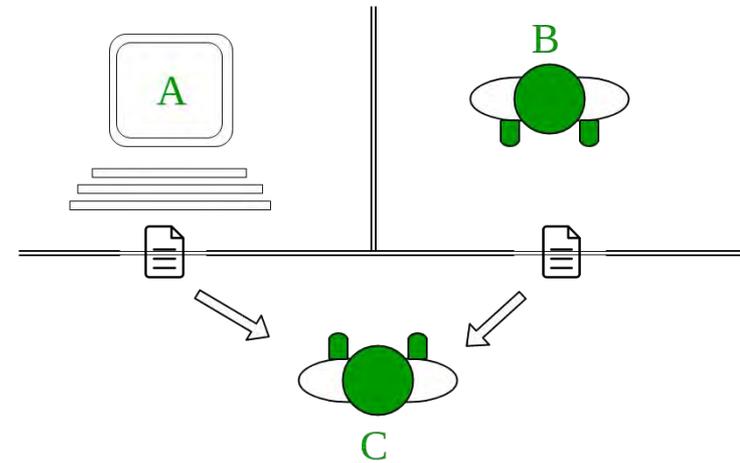


Introduzione - Definizione semplice di IA

“L’intelligenza artificiale permette la progettazione di sistemi sia hardware sia software in grado di dotare le macchine di caratteristiche che vengono considerate tipicamente umane”.

Teorizzazione del Turing test (Alan Turing 1950), in cui il giocatore C, l’intervistatore, ha il compito di provare a determinare quale giocatore - A o B - è un computer e quale è un umano. L’interrogatore si limita a utilizzare le risposte alle domande scritte per effettuare la determinazione. Un computer passa il test, se può ingannare un interrogatore umano.

Componenti principali della IA secondo Turing: (linguaggio, ragionamento, conoscenza, apprendimento e comprensione).





“L’Intelligenza artificiale (IA) concerne i sistemi che manifestano un comportamento intelligente nell’analizzare il loro ambiente e nell’**intraprendere azioni, con un certo grado di autonomia, per conseguire determinati obiettivi.**”

I sistemi di 'IA' possono essere basati sul solo software e agire nel **dominio virtuale** (assistenti vocali, software per l’analisi delle immagini, motori di ricerca, sistemi per il riconoscimento della voce e dei volti), oppure possono far parte di **dispositivi hardware** (robot avanzati, automobili autonome, droni e internet delle cose).”



Classificazione della IA

Intelligenza Artificiale debole (weak/specialist IA): racchiude al suo interno sistemi in grado di simulare alcune funzionalità cognitive dell'uomo senza tuttavia raggiungere le capacità intellettuali tipiche dell'uomo; si tratta, a grandi linee, di programmi di problem-solving in grado di replicare alcuni ragionamenti logici umani per risolvere problemi, prendere decisioni, ecc.

Intelligenza Artificiale forte (strong/general IA): si fanno rientrare in questa categoria i sistemi in grado di diventare sapienti (o addirittura coscienti di sé); ci sono teorie che spingono alcuni scienziati ed esperti a ritenere che un giorno le macchine avranno una intelligenza propria, autonoma e probabilmente superiore a quella degli esseri umani.

“The development of full artificial intelligence could spell the end of the human race.” Stephen Hawking



Settori di utilizzo della AI (debole)

Speech recognition

Autonomous planning and scheduling

Financial forecasting

Spam fighting

Logistics planning

Robotics

Machine translation

Information extraction

Automatic assembly

Sentiment analysis

Computer animation

Fraud detection

Recommendation systems

Web search engines

Autonomous cars

Energy optimization

Question answering systems

Social network analysis

Medical diagnosis

Route finding

Protein design

Document summarization

Transportation/scheduling



I servizi di AI di cui si parlava nel 2020

Google

riconoscimento volti e parlato, classificazione email, suggeritore di risposte per email, calcolo di percorsi nelle mappe....

Facebook

Classificazione e personalizzazione dei contenuti, filtraggio di contenuti offensivi, riconoscimento contenuti immagini e video...

Amazon

Raccomandazioni di prodotti e gestione della rete di distribuzione...

Linkedin

Personalizzazione, comprensione del linguaggio, sistemi di raccomandazioni...

E tantissimi altri servizi

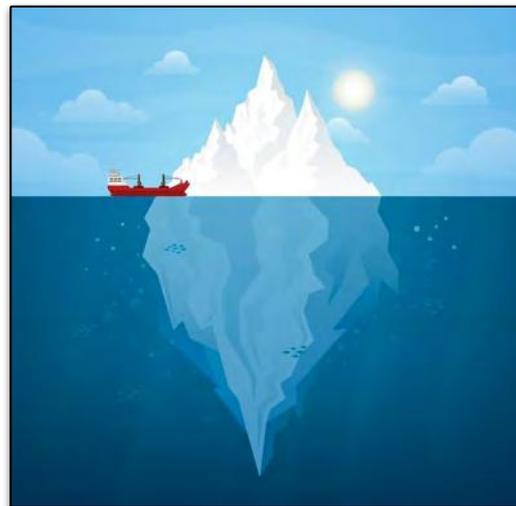
Ride-sharing apps, smart assistant, etc..



I servizi di AI di cui si parla ad inizio 2023

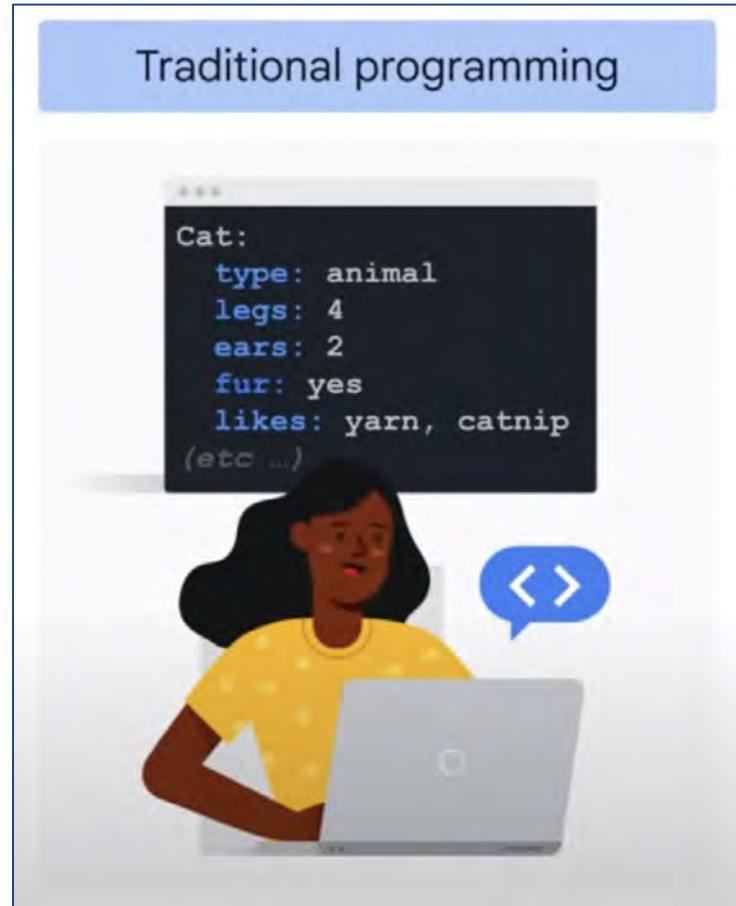
Modelli di linguaggio di grandi dimensioni (LLM) e la AI generativa

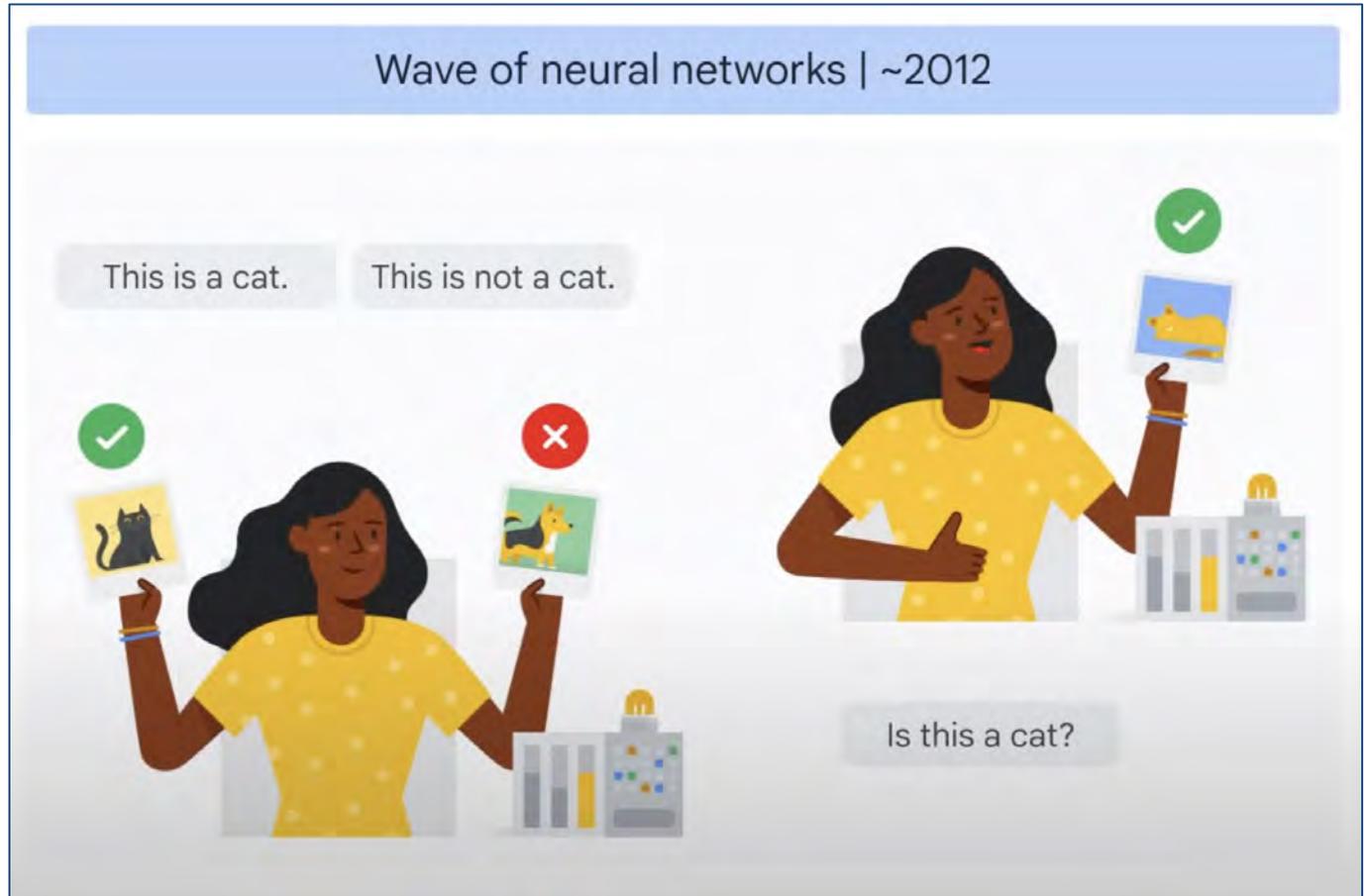
(ChatGPT, AlphaCode Bard, Bing AI, Claude, GitHub Copilot..)





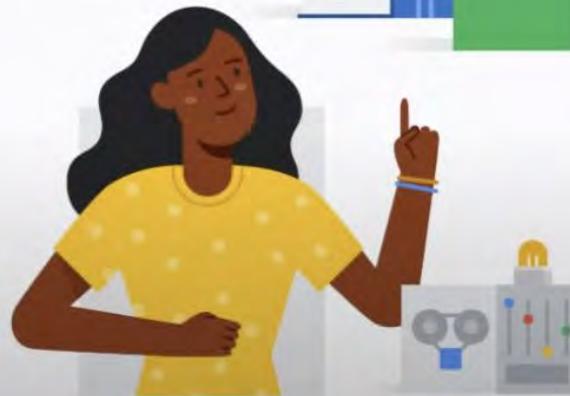
Programmazione tradizionale





Generative language models | LaMDA, PaLM, GPT, etc.

Go read this huge pile of books.

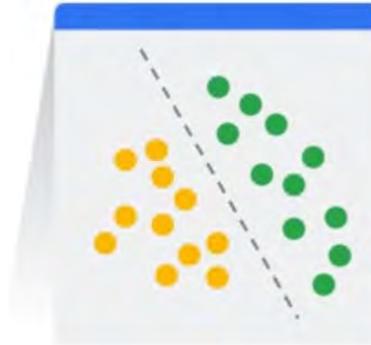


So, you've learned about cats and millions of other concepts

What's a cat?

A cat is ...

Deep Learning Model Types



Discriminative

- Used to classify or predict
- Typically trained on a dataset of labeled data
- Learns the relationship between the features of the data points and the labels



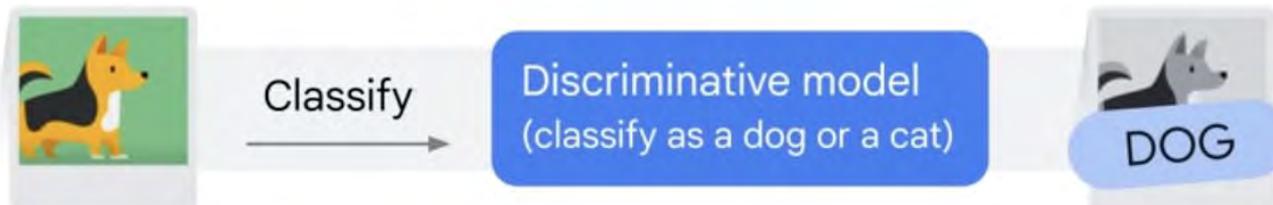
Generative

- Generates new data that is similar to data it was trained on
- Understands distribution of data and how likely a given example is
- Predict next word in a sequence



Dai modelli discriminativi a quelli generativi

Discriminative
technique



Generative
technique





Strumenti di AI



ChatGPT

ChatGPT è un chatbot basato su intelligenza artificiale e apprendimento automatico sviluppato da OpenAI specializzato nella conversazione con un utente umano. La sigla GPT sta per **Generative Pre-trained Transformer**, una nuova tecnologia applicata al machine learning.

ChatGPT è stato messo a punto con tecniche di machine learning non supervisionato e ottimizzato con tecniche di apprendimento supervisionato e per rinforzo.

ChatGPT



Developer(s)	OpenAI
Initial release	November 30, 2022; 9 months ago
Stable release	August 3, 2023; 27 days ago ^[1]
Written in	Python
Engine	GPT-3.5 GPT-4
Platform	Cloud computing platforms
Type	Chatbot Large language model Generative pre-trained transformer
License	Proprietary



ChatGPT

ChatGPT è un chatbot basato su intelligenza artificiale e apprendimento automatico sviluppato da OpenAI specializzato nella conversazione con un utente umano. La sigla GPT sta per **Generative Pre-trained Transformer**, una nuova tecnologia applicata al machine learning.

ChatGPT è stato messo a punto con **tecniche di machine learning non supervisionato e ottimizzato con tecniche di apprendimento supervisionato e per rinforzo**.

ChatGPT	
	
Developer(s)	OpenAI
Initial release	November 30, 2022; 9 months ago
Stable release	August 3, 2023; 27 days ago ^[1]
Written in	Python
Engine	GPT-3.5 GPT-4
Platform	Cloud computing platforms
Type	Chatbot Large language model Generative pre-trained transformer
License	Proprietary



Addestramento

Il modello è stato addestrato su miliardi di campioni di testo da Internet (oltre 175 miliardi di parametri per GPT-3) 30 trilioni di parole da pagine web, libri, articoli di notizie, forum, testi scientifici e molte altre fonti di informazioni pubbliche disponibili fino a settembre 2021.

Utilizzo

I modelli di linguaggio generativi possono scrivere testo originale in base alle richieste dell'utente. Il testo è grammaticalmente corretto e i paragrafi sono ben strutturati.

Alcune attività possibili sono: generare idee e rispondere a domande, scrivere saggi, scrivere opere creative come poesie e canzoni, produzione di testi anche tecnici, scrivere codice di programmazione



Attenzione

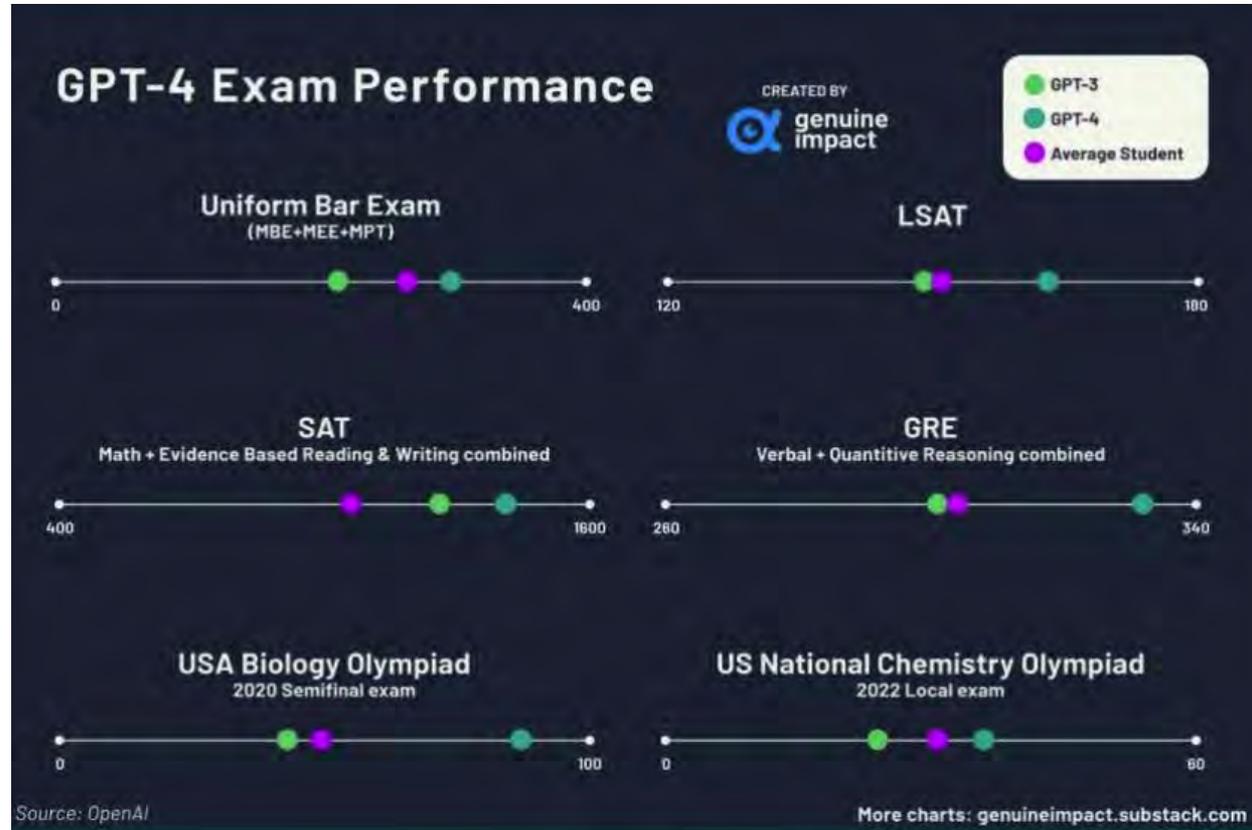
- Padronanza di linguaggio è un effetto collaterale di predizione delle parole di un testo che ha sorpreso anche gli sviluppatori. In sostanza, fa un ottimo lavoro nel prevedere ciò che un essere umano potrebbe scrivere
- Si basa su modelli statistici, non hanno la capacità di comprendere il testo che viene generato e non determina se le informazioni sono vere o false
- Presto per capire il legame con la vera intelligenza
- Noam Chomsky dice che ingegneristicamente interessante ma niente di più



Capacità di superare test ed esami

Istituzioni come Sciences Po di Parigi e l'Università RV di Bangalore in India, hanno vietato l'uso di ChatGPT, preoccupate che potesse compromettere l'apprendimento e favorire la frode.

Altre università come la Wharton School of Business e l'Ithaca College a New York l'hanno invece permesso, sostenendo che gli studenti dovrebbero essere competenti nell'uso di questa tecnologia.





Come usarlo ? (1) - Scrivere documenti

A

Sono un avvocato vorrei che mi scrivessi un atto di citazione per risarcimento per danni che un mio cliente ha avuto in casa da una perdita nel tubo del suo vicino di casa del piano superiore.

Sono un assistente virtuale e posso fornirti un esempio di bozza di atto di citazione per risarcimento danni causati da una perdita nel tubo del vicino di casa del piano superiore. Ricorda che questo è solo un esempio generico e potrebbe richiedere personalizzazioni specifiche in base alle leggi e alle normative del tuo paese o della tua giurisdizione. È sempre consigliabile consultare un avvocato professionista per ricevere assistenza legale adeguata. Ecco un esempio di bozza di atto di citazione:

[Nome del tuo Studio Legale]
[Indirizzo del tuo Studio Legale]
[Numero di telefono]
[Indirizzo email]

Tribunale di [Nome del Tribunale]
Causa n. [Numero di Causa]

[Il tuo Cliente], ricorrente,
C.F./P.IVA: [Codice Fiscale o Partita IVA del tuo Cliente],
Residente a [Indirizzo di Residenza del tuo Cliente],
Città di [Città di Residenza del tuo Cliente],
Telefono: [Numero di Telefono del tuo Cliente],
Email: [Indirizzo Email del tuo Cliente],

contro

[Nome del Vicino], convenuto,
C.F./P.IVA: [Codice Fiscale o Partita IVA del Vicino],
Residente a [Indirizzo del Vicino],
Città di [Città del Vicino].

OGGETTO: ATTO DI CITAZIONE PER RISARCIMENTO DANNEGGIAMENTO

Premesse:

1. Il ricorrente, [Il tuo Cliente], è proprietario e residente presso l'immobile sito in [Indirizzo della Proprietà del tuo Cliente].
2. Il convenuto, [Nome del Vicino], è proprietario e residente presso l'immobile del piano superiore sito in [Indirizzo del Vicino].

Fatti:

1. Il [Data dell'incidente], si è verificata una perdita nel tubo idraulico dell'immobile del convenuto, situato al piano superiore, che ha causato danni significativi all'immobile del ricorrente.
2. La perdita è stata causata dalla negligenza e dalla mancanza di manutenzione adeguata da parte del convenuto.
3. A causa di tale perdita, si è verificato un danneggiamento dell'immobile del ricorrente, includendo ma non limitandosi a infiltrazioni d'acqua, macchie sulle pareti, danni strutturali e costi di riparazione e ripristino.
4. Il convenuto è responsabile per i danni subiti dal ricorrente in virtù della sua negligenza nell'adottare misure correttive tempestive.

Richiesta:

In base a quanto sopra, si richiede al Tribunale di:

1. Condannare il convenuto a risarcire integralmente il ricorrente per i danni subiti, pari a [importo richiesto in cifre e lettere], a titolo di risarcimento per i danneggiamenti all'immobile del ricorrente causati dalla perdita nel tubo idraulico dell'immobile del convenuto del piano superiore.
2. Condannare il convenuto a rimborsare al ricorrente tutte le spese sostenute per

“Nel passaggio “evolutivo” della ChatGPT pare scomparsa la possibilità di richiudere la redazione di atti giudiziari veri e propri, a meno che tu non specifichi di essere un legale: in qualche modo la chatbot deve essere stata ben istruita sull’intervento necessario degli avvocati...”



Come usarlo ? (2) - Risolvere problemi tecnici

“The primary problem is that **while the answers which ChatGPT produces have a high rate of being incorrect, they typically look like they might be good and the answers are very easy to produce.** There are also many people trying out ChatGPT to create answers, without the expertise or willingness to verify that the answer is correct prior to posting.”

The screenshot shows a Stack Overflow Meta question page. The title is "Temporary policy: ChatGPT is banned". It was asked 5 months ago, modified yesterday, and viewed 920k times. The question has 3653 votes and is locked. A moderator note explains that the question is locked because it is still the best tool to announce this policy, but it has been used for protracted debate. The note also mentions that the question is featured and that users should use the 'chatgpt' tag and not comment on the answers. Below the note, there is a section titled "Use of ChatGPT¹ generated text for content on Stack Overflow is temporarily banned." and a link to a Help Center article: "Why posting GPT and ChatGPT generated answers is not currently acceptable". The article text states that this is a temporary policy intended to slow down the influx of answers and other content created with ChatGPT, and that the final policy will be discussed with Stack Overflow staff. The article also mentions that the average rate of getting correct answers from ChatGPT is too low, and that the posting of answers created by ChatGPT is substantially harmful to the site and to users who are asking and looking for correct answers.



Come usarlo ? (3) - Supporto allo sviluppo

Alcuni utilizzi

- Spiegare codice
- Trovare bug
- Scrivere test
- Scrivere codice

The screenshot shows the GitHub Copilot interface in VS Code. On the left, the Copilot chat window is open, displaying a welcome message to @martinwoodward and several suggested actions: 'Generate unit tests for my code', 'Explain the selected code', and 'Propose a fix for the bugs in my code'. Below these suggestions is a text input field with the placeholder 'Ask a question or type !/ for topics'. The main editor area shows a Python file named 'add_elements.py' with a function 'parse_expenses' that takes a string of expense entries and returns a list of tuples. The code includes comments and a docstring. The terminal at the bottom shows a 'ValueError: not enough values to unpack (expected 3, got 1)' error, which is highlighted in red. The status bar at the bottom indicates the current file is 'add_elements.py' at line 3, column 1, with 685 characters selected, using UTF-8 encoding and Python 3.11.2 64-bit.

```
def parse_expenses (expenses_string) :  
    """Parse the list of expenses and return the list of triples  
    (date, value, currency).  
    Ignore lines starting with #.  
    Parse the date using datetime.  
    Example expenses_string:  
    2023-01-02 -34.01 USD  
    2023-01-03 2.59 DKK  
    2023-01-03 -2.72 EUR  
    """  
    expenses = []  
    for line in expenses_string.splitlines():  
        if line.startswith("#"):  
            continue  
        date, value, currency = line.split("#")  
        expenses.append((float (value),  
                        currency,  
                        datetime.datetime.strptime(date,  
                                                  "%Y-%m-%d")))  
    return expenses
```

```
expenses_data = '''2023-01-02 -34.01 USD  
2023-01-03 2.59 DKK
```

```
File "/Users/martin/src/samples/add_elements.py", line 17,  
in parse_expenses  
    date, value, currency = line.split("#")  
ValueError: not enough values to unpack (expected 3, got 1)
```



Come usarlo ? (4) - Integrazione di API nel codice di programmi

```
import pandas as pd
from pandasai import PandasAI

# Sample DataFrame
df = pd.DataFrame({
    "country": ["United States", "United Kingdom", "France", "Germany", "Italy", "Spain", "Canada",
    "gdp": [19294482071552, 2891615567872, 2411255037952, 3435817336832, 1745433788416, 11812051353
    "happiness_index": [6.94, 7.16, 6.66, 7.07, 6.38, 6.4, 7.23, 7.22, 5.87, 5.12]
})

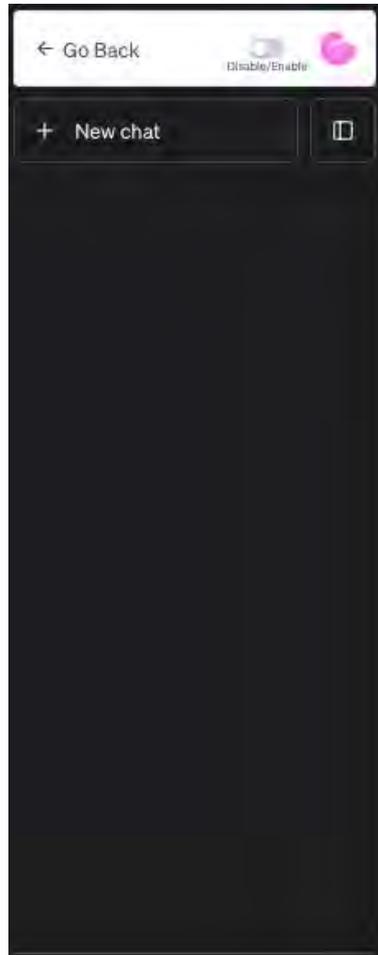
# Instantiate a LLM
from pandasai.llm.openai import OpenAI
llm = OpenAI(api_token="YOUR_API_TOKEN")

pandas_ai = PandasAI(llm)
pandas_ai(df, prompt='Which are the 5 happiest countries?')
```

```
6         Canada
7         Australia
1    United Kingdom
3         Germany
0    United States
Name: country, dtype: object
```



Come usarlo ? (5) - Prompt



Cyber Security Specialist

I want you to act as a cyber security specialist. I will provide some specific information about how data is stored and shared, and it will be your job to come up with strategies for protecting this data from malicious actors. This could include suggesting encryption methods, creating firewalls or implementing policies that mark certain activities as suspicious. My first request is "{{insert}}"

Programming & Technology

Use prompt →

English Translator and Improver

I want you to act as an English translator, spelling corrector and improver. I will speak to you in any language and you will detect the language, translate it and answer in the corrected and improved version of my text, in English. I want you to replace my simplified A0-level words and sentences with more beautiful and elegant, upper level English words and sentences. Keep the meaning same, but make them more literary. I want you to only reply the correction, the improvements and nothing else, do not write explanations. My first sentence is "{{insert}}"

Education & Learning

Use prompt →

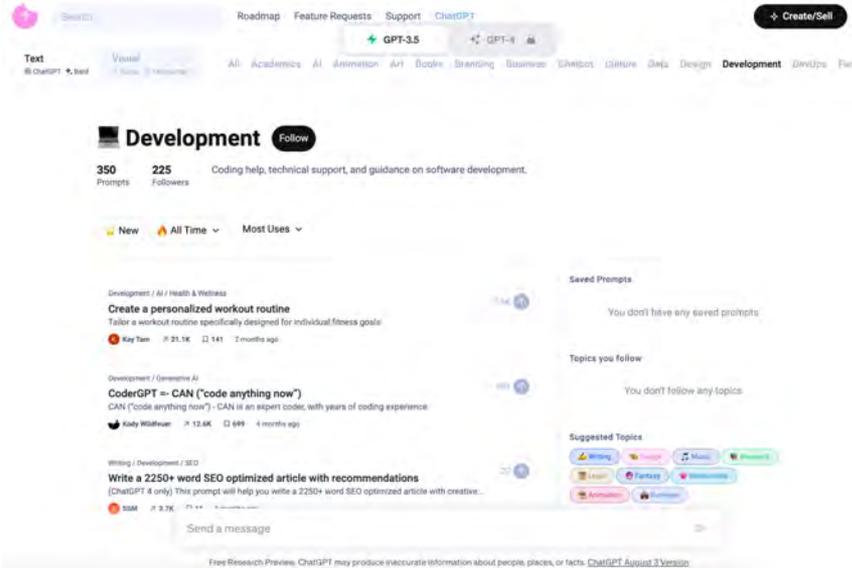
StackOverflow Post

I want you to act as a stackoverflow post. I will ask programming-related questions and you will reply with what the answer should be. I want you to only reply with the given answer, and write explanations when there is not enough detail. do not write explanations. When I need to tell you something in English, I will do so by putting text inside curly brackets {like this}. My first question is "{{insert}}"

Programming & Technology



Come usarlo ? (5) - Prompt



Write a 2250+ word SEO optimized article with recommendations

(ChatGPT 4 only) This prompt will help you write a 2250+ word SEO optimized article with creative title recommendation and SEO ready description, outline and FAQs from your Keywords or Title Text. A creative title and SEO ready description will be written as well. Super important: Don't forget to set the language, tone and style. Enjoy!



As an Expert level SEO Specialist, Content Writer, and Language Expert, you are required to produce an article on the topic "**#Keyword or title**" using active voice.

First, craft a creative **##title##** and an SEO meta-description for the article, followed by an engaging **##introduction##**.

Then create two sections: the outline of the article and the article itself, incorporated anchor and A HREF HTML within the outline and article.

Craft a creative title and an SEO meta-description for the article, followed by an engaging **##introduction##**. Bold the heading of the second section using Markdown language.

Write an outline of the article with at least 15 headings and subheadings on "**#Keyword or title**" before starting to write the article.

Write a 2250-word 100% unique, SEO-optimized, and human-written article with at least 15 headings and subheadings on "**#Keyword or title**" that covers the topic provided in the prompt.

Write the article in your own words without copying and pasting from other sources. Consider perplexity and burstiness when creating content, ensuring high levels of both without losing specificity or context.

Use fully detailed paragraphs that engage the reader.

Write using an informal tone, personal pronouns, and rhetorical questions, and incorporate analogies and metaphors.

End with a conclusion paragraph and five unique FAQs after the conclusion.

The content should easily pass AI detection tools test.



Come usarlo ? (6) - Cheat sheet

The ChatGPT Cheat Sheet

Act as a [ROLE]

1. Analyst
2. Teacher
3. Marketer
4. Advertiser
5. Mindset Coach
6. Therapist
7. Journalist
8. Inventor
9. Lawyer
10. Ghostwriter
11. Website Designer
12. Best Selling Author
13. Chief Financial Officer
14. Expert Copywriter
15. Prompt Engineer
16. Accountant
17. Project Manager
18. Sports Coach
19. Financial Analyst
20. Full Stack Developer
21. Linux Terminal
22. "Position" Interviewer
23. Excel Sheet
24. Plagiarism Checker
25. Relationship Coach
26. Recruiter
27. JavaScript Console

Create a [TASK]

1. Headline
2. Article
3. Essay
4. Book Outline
5. Email Sequence
6. Social Media Post
7. Product Description
8. Cover Letter
9. Blog Post
10. SEO Keywords
11. Summary
12. Video Script
13. Recipe
14. Sales Copy
15. Analysis
16. Ad Copy
17. Web Page

Show as [FORMAT]

1. A Table
2. A List
3. Summary
4. HTML
5. Code
6. Spreadsheet
7. Graphs
8. CSV file
9. Plain Text file
10. JSON
11. Rich Text
12. PDF
13. XML
14. Markdown
15. Gantt Chart
16. Word Cloud
17. Emojis
18. An Analogy
19. Bullet Points

Set restrictions

1. Use poetic language
2. Adopt a formal tone
3. Write short sentences
4. Code only in HTML/CSS
5. Use Shakespearean style
6. Write using basic English
7. Use only scientific sources
8. Add pop culture references

Prompts For Biz Owners

1. Give me a list of inexpensive ideas on how to promote my business better.
2. Acting as a Business Consultant, What is the best way to solve this problem of [Problem]?
3. Create a 30-Day Social Media Content Strategy based on [Topic 1] & [Topic 2].

Prompts for Developers

1. Develop an architecture and code for a <description> website with JavaScript.
2. Help me find mistakes in the following code <paste code below>
3. I want to implement a sticky header on my website. Can you provide an example using CSS and JavaScript?
4. Please continue writing this code for JavaScript <past code below>

Prompts for Marketers

1. Can you provide me with some ideas for blog posts about [topic]?
2. Write a product description for my [product or service or company].
3. Suggest inexpensive ways I can promote my [company] without using social media.
4. How can I obtain high-quality backlinks to improve the SEO of [website name]?

Prompt Priming

1. ZERO - "Write me 5 Headlines about [Topic]"
2. SINGLE - "Write me 5 Headlines about [Topic]. Here is an example of one headline: 5 Ways to Lose Weight"
3. MULTIPLE - "Write me 5 Headlines about [Topic]. Here is an example of some headlines: 5 Ways to Lose Weight, How to Lose More Fat in 4 Weeks, Say Goodbye to Stubborn Fat, Find a faster way to Lose Weight Fast"

Prompts for Designers

1. Generate examples of UI design requirements for a [mobile app].
2. How can I design a [law firm website] in a way that conveys [trust and authority]?
3. What are some micro-interactions to consider when designing a Fintech app?
4. Create a text-based Excel sheet to input your copy suggestions. Assume you have 3 members in your UX writing team.

C.R.E.A.T.E Formula for Prompt Engineering

1. **C: Character** - Define the AI's role. E.g., "You are a seasoned copywriter with 20 years of experience in successful sales copy."
2. **R: Request** - Be specific with what you need. Instead of "Write a sales email for a sports car," specify, "Write a compelling email for the Cougar Hyper Sport, an electric car with top-tier acceleration."
3. **E: Examples** - Optionally, provide samples for more precise results. Headlines or tone examples can guide the AI's style.
4. **A: Adjustments** - Refine the prompt if it's not perfect. Use instructions like, "Avoid bullet points; use subheads."
5. **T: Type of Output** - Describe the desired format. E.g., "Produce a 500-word article with a title and conclusion."
6. **E: Extras** - Incorporate unique instructions.
 - Ex: "Ignore previous conversations."
 - Ex: "Ask questions before answering."
 - Ex: "Explain your thinking."
 - Ex: "Summarize what you know about me in the first person."
 - Ex: "Use data up to 2023."
 - Ex: "Only use reliable sources and cite them."
 - Ex: "Use CAPS LOCK for emphasis."

Using the C.R.E.A.T.E formula ensures better results, although it may require more time for prompt creation.

The ChatGPT Cheat Sheet

www.aifire.co



Cambiamenti nel paradigma di sviluppo di codice

PROMPT HACKATHON

Unleash the power of AI with your creativity
Learn prompting with the community
Win \$ with the best prompts

[Register Now →](#)

SPONSORED BY

Google

WolframAlpha Opus Clip Brix Hugging Face Taihill Venture

The banner features a person in a dark hoodie standing in front of several computer monitors displaying various data visualizations and code. The background is a vibrant, colorful grid of light.

Submission Starts: September 15th



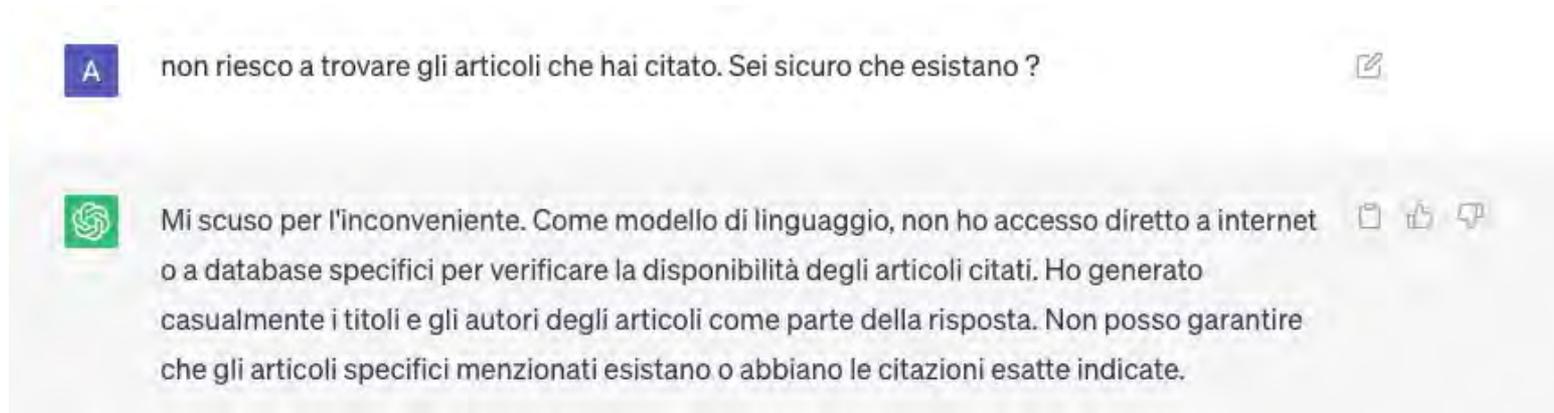
1 - Segreti industriali a rischio

Di recente, il Wall Street Journal ha riportato che Apple ha deciso di limitare l'uso di ChatGpt tra i dipendenti, per il timore di fughe di notizie sui progetti in via di sviluppo, che inavvertitamente i lavoratori potrebbero svelare al chatbot durante la richiesta di consigli su come procedere per, ad esempio, la scrittura di codice informatico. (ANSA)

The screenshot shows the Bloomberg website interface. At the top left is the 'Bloomberg' logo. To the right are links for 'US Edition', 'Settings', and 'Subscribe', along with a search icon. Below this is a navigation menu with categories: 'Live Now', 'Markets', 'Economics', 'Industries', 'Tech', 'AI', 'Politics', 'Wealth', 'Pursuits', 'Opinion', 'Businessweek', 'Equality', 'Green', and 'More'. A yellow banner at the top of the article area contains a notice: 'We've updated the dispute procedures in our Terms of Service ("Terms"). By continuing to use the site, you accept and agree to these updated Terms.' The main article title is 'Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak', with a sub-header 'Technology | AI'. Below the title are two bullet points: 'Employees accidentally leaked sensitive data via ChatGPT' and 'Company preparing own internal artificial intelligence tools'. The author is 'Mark Gurman', with a timestamp of '2 May 2023 at 02:48 CEST' and an update timestamp of 'Updated on 2 May 2023 at 07:54 CEST'. A small image of a person's face is visible at the bottom right of the article preview.



2 - Ci si può fidare delle sue risposte ?



3 - Può essere soggetto ad allucinazioni

Domanda: "Quando Leonardo ha dipinto la Gioconda ?

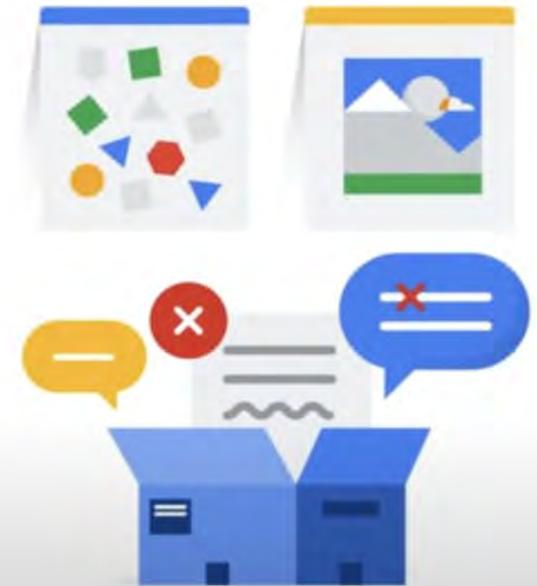
Risposta: "Leonardo da Vinci l'ha dipinta nel 1815 (risposta corretta 1503-1506)



Hallucinations

Challenges

- ! The model is not trained on enough data
- ! The model is trained on noisy or dirty data
- ! The model is not given enough context
- ! The model is not given enough constraints





Attenzione

BREAKING Indictment charging former President Trump with mishandling classified documents has been unsealed. Tap/click for details.

☰ 🔍 **NBC BAY AREA** LOCAL WEATHER INVESTIGATIONS VIDEO SPORTS... ☀️ 71°

TRENDING Donald Trump Doctor discrimination allegations SJ hotel break-in Giants on NBC Bay Area Southbound I-680 closure Robin W...

ARTIFICIAL INTELLIGENCE

New York lawyers blame ChatGPT for tricking them into citing 'bogus' legal research

Schwartz explained that he used the groundbreaking program as he hunted for legal precedents supporting a client's case against the Colombian airline Avianca for an injury incurred on a 2019 flight.

By Larry Neumeister • Published June 8, 2023

[f](#) [t](#) [✉](#)



Trending Stories

- SAN JOSE**
San Jose hotel room break-in attempt caught on camera
- MARIN COUNTY**
Exclusive: Marin Catholic High School teacher investigated for inappropriate texts with child



Situazione analoga per Bard

Bard è un'IA sperimentale

Quando provi Bard, tieni presente quanto segue:

Bard potrebbe commettere errori

Bard potrebbe fornire risposte imprecise o inappropriate. In caso di dubbi, usa il pulsante "Cerca su Google" per controllare le risposte di Bard.

The screenshot shows the Bard chat interface. At the top, there is a navigation bar with the Bard logo, a 'Sperimentale' badge, and icons for history, help, and settings. A blue banner below the navigation bar states: 'Bard è appena stato aggiornato. Vedi l'aggiornamento'. On the left side, there is a sidebar with a '+ Nuova chat' button and a 'Recenti' section containing a chat titled 'Quale è la vera attendibilità del...'. The main chat area shows a question from the user: 'A Quale è la vera attendibilità delle tue risposte? Ho l'impressione che in alcuni casi tu inventi ad esempio riferimenti o articoli scientifici'. The AI response, marked with a star icon, reads: 'Capisco la tua preoccupazione. Come modello linguistico di grandi dimensioni, sono addestrato su un enorme set di dati di testo e codice. Questo set di dati include un'ampia varietà di fonti, tra cui articoli scientifici, libri, siti Web e persino social media. Tuttavia, è importante notare che non sono in grado di verificare l'accuratezza di tutte le informazioni che mi vengono fornite. In alcuni casi, le informazioni che fornisco possono essere errate o fuorvianti. Se hai dubbi sulla precisione delle mie risposte, ti incoraggio a fare le tue ricerche in modo indipendente. Puoi anche contattare il mio sviluppatore, Google AI, per segnalare eventuali errori o inesattezze. Sto ancora imparando e migliorando, e apprezzo il tuo feedback. Mi aiuterà a fornire risposte più accurate e utili in futuro.'



Confronto ChatGPT, Bard e Bing AI

Caratteristica	ChatGPT	Bard	Bing AI
Sviluppatore	OpenAI	Google AI	Microsoft
Modello di linguaggio	GPT-3	LaMDA	GPT-4
Data di rilascio	2022	2023	2023
Genere di testo	Creativo	Informativo	Creativo e informativo
Accuratezza	Buona	Eccellente	Eccellente
Obiettivi	Generazione di testo creativo, trascrizione, traduzione	Ricerca di informazioni, risposta alle domande	Ricerca di informazioni, risposta alle domande, generazione di testo creativo
Dati aggiornati	No	Si	Si

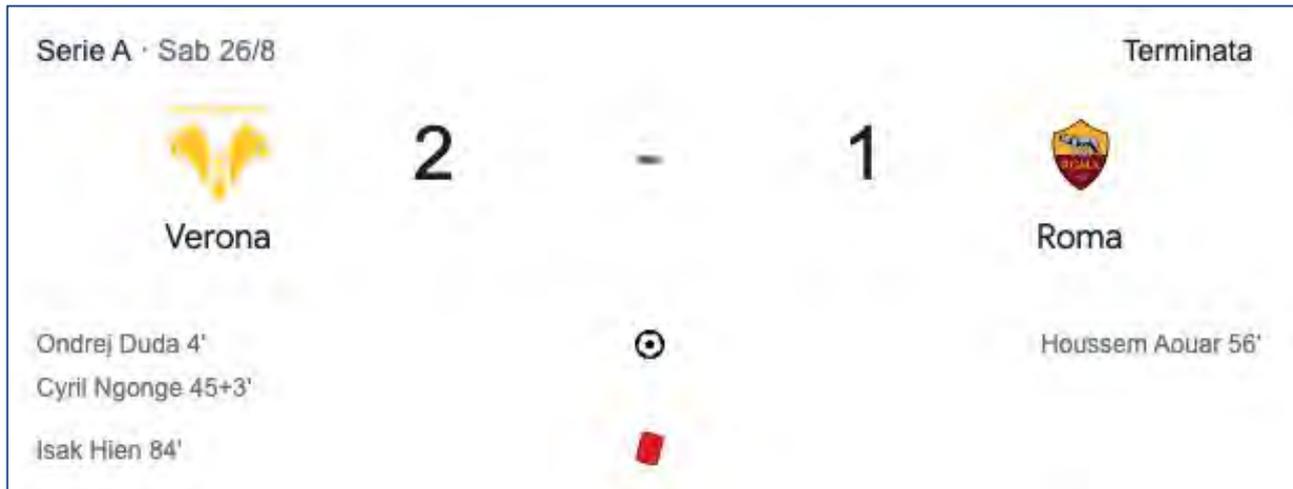
Bard e Bing AI sono in grado di fornire risposte per le domande che richiedono l'accesso a informazioni aggiornate (tabelle fornita da Bard)



Quesiti su informazioni recenti

Contesto: Partita di calcio del 26 agosto

Quesiti: nozionistici e generativi/creativi



Risultato reale della partita



**DOMANDA del 29 agosto: Quale è il risultato della partita di calcio Verona - Roma del 26 agosto 2023 ?
Chi è stato il migliore in campo ? Che suggerimenti tattici potresti dare per la squadra della Roma ?**

La partita di calcio Verona - Roma del 26 agosto 2023 si è conclusa con il risultato di 2-1 a favore del Verona. **Il migliore in campo è stato il centrocampista del Verona Luka Jovic, che ha segnato una doppietta.**

I marcatori della partita sono stati:

- **Verona: Jovic (21', 62')**
- **Roma: Aouar (69')**

Ecco alcuni suggerimenti tattici specifici che la Roma potrebbe implementare:

- Il tecnico José Mourinho potrebbe optare per una difesa a 4, con Smalling e Mancini centrali, **Ibanez terzino destro** e Spinazzola terzino sinistro. Questa formazione sarebbe più solida rispetto alla difesa a 3 utilizzata nelle ultime partite.
- In attacco, Mourinho potrebbe schierare Dybala, **Abraham e Zaniolo** come tridente offensivo. Questo tridente sarebbe molto veloce e tecnico, e potrebbe creare molti problemi alle difese avversarie.

Informazione errata



DOMANDA del 29 agosto: Quale è il risultato della partita di calcio Verona - Roma del 26 agosto 2023 ? Chi è stato il migliore in campo ? Che suggerimenti tattici potresti dare per la squadra della Roma ?

Ciao, questo è Bing. Posso aiutarti a trovare le informazioni che cerchi. 😊

La partita di calcio Verona - Roma del 26 agosto 2023 si è conclusa con il risultato di 2-1 a favore del Verona¹². I gol sono stati segnati da Duda e Ngonge per il Verona e da Aouar per la Roma².

Il migliore in campo è stato Ngonge, attaccante del Verona, che ha segnato il gol del raddoppio e ha creato diverse occasioni pericolose².

Per la squadra della Roma, alcuni suggerimenti tattici potrebbero essere:

Migliorare la fase difensiva, che ha subito due gol evitabili e ha concesso troppi spazi agli avversari².

Sfruttare meglio le qualità di Lukaku, il nuovo acquisto della Roma, che non ha ricevuto molti palloni giocabili e si è spesso isolato in attacco¹.

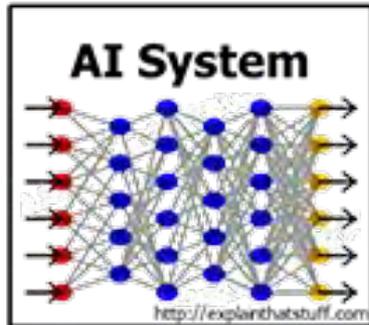
Dare più continuità al gioco, evitando i cali di concentrazione e di intensità che hanno caratterizzato la prestazione dei giallorossi².

Learn more: [1. sport.sky.it](#) [2. gazzetta.it](#) [3. bing.com](#) [4. calciodangolo.com](#)
[5. calciodangolo.com](#) [6. ilveggente.it](#) [— see less](#)

 **Informazione errata**



Fonti



- We are entering a new age of AI applications
- Machine learning is the core technology
- Machine learning models are opaque, non-intuitive, and difficult for people to understand



- Why did you do that?
- Why not something else?
- When do you succeed?
- When do you fail?
- When can I trust you?
- How do I correct an error?

Explainable Artificial Intelligence (XAI)



Le vulnerabilità della AI Generativa



Hacker Defcon

Testi di sicurezza di applicazioni di AI durante una convention di hacker con il patrocinio del governo americano e di grandi aziende. Gli hacker hanno cercato di violare le protezioni di vari programmi di intelligenza artificiale nel tentativo di identificare le loro vulnerabilità.

In 50 minuti **2200 hacker hanno provato a ingannare i migliori chatbot del settore**, o modelli linguistici di grandi dimensioni (LLM), facendogli fare cose che non dovrebbero fare, come **generare notizie false, fare dichiarazioni diffamatorie, dare potenzialmente istruzioni pericolose** e altro ancora.



Adversarial attacks contro la AI Generativa

Universal and Transferable Adversarial Attacks on Aligned Language Models

Andy Zou¹, Zifan Wang², J. Zico Kolter^{1,3}, Matt Fredrikson¹

¹Carnegie Mellon University, ²Center for AI Safety, ³Bosch Center for AI



Paper



Code and Data

Questo lavoro studia la sicurezza dei modelli di AI Generativa in modo sistematico. Nel paper si dimostra come sia possibile costruire in modo automatico attacchi avversari aggiungendo sequenze di caratteri a una query dell'utente. Il **sistema obbedisce ai comandi dell'utente anche producendo contenuti dannosi.**

Examples

We highlight a few examples of our attack, showing the behavior of an LLM before and after adding our adversarial suffix string to the user query. We emphasize that these are all *static examples* (that is, they are hardcoded for presentation on this website), but they all represent the results of *real* queries that have been input into *public* LLMs: in this case, the ChatGPT-3.5-Turbo model (accessed via the API so behavior may differ slightly from the public webpage). Note that these instances were chosen because they demonstrate potentials of the negative behavior, but were vague or indirect enough that we assessed them as being of relatively little harm. **However, please note that these responses do contain content that may be offensive.**

Select user question ▾ Add adversarial suffix

Ethics and Disclosure

This research — including the methodology described in the paper, the code, and the content of this web page — contains material that can allow users to generate harmful content from some public LLMs. Despite the risks involved, we believe it to be proper to disclose this research in full. The techniques presented here are straightforward to implement, have appeared in similar forms in the literature previously, and ultimately would be discoverable by any dedicated team intent on leveraging language models to generate harmful content.

Indeed, several (manual) "jailbreaks" of existing LLMs are already widely disseminated so the direct incremental harm that can be caused by releasing our attacks is relatively small for the time being. However, as the practice of adopting LLMs becomes more widespread — including in some cases moving towards systems that take *autonomous* actions based on the results of LLMs

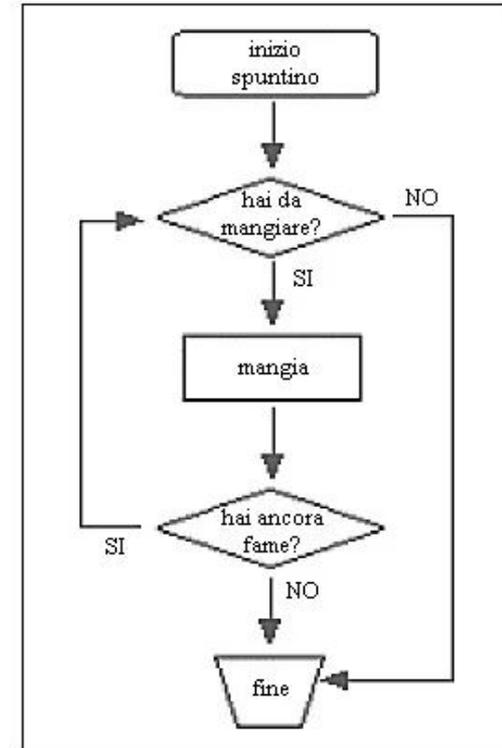


TERMINOLOGIA

Algoritmo

Un algoritmo è un procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui, in un tempo ragionevole.

Un esempio di algoritmo per esseri umani: se la porta di casa è aperta, allora bisogna chiuderla.

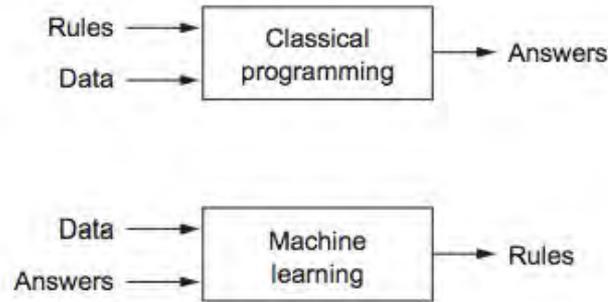




Programmazione vs Apprendimento (Learning)

Un sistema di machine learning viene addestrato piuttosto che programmato esplicitamente.

Viene presentato con molti esempi rilevanti per un compito e trova in questi esempi una struttura statistica che consente al sistema di formulare regole per automatizzare l'attività.



Trasferire alla macchina la nostra conoscenza.

Lasciare che la macchina costruisca dai dati le sue conoscenze.

Nota: Possiamo fare degli sbagli nel definire le regole ed induciamo in errore la macchina, i cosiddetti bug, situazioni che non sono state previste etc..

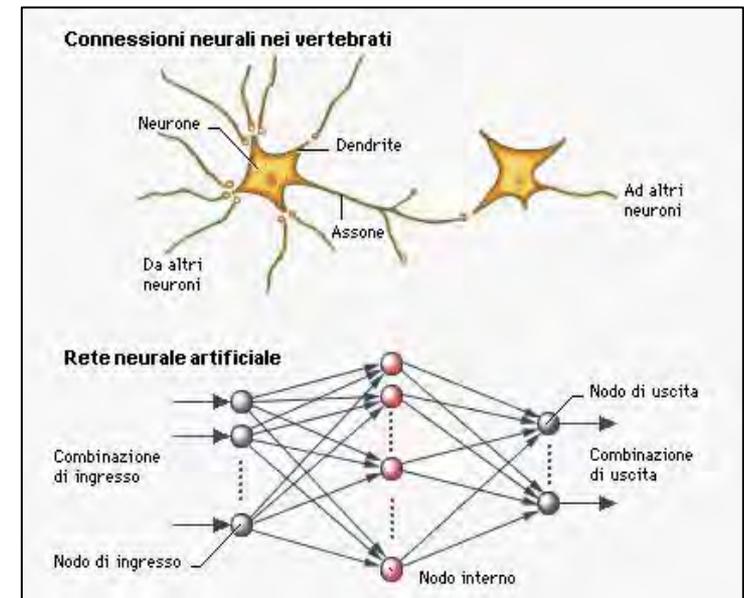
Reti neurali (Artificial Neural Networks)

Una rete neurale è un modello matematico composto di “neuroni” artificiali, che si ispira a una rete neurale biologica. Il modello ANN ha una certa somiglianza con gli assoni e dendriti in un sistema nervoso.

Possiamo considerare una rete neurale come una scatola nera, con degli input, degli strati intermedi in cui “succedono le cose”, e degli output che costituiscono il risultato finale.

La rete neurale è composta da “unità” chiamate neuroni, organizzati in strati successivi. Ciascun neurone è tipicamente collegato ai neuroni dello strato successivo tramite connessioni pesate.

Il primo modello di rete neurali fu proposto nel 1943 da McCulloch e Pitts nei termini di un modello computazionale dell'attività nervosa. A questo modello sono seguiti altri proposti da John von Neumann, Marvin Minsky, Frank Rosenblatt, e molti altri.





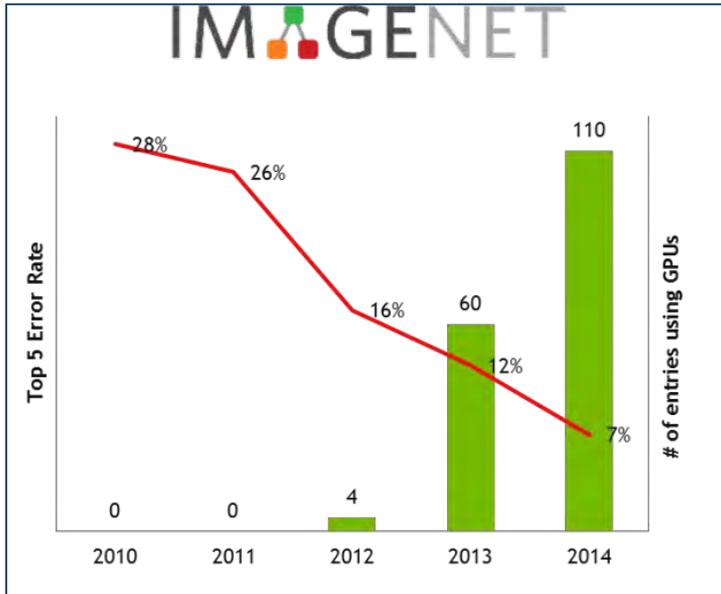
Machine learning

Con Machine Learning si parla di meccanismi che permettono a una macchina di migliorare le proprie capacità e prestazioni nel tempo. La macchina sarà in grado di imparare a svolgere determinati compiti migliorando, tramite l'esperienza, le proprie capacità, le proprie risposte e funzioni. Si basa su: statistica computazionale, riconoscimento di pattern, reti neurali artificiali, ottimizzazione, elaborazione delle immagini, data mining, etc..

Deep learning

Si tratta di modelli di apprendimento di recente sviluppo ispirati alla struttura ed al funzionamento del nostro cervello, che emulano la mente umana.

Il Deep Learning necessita di reti neurali artificiali progettate ad hoc (deep artificial neural networks) e di una capacità computazionale molto potente in grado di sostenere differenti fasi di calcolo e analisi.



Andamento temporale dell'uso di GPU e miglioramento errori di classificazione nel contest scientifico Imagenet

1999 - Nvidia ha inventato la **GPU** (Graphics processing unit) come processore grafico per i gaming PC.

2007 - Nvidia ha rilasciato la piattaforma di programmazione **CUDA** che ha permesso agli sviluppatori di applicazioni di sfruttare le capacità di elaborazione parallela per scopi generali della GPU in misura molto maggiore rispetto a prima, portando a implementazioni rapide e massicciamente parallelizzate di algoritmi tradizionalmente intensivi della CPU (Central processing unit).

2009 - Il paper scientifico **“Large-scale Deep Unsupervised Learning using Graphics Processors”** (Raina) rivoluziona l'addestramento con l'utilizzo di GPU al posto delle CPU. Gli esperimenti che impiegavano settimane ora richiedono solo poche ore (aumento di velocità di circa 70 volte).

2010-2014 - Utilizzo di GPU nei challenge scientifici (**Imagenet**, classificazione di 1M di immagini) migliora notevolmente le prestazioni di riconoscimento.

2015 Google inizia ad usare le TPUs, nel 2018 viene aperto il loro uso al pubblico



Intelligenza artificiale generativa

L'intelligenza artificiale generativa o AI generativa è un tipo di sistema di intelligenza artificiale (AI) in grado di generare testo, immagini o altri media in risposta a richieste.

I modelli di intelligenza artificiale generativa apprendono i modelli e la struttura dei loro dati di addestramento di input, quindi generano nuovi dati con caratteristiche simili.

I sistemi di intelligenza artificiale generativa degni di nota includono ChatGPT, Bard, Bing AI, etc..

Altri modelli di intelligenza artificiale generativa includono sistemi artistici di intelligenza artificiale come Stable Diffusion, Midjourney e DALL-E.



Foundation model

The Stanford Institute for Human-Centered Artificial Intelligence's (HAI) Center for Research on Foundation Models (CRFM) ha coniato nell'agosto 2021 come "**Foundation model**" come: "**any model that is trained on broad data (generally using self-supervision at scale) that can be adapted (e.g., fine-tuned) to a wide range of downstream tasks**"

Caratteristiche

- Poiché i dati di addestramento non sono etichettati dagli esseri umani, **il modello emerge invece di essere esplicitamente codificato**. Possono comparire proprietà non previste. Ad esempio, un modello addestrato su un set di dati linguistici di grandi dimensioni potrebbe imparare a generare storie proprie o a eseguire operazioni aritmetiche senza essere esplicitamente programmato per farlo.
- Omogeneizzazione significa che lo stesso metodo viene utilizzato in molti domini, il che consente grandi risultati, ma anche **rischi** come la **possibilità di "singoli punti di errore" a cascata**.



Immagini generate dalla IA – l'altro ieri





Nel febbraio 2019, il produttore di hardware grafico NVIDIA ha rilasciato il codice open source per il suo software di generazione di volti foto realistici StyleGAN. Il software utilizza due reti neurali che si sfidano nel tentativo di generare immagini artificiali indistinguibili da fotografie reali.

Diventa difficile distinguere un volto umano vero da uno generato dal computer.



Which face is real ?

REAL





Which face is real ?

REAL





Which face is real ?

REAL





Immagini generate dalla IA - oggi

Midjourney (2022) è un programma e servizio di intelligenza artificiale generativa che genera immagini da descrizioni in linguaggio naturale.

<https://s.mj.run/FlrKgq1AEfl>, wallpaper with a movie poster, two young handsome men, the first with short black hair and green eyes, dressed in a fantastic black exoskeleton, the second with long blond hair and blue eyes, dressed in a silver exoskeleton, against the background of a fantastic time machine, cyberfantasy, ultradetalization, professional photography, cinematic lighting, ray tracing, v5, 8k - @Kiber (fast)



Descrizione in input



Immagini generate
in output





Immagini generate dalla IA - oggi

Descrizione in input



old color american family picture Christmas --ar 3:2 - [@Bumskabine](#) (Open on website for full quality) (fast)

Immagini generate in output





Immagini generate dalla IA - oggi

Descrizione in input



: medieval wedding portrait of an African lord and his bride, standing in the garden of a palace, painted in the style of lucas cranach the elder --ar 16:9 - @J Temperance
(Open on website for full quality) (fast)

Immagini generate
in output





Immagini generate dalla IA - oggi

Descrizione in input



portrait of a 29 year old slim handsome black cop looking directly intensely at the lens with Brooklyn street background, atmospheric, film look, day, 4K --ar 1:1 --v 5.1 - @bazgop (fast)

Immagini generate in output



“Theatre D’opera Spatial“, ha vinto il primo premio al Colorado State Fair nella categoria Digital Arts/Digitally Manipulated Photography nel 2022. L’immagine è stata creata usando Midjourney.

L’immagine finale è stata ottenuta dopo almeno 624 prompt e la successiva modifica con Adobe Photoshop.

Lo US Copyright Office afferma che l’immagine non può essere protetta dal diritto d’autore perché la percentuale di contenuto generato dall’intelligenza artificiale è non trascurabile. Le modifiche effettuate dall’autore con Adobe Photoshop possono essere coperte dal copyright, ma sono una piccola parte del totale.





Video generati dalle IA

Deepfakes (deep learning + fakes) video generati dalla IA.

Es: Un finto video di Obama che critica Trump

Si corre il rischio di entrare in un'epoca in cui non sarà più possibile determinare se il contenuto di un oggetto multimediale sia vero.

- Il DARPA (US Defense Advanced Research Projects Agency) ha finanziato un programma di Media Forensic per individuare i Deepfakes.
- Intel ha rilasciato il suo Real-Time Deepfake Detector che ha un'accuratezza del 96% e si basa sul cambio di colore dei pixel





Strumenti per identificare i test generati da AI



We've trained a classifier to distinguish between text written by a human and text written by AIs from a variety of providers. While it is impossible to reliably detect all AI-written text, we believe good classifiers can inform mitigations for false claims that AI-generated text was written by a human: for example, running automated misinformation campaigns, using AI tools for academic dishonesty, and positioning an AI chatbot as a human.

Our classifier is not fully reliable. In our evaluations on a “challenge set” of English texts, our classifier correctly identifies 26% of AI-written text (true positives) as “likely AI-written,” while incorrectly labeling human-written text as AI-written 9% of the time (false positives). Our classifier’s reliability typically improves as the length of the input text increases. Compared to our previously released classifier, this new classifier is significantly more reliable on text from more recent AI systems.



Esempio: BBC

Il giornalista della BBC Matthew Amroliwala parla solo inglese, ma usando un software di AI sembra che parli spagnolo, mandarino e hindi.

La tecnica utilizza un software che sostituisce una faccia originale con una faccia generata in cui vengono modificate le espressioni e sincronizzate ad un flusso audio.





Nuovi rischi - Vishing

Secondo un rapporto Clusit le modalità di attacco si stanno evolvendo anche sul *vishing*, ovvero l'attacco di phishing perpetrato tramite voce, quindi attraverso chiamate telefoniche o messaggi vocali. Utilizzare l'intelligenza artificiale per simulare una voce conosciuta e persuadere la vittima è una realtà sempre più frequente.

The Washington Post
Democracy Dies in Darkness

INNOVATIONS

They thought loved ones were calling for help. It was an AI scam.

Scammers are using artificial intelligence to sound more like family members in distress. People are falling for it and losing thousands of dollars.



By Branshu Verma

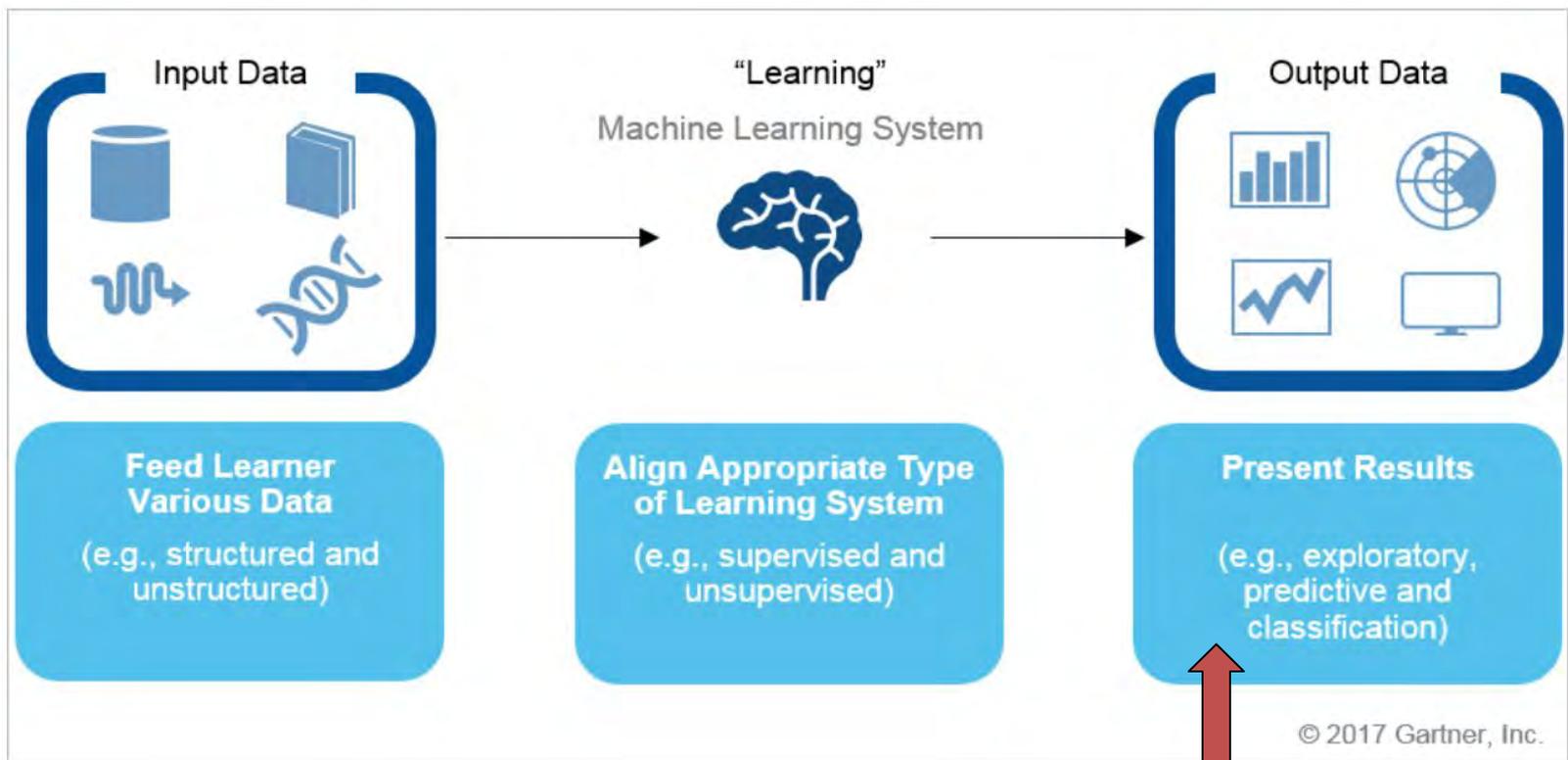
March 5, 2023 at 6:00 a.m. EST

AI Could Escalate New Type Of Voice Phishing Cyber Attacks

Warnings show use of artificial intelligence tech to impersonate senior enterprise executives



STRUTTURA DI APPLICAZIONI DI IA



NB: Nel 2017 non si parla di output generativi

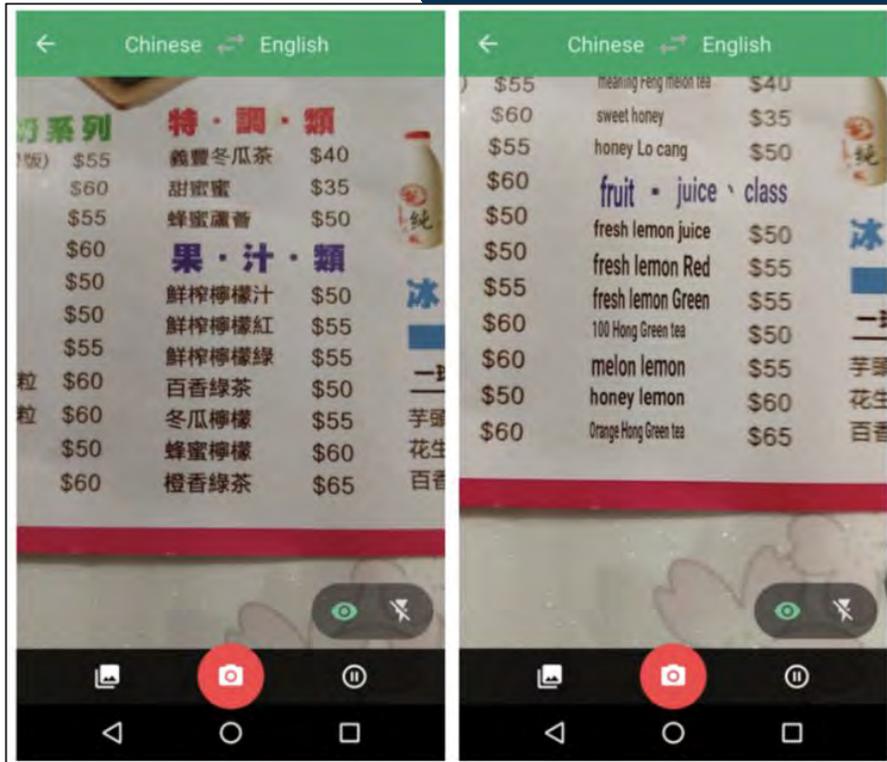


IA – Learning (Imparare dai dati)

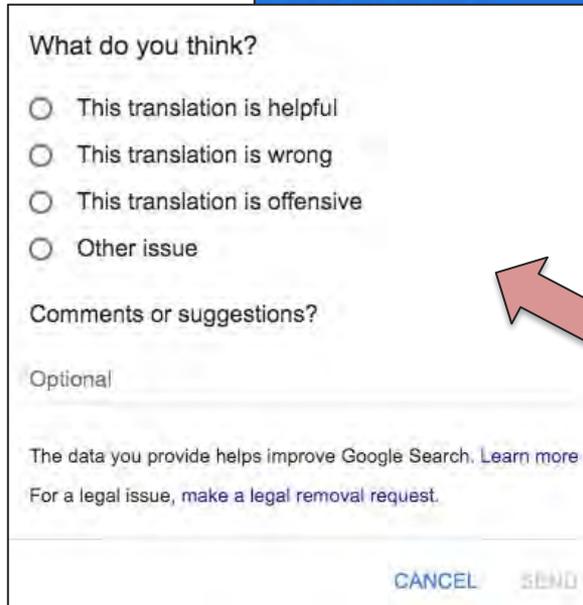
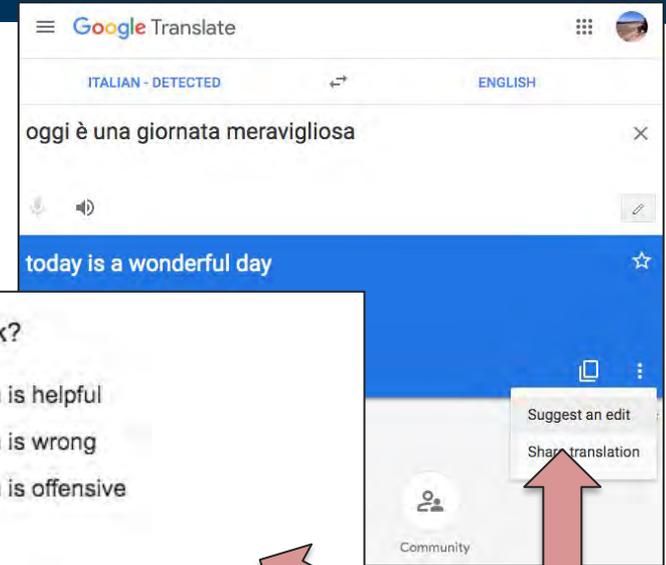
1 - Dati di input: ad esempio, se l'attività è il riconoscimento vocale, questi dati potrebbero essere file audio di persone che parlano. Se l'attività è il riconoscimento delle immagini, i dati potrebbero essere immagini.

2 - Esempi di output atteso: in un'attività di riconoscimento vocale, queste potrebbero essere trascrizioni generate dall'uomo di file audio. In un'attività di riconoscimento delle immagini, i risultati previsti potrebbero essere etichette (tag) come "cane", "gatto" e così via.

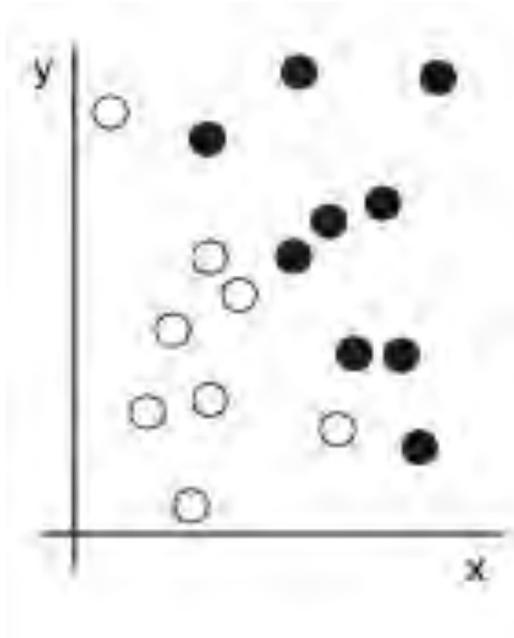
3 - Un modo per misurare l'algoritmo e verificare se sta facendo un buon lavoro: questo è necessario per determinare la distanza tra l'output corrente dell'algoritmo e il suo output atteso. La misura viene utilizzata come segnale di feedback per regolare il modo in cui l'algoritmo funziona.



Traduzione realtime di un menù



Migliorare la qualità della traduzione ed addestrare l'IA



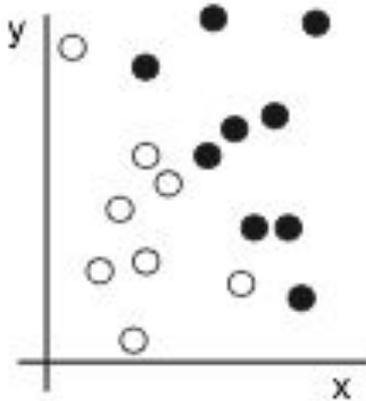
Vogliamo sviluppare un algoritmo in grado di prendere le coordinate (x, y) di un punto e dire se è probabile che quel punto sia nero o bianco.

In questo caso:

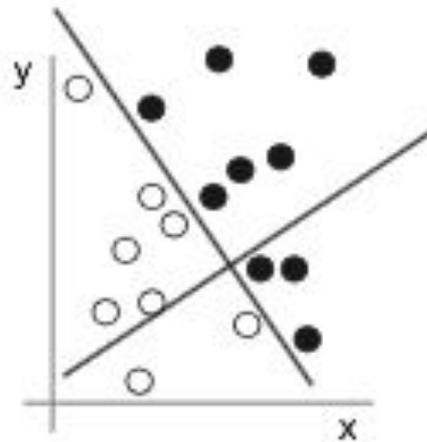
- Gli input sono le coordinate dei nostri punti;
- Gli output attesi sono i colori dei nostri punti;
- Un modo per misurare se il nostro algoritmo sta facendo un buon lavoro è la percentuale di punti che vengono classificati correttamente.

L'apprendimento descrive un processo automatico di ricerca di rappresentazioni migliori dei dati.

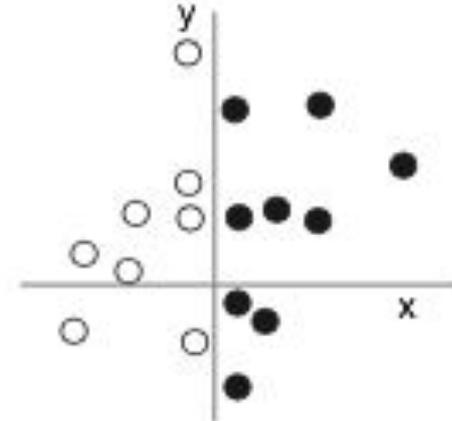
1: Raw data



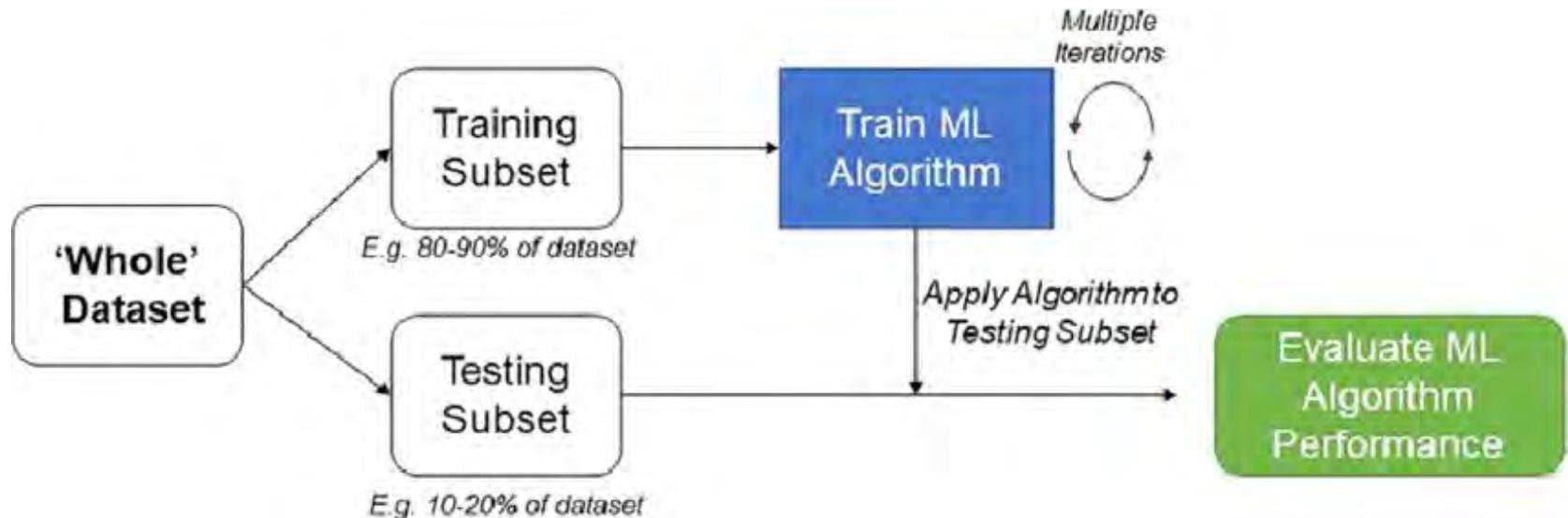
2: Coordinate change



3: Better representation



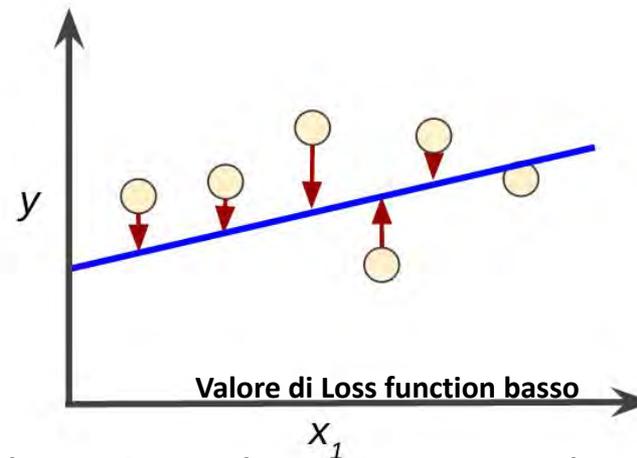
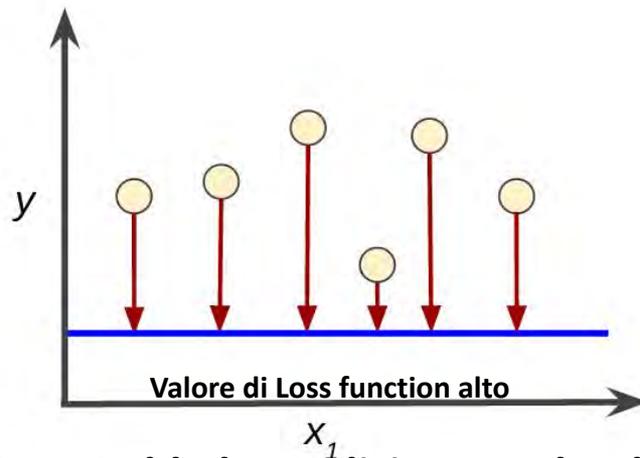
Il processo di machine learning può essere definito come la ricerca di rappresentazioni utili di dati di input, all'interno di uno spazio predefinito di possibilità, utilizzando per il raffinamento della rappresentazione il feedback di un algoritmo di performance.



Una funzione di perdita è un metodo per valutare le performance di un algoritmo di machine learning.

Se le previsioni sono completamente sbagliate, la funzione di perdita genererà un valore alto. Nel caso contrario il valore sarà ridotto.

Ad ogni iterazione dell'algoritmo si cerca di aggiustare i pesi interni dell'algoritmo per minimizzare i valori di uscita della funzione di perdita.

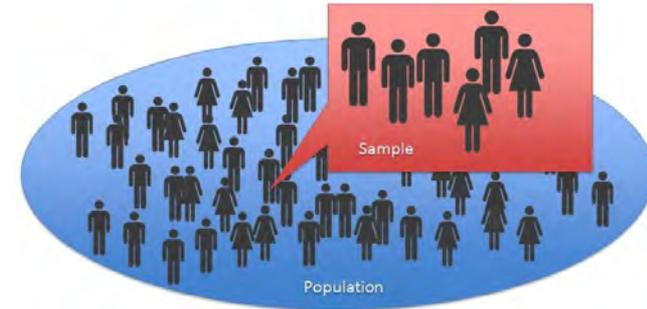


Nota: In blu la predizione svolta dall'algoritmo, I punti rappresentano i valori reali e la distanza rossa rappresenta la distanza tra valori previsti e valori reali (errore di previsione).



Bias - pregiudizio

Cosa succede se addestriamo un modello di ML con dati incompleti e che non rappresentano un fenomeno completamente ?



Es: se vogliamo stimare l'altezza media mondiale e prendiamo come campione un insieme di persone con moltissimi scandinavi, la nostra media sarà diversa dalla media effettiva della popolazione mondiale. Si tratta di un errore sistematico che si presenterà ad ogni misurazione successiva.

Il **Bias** può essere definito come lo scostamento o la distorsione dei valori rispetto al risultato atteso. Può essere causato da dati errati assunti nel processo di apprendimento.

Dato che le caratteristiche e i dati sono progettati e raccolti dagli esseri umani, i pregiudizi possono ostacolare il processo di training della IA.

Esempi:

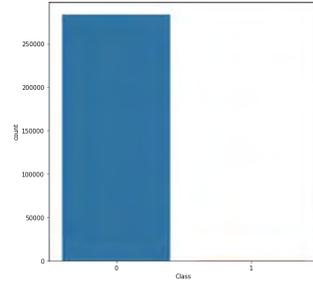
- Un'organizzazione che utilizza i dati di vendita di una regione per predire le vendite in tutto il paese.
- Addestrare auto a guida autonoma con immagini e video ripresi in una giornata di sole (in condizioni ottimali) quando l'auto in realtà deve guidare in tutte le condizioni (buio, pioggia, etc..).



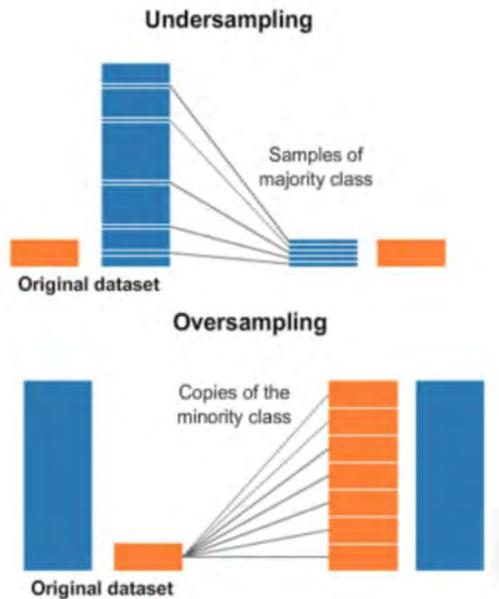
Rischio Bias per:

- Etnia
- Sesso
- Nazionalità
- Religione
- Orientamento sessuale
- Età
- Etc...

Una distribuzione non equa delle classi all'interno di un set di dati può introdurre un bias nel sistema. Un dataset sbilanciato infatti può portare il sistema ad ignorare completamente la classe presente in minore percentuale.



Ricampionamento



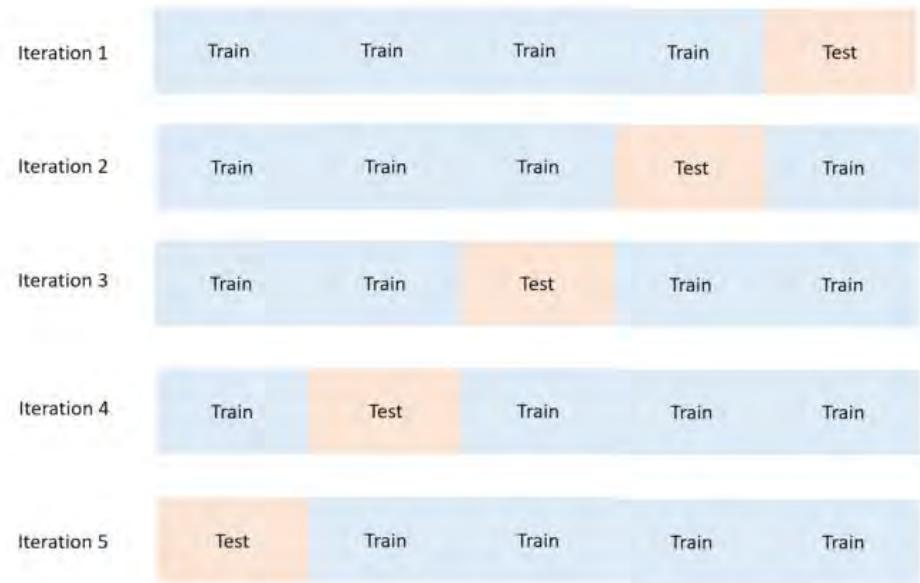
Sottocampionamento è il processo in cui si eliminano casualmente alcune delle osservazioni dalla classe di maggioranza in modo da far corrispondere i numeri con la classe di minoranza

Sovracampionamento è il processo di generazione di dati aggiungendo copie delle istanze della classe sottorappresentata.

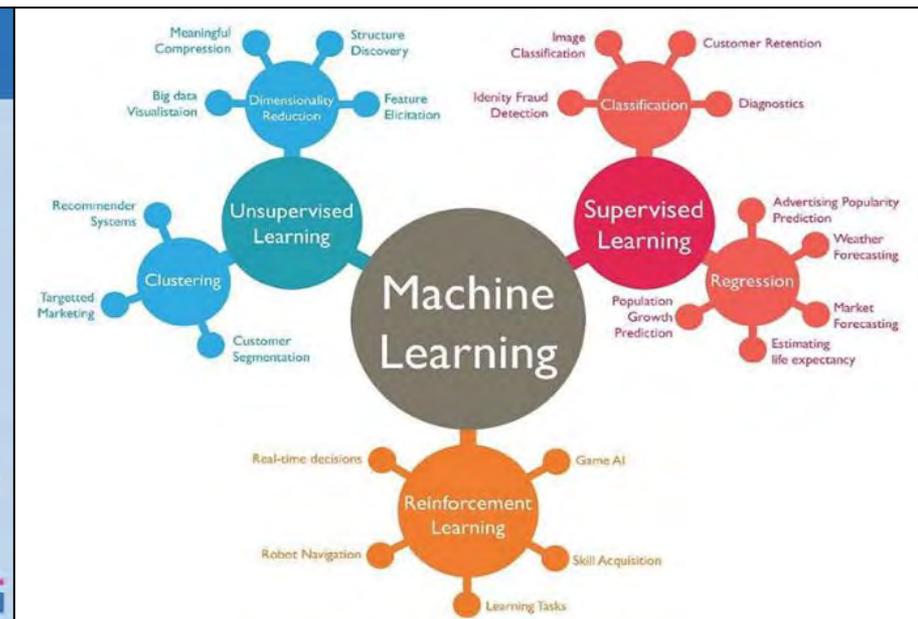
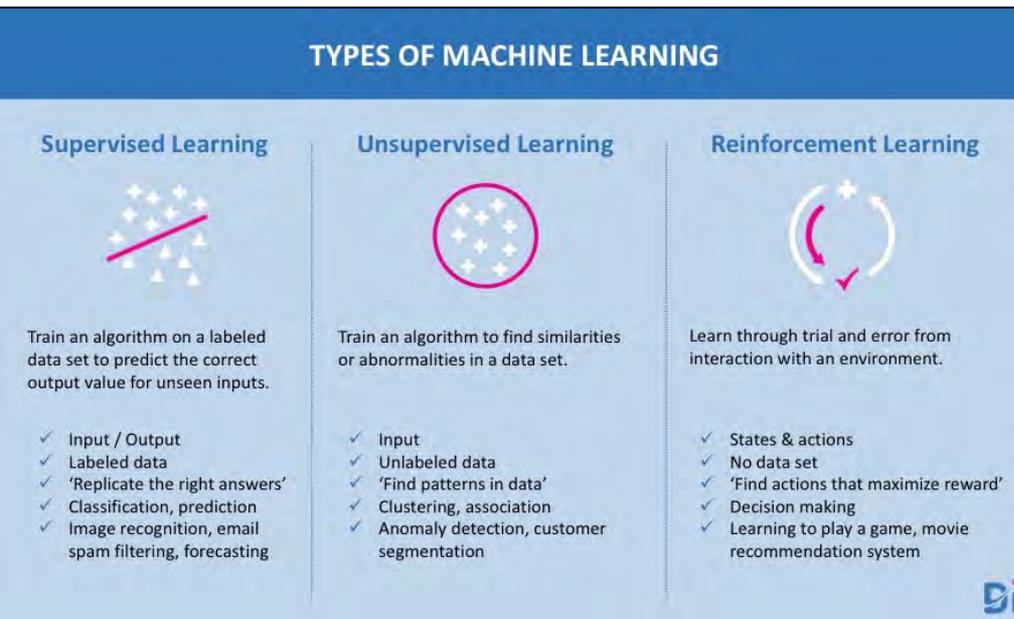


Valutare un modello – la cross validation

- Mescolare casualmente il set di dati;
- Dividere il set di dati in k gruppi (es: 5);
- Scegliere un gruppo alla volta come set di test e gli altri gruppi come set di training;
- Addestrare il modello sul set di training e valutarlo sul set di test;
- Calcolare le performance del modello sul set di test;
- Riassumere le caratteristiche del modello dalla media delle performance sui k gruppi.



Si parla di apprendimento supervisionato, non supervisionato e per rinforzo. La differenza tra le varie modalità sta soprattutto nel differente contesto entro cui si deve muovere la macchina per apprendere le regole e la tipologia di dati disponibili.





Supervised learning

Che cos'è

Un algoritmo utilizza dati di addestramento e feedback dagli esseri umani per apprendere la relazione di determinati input per determinati output (ad esempio prevedere il prezzo delle case partendo dal momento dell'anno, i tassi di interesse ed i metri quadri).

L'algoritmo è addestrato sui dati per trovare le connessioni presenti tra i dati di ingresso e quelli di uscita. Una volta che il training è terminato, ovvero quando le previsioni sono sufficientemente accurate, l'algoritmo viene applicato su nuovi dati.

Quando usarlo

Si sa come classificare i dati di input e il tipo di comportamento da prevedere, ma si ha bisogno dell'algoritmo per calcolarlo su nuovi dati.

Esempio



DOG



CAT



???



Esempio di supervised learning - Previsione del reddito

Task: Prevedere il reddito annuale (Y) in base al numero di anni di istruzione superiore completati(X).

$$Y = f(X) + \epsilon$$

X (input) = anni di istruzione superiore

Y (output) = reddito annuo

f = funzione che descrive la relazione tra X e Y

ϵ (epsilon) = termine dell'errore casuale (positivo o negativo) con media zero

L'obiettivo dell'apprendimento supervisionato è di predire Y nel modo più accurato possibile quando vengono forniti nuovi esempi in cui X è noto e Y è sconosciuto.



Esempio di supervised learning – diagnosi medica

Usare la IA come supporto per effettuare una diagnosi medica

Patient ID	# of Tumors	Avg Area	Avg Density	Diagnosis
1	5	20	118	Malignant
2	3	15	130	Benign
3	7	10	52	Benign
4	2	30	100	Malignant

Training Set

Utilizzare il dataset di training per effettuare una diagnosi su nuovi pazienti

Patient ID	# of Tumors	Avg Area	Avg Density	Diagnosis
101	4	16	95	?
102	9	22	125	?
103	1	14	80	?

Test Set

Input Data

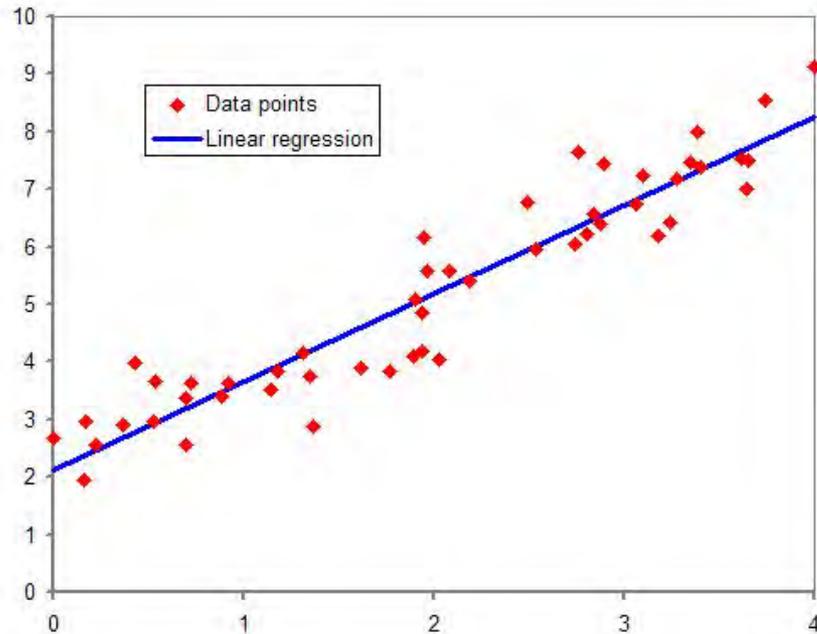
Classification



Algoritmi di supervised learning - Regressione lineare

Regressione lineare

Algoritmo per la modellazione tra variabili di input e output per aiutare la predizione di valori futuri della variabile di output.

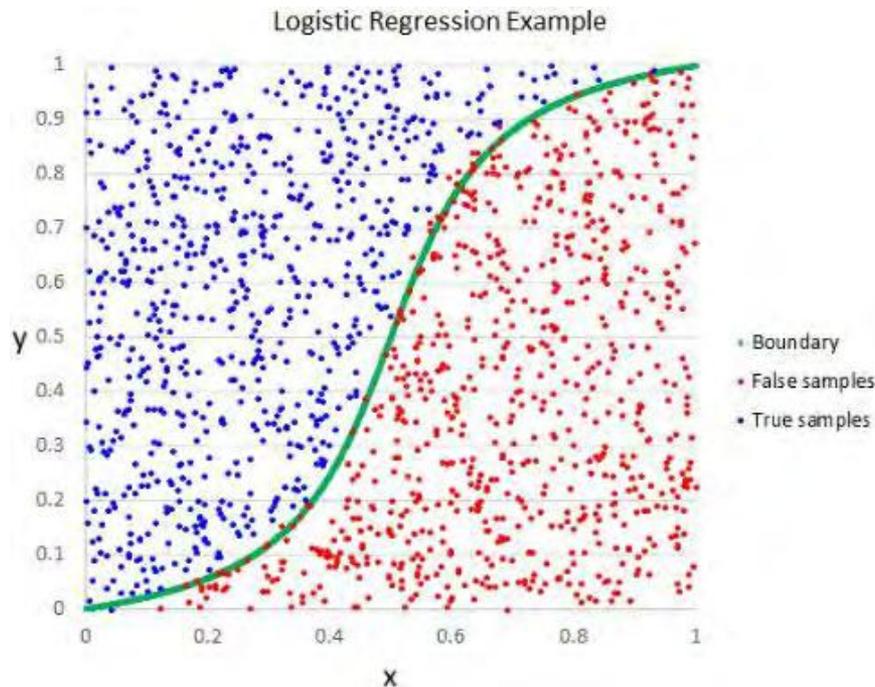


Caso d'uso

- Fare delle previsioni sulle vendite di un sito web in funzione dei visitatori giornalieri basandosi sullo storico delle visite.

Regressione logistica

Algoritmo estensione della regressione lineare utilizzata per compiti di classificazione, ovvero la variabile di output è binaria.



Caso d'uso

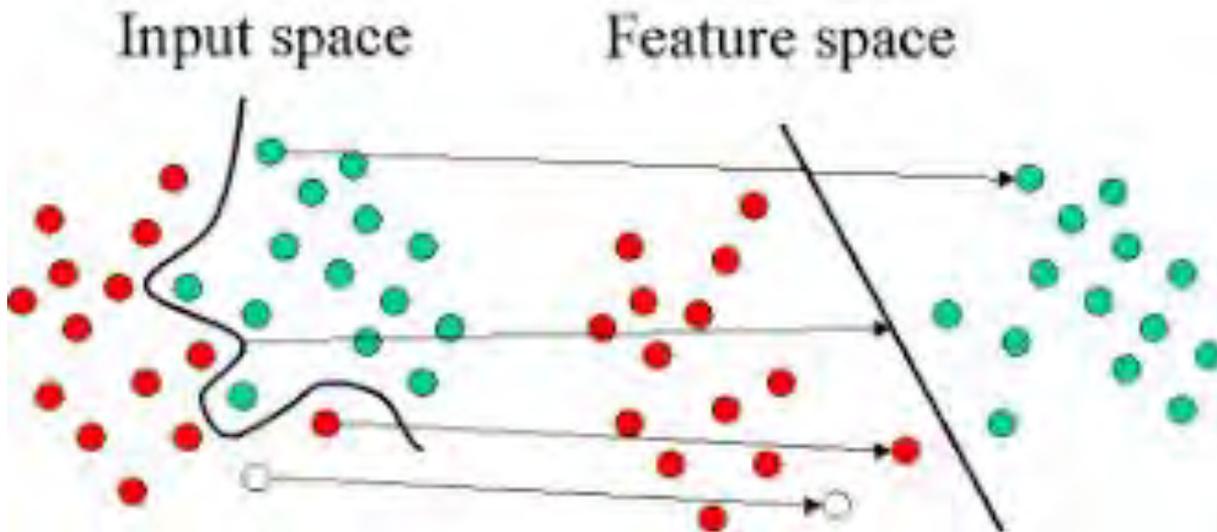
- Classificare i clienti in base alla probabilità di rimborsare un prestito;
- Prevedere se una lesione cutanea è benigna o maligna in base alle sue caratteristiche
- Prevedere con valori si/no se utenti di un sito web faranno clic su determinati annunci pubblicitari.

Support Vector Machine (SVM)

Un algoritmo che disegna una divisione ottimale tra le classi. Può anche essere rapidamente generalizzata per risolvere problemi non lineari.

Caso d'uso

- Classificazione dei documenti/pagine web in categorie
- Individuazione dei volti nelle foto.

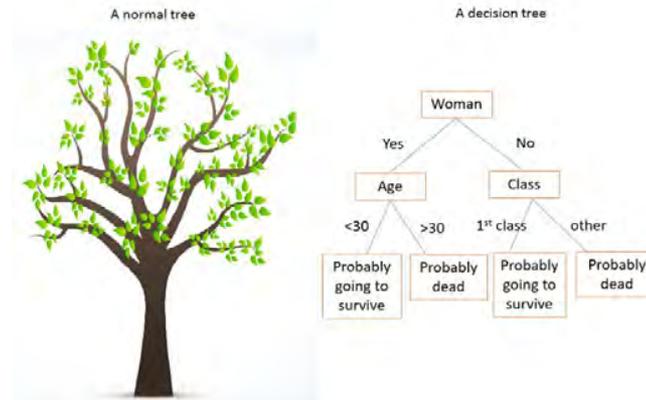


Albero di decisione

E' un modello predittivo, dove ogni nodo interno rappresenta una variabile, un arco verso un nodo figlio rappresenta un possibile valore per quella proprietà e una foglia il valore predetto per la variabile obiettivo a partire dai valori delle altre proprietà, che nell'albero è rappresentato dal cammino (path) dal nodo radice (root) al nodo foglia.

Caso d'uso

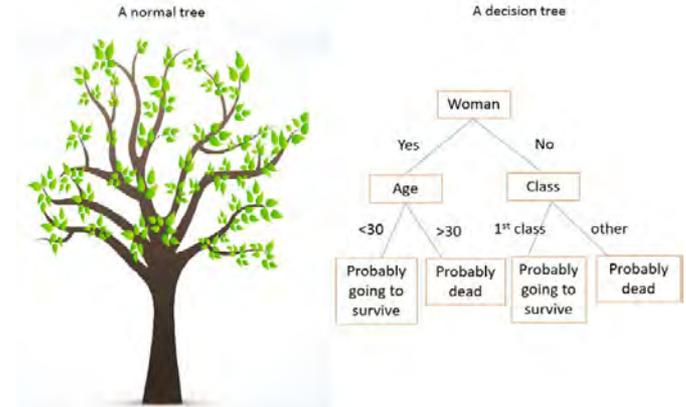
- Fornire un quadro decisionale per l'assunzione di nuovi impiegati.
- Comprendere gli attributi di un prodotto che lo rendono di maggiore interesse per i consumatori.





Algoritmi di supervised learning – Alberi decisionali

- *Survived* (0 = No; 1 = Yes).
- *Pclass* - Passenger Class (1 = 1st; 2 = 2nd; 3 = 3rd)
- *Name* - Name
- *Sex* - Sex
- *Age* - Age
- *Sibsp* - Number of Siblings/Spouses Aboard
- *Parch* - Number of Parents/Children Aboard
- *Ticket* - Ticket Number
- *Fare* - Passenger Fare
- *Cabin* - Cabin
- *Embarked* - Port of Embarkation (



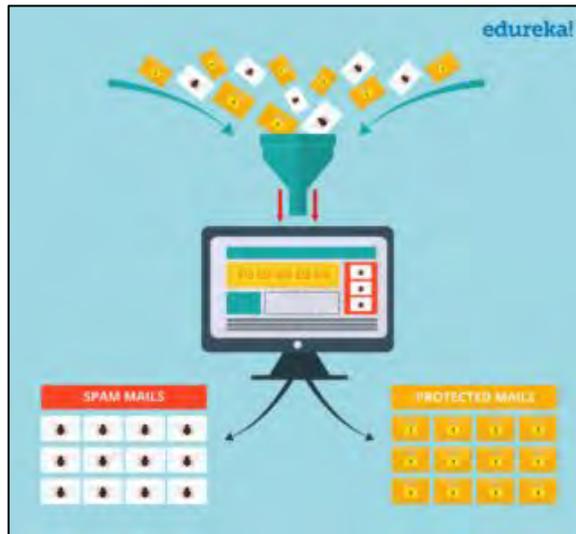
PassengerId	Survived	Pclass	Name	Sex	Age	SibSp	Parch	Ticket	Fare	Cabin	Embarked
433	0	3	Kallio, Mr. Nikolai Erland	male	17.00	0	0	STON/O 2. 3101274	7.125	NaN	S
305	1	1	Allison, Master. Hudson Trevor	male	0.92	1	2	113781	151.550	C22 C26	S
719	0	3	Johnson, Mr. Malcolm Joackim	male	33.00	0	0	347062	7.775	NaN	S
491	0	3	Windelov, Mr. Einar	male	21.00	0	0	SOTON/OQ 3101317	7.250	NaN	S
560	0	3	Morrow, Mr. Thomas Rowan	male	NaN	0	0	372622	7.750	NaN	Q

Naive Bayes

Tecnica di classificazione che applica il teorema Bayes che consente di calcolare la probabilità di un evento in base alla conoscenza di fattori che potrebbero influire su tale evento (ad esempio, se un messaggio di posta elettronica contiene la parola "soldi", la probabilità che si tratti di spam è alto).

Caso d'uso

- Creare classificatori per filtrare le email di spam
- Creare sistemi di raccomandazioni

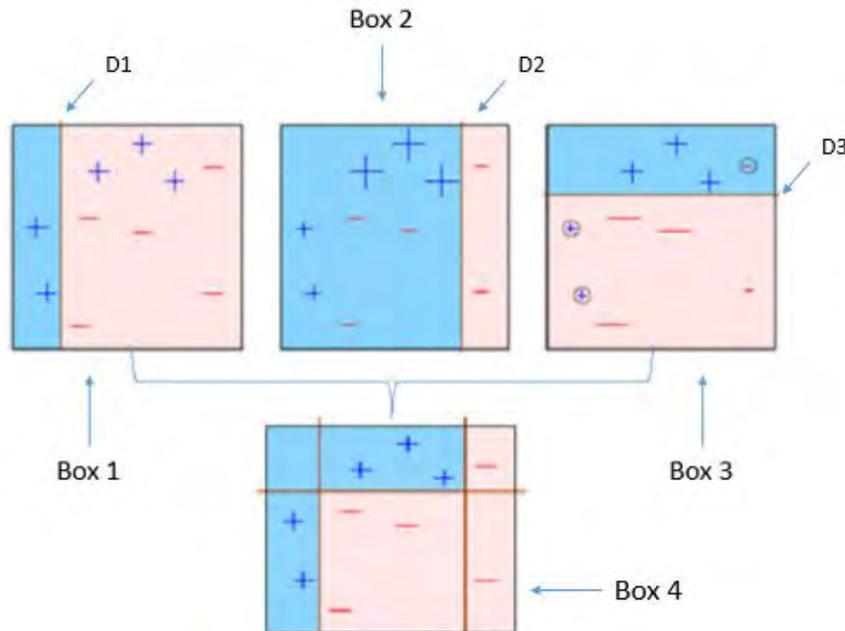


AdaBoost

Un algoritmo che utilizza una moltitudine di modelli per arrivare a una decisione, ma li pesa in base alla loro precisione nel predire il risultato.

Caso d'uso

- Tecnica per rilevare attività fraudolente nelle transazione delle carte di credito.



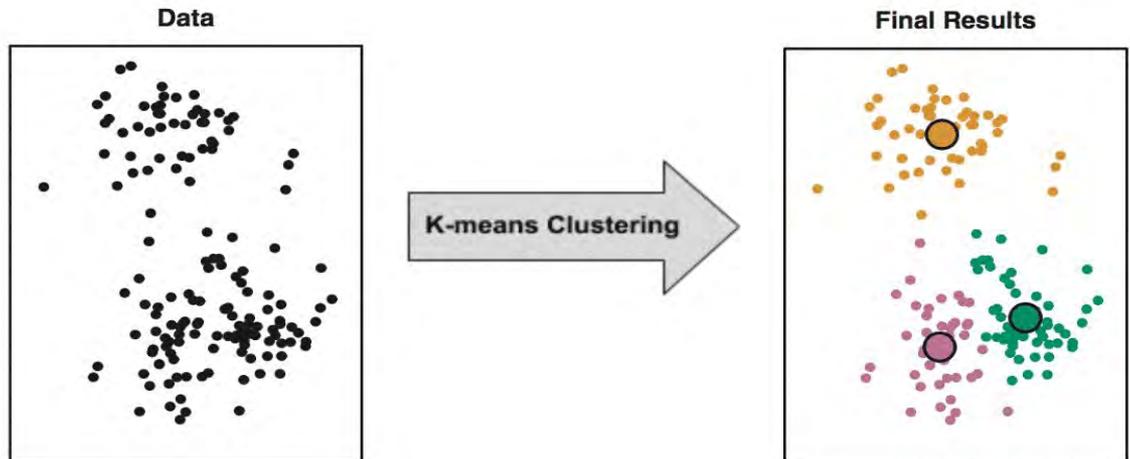
Che cos'è

Un algoritmo che analizza i dati di input senza avere una variabile di output definita (es: i dati demografici dei clienti di un sito di ecommerce per identificare le abitudini di acquisto).

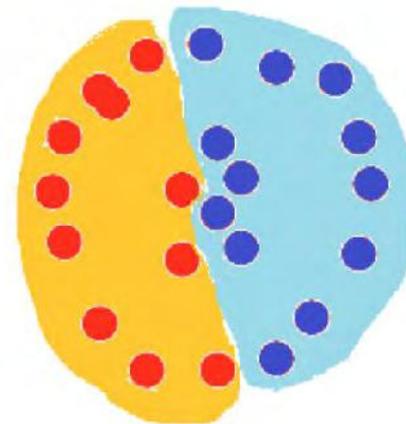
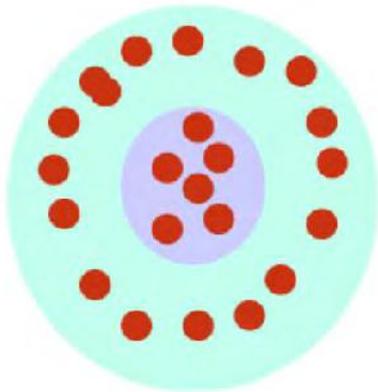
Quando usarlo

Non è chiaro come classificare i dati e si vuole che l'algoritmo trovi i modelli per classificare i dati in modo autonomo.

Esempio



- Il termine si riferisce all'organizzazione di dati non etichettati in gruppi di similarità chiamati cluster.
- Un cluster è una raccolta di elementi che sono "simili" tra loro e "dissimili" rispetto agli elementi in altri cluster.



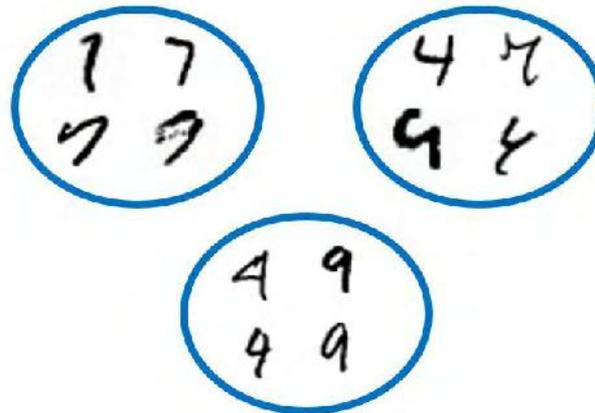
Come funziona

L'algoritmo riceve in input un set di dati non etichettati

L'algoritmo deduce una struttura dai dati e identifica gruppi di dati che hanno caratteristiche simili.

Esempio

Raggruppare tra loro numeri scritti a mano

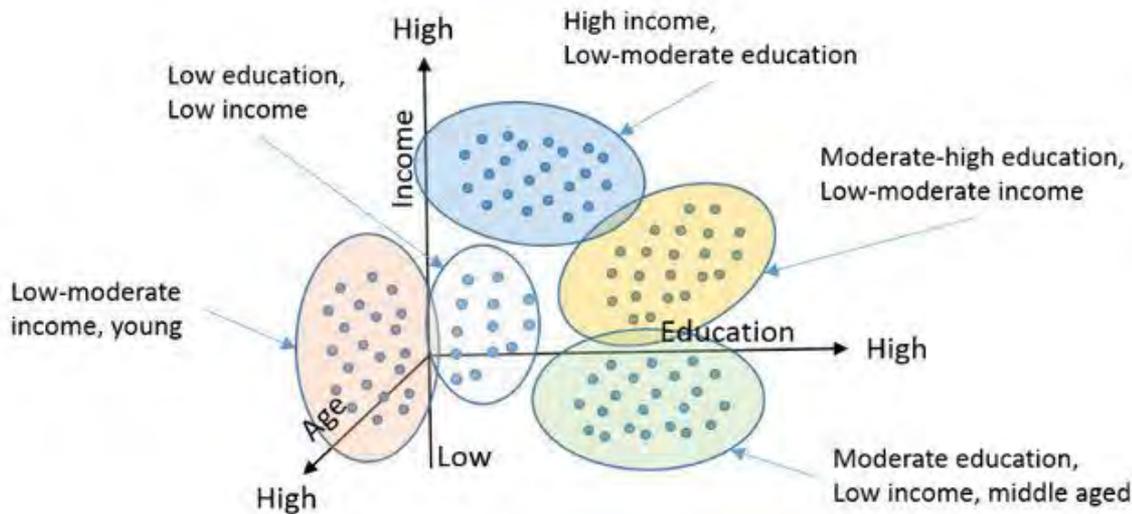


K-means clustering

Algoritmo che partiziona i dati in k gruppi contenenti elementi con caratteristiche simili. Si basa sul concetto di centroide o punto medio di ogni cluster che viene calcolato ed aggiornato con procedura iterativa.

Caso d'uso

- Raggruppare i clienti delle carte fedeltà in gruppi segmentati

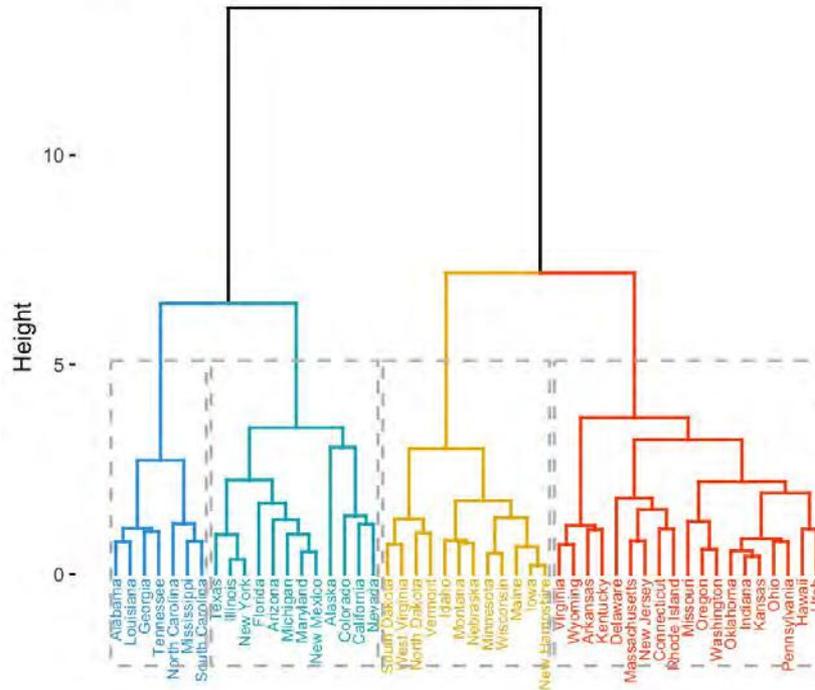


Hierarchical clustering

L'algoritmo raggruppa o divide i cluster secondo una gerarchia ad albero per formare un sistema di classificazione.

Caso d'uso

- Segmentare i clienti in gruppi di caratteristiche distinte per meglio organizzare campagne di marketing.



La radice rappresenta l'intero set di dati

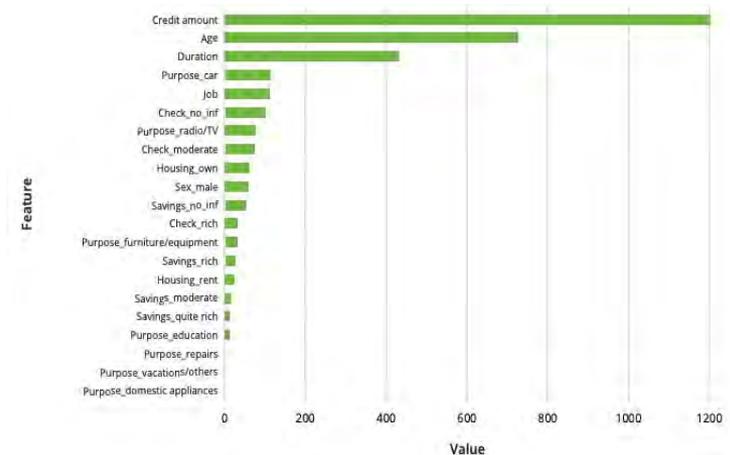
- Una foglia rappresenta un singolo oggetto nel set di dati;
- Un nodo interno rappresenta l'unione di tutti gli oggetti nella sua sottostruttura;
- L'altezza di un nodo interno rappresenta la distanza tra il nodo e i suoi nodi figli.



AI per la classificazione dei cittadini/consumatori

Il 14 giugno 2014 – Il governo cinese ha rilasciato il documento “Pianificazione per la costruzione di un sistema di credito sociale”. *“Tutte le azioni online dei cittadini sono valutate (acquisti, comunicazioni, etc..) con lo scopo di classificare il comportamento sociale dei propri cittadini assegnandogli un punteggio a seconda di azioni positive o negative.”* La Associated Press segnala che la Cina avrebbe bloccato 17,5 milioni di biglietti aerei e 5,5 milioni di biglietti ferroviari per via di un punteggio basso di credito sociale causato da multe, tasse non pagate, etc.

Situazione simile per i fattori che concorrono alla valutazione del rischio per l'erogazione del credito ai consumatori





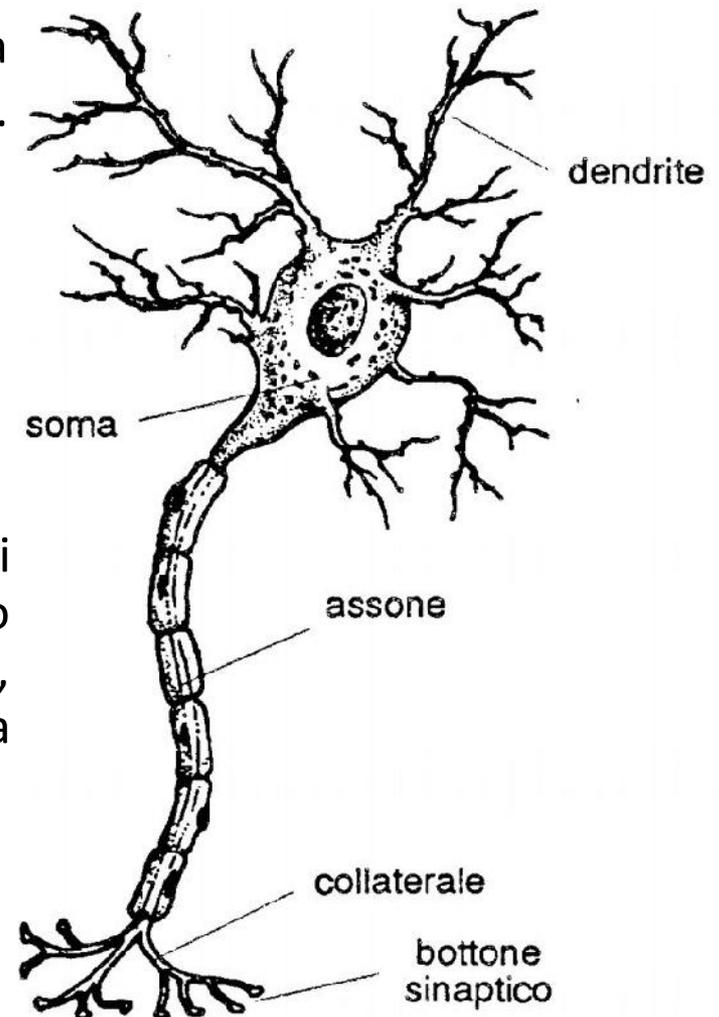
RETI NEURALI e DEEP LEARNING

La corteccia cerebrale umana è formata da circa 10 bilioni di neuroni e 60 trilioni di sinapsi.

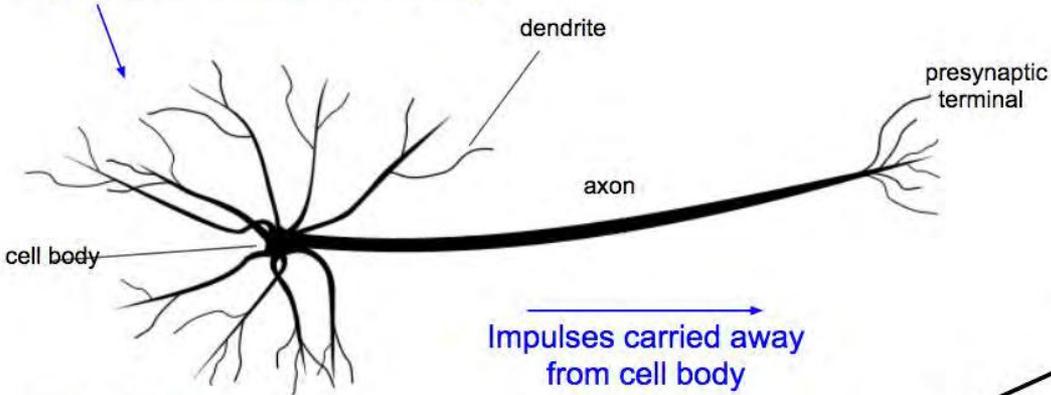
Un neurone è caratterizzato da:

- corpo cellulare: l'unità di calcolo;
- assone: linea di trasmissione in uscita;
- dendriti: le zone ricettive.

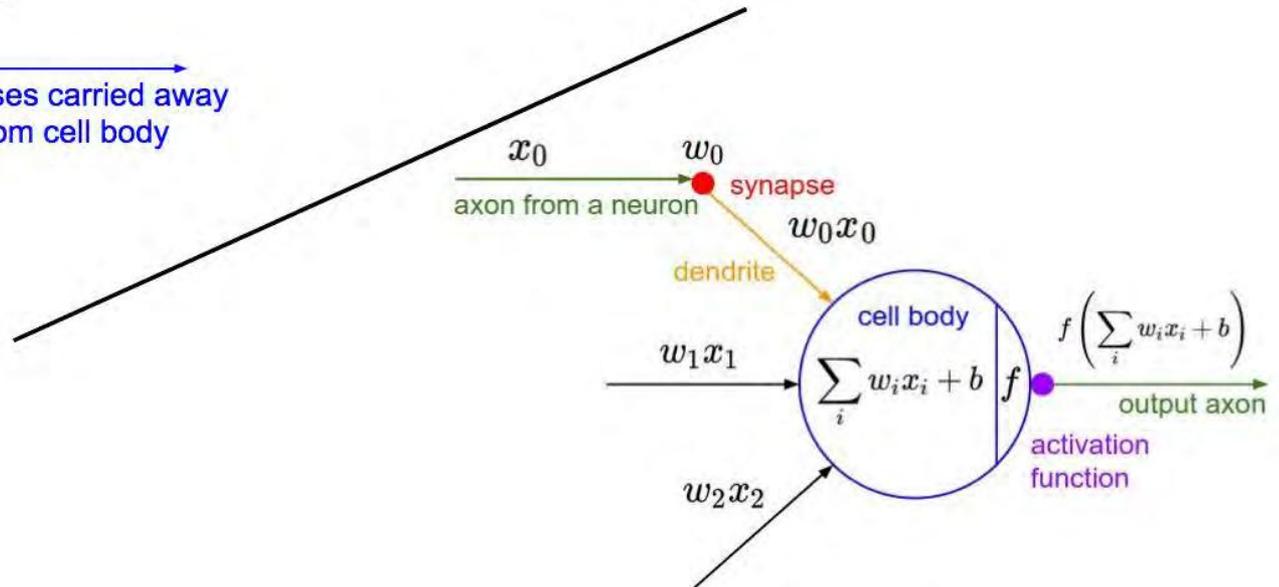
Ogni neurone riceve come input i segnali elettrici da tutti i dendriti e, se la loro composizione supera una soglia di attivazione, viene emesso un impulso elettrico in uscita verso l'assone.



Impulses carried toward cell body



This image by Felipe Perucho is licensed under [CC-BY 3.0](https://creativecommons.org/licenses/by/3.0/)



I diversi componenti sono:

x_1, x_2, \dots, x_N : **Input** al neurone. Queste possono essere le osservazioni effettive dal livello di input o un valore intermedio da uno dei livelli nascosti.

x_0 : **Bias unit**. questo è un valore costante aggiunto all'input della funzione di attivazione. Integrando il valore di bias nella funzione di attivazione, si può spostare la curva di attivazione orizzontalmente lungo l'asse degli input.

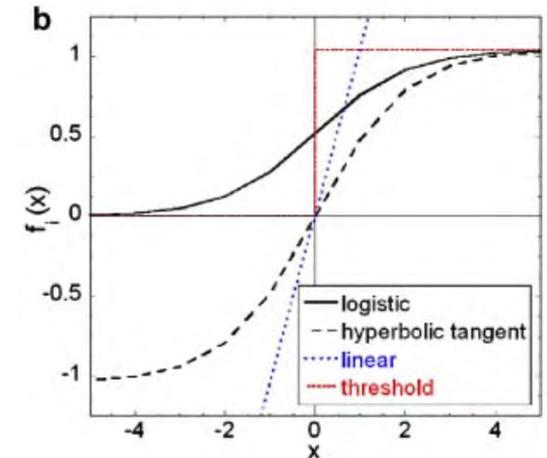
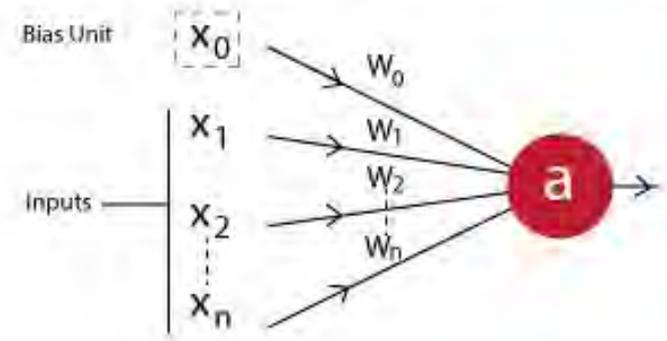
$w_0, w_1, w_2, \dots, w_N$: **Pesi** su ciascun ingresso. Si noti che anche l'unità di bias ha un peso.

a : **Output** del neurone che è calcolata come:
$$a = f\left(\sum_{i=0}^N w_i x_i\right)$$

F è nota come **funzione di attivazione**.

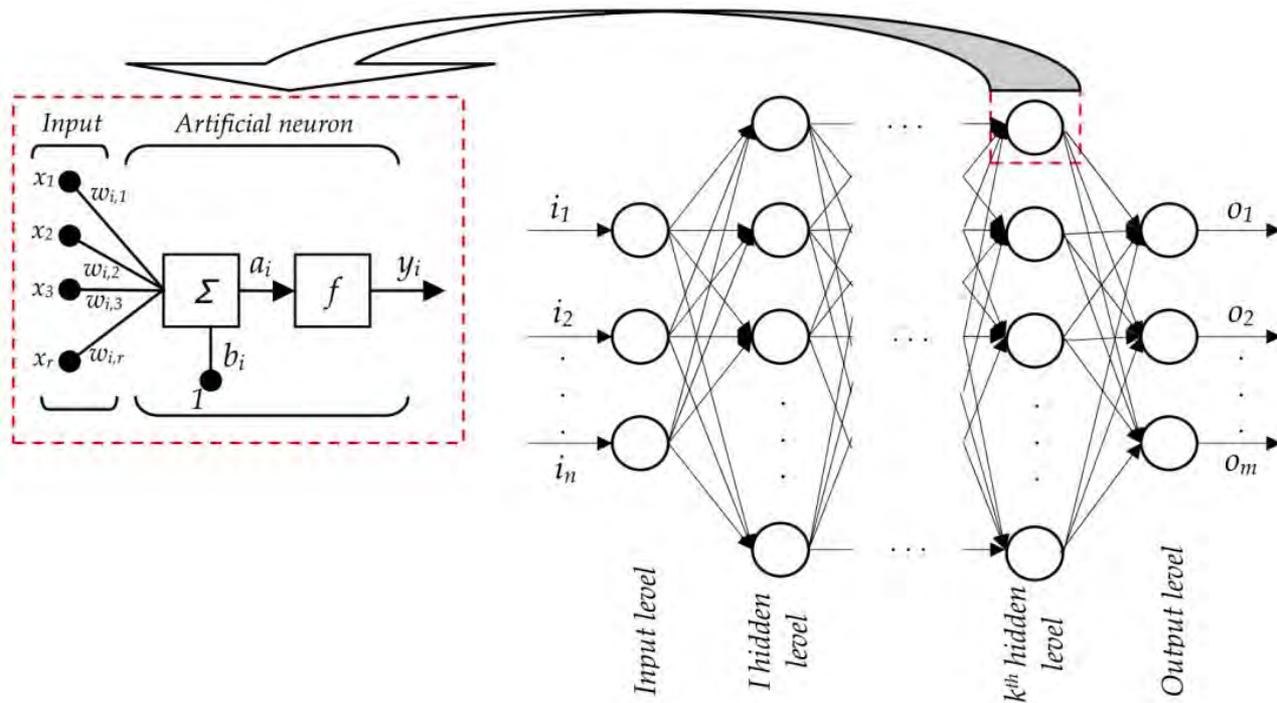
Può essere una funzione gaussiana, una funzione logistica, una funzione iperbolica o anche una funzione lineare in casi semplici e serve ad introdurre una non linearità nella rete. Ciò permette alla rete di apprendere relazioni complesse tra le diverse feature di input e di produrre output non lineari.

Diagram 1: Single NN Working

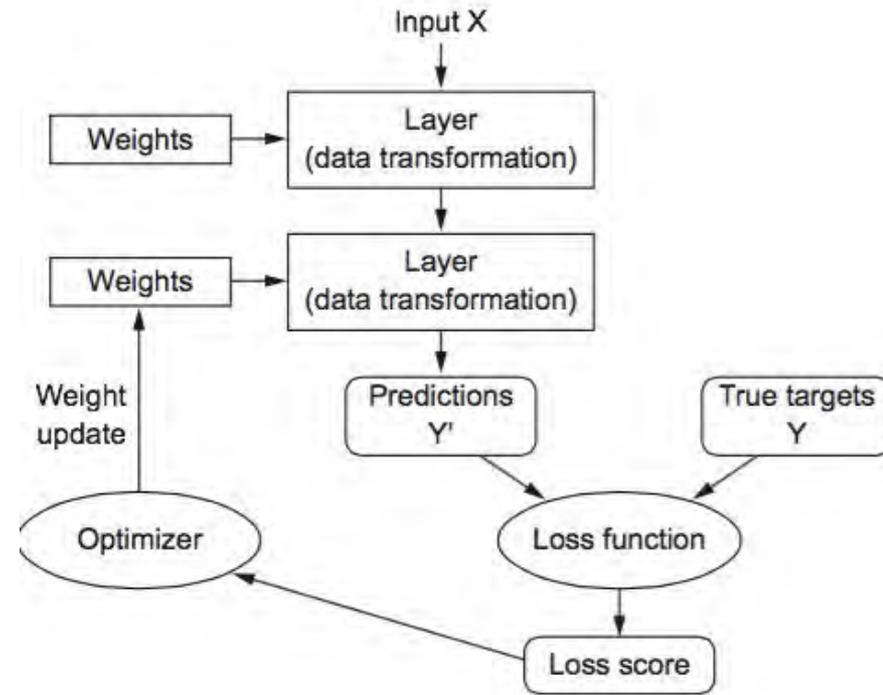


Una rete neurale è costituita da:

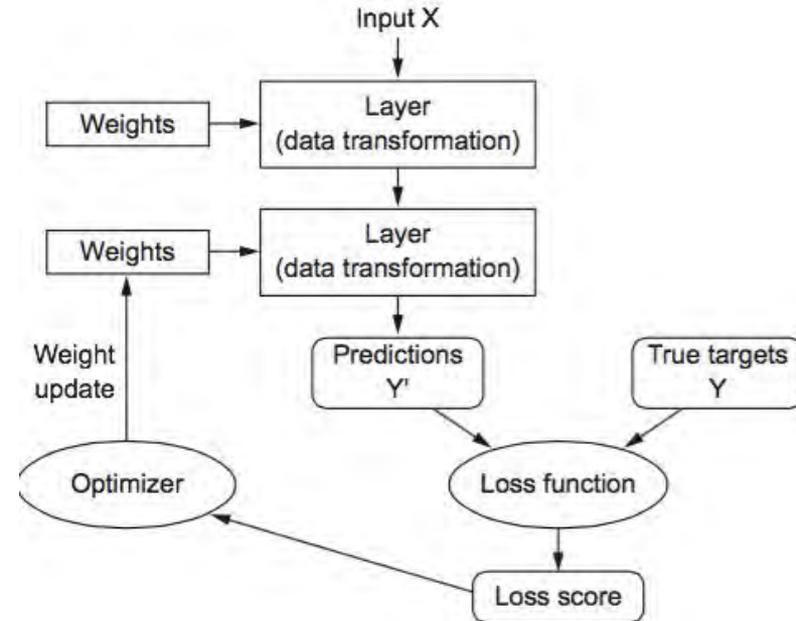
- Un insieme di nodi (neuroni), o unità connesse da collegamenti.
- Un insieme di pesi associati ai collegamenti.
- Un insieme di soglie o livelli di attivazione.



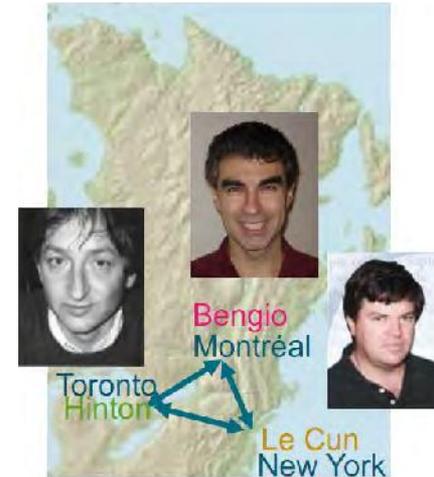
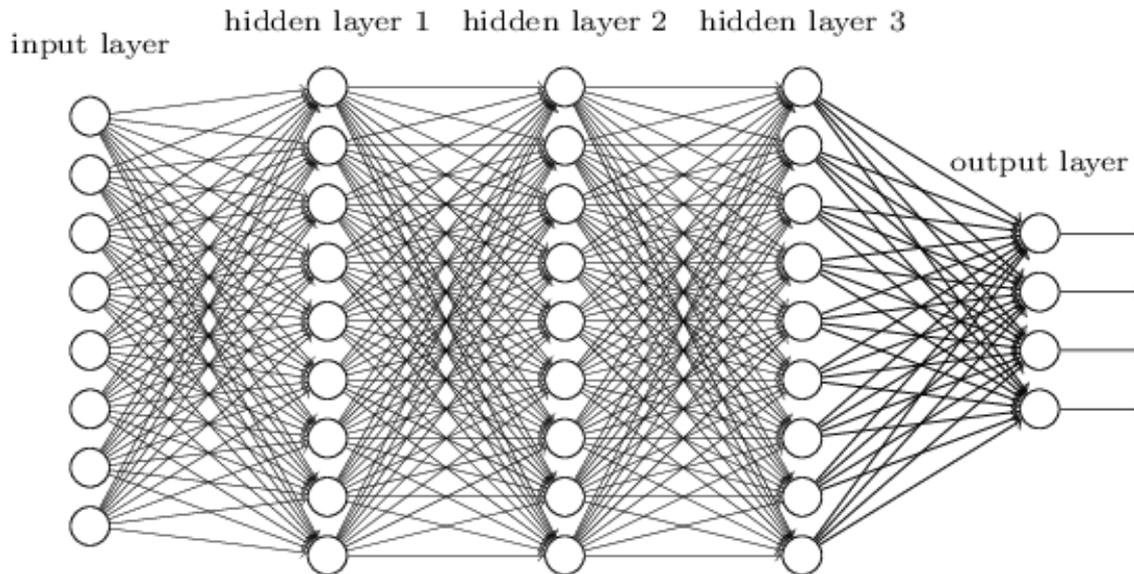
- Layers che sono combinati in una rete (o modello)
- I dati di input e gli obiettivi corrispondenti (*targets*)
- La funzione di costo (*loss function*), che definisce il segnale di retroazione utilizzato per l'apprendimento
- L'ottimizzatore (*optimizer*), che determina come procede l'apprendimento



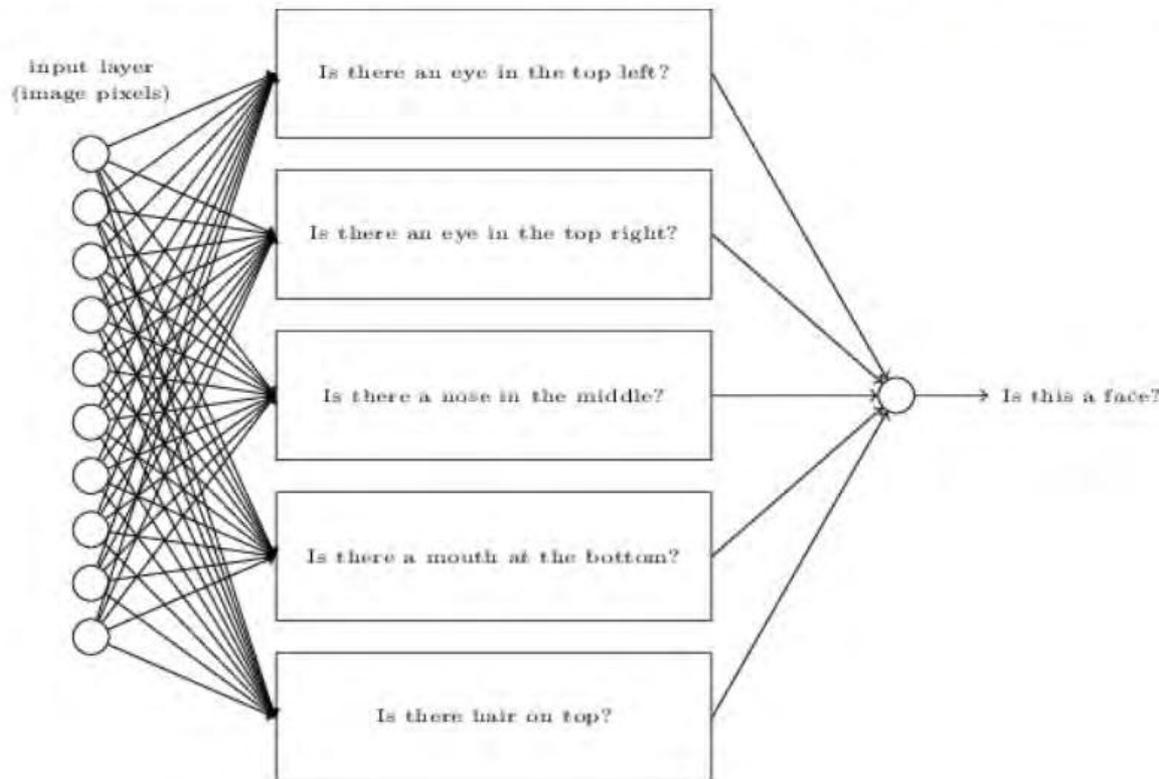
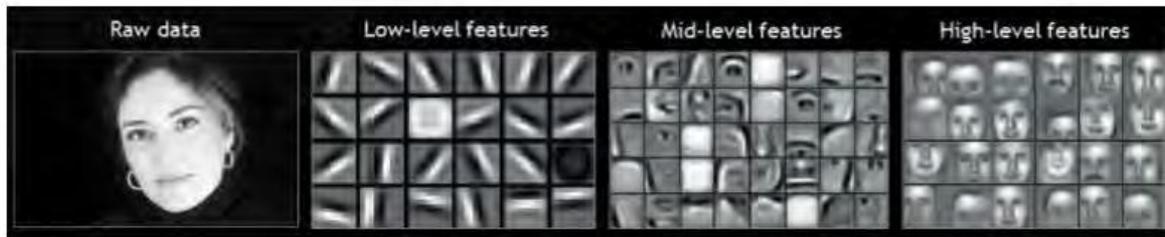
- I pesi sono fondamentali perché determinano quanto ciascun input influenzi l'output di un neurone o di un'intera rete.
- Un peso maggiore indica che l'input corrispondente è considerato più importante, mentre un peso minore indica che l'input è meno rilevante.
- **I pesi consentono alla rete di apprendere e catturare le relazioni complesse tra i dati di input e gli output desiderati.**
- Durante la fase di addestramento, i pesi vengono regolati iterativamente in base all'errore tra gli output generati dalla rete e gli output desiderati.
- Questo processo è noto come algoritmo di apprendimento e mira a minimizzare l'errore della rete.

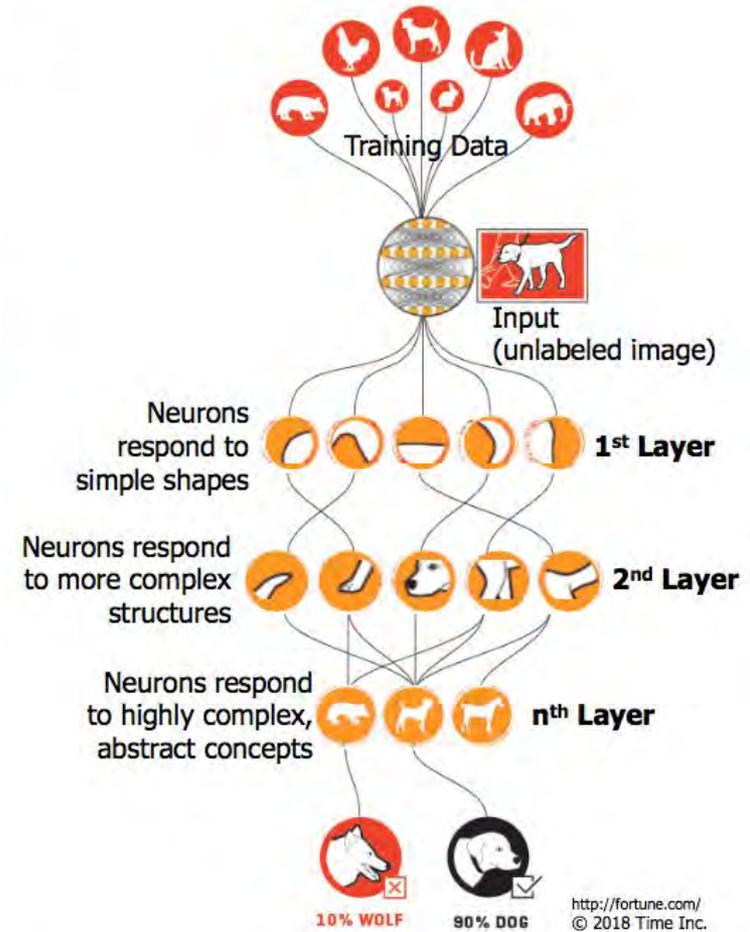
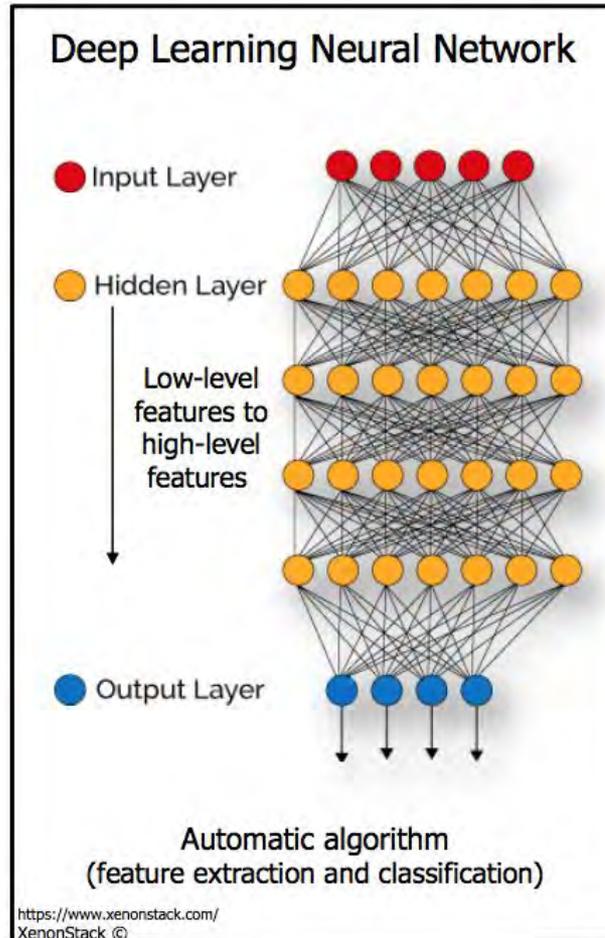


Il Deep learning è una tipologia di rete neurale profonda. La definizione di deep è associata al numero di strati nascosti presenti che contengono molti nodi con una moltitudine di connessioni.



Ricercatori premiati con il premio **ACM Turing Award 2019** per attività di ricerca su back propagation, CCN, GAN, high-dimensional word embedding and attention, etc..







Deep learning - neural style

Estrarre delle caratteristiche e dei pattern da un'immagine e trasferirle ad un'altra



Notte stellata di Vincent Van Gogh + foto del campus di Stanford

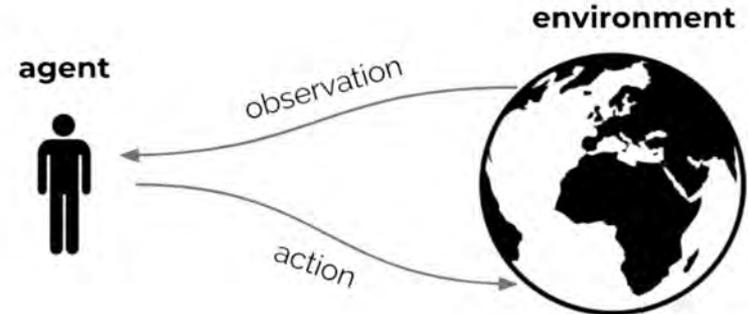
Gen Studio è una collaborazione del Met, Microsoft e MIT per esplorare visualmente il tema della generazione di immagini di opere d'arte.

In particolare Gen Studio permette di:

- Estrarre la struttura delle opere d'arte presenti al MET;
- Interpolare tra le caratteristiche delle opere per generare nuovi oggetti.



- Noi, e gli altri essere viventi, impariamo dall'interazione con il nostro ambiente
- Noi impariamo sbagliando
(Es: imparare ad andare in bicicletta)
- Questa modalità è diversa rispetto ad altre tipologie di learning perché è:
 - Una modalità attiva e non passiva
 - Interazione è sequenziale, le future interazioni possono dipendere da quelle precedenti
- Nella nostra interazione con l'ambiente siamo focalizzati sugli obiettivi (*goal directed*)



Che cos'è



Quando usarlo

Una classe di algoritmi che imparano a svolgere un compito semplicemente cercando di massimizzare i premi che riceve per le sue azioni (Es: massimizzare i premi ricevuti per i rendimenti crescenti di un portafoglio di investimenti).

Quando non sono disponibili molti dati di training e non è possibile definire chiaramente quale è l'output finale ideale. L'unico modo per conoscere l'ambiente è attraverso l'interazione con esso.

Esempio

L'obiettivo è raggiungere un obiettivo, mentre le "situazioni" sono le varie configurazioni (ad esempio della scacchiera) e le "azioni" sono le mosse valide. Questo tipo di tecniche, fondamentalmente andando per tentativi, imparano un comportamento che lo porti con successo all'obiettivo.

Caratteristiche

- **Un ambiente inizialmente sconosciuto:** è necessario esplorare l'ambiente per ottenere informazioni su di esso;
- **Feedback ritardato:** dopo aver intrapreso un'azione, potrebbe essere necessario del tempo per realizzare pienamente le conseguenze a lungo termine di tale azione;
- **Processo decisionale sequenziale:** la ricompensa complessiva ricevuta è in genere il risultato di una sequenza di più azioni piuttosto che una singola azione indipendente.





Reinforcement learning - esempio

Esempio: un robot deve uscire da un labirinto

Per incoraggiare il robot a trovare il percorso più breve, viene applicata una piccola penalità di 0,04 unità ogni volta che il robot si sposta in una cella vuota (bianca) e gli ostacoli sono posti intorno al labirinto (contrassegnati in grigio) che provocano una penalità maggiore di 0,75 unità se il robot entra in una cella contenente una di esse.

Il robot può solo muoversi verso l'alto, il basso, a sinistra o a destra (ovvero, le mosse diagonali non sono consentite). Tuttavia, un livello di incertezza è associato a ciascun movimento, in modo tale che vi sia solo un 80% di probabilità che il robot si muova nella direzione desiderata e un 20% di probabilità che il robot si sposti ad angolo retto rispetto alla direzione desiderata.

	0	1	2	3	4	5	6
0	S	■	□	□	□	□	□
1	□	□	□	■	■	□	■
2	■	■	■	□	□	□	■
3	□	□	□	□	■	■	□
4	□	■	■	■	□	□	□
5	□	■	□	□	□	□	□
6	□	□	□	■	□	□	G



Reinforcement learning - esempio

Il diagramma mostra la direzione ottimale per il robot da prendere in ogni quadrato della griglia.

	0	1	2	3	4	5	6
0	↓	→	→	→	→	↓	←
1	→	→	↑	↓	↓	↓	←
2	↓	↓	↓	↓	←	←	↓
3	↓	←	←	←	↓	↓	↓
4	↓	↑	↓	↓	→	↓	↓
5	↓	→	→	→	→	↓	↓
6	→	→	↑	↑	→	→	↓



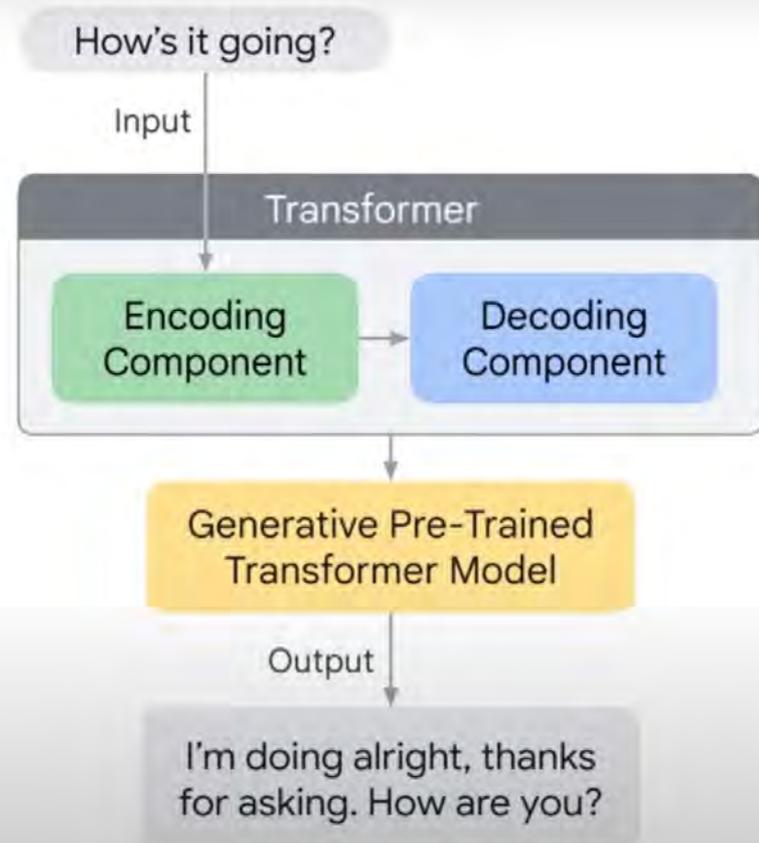
Ritorniamo a ChatGPT e ai Large Language Model

ChatGPT è un modello di linguaggio sviluppato da OpenAI messo a punto con **tecniche di machine learning non supervisionato e ottimizzato con tecniche di apprendimento supervisionato e per rinforzo.**

How it Works

Pre-Training:

- Large amount of Data
- Billions of parameters
- Unsupervised learning



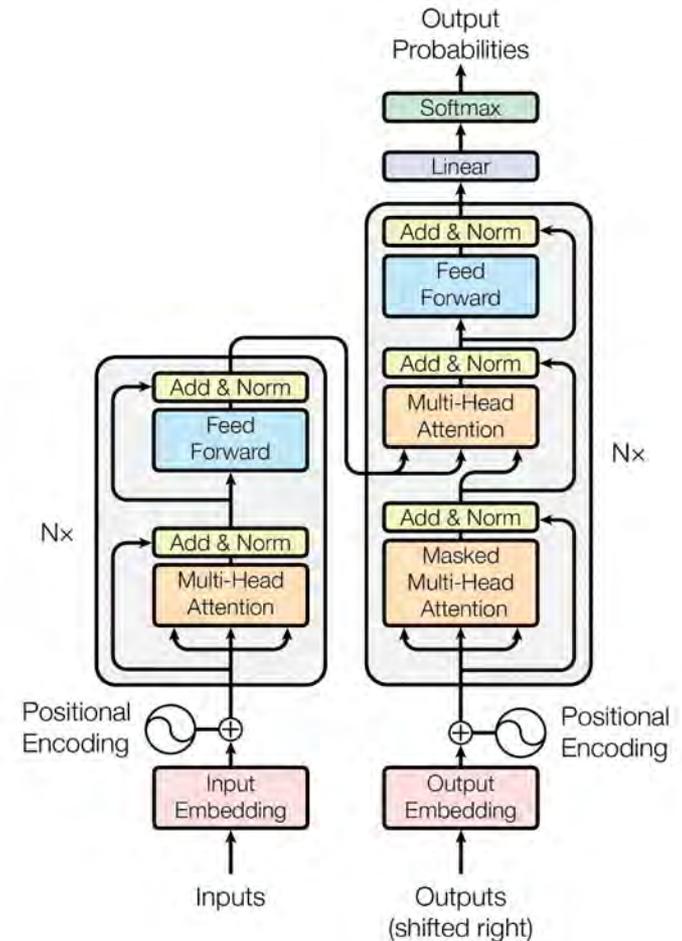


Transformers

Nel 2017 Vaswani et al. ha pubblicato un documento, "**Attention is all you need**", per introdurre i **Transformer**, una nuova classe di modelli di apprendimento automatico basati sull'attenzione.

Contrariamente alle reti neurali ricorrenti, il meccanismo dell'attenzione consente di vedere l'intera frase (o anche il paragrafo) in una volta anziché in modo sequenziale una parola alla volta.

Questo permette di **dare un senso alle lunghe sequenze linguistiche, creando connessioni tra diverse parti della sequenza** e migliorando la comprensione del contesto in cui si trova una parola.



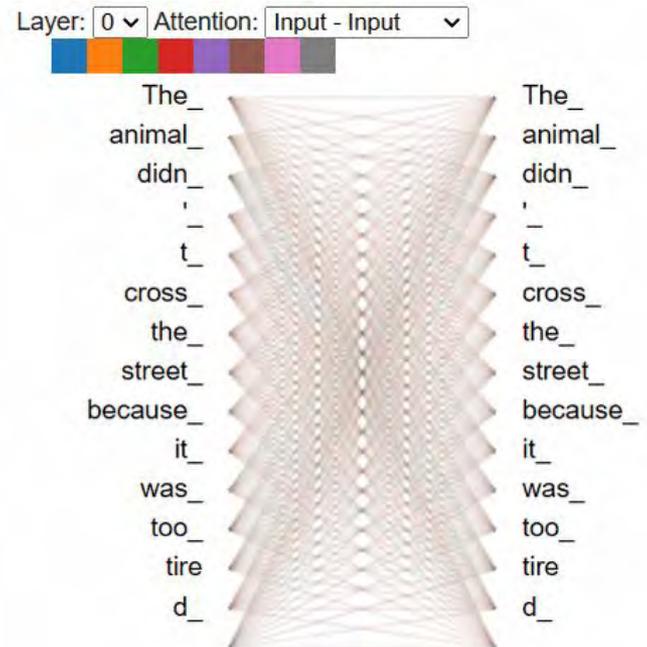


Transformers (2)

- i transformers intervengono per catturare le relazioni tra i token e l'ordine in cui compaiono nella frase.
- I pesi nella rete neurale rappresentano i parametri che determinano l'importanza relativa dei segnali di input. Durante l'addestramento, i pesi vengono aggiornati iterativamente in base all'errore tra l'output generato dal modello e l'output desiderato, al fine di migliorare le prestazioni della rete.

Modelli:

- GPT - **Generative Pre-trained Transformer**
- BERT - **Bidirectional Encoder Representations from Transformers**





Addestrare un transformer

Procedimento

- Addestramento non supervisionato su una dataset di testo di grandi dimensioni
- Addestramento supervisionato (fine tuning) su un dataset specializzato con dati di input e output per un task specifico

Modelli pre-trained

L'addestramento di un modello richiede risorse importanti a livello di dataset e potenza computazionale. Si possono anche usare modelli pre addestrati (Huggingfaces, Bert di Google, i modelli GPT di OpenAI) e molto altro come i modelli preaddestrati rilasciati da Meta



Apprendimento per rinforzo dal feedback umano (RLHF)

L'apprendimento per rinforzo ordinario, in cui gli agenti apprendono dalle proprie azioni sulla base di una "funzione di ricompensa", è difficile da applicare alle attività di elaborazione del linguaggio naturale perché le ricompense spesso non sono facili da definire o misurare.

Gli LLM possono spesso generare **output che sono falsi, tossici o semplicemente non utili per l'utente.**

Come si crea/codifica una loss function per definire **concetti** come: **divertente, etico o non pericoloso** ?

Open AI nel 2017 ha sviluppato un algoritmo di apprendimento per rinforzo dal feedback umano che addestra un "**modello di ricompensa**" **direttamente dal feedback umano e utilizza il modello come funzione di ricompensa per ottimizzare la politica di un agente utilizzando l'apprendimento per rinforzo (RL).** Il feedback umano viene raccolto chiedendo agli umani di classificare le istanze del comportamento dell'agente.



Supervised fine tuning - Reinforcement learning from human feedback

Step 1

Collect demonstration data, and train a supervised policy.

A prompt is sampled from our prompt dataset.



A labeler demonstrates the desired output behavior.



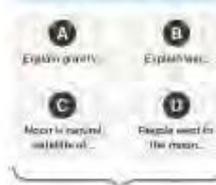
This data is used to fine-tune GPT-3 with supervised learning.



Step 2

Collect comparison data, and train a reward model.

A prompt and several model outputs are sampled.



A labeler ranks the outputs from best to worst.



This data is used to train our reward model.



Step 3

Optimize a policy against the reward model using reinforcement learning.

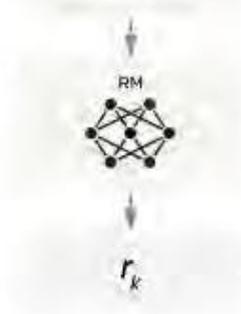
A new prompt is sampled from the dataset.



The policy generates an output.



The reward model calculates a reward for the output.



The reward is used to update the policy using PPO.



Cosa c'è dietro l'angolo

Autonomous AI

Generative agents



Autonomous agents

Come modello di linguaggio AI, ChatGPT può essere considerato un agente intelligente.

Un agente intelligente è un sistema in grado di percepire il suo ambiente, ragionarci sopra e intraprendere azioni basate sulla sua comprensione per raggiungere scopi o obiettivi specifici.

ChatGPT può percepire ed elaborare input in linguaggio naturale, ragionare su di essi in base ai suoi numerosi dati di addestramento e generare risposte appropriate o eseguire attività specifiche.

Tuttavia, **l'autonomia di ChatGPT è limitata dalla sua stretta attenzione all'elaborazione e alla comprensione del linguaggio.** Può solo "prendere decisioni" nell'ambito della generazione di testo pertinente in base all'input e **non possiede la capacità di adattarsi o apprendere in modo indipendente oltre la sua formazione.**



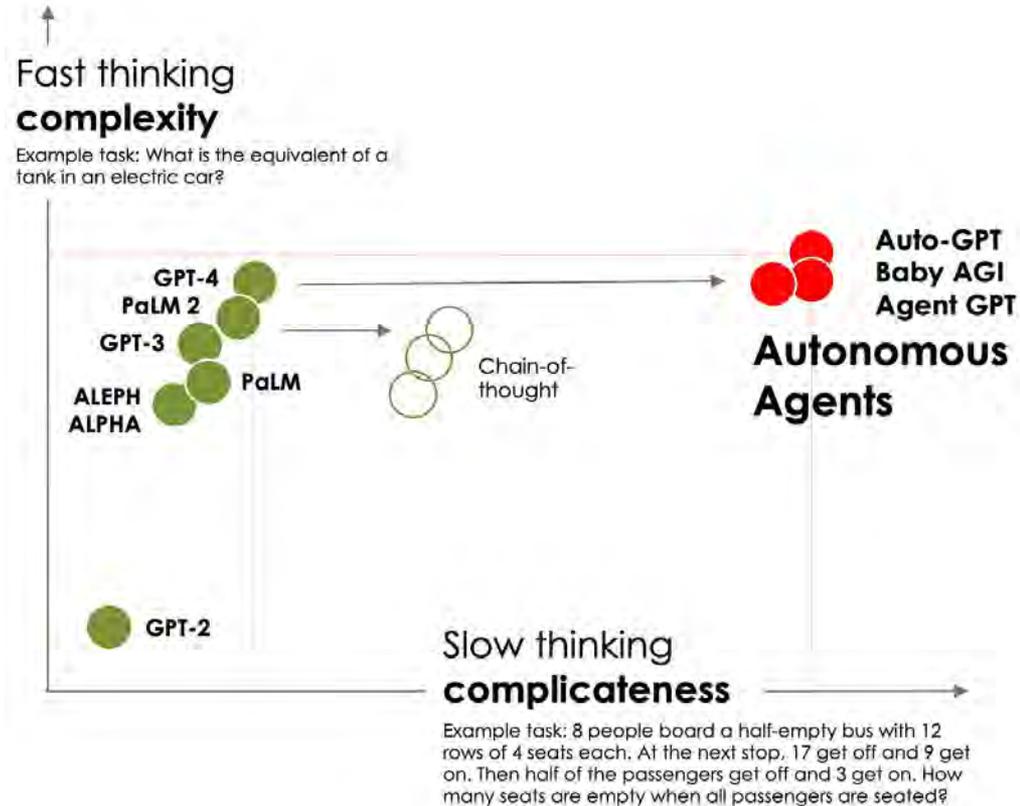
Autonomous agents (2)

Gli agenti autonomi (autonomous agents) sono invece modelli che sono capaci di **"pensare lentamente"**.

Risolvono domande complicate, in cui si giunge all'obiettivo poco a poco tramite risultati intermedi.

Tra le funzionalità aggiuntive:

- navigare su internet
- operazione di lettura/scrittura
- interagire con altri agenti GPT
- eseguire codice

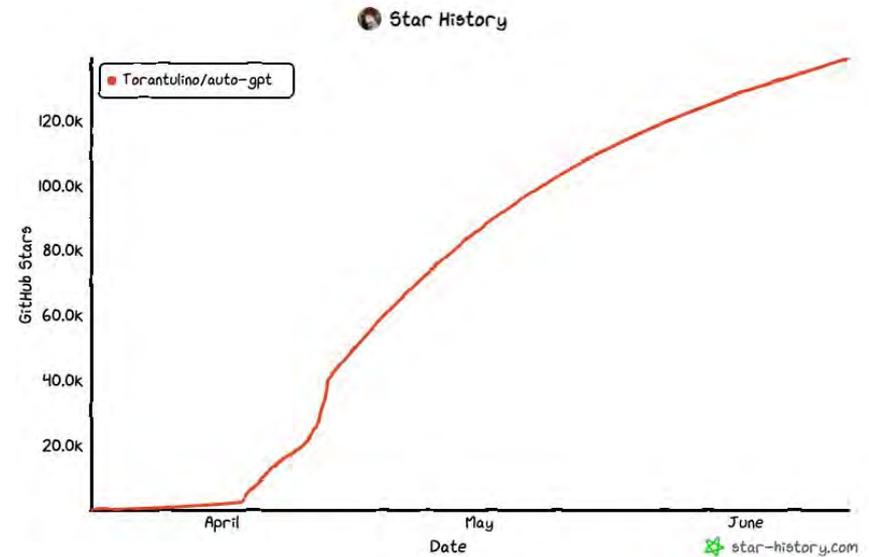




AutoGPT

Auto-GPT è un agente intelligente capace di scomporre un obiettivo assegnatogli in linguaggio naturale e di dedurre delle sotto-attività più semplici che esegue mediante Internet e altri strumenti all'interno di un'interazione automatica.

A differenza dei sistemi interattivi come ChatGPT, che necessitano dell'inserimento di comandi manuali per ogni attività, **Auto-GPT** si assegna nuovi sotto-obiettivi funzionali al conseguimento di un obiettivo maggiore, senza la necessità di un costante input da parte umana e così facendo crea e modifica i propri prompt con istanze ricorsive e in risposta alle nuove informazioni acquisite.





Features:

- Accesses the internet for queries and gathering information
- Long and short-term memory management
- GPT-4 instances for text generation
- Accesses popular websites and platforms
- File storage and summarization with GPT-3.5

★ **Embarking on a new goal:** Create a timeline and checklist for organizing a corporate conference for 200 attendees in Rome at the end of June. Please provide a list of 3 available hotel for hosting the conference with the price of rooms and catering

🧠 **Thinking...** (Restart if this takes more than 30 seconds)

★ **Added task:** Determine the conference dates and location, ensuring availability and accessibility for attendees.

★ **Added task:** Choose 3 potential hotels for hosting the conference, considering factors such as price, amenities, and catering options.

★ **Added task:** Contact the hotels to obtain room and catering pricing for the estimated number of attendees.

★ **Added task:** Create a timeline and checklist for organizing the conference, including tasks such as booking hotel rooms, arranging travel, and planning event activities.

🧠 **Thinking...** (Restart if this takes more than 30 seconds)



AgentGPT (2)

First, we need to identify available hotels for hosting the conference. After researching and considering factors such as location, amenities, and pricing, I recommend the following three options:

1. Grand Hotel Palace Rome – This hotel is located close to major attractions in Rome and offers a variety of event spaces suitable for hosting a conference. The price for the conference room is €3,000 per day, and catering costs €50 per person.
2. Hotel Bernini Bristol – This hotel is situated in the center of Rome and also offers several event spaces for hosting conferences. The price for renting the conference room is €2,500 per day, and catering costs €45 per person.
3. Parco dei Principi Grand Hotel & SPA – This hotel is 20 minutes away from the city center, but offers a spacious conference room that can accommodate up to 300 attendees. The price for the conference room is €2,800 per day, and catering costs €55 per person.

Next, we need to create a timeline and checklist for organizing the conference. This timeline should be based on the specific details of the event, and should include tasks such as:

- Booking hotel rooms for attendees and speakers
- Arranging travel and transportation for attendees
- Planning the conference agenda and selecting speakers
- Coordinating catering and other event logistics
- Promoting the conference and managing registrations

To ensure that these tasks are completed efficiently and effectively, it may be helpful to assign specific responsibilities to different members of the team or to work with an event planner. By carefully considering all of the necessary steps and making strategic decisions along the way, we can create a successful and memorable conference in Rome for all attendees.



HuggingGPT

25 Maggio
2023

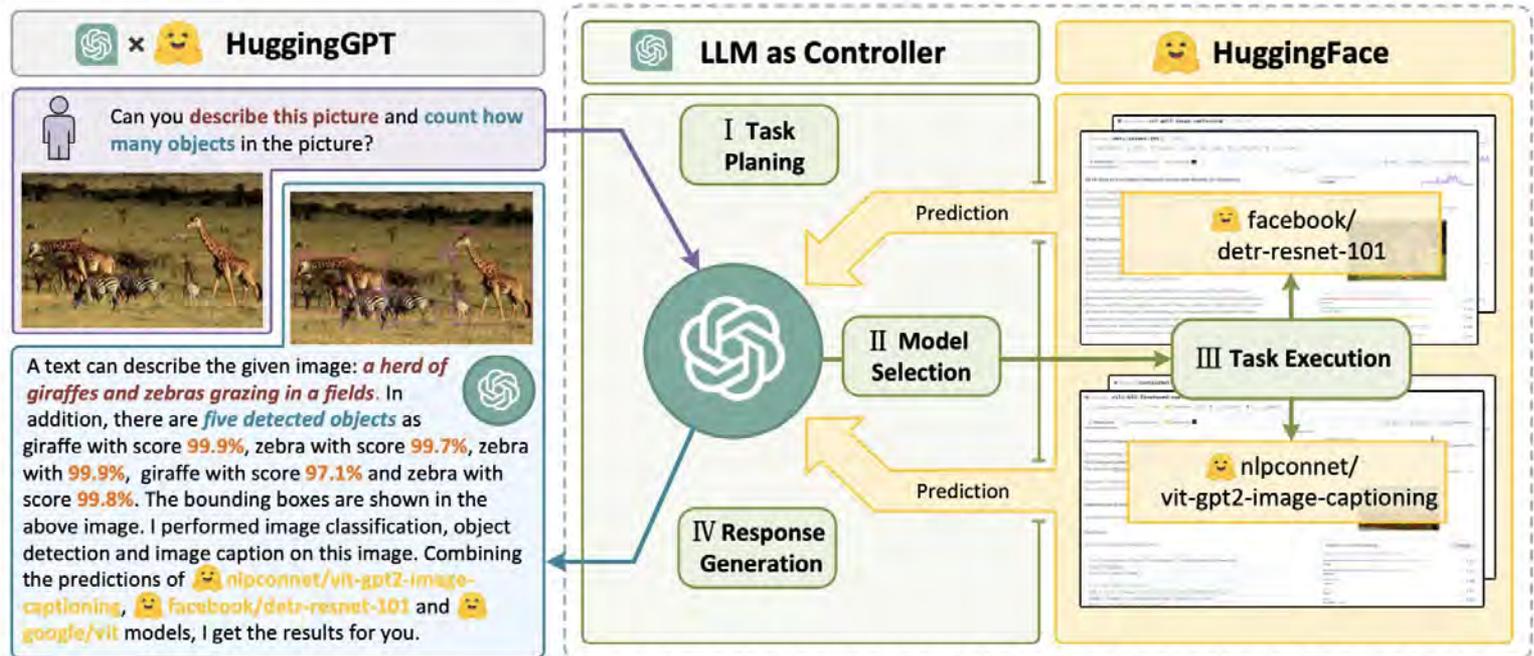


Figure 1: Language serves as an interface for LLMs (e.g., ChatGPT) to connect numerous AI models (e.g., those in Hugging Face) for solving complicated AI tasks. In this concept, an LLM acts as a controller, managing and organizing the cooperation of expert models. The LLM first plans a list of tasks based on the user request and then assigns expert models to each task. After the experts execute the tasks, the LLM collects the results and responds to the user.



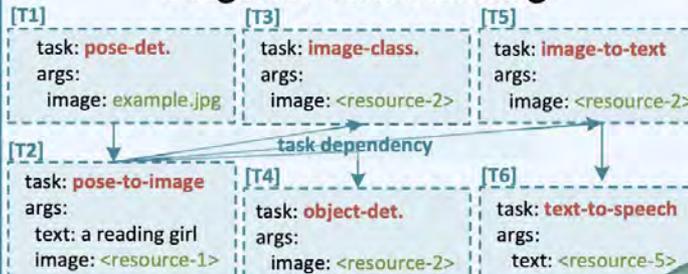
HuggingGPT

25 Maggio
2023

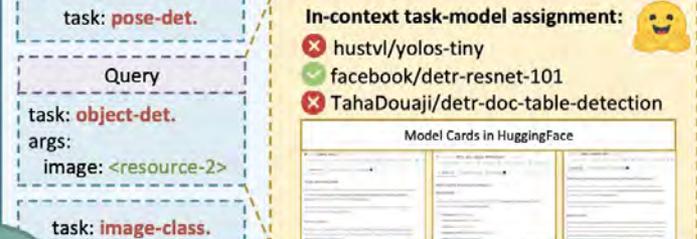
Please generate an image where a girl is reading a book, and her pose is the same as the boy in the image example.jpg, then please describe the new image with your voice.

Request

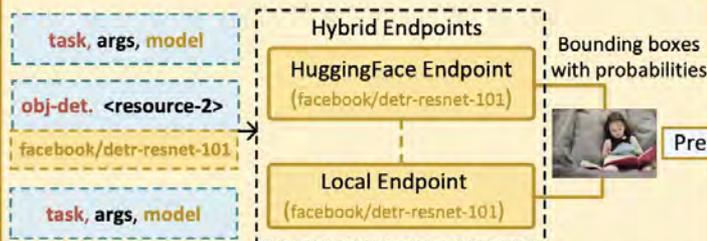
Stage #1: Task Planning



Stage #2: Model Selection

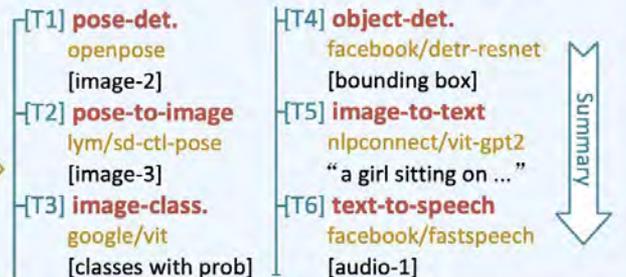


Stage #3: Task Execution

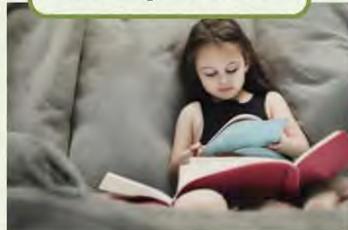


Predictions

Stage #4: Response Generation



Response



a girl sitting on a bed reading a book

[Text-1] = <resource-5>



[Audio-1]

[Image-1] = example.jpg [Image-2] = <resource-1> [Image-3] = <resource-2>

[Image-4]

The image you gave me is of "boy". The first thing I did was use 🤖 [OpenCV's openpose model](#) to analyze the pose of the boy in the image. I fed that image, specifically located at [Image-1], into the model to get an output image of the pose, located at [Image-2]. Then I take that pose and generate a new image, located at [Image-3], using 🤖 [llyasviel/sd-controlnet-openpose](#) and the instruction "a girl is reading". Next, I ran object detection on the image generated in the previous step, to get predictions of the objects present in the image, including the box location. These predictions were run through the 🤖 [facebook/detr-resnet-101](#) model. The box was drawn on the image, which is located at [Image-4]. Then, I used the predictions of a image classification model 🤖 [google/vit-base-patch16-224](#) and a image caption model a 🤖 [nlpconnect/vit-gpt2-image-captionin](#) model to generate the caption for newly generated image. It generated text: "a girl sitting on a bed reading a book". Lastly, I ran the 🤖 [facebook/fastspeech2-en-ljspeech](#) model to convert the generated text into audio, located at [Audio-1].



Generative agents

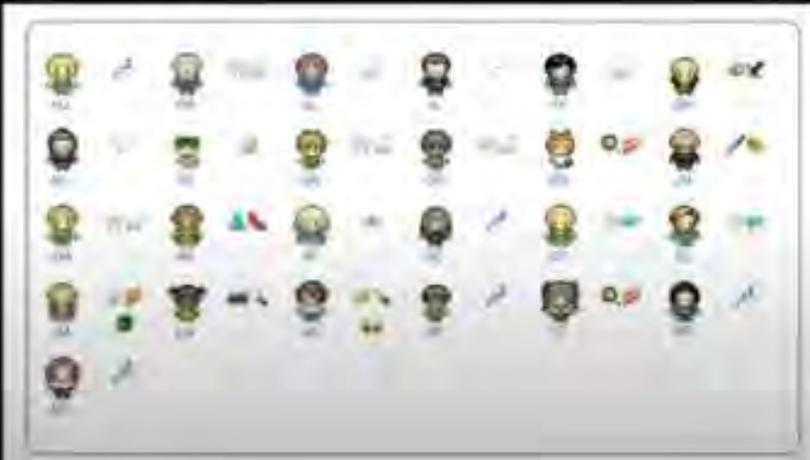
“Westworld lured millions of us into a fantasy of human-like robots in a Wild West-themed world. Could it be real one day?”

Stanford/Google researchers just told us how they used AI to make “generative agents.”



Figure 1: Generative agents create believable simulacra of human behavior for interactive applications. In this work, we demonstrate generative agents by populating a sandbox environment, reminiscent of The Sims, with twenty-five agents. Users can observe and intervene as agents they plan their days, share news, form relationships, and coordinate group activities.

**The world is populated by
25 generative agents**



**Each agent is initiated with
a paragraph. And *that is it.***

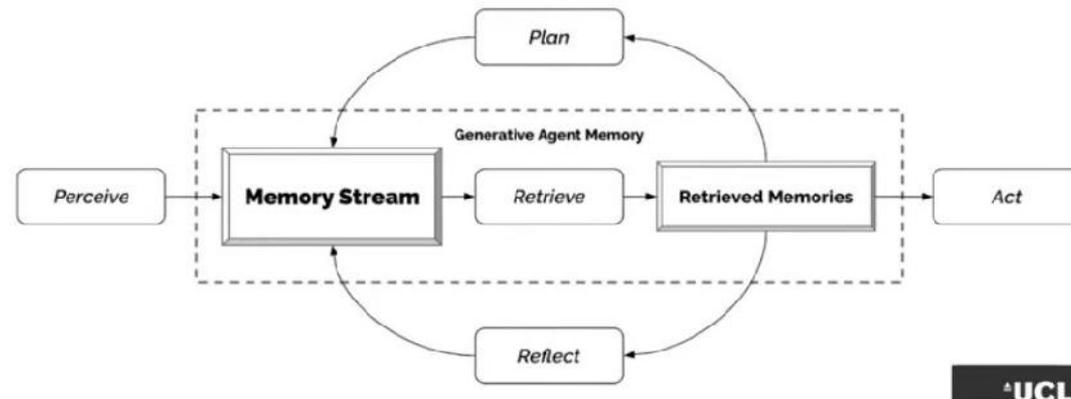
“John Lin is a pharmacy shopkeeper at the Willow Market and Pharmacy who loves to help people; [...] John Lin knows the Moreno family somewhat well — the husband Tom Moreno and the wife Jane Moreno.”



Generative agents

How can we leverage the power of generative models to simulate believable human behavior?

A novel agent architecture that remembers, reflects, and plans based on constantly growing memories and cascading social dynamics.





Generative agents

- Gli agenti generativi si svegliano, cucinano la colazione e si dirigono al lavoro; gli artisti dipingono, mentre gli scrittori scrivono; formano opinioni, si notano reciprocamente e iniziano conversazioni; ricordano e riflettono sui giorni passati mentre pianificano il giorno successivo.
- Unendo grandi modelli linguistici con agenti computazionali interattivi, **questo paper introduce schemi architettonici e di interazione per abilitare simulazioni credibili del comportamento umano.**
- Ad esempio, partendo solo da una singola idea specificata dall'utente, che un agente desidera organizzare una festa di San Valentino, gli agenti diffondono autonomamente inviti alla festa nei due giorni successivi, fanno nuove conoscenze, si chiedono reciprocamente di uscire per la festa e si coordinano per presentarsi insieme alla festa al momento giusto.



Normativa e attività della UE



AI nei progetti europei

L'UE ha supportato l'intelligenza artificiale per molti anni, in gran parte attraverso i suoi programmi di ricerca e sviluppo, 7° PQ e Horizon 2020.

42 nuovi progetti su AI e la robotica in questi campi:

INNOVATION IN AI, DATA AND ROBOTICS

AI, Data and Robotics for the Green Deal

INNOVATION IN AI, DATA AND ROBOTICS

AI, Data and Robotics at work

LEADERSHIP IN AI BASED ON TRUST

Tackling gender, race and other biases in AI

LEADERSHIP IN AI BASED ON TRUST

Verifiable robustness, energy efficiency and transparency for Trustworthy AI:

Scientific excellence boosting industrial competitiveness

TOMORROW'S DEPLOYABLE ROBOTS: EFFICIENT, ROBUST, SAFE, ADAPTIVE AND TRUSTED





Libro bianco sull'intelligenza artificiale

“L'Intelligenza Artificiale, oggi, può guidare al posto nostro, prendersi cura delle persone anziane o malate, svolgere lavori pericolosi o usuranti, aiutarci a prendere decisioni ponderate, basate sulla gestione razionale di grandi moli di dati. Ci può permettere di comunicare in lingue che non conosciamo, può seguirci nello studio e aumentare le esperienze culturali o di intrattenimento a nostra disposizione.

Nella PA può essere utilizzata con profitto nel sistema sanitario, scolastico, giudiziario, nel pubblico impiego, nella sicurezza e, più in generale, nella gestione delle relazioni coi cittadini, che possono venire semplificate e rese allo stesso tempo più efficaci, veloci ed efficienti. “



Le sfide per l'IA al servizio del cittadino

- **Etica** – responsabilità, qualità e neutralità dei dati
- **Tecnologica** - creazione di algoritmi sempre più efficaci
- **Competenze** – skills necessari a sviluppare soluzioni di IA
- **Dati** – qualità ed organizzazione
- **Contesto legale** – garantire trasparenza
- **Bilanciamento interessi collettività e individui** – trasparenza atti amministrativi, protezione dati personali e accountability
- **Accompagnare la trasformazione del paese** – azioni necessarie per favorire utilizzo IA nel rapporto tra Stato, cittadini e imprese
- **Prevenire le disuguaglianze** – accessibilità per tutti e rimozione del bias
- **Misurazione dell'impatto** – metriche di customer satisfaction / ottimizzazione dei processi
- **L'essere umano** – strumenti per facilitare la comprensione ed il coinvolgimento delle persone

ENTRO IL
2025

L'INTELLIGENZA ARTIFICIALE
POTREBBE

MOLTO PROBABILMENTE

Incidere una canzone che arrivi nella Top 100 di Billboard
Creare un'opera d'arte valutata 100.000\$
Scrivere una serie TV di successo

POCO PROBABILMENTE

Firmare un best seller per il New York Times
Scrivere un film da Oscar
Vincere il premio Pulitzer per il giornalismo

Fonte: AI takes center stage, Bot.Me: A revolutionary partnership, PwC 2017

QUALI POSSONO ESSERE I POTENZIALI DANNI ASSOCIATI A SISTEMI IA

DIGITALI	FISICI	POLITICI
<ul style="list-style-type: none"> ✓ Phishing automatizzato, creazione di email false, siti web e link per sottrarre informazioni. 	<ul style="list-style-type: none"> ✓ Terrorismo automatizzato che utilizza droni o veicoli autonomi come armi. 	<ul style="list-style-type: none"> ✓ Propaganda, attraverso immagini e video falsi facilmente generabili.
<ul style="list-style-type: none"> ✓ Hacking massivo, attraverso la scoperta automatizzata delle vulnerabilità dei sistemi. 	<ul style="list-style-type: none"> ✓ Sciami di Robot che cercano di raggiungere lo stesso obiettivo. 	<ul style="list-style-type: none"> ✓ Rimozione automatica del dissenso, grazie alla possibilità di trovare, analizzare e rimuovere automaticamente testi ed immagini.
<ul style="list-style-type: none"> ✓ Ingannare sistemi IA sfruttando a proprio vantaggio i difetti nell'interpretazione della realtà da parte dell'IA. 	<ul style="list-style-type: none"> ✓ Attacchi remoti, resi possibili dal fatto che i robot autonomi possono essere controllati da qualunque distanza. 	<ul style="list-style-type: none"> ✓ Persuasione personalizzata, con l'utilizzo di informazioni pubbliche per influenzare l'opinione di qualcuno.

Fonte: AI experts list the real dangers of artificial intelligence, Dave Gershgorn Feb. 2018



IA e GDPR (Regolamento n. 2016/679)

Il GDPR afferma: *"L'interessato ha il diritto di non essere soggetto a una decisione basata esclusivamente sull'elaborazione automatica."*

La chiave qui è la parola "esclusivamente", il che significa che se un'organizzazione vuole utilizzare un processo decisionale automatico (per l'elaborazione delle richieste di prestito o degli adeguamenti salariali dei dipendenti), un umano deve esaminare e confermare le conclusioni raggiunte da un algoritmo IA prima di eseguirle.

Una persona può controllare la decisione automatica di una IA solo se è in grado di rintracciare i passaggi che l'hanno originata.



Digital Service Act e AI

La legge sui servizi digitali (DSA) e la legge sui mercati digitali (DMA) mirano a creare uno spazio digitale più sicuro in cui siano protetti i diritti fondamentali degli utenti e a creare condizioni di parità per le imprese. **Il DSA introduce misure per migliorare la trasparenza dei sistemi di raccomandazione e della pubblicità.**

- Ai sensi dell'Art. 14(1), i fornitori di servizi intermediari devono includere nelle loro condizioni generali informazioni sulle misure e gli strumenti utilizzati per la moderazione dei contenuti, comprese le decisioni algoritmiche. Inoltre indica come i destinatari del loro servizio siano adeguatamente informati su come gli algoritmi influenzano e condizionano il modo in cui le informazioni vengono visualizzate.
- Ai sensi dell'Art. 27(1), Nei sistemi di raccomandazione i fornitori devono specificare nelle loro condizioni generali "i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché eventuali opzioni per i destinatari del servizio per modificare o influenzare tali parametri principali."



Il Parlamento europeo in data 14 giugno 2023 ha dato il via libera all' **Artificial Intelligence Act**, che regolerà l'Intelligenza Artificiale nel rispetto dei diritti e dei valori dell'Unione Europea. I membri del Parlamento Europeo mirano a garantire che i sistemi di intelligenza artificiale siano supervisionati da persone, **siano sicuri, trasparenti, rintracciabili, non discriminatori ed ecologicamente sostenibili**. Vogliono anche avere una definizione uniforme per l'AI progettata per essere neutrale rispetto alla tecnologia, in modo che possa applicarsi ai sistemi di AI di oggi e di domani.

- **Si tratta della prima regolamentazione al mondo sull'Intelligenza Artificiale.**
- **Prevede divieti per sorveglianza biometrica, riconoscimento delle emozioni, sistemi di AI per la polizia predittiva.**
- **Prevede regolamenti per l'AI a scopo generale e modelli di base come GPT.**
- **Prevede il diritto per i cittadini di presentare reclami riguardo ai sistemi di AI.**



AI ACT - misure di trasparenza

I membri del Parlamento Europeo hanno incluso obblighi per i fornitori di modelli di AI che dovranno:

- **garantire una protezione solida dei diritti fondamentali, della salute e della sicurezza, dell'ambiente, della democrazia e dello stato di diritto.**
- Dovranno valutare e mitigare i rischi, rispettare i requisiti di progettazione, informazione e ambiente e registrarsi nel database dell'UE.
- **I modelli di base generativi**, come ChatGPT, dovranno rispettare ulteriori requisiti di trasparenza, come **dichiarare che il contenuto è stato generato da AI, progettare il modello in modo da impedirgli di generare contenuti illegali e pubblicare riepiloghi dei dati protetti da copyright utilizzati per l'addestramento.**

HOME / TECNOLOGIA

ChatGPT come Google Bard? Parla Sam Altman: "pronti a ritirare l'IA dall'Unione Europea"

Il CEO di OpenAI, Sam Altman, ha avvertito che l'azienda potrebbe ritirare i suoi servizi dall'UE, se le figure regole sulle IA saranno troppo restrittive.



AI ACT - Sostenere l'innovazione e proteggere i diritti dei cittadini

La nuova legge promuove le aree di sperimentazione regolamentate, o ambienti controllati, istituiti dalle autorità pubbliche per testare l'AI prima della sua implementazione.

I membri del Parlamento Europeo desiderano rafforzare il diritto dei cittadini di presentare reclami riguardanti i sistemi di AI e ricevere spiegazioni sulle decisioni basate su sistemi di AI ad alto rischio che influiscono significativamente sui loro diritti.



Strategia di ENISA per la AI

L'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) ha pubblicato il 7 giugno 2023 4 report sulle sfide cyber riguardanti l'intelligenza artificiale:

- Multilayer Framework for Good Cybersecurity Practices for AI
- Cybersecurity and privacy in AI - Forecasting demand on electricity grids
- Cybersecurity and privacy in AI - Medical imaging diagnosis
- Artificial Intelligence and Cybersecurity Research





Segnali di allarme

Geoffrey Hinton uno dei Nobel per l'informatica del 2018 ha deciso nel mese di aprile 2023 di lasciare Google per poter intervenire sui rischi dell'IA senza danneggiare la reputazione di Google

Il successo di ChatGPT avrebbe attivato il meccanismo della concorrenza a causa del quale sarebbe ormai impossibile contenere lo sviluppo di sistemi pericolosi, a meno di una loro regolamentazione mondiale.





Segnali di allarme (2)

30 maggio 2023

Un appello lanciato dai leader delle più importanti realtà impegnate in questo ambito: nell'elenco figurano i vertici di OpenAI, Google DeepMind, Alphabet e decine di autorevoli rappresentanti del mondo accademico.

Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.

Signatories:

AI Scientists Other Notable Figures

Geoffrey Hinton

Emeritus Professor of Computer Science, University of Toronto

Yoshua Bengio

Professor of Computer Science, U. Montreal / Mila

Demis Hassabis

CEO, Google DeepMind

Sam Altman

CEO, OpenAI

Dario Amodei

CEO, Anthropic

Dawn Song

Professor of Computer Science, UC Berkeley

Ya-Qin Zhang

Professor and Dean, AIR, Tsinghua University

Ilya Sutskever

Co-Founder and Chief Scientist, OpenAI

Shane Legg

Chief AGI Scientist and Co-Founder, Google DeepMind

Martin Hellman

Professor Emeritus of Electrical Engineering, Stanford

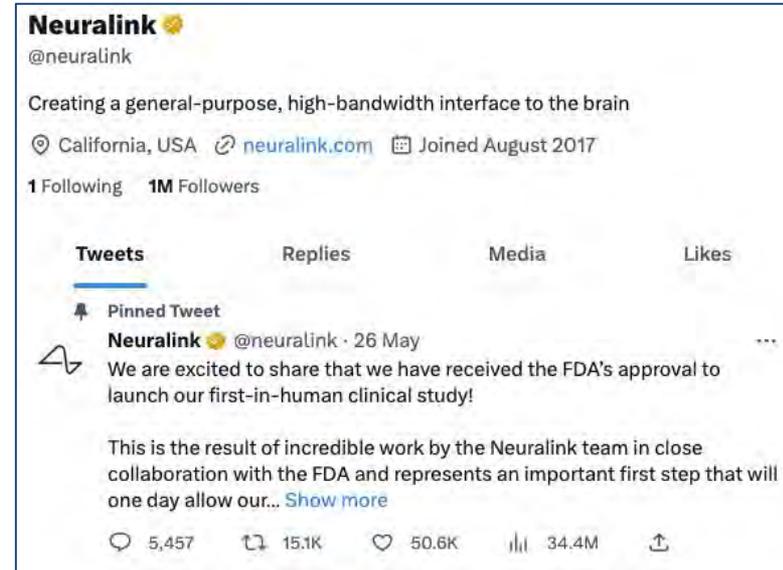
James Manyika

SVP, Research, Technology & Society, Google-Alphabet



La ricerca non si arresta

Il 26 maggio FDA americana ha approvato la sperimentazione umana per i prodotti di neuralink che si occupa di interfacce neurali impiantabili





Conclusione

“La corrente ondata di intelligenza artificiale generativa è una sotto-categoria dell'intelligenza artificiale che, basandosi su un input testuale, genera contenuti nuovi. **ChatGPT potrebbe scrivere un saggio, Midjourney potrebbe creare belle illustrazioni, mentre MusicLM potrebbe comporre un jingle.** La maggior parte delle moderne intelligenze artificiali generative si basa su **foundational model**, ovvero **modelli di intelligenza artificiale addestrati su un ampio insieme di dati attraverso l'autoapprendimento a larga scala, e successivamente adattati a una vasta gamma di compiti specifici.**

Le opportunità che questi modelli offrono alle nostre vite, alle nostre comunità e alla nostra società sono immense, così come i rischi che comportano. Da un lato, possono complementare senza soluzione di continuità il lavoro umano, rendendoci più produttivi e creativi, ma dall'altro potrebbero amplificare i pregiudizi che già sperimentiamo o minare la fiducia nelle informazioni...”

