

1+1 = Forse. La fiducia nei PC pre e post LLM

Dott. Ing. Gabriele La Milia
Università degli studi di Palermo



Università
degli Studi
di Palermo

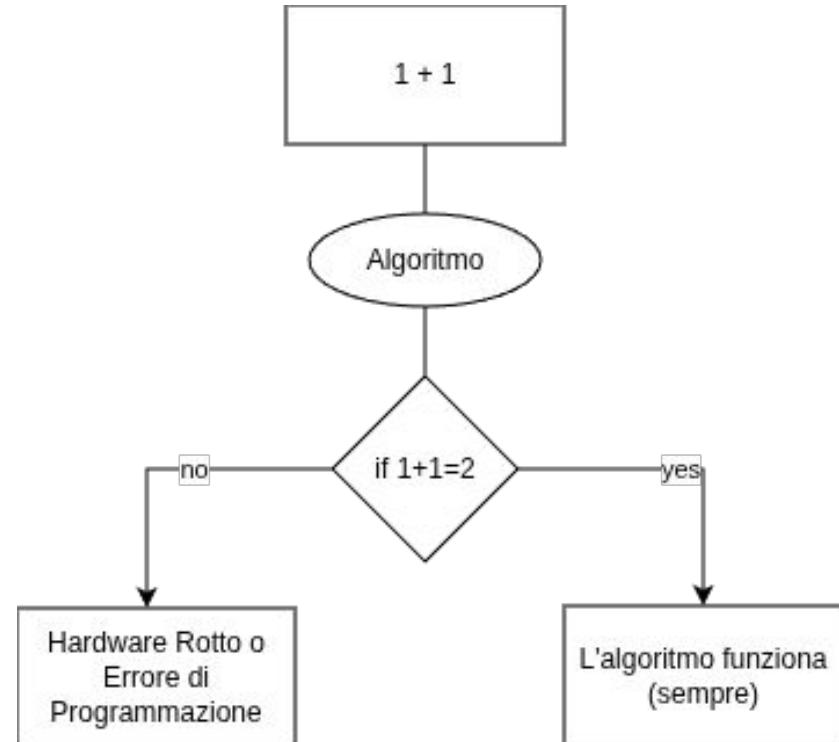


Il rapporto con i PC a partire dagli anni '60

La fiducia nei computer era basata sulla **coerenza** e sulla **ripetibilità**.

Si esegue un algoritmo o un software con un risultato **deterministico**.

Riducevano a **zero** l'errore umano fornendo output perentori



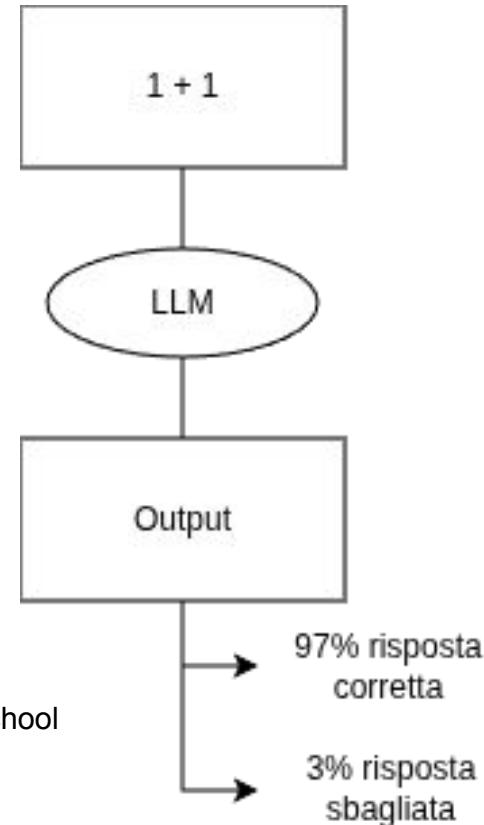
L'era dei Large Language Models (LLM)

Un LLM genera la risposta in base ai dati su cui è addestrato.

È impossibile risalire all'esatto percorso che ha portato alla soluzione

97% taken from GSM8k. Model: GPT-4.5

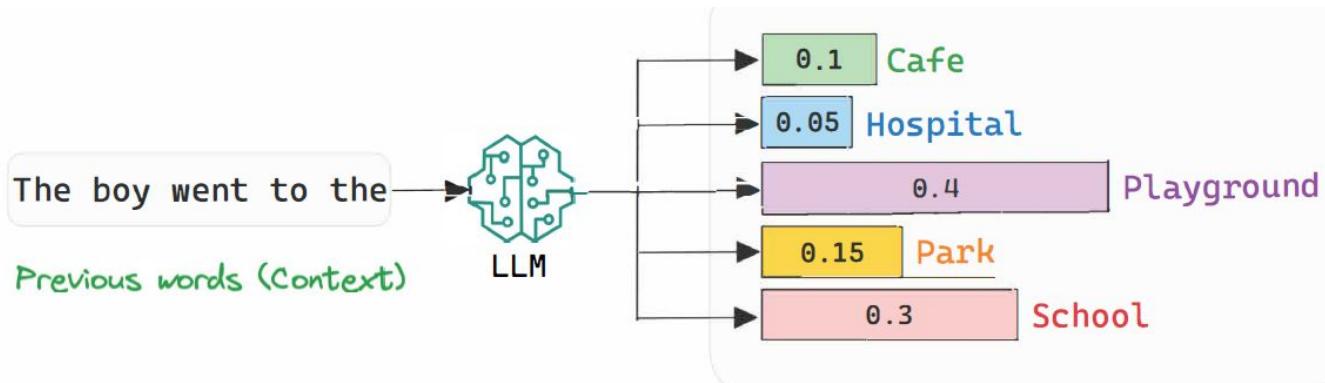
Grade School Math 8K, a dataset of 8.5K high-quality linguistically diverse grade school math word problems requiring multi-step reasoning and elementary arithmetic operations.



Cosa significa “risposta esatta in probabilità”

Un LLM non fornisce mai una risposta certa al 100% perché non cerca risposte in un database, ma le genera statisticamente.

L'output è semplicemente la sequenza di parole che il modello ritiene essere la più probabile in base a tutto il testo che ha letto.



E questa cosa non potrà cambiare

Gli autori dimostrano che è impossibile per un LLM apprendere tutte le possibili funzioni di "verità" (Ground Truth) del mondo che ci circonda.

Quando la catena logica diventa troppo lunga o complessa, il modello non calcola la verità, ma "tira a indovinare" basandosi sulla somiglianza col testo visto, generando allucinazioni logiche.

Hallucination is Inevitable: An Innate Limitation of Large Language Models

Ziwei Xu Sanjay Jain Mohan Kankanhalli
School of Computing, National University of Singapore
ziwei.xu@u.nus.edu {sanjay,mohan}@comp.nus.edu.sg

Abstract

Hallucination has been widely recognized to be a significant drawback for large language models (LLMs). There have been many works that attempt to reduce the extent of hallucination. These efforts have mostly been empirical so far, which cannot answer the fundamental question whether it can be completely eliminated. In this paper, we formalize the problem and show that it is impossible to eliminate hallucination in LLMs. Specifically, we define a formal world where hallucination is defined as inconsistencies between a computable LLM and a computable ground truth function. By employing results from learning theory, we show that LLMs cannot learn all the computable functions and will therefore inevitably hallucinate if used as general problem solvers. Since the formal world is a part of the real world which is much more complicated, hallucinations are also inevitable for real world LLMs. Furthermore, for real world LLMs constrained by provable time complexity, we describe the hallucination-prone tasks and empirically validate our claims. Finally, using the formal world framework, we discuss the possible mechanisms and efficacies of existing hallucination mitigators as well as the practical implications on the safe deployment of LLMs.

1 Introduction

The emergence of large language models (LLMs) has marked a significant milestone in the field of artificial intelligence, particularly in natural language processing. These models, with their vast knowledge bases and ability to generate coherent and contextually relevant text, have greatly impacted research, industry, and society. However, one of the critical challenges they face is the problem of "*hallucination*," where the models generate plausible but factually incorrect or nonsensical information. This issue has brought increasing concerns about safety and ethics as LLMs are being applied widely, resulting in a growing body of literature trying to classify, understand, and mitigate it.

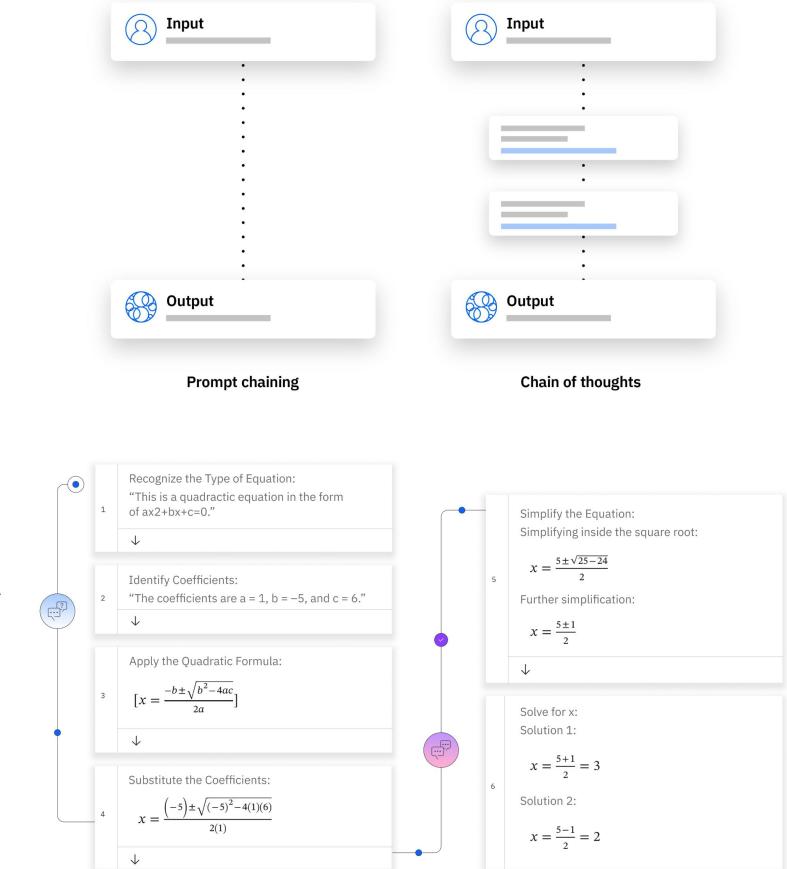
Prior works have identified multiple possible sources of hallucination in LLMs from the data collection

Chain of Thoughts

Si tratta di una tecnica utilizzata nei modelli linguistici per migliorare sensibilmente l'output.

Un LLM scomponete problemi complessi in passaggi logici intermedi più semplici, proprio come farebbe un umano.

Prima implementato solo tramite prompting, da OpenAI o1 viene integrato nel processo di addestramento ed è “visibile” prima della generazione effettiva della risposta.

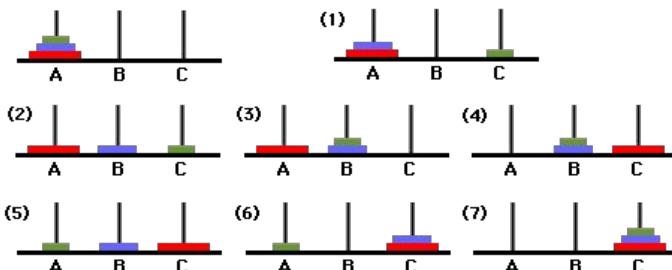


Quindi pensano davvero?

CAPACITÀ LOGICA:

MEMORIA E PATTERN MATCHING:

Inoltre i modelli aumentano il pensiero fino a un certo punto. Avvicinandosi alla soglia di collasso (dove il problema diventa troppo difficile), iniziano a pensare meno, riducendo lo sforzo di ragionamento proprio quando ne servirebbe di più.



The Illusion of Thinking:
Understanding the Strengths and Limitations of Reasoning Models
via the Lens of Problem Complexity

Parshin Shojaee*† Iman Mirzadeh* Keivan Alizadeh
Maxwell Horton Samy Bengio Mehrdad Farajtabar

Apple

Abstract

Recent generations of frontier language models have introduced Large Reasoning Models (LRMs) that generate detailed thinking processes before providing answers. While these models demonstrate improved performance on reasoning benchmarks, their fundamental capabilities, scaling properties, and limitations remain insufficiently understood. Current evaluations primarily focus on established mathematical and coding benchmarks, emphasizing final answer accuracy. However, this evaluation paradigm often suffers from data contamination and does not provide insights into the reasoning traces' structure and quality. In this work, we systematically investigate these gaps with the help of controllable puzzle environments that allow precise manipulation of compositional complexity while maintaining consistent logical structures. This setup enables the analysis of not only final answers but also the internal reasoning traces, offering insights into how LRMs "think". Through extensive experimentation across diverse puzzles, we show that frontier LRMs face a complete accuracy collapse beyond certain complexities. Moreover, they exhibit a counter-intuitive scaling limit: their reasoning effort increases with problem complexity up to a point, then declines despite having an adequate token budget. By comparing LRMs with their standard LLM counterparts under equivalent inference compute, we identify three performance regimes: (1) low-complexity tasks where standard models surprisingly outperform LRMs, (2) medium-complexity tasks where additional thinking in LRMs demonstrates advantage, and (3) high-complexity tasks where both models experience complete collapse. We found that LRMs have limitations in exact computation: they fail to use explicit algorithms and reason inconsistently across scales and problems. We also investigate the reasoning traces in more depth, studying the patterns of explored solutions and analyzing the models' computational behavior, shedding light on their strengths, limitations, and ultimately raising questions about the nature for their reasoning capabilities.

Secondo Apple i modelli hanno imparato probabilisticamente come "sembra" una soluzione per problemi presenti nel loro training set

Al fuoco con il fuoco

Gli autori smontano le tesi di Apple, sostenendo che il crollo delle prestazioni dei modelli non è dovuto ad una mancanza di ragionamento profondo, ma a gravi errori nella progettazione del test.

Per risolvere i puzzle il modello deve generare un testo lunghissimo che supera il suo limite di token. Quindi la limitazione riguarda soltanto lo spazio/memoria.

The Illusion of the Illusion of Thinking

A Comment on Shojaee et al. (2025)

C. Opus* A. Lawsen†

June 10, 2025

Abstract

Shojaee et al. (2025) report that Large Reasoning Models (LRMs) exhibit “accuracy collapse” on planning puzzles beyond certain complexity thresholds. We demonstrate that their findings primarily reflect experimental design limitations rather than fundamental reasoning failures. Our analysis reveals three critical issues: (1) Tower of Hanoi experiments systematically exceed model output token limits at reported failure points, with models explicitly acknowledging these constraints in their outputs; (2) The authors’ automated evaluation framework fails to distinguish between reasoning failures and practical constraints, leading to misclassification of model capabilities; (3) Most concerningly, their River Crossing benchmarks include mathematically impossible instances for $N \geq 6$ due to insufficient boat capacity, yet models are scored as failures for not solving these unsolvable problems. When we control for these experimental artifacts, by requesting generating functions instead of exhaustive move lists, preliminary experiments across multiple models indicate high accuracy on Tower of Hanoi instances previously reported as complete failures. These findings highlight the importance of careful experimental design when evaluating AI reasoning capabilities.

1 Introduction

Shojaee et al. (2025) claim to have identified fundamental limitations in Large Reasoning Models through systematic evaluation on planning puzzles. Their central finding—that model accuracy “collapses” to zero beyond certain complexity thresholds—has significant implications for AI reasoning research. However, our analysis reveals that these apparent failures stem from experimental design choices rather than inherent model limitations.

2 Models Recognize Output Constraints

A critical observation overlooked in the original study: models actively recognize when they approach output limits. A recent replication by @scaling01 on Twitter [2] captured model outputs explicitly stating “The pattern continues, but to avoid making this too long, I’ll stop here” when solving Tower of Hanoi problems. This demonstrates that models understand the solution pattern but choose to truncate output due to practical constraints.

Tra i due litiganti...

I modelli sanno scrivere il codice per risolvere il problema, ma il test originale chiedeva di eseguire i passaggi manualmente. Sono due abilità diverse!

Scrivere il codice dimostra che il modello ha conoscenza algoritmica (probabilmente memorizzata dai dati di addestramento dato che la Torre di Hanoi è un classico).

Eseguire migliaia di passaggi manualmente richiede state tracking e concentrazione prolungata.

Il fatto che il modello sappia scrivere la formula non prova che sappia applicarla passo dopo passo senza distrarsi.

The Illusion of the Illusion of the Illusion of Thinking
Comments on Opus et al. (2025)

G. Pro V. Dantas

June 16, 2025

Abstract

A recent paper by Shojaee et al. (2025), *The Illusion of Thinking*, presented evidence of an “accuracy collapse” in Large Reasoning Models (LRMs), suggesting fundamental limitations in their reasoning capabilities when faced with planning puzzles of increasing complexity. A compelling critique by Opus and Lawsen (2025), *The Illusion of the Illusion of Thinking*, argued these findings are not evidence of reasoning failure but rather artifacts of flawed experimental design, such as token limits and the use of unsolvable problems. This paper provides a tertiary analysis, arguing that while Opus and Lawsen correctly identify critical methodological flaws that invalidate the most severe claims of the original paper, their own counter-evidence and conclusions may oversimplify the nature of model limitations. By shifting the evaluation from sequential execution to algorithmic generation, their work illuminates a different, albeit important, capability. We conclude that the original “collapse” was indeed an illusion created by experimental constraints, but that Shojaee et al.’s underlying observations hint at a more subtle, yet real, challenge for LRMs: a brittleness in sustained, high-fidelity, step-by-step execution. The true illusion is the belief that any single evaluation paradigm can definitively distinguish between reasoning, knowledge retrieval, and pattern execution.

1 Introduction

The debate over the true reasoning capabilities of Large Language and Reasoning Models (LLMs and LRMs) is central to the field of artificial intelligence. A significant contribution to this discourse came from Shojaee et al. [1], who used controlled puzzle environments to test state-of-the-art LRMs. Their primary finding was a dramatic “accuracy collapse” on tasks like the Tower of Hanoi and River Crossing as complexity scaled, which they interpreted as evidence of fundamental limitations in generalizable reasoning.

This conclusion was swiftly challenged by Opus and Lawsen [2] in a direct commentary. They contended that the observed failures were illusory, stemming directly from experimental design choices. Specifically, they identified three major issues: (1) Tower of Hanoi experiments exceeded model output token limits, (2) the evaluation framework misclassified output truncation as reasoning failure, and (3) the River Crossing benchmarks included mathematically impossible instances for which models were unfairly penalized.

...anche se sappiamo che manca qualcosa

- 52% di risposte errate: Più della metà delle risposte fornite da ChatGPT conteneva informazioni inesatte.
- *Errori concettuali (54%): ChatGPT non ha capito il contesto della domanda.*
- *Errori fattuali (36%): Informazioni inventate o false.*
- *Errori di codice (28%): Codice che non funziona o usa logica sbagliata.*
- 77% delle risposte di ChatGPT sono verbose (lunghe)

Nello studio è emerso un paradosso pericoloso:

- Gli utenti hanno preferito nel 35% delle risposte ChatGPT
- Il 39% delle volte non si sono accorti che la risposta conteneva errori

arXiv:2308.02312v4 [cs.SE] 7 Feb 2024

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

Samia Kabir
Purdue University
West Lafayette, USA

Bonan Kou
Purdue University
West Lafayette, USA

David N. Udo-Imeh
Purdue University
West Lafayette, USA

Tianyi Zhang
Purdue University
West Lafayette, USA

ABSTRACT

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

CCS CONCEPTS

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

KEYWORDS

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

ACM Reference Format:

Samia Kabir, David N. Udo-Imeh, Bonan Kou, and Tianyi Zhang. 2024. Is Stack Overflow Obsolete? An Empirical Study of the Characteristics of ChatGPT Answers to Stack Overflow Questions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*, May 11–16,

2024, Honolulu, HI, USA. ACM, New York, NY, USA, 17 pages. <https://doi.org/10.1145/3613994.3642596>

1 INTRODUCTION

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

Despite the rising popularity of ChatGPT, there are also many increasing concerns. Previous studies show that LLMs can acquire factually incorrect knowledge during training and propagate the incorrect knowledge to generated content [9, 33, 35, 39, 56]. Besides, LLMs often generate fabricated texts that mimic truthful information and are hard to recognize, especially for users who lack the expertise [14, 21, 29]. Like other LLMs, ChatGPT is also plagued with these issues [15, 41, 50, 58]. The prevalence of misinformation, which can easily mislead users, has prompted Stack Overflow to impose a ban on answers generated by ChatGPT [64].

Recent studies have compared ChatGPT to human experts in legal, medical, and financial domains [34, 41]. To the best of our knowledge, no comprehensive analysis has been conducted to investigate ChatGPT's capability to answer programming questions, especially the quality and characteristics of ChatGPT answers in comparison to human answers. If misinformation is prevalent in ChatGPT answers and is hard to recognize, it may inevitably lead

È la fatica che crea l'apprendimento?

Nel seguente esperimento (Fase 1):

- 1000 studenti delle superiori (Turchia), Matematica
- Divisi in accesso solo a libri/appunti e a GPT-4

Utilizzare un LLM per le risposte ha permesso di ottenere un numero maggiore di risposte esatte rispetto al gruppo che utilizzava solo libri e/o appunti (miglioramento tra il +48% e +127%)

Togliendo poi l'LLM al gruppo “avvantaggiato” (Fase 2):

- Risultati peggiori del 17% rispetto a chi ha utilizzato solo libri/appunti per svolgere gli esercizi

Inoltre gli studenti che usavano l'IA erano convinti di aver imparato tantissimo e di essere andati bene all'esame

Generative AI Can Harm Learning

Hamsa Bastani,^{1*} Osbert Bastani,^{2*} Alp Sungu,^{1,†}
Haosen Ge,³ Özge Kabakci,⁴ Rei Mariman

¹Operations, Information and Decisions, University of Pennsylvania

²Computer and Information Science, University of Pennsylvania

³Wharton AI & Analytics, University of Pennsylvania

⁴Budapest British International School

*These authors (H.B., O.B., A.S.) contributed equally.

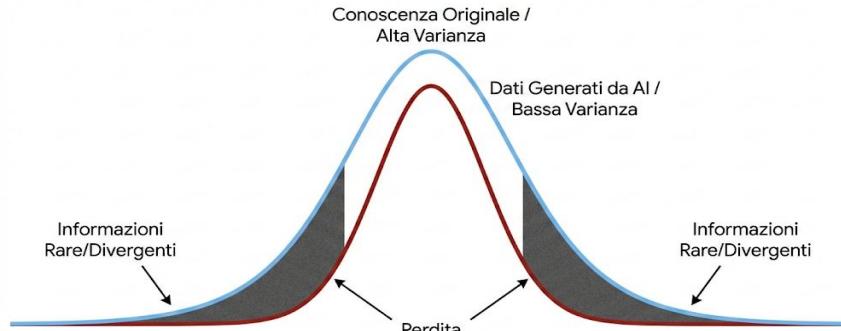
†To whom correspondence should be addressed; E-mail: alpsungu@wharton.upenn.edu.

Generative artificial intelligence (AI) is poised to revolutionize how humans work, and has already demonstrated promise in significantly improving human productivity. However, a key remaining question is how generative AI affects *learning*, namely, how humans acquire new skills as they perform tasks. This kind of skill learning is critical to long-term productivity gains, especially in domains where generative AI is fallible and human experts must check its outputs. We study the impact of generative AI, specifically OpenAI's GPT-4, on human learning in the context of math classes at a high school. In a field experiment involving nearly a thousand students, we have deployed and evaluated two GPT based tutors, one that mimics a standard ChatGPT interface (called GPT Base) and one with prompts designed to safeguard learning (called GPT Tutor). These tutors comprise about 15% of the curriculum in each of three grades. Consistent with prior work, our results show that ac-

Se pensi di studiare solo dagli LLM per il resto della tua vita stai commettendo un grosso errore

Gli LLM sono macchine statistiche. Tendono a convergere verso la media, perdendo l'informazione nelle code.

E se vengono addestrati su dati sintetici che hanno già perso le code, i modelli successivi convergono verso una media sempre più stretta. La varianza crolla. La realtà si appiattisce.



Article

AI models collapse when trained on recursively generated data

<https://doi.org/10.1038/s41586-024-07566-y>

Received: 20 October 2023

Accepted: 14 May 2024

Published online: 24 July 2024

Open access

Check for updates

Ilia Shumailov^{1,2*}, Zakhar Shumaylov^{2,3}, Yiren Zhao², Nicolas Papernot^{4,5}, Ross Anderson^{6,7} & Yarin Gal^{1,2}

Stable diffusion revolutionized image creation from descriptive text. GPT-2 (ref. 1), GPT-3.5 (ref. 2) and GPT-4 (ref. 3) demonstrated high performance across a variety of language tasks. ChatGPT introduced such language models to the public. It is now clear that generative artificial intelligence (AI) such as large language models (LLMs) is here to stay and will substantially change the ecosystem of online text and images. Here we consider what may happen to GPT- n once LLMs contribute much of the text found online. We find that indiscriminate use of model-generated content in training causes irreversible defects in the resulting models, in which tails of the original content distribution disappear. We refer to this effect as ‘model collapse’ and show that it can occur in LLMs as well as in variational autoencoders (VAEs) and Gaussian mixture models (GMMs). We build theoretical intuition behind the phenomenon and portray its ubiquity among all learned generative models. We demonstrate that it must be taken seriously if we are to sustain the benefits of training from large-scale data scraped from the web. Indeed, the value of data collected about genuine human interactions with systems will be increasingly valuable in the presence of LLM-generated content in data crawled from the Internet.

The development of LLMs is very involved and requires large quantities of training data. Yet, although current LLMs^{2,4–6}, including GPT-3, were trained on predominantly human-generated text, this may change. If the training data of most future models are also scraped from the web, then they will inevitably train on data produced by their predecessors. In this paper, we investigate what happens when data produced by, for example, a version of GPT forms most of the training dataset of following models. What happens to GPT generations GPT- n as n increases? We discover that indiscriminately learning from data produced by other models causes ‘model collapse’ – a degenerative process whereby, over time, models forget the true underlying data distribution, even in the absence of a shift in the distribution over time. We give examples of model collapse for GMMs, VAEs and LLMs. We show that, over time, models start losing information about the true distribution, which first starts with tails disappearing, and learned behaviours converge over the generations to a point estimate with very

the broader implications of model collapse. We note that access to the original data distribution is crucial in learning tasks in which the tails of the underlying distribution matter, one needs access to real human-produced data. In other words, the use of LLMs at scale to publish content on the Internet will pollute the collection of data to train their successors: data about human interactions with LLMs will be increasingly valuable.

What is model collapse?

Definition 2.1 (model collapse). Model collapse is a degenerative process affecting generations of learned generative models, in which the data they generate end up polluting the training set of the next generation. Being trained on polluted data, they then mis-perceive reality. The process is depicted in Fig. 1a. We separate two special cases: early model collapse and late model collapse. In early model collapse,

Una panoramica degli LLM nell'educazione

- Tutor 1-1 intelligenti (2 Sigma Problem di Benjamin Bloom 1984).
- Gli insegnanti si possono concentrare maggiormente sulla didattica risparmiando tempo per piani, quiz e materiali.
- Se usata in modo socratico può aiutare concretamente.
- L'AI viene vista come un “compagno di squadra” e non come un professore, un muro distante dallo studente.
- L'AI può inventare fatti. Bisogna educare gli studenti alla verifica delle fonti.
- Bias nei Dati (anche i libri li hanno) e svantaggio linguistico.
- Problema dei dati degli studenti inviati a server mondiali.

The Revolution Has Arrived: What the Current State
of Large Language Models in Education Implies for the
Future

Russell Beale

Abstract

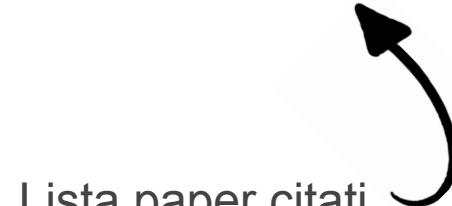
Large language Models have only been widely available since 2022 and yet in less than three years have had a significant impact on approaches to education and educational technology. Here we review the domains in which they have been used, and discuss a variety of use cases, their successes and failures. We then progress to discussing how this is changing the dynamics for learners and educators, consider the main design challenges facing LLMs if they are to become truly helpful and effective as educational systems, and reflect on the learning paradigms they support. We make clear that the new interaction paradigms they bring are significant and argue that this approach will become so ubiquitous it will become the default way in which we interact with technologies, and revolutionise what people expect from computer systems in general. This leads us to present some specific and significant considerations for the design of educational technology in the future that are likely to be needed to ensure acceptance by the changing expectations of learners and users.

1. Introduction

Large Language Models (LLMs) – massive deep learning neural networks trained on vast text corpora – have rapidly emerged as powerful tools for education: the public release of models like OpenAI's ChatGPT in late 2022 catalyzed global interest in applying LLMs in classrooms and curricula. Educators and researchers are exploring how these AI systems can revolutionize teaching and learning across primary schools, secondary education, and universities. Early commentaries heralded LLMs' potential to generate content, engage learners in dialogue, and personalize learning at scale, while also warning of challenges around accuracy, bias, and academic integrity (Kasneci et al., 2023)[24]. Since then, a fast-growing body of research – spanning computer science, education, and learning sciences – has begun to systematically investigate LLM-driven educational innovations. Recent surveys provide overviews of this

Conclusioni

- Un LLM fornisce risposte probabilistiche (non deterministiche) al prompt richiesto.
- È impossibile addestrare un LLM con 100% di accuratezza e 0% di allucinazioni.
- Spesso ci dicono solo quello che vorremmo sentirci dire.
- Non sempre ce ne accorgiamo quando sbagliano.
- Pensare di sostituire con una risposta di un LLM un'esperienza trascorsa è un grave errore.
- Utilizzando un LLM si perdono le “code” della conoscenza.



Lista paper citati