Generative AI in Action: Use Cases, Risks, and Future Prospects

Goran S. Milovanović, Phd ไปคนเททธุรหมาล

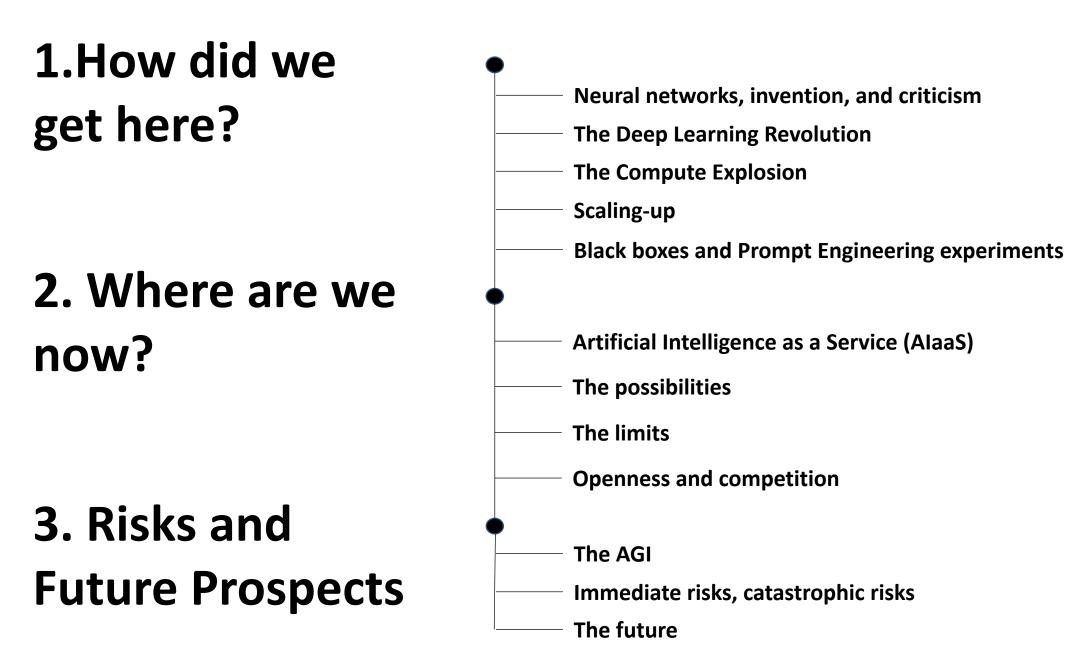
Slobodan Marković, MA





Паминерија





1.How did we get here?



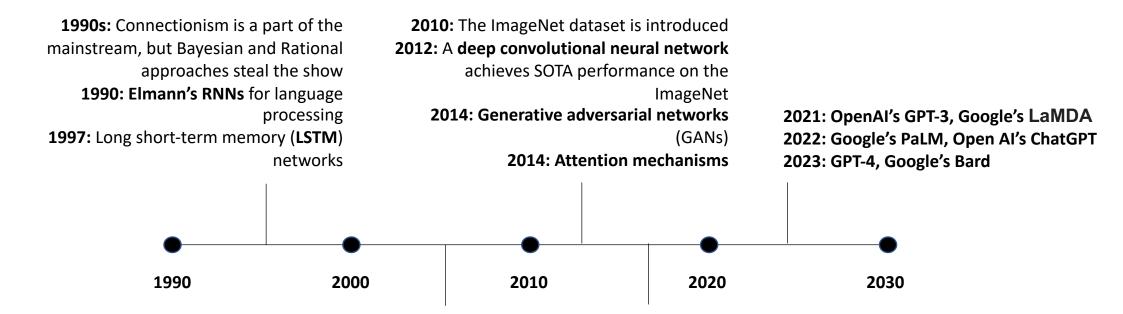
Neural networks, invention, and criticism



1956: The term "artificial intelligence" is coined at the Dartmouth 1957: Skinner's "Verbal Behaviour"
1957: Chomsky's "Syntactic Structures": enter generative grammars 1958: The perceptron algorithm is developed by Frank Rosenblatt 1959: Chomsky's review of Skinner's "Verbal Behaviour"

1970: Seppo Linnainmaa introduces the backpropagation algorithm in his MA Thesis **1970s: Backpropagation** is rediscovered independently by multiple researchers, including Paul Werbos, David Rumelhart, and Geoffrey Hinton.

Neural networks, invention, and criticism

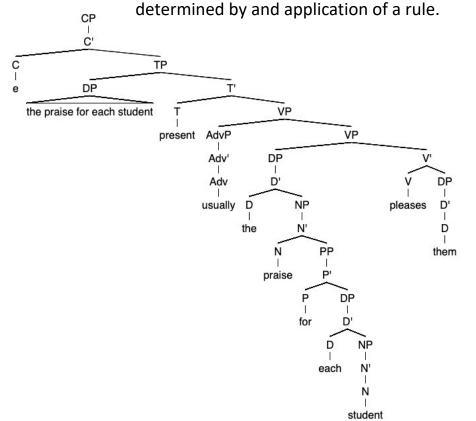


2006: Geoffrey Hinton and colleagues introduce the idea of **Deep Learning**, which involves training neural networks with many layers 2015: Google DeepMind's AlphaGo
2017: "Attention is all you need": the
Transformer architecture
2018: OpenAl's GPT-2
2018: Hinton, Bengio, LeCun Turing Award

Neural networks, invention, and criticism

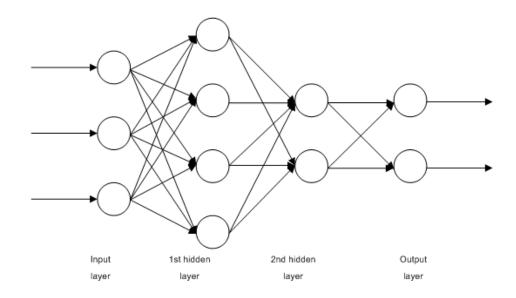
Symbolic Cognition

 There are variables that represent things and can take certain values, (2) there are rules of a formal system of reasoning that constrain the possible combinations of variables, (3) the meaning of more complex things is a function of the meaning of its constituents and can be



Associative Learning

(1) A distributed system powerful enough will learn from correlations in the spatiotemporal arrangement of things in the world and what seems to be (2) rules will in the end show up as emergent properties of huge, associative, neural network; principles at work are (3a) supervised, (3b) reinforced (RL), and (3c) unsupervised learning.



The Compute Explosion: Scaling-Up

Example dataset

OpenAI GPT-3 Training Set

Common Crawl: petabytes of data, basically everything that can be accessed online, 380Tb in October 22 (3.15 billion web-pages).

Dataset	Tokens	% in training
Common Crawl	410 billion	60%
WebText2	19 billion	22%
Books1	12 billion	8%
Books2	55 billion	8%
Wikipedia	3 billion	3%

OpenAI DALL-E 2 Training Set

An image generative model, DALL-E 2 was trained on approximately 650 million imagetext pairs scraped from the Internet

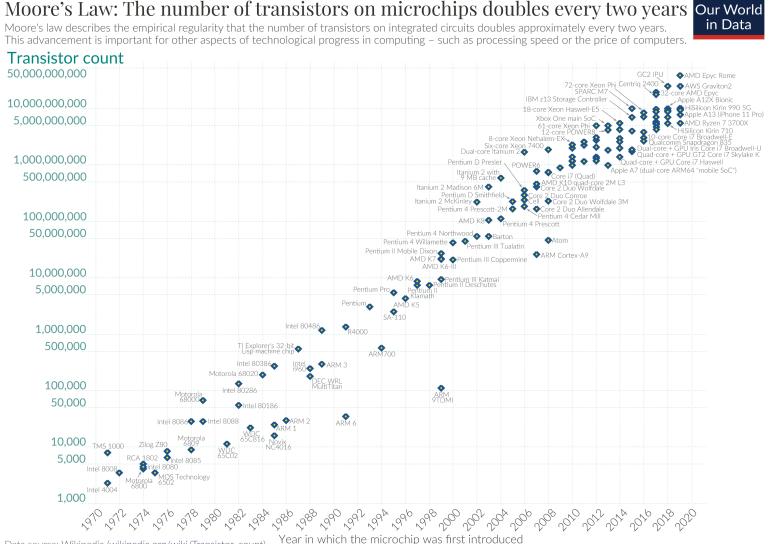
The Compute Explosion: Scaling-Up

How to train your dragon?

- **Data preparation.** Collecting a huge amount of various text (usually from the internet, but also from other sources) which is transformed into smaller processing units tokens (words or parts of words).
- Model training (unsupervised/self-supervised pretraining). Developing an algorithm that goes through sequences of raw text, analyzing relationships between words (tokens) and calculating the probability of the next word (token) appearing. Through this process, the model gains implicit knowledge about different aspects of language, such as word forms, their meanings, sentence formation, etc.
- Supervised fine-tuning / instruction tuning. To adapt the model to specific tasks (e.g. answering questions, summarizing, sentiment analysis, translation), it is further trained on a smaller set of annotated data.
- **Reinforced learning from human feedback.** Additional adjustment of the model to generate more desirable responses. People evaluate/rank the responses generated by the model, which is then used for further adjustment.

These are just the most typical steps in the training of a contemporary Large Language Model (LLM). Model training can take various forms and be organized in different ways as well.

The Compute Explosion: Scaling-Up



Model Year **Parameters Google BERT** 2018 340 million 2019 1.5 billion **OpenAl GPT-2 OpenAl GPT-3** 2021 175 billion Microsoft/Nvidia 2021 530 billion **Megatron-Turing** NLG **Google LaMDA** 2022 137 billion **Google PaLM** 2022 540 billion **OpenAl GPT-4** 2023 unknown

Data source: Wikipedia (wikipedia.org/wiki/Transistor_count) Tear in which the microchip was first OurWorldinData.org – Research and data to make progress against the world's largest problems.

Black boxes and Prompt Engineering experiments







There seems to be more to it

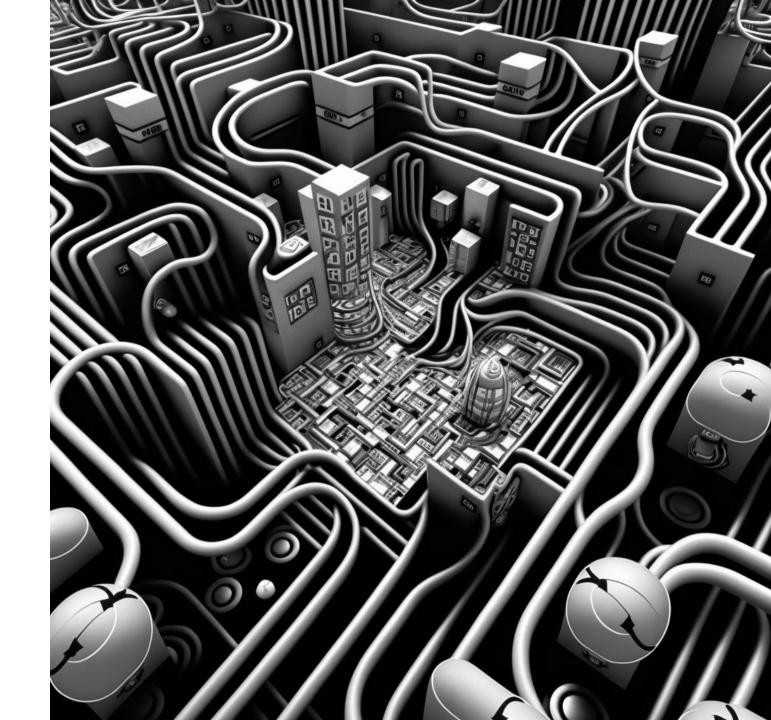
"Recent investigations like the one Dyer worked on have revealed that LLMs can produce hundreds of "emergent" abilities — tasks that big models can complete that smaller models can't, many of which seem to have little to do with analyzing text."

"That language models can do these sort of things was never discussed in any literature that I'm aware of," said Rishi Bommasani, a computer scientist at Stanford University. Last year, he helped compile a list of dozens of emergent behaviors, including several identified in Dyer's project. That list continues to grow."

Yi Tay, a scientist at Google Brain who worked on the systematic investigation of breakthroughs, points to recent work suggesting that **chain-of-thought prompting** changes the scaling curves and therefore the point where emergence occurs. [...] Such prompts, which ask the model to explain its reasoning, may help researchers begin to investigate why emergence occurs at all.

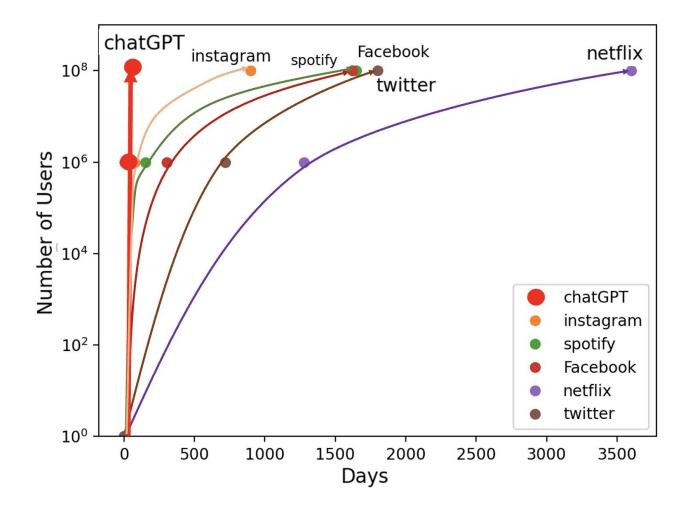
-- <u>The Unpredictable Abilities Emerging From Large Al Models, Stephen Ornes, March 16,</u> 2023, Quanta Magazine

2. Where are we now?



The current situation and the near future

The first half of 2022 was marked by image generation models (DALL-E 2, Midjourney, Stable Diffusion), but the end of the year was certainly marked by ChatGPT, which exploded to 1 million users in just one week and 100 million in two months.



Artificial Intelligence as a Service (AlaaS)

gpt-4 More capable than any GPT-3.5 model, able to do more complex tasks, and optimized for chat (8,192 tokens) **gpt-4-0314** Snapshot of gpt-4 from March 14th 2023. Unlike gpt-4, this model will not receive updates, and will only be supported for a three month period ending on June 14th 2023. (8,192 tokens) **gpt-4-32k** - Same capabilities as the base gpt-4 mode but with 4x the context length (32,768 tokens) gpt-4-32k-0314 - Snapshot of gpt-4-32 from March 14th 2023. Unlike gpt-4-32k, this model will not receive updates, and will only be supported for a three month period ending on June 14th 2023. (32,768 tokens) **code-davinci-002**: good for pure code-completion tasks text-davinci-002: is an InstructGPT model based on code-davinci-002 text-davinci-003: is an improvement on text-davinci-002 gpt-3.5-turbo-0301: is an improvement on textdavinci-003, optimized for chat (...only be supported for a three month period ending on June 1st 2023) gpt-3.5-turbo: most capable GPT-3.5 model and optimized for chat at 1/10th the cost of text-davinci-003. Will be updated with our latest model iteration. **davinci**: Most capable GPT-3 model. Can do any task the other models can do, often with higher quality (2,049 tokens, Up to Oct 2019) **CUrie:** Very capable, but faster and lower cost than Davinci (2,049 tokens, Up to Oct 2019) **babbage**: Capable of straightforward tasks, very fast, and lower cost (2,049 tokens, Up to Oct 2019) **ada**: Capable of very simple tasks, usually the fastest model in the GPT-3 series, and lowest cost (2,049 tokens, Up to Oct 2019) text-moderation-stable text-moderationlatest

OpenAl

Amazon Bedrock

Generative AI on Google Cloud

MS Azure OpenAl Service

The possibilities

Over 300 applications are delivering GPT-3– powered search, conversation, text completion, and other advanced AI features through our API.

-- OpenAI, GPT-3 powers the next generation of apps March 25, 2023

> Algolia: semantic search Duolingo: language courses Khan Academy: education GitHub Copilot: software engineering Microsoft Bing: search Microsoft 365 Copilot: office

Natural Language Processing (NLP) Chatbots and virtual assistants Content generation Search and recommendation systems Customer service

Medical diagnosis and research Language learning Content moderation

Data analysis

...

Marketing and advertising Creative writing and storytelling Education

Knowledge management

Legal research and analysis Financial analysis and forecasting

Code completion, Code generation, Code review, Bug detection

Autocomplete, text summarization, recommendation of similar content, semantic search.



X

- Q large language
- Q large language model tools
- Q large language models
- Q large language models wikipedia
- Q large language **model**
- large language models are zero-shot reasoners

large la	nguage mo	odels			×	Ļ	١	٩
Q Sve	🖍 Slike	🗉 Vesti	▶ Video	: Još			AI	latke

Oko 1.100.000.000 rezultata (0,38 sekunde/i)

A large language model (LLM) is a language model consisting of a neural network with many parameters (typically billions of weights or more), trained on large quantities of unlabelled text using unsupervised learning. LLMs emerged around 2018 and perform well at a wide variety of tasks.

Large language model - Wikipedia

O istaknutim fragmentima • Povratne informacije

Drugi žele da znaju

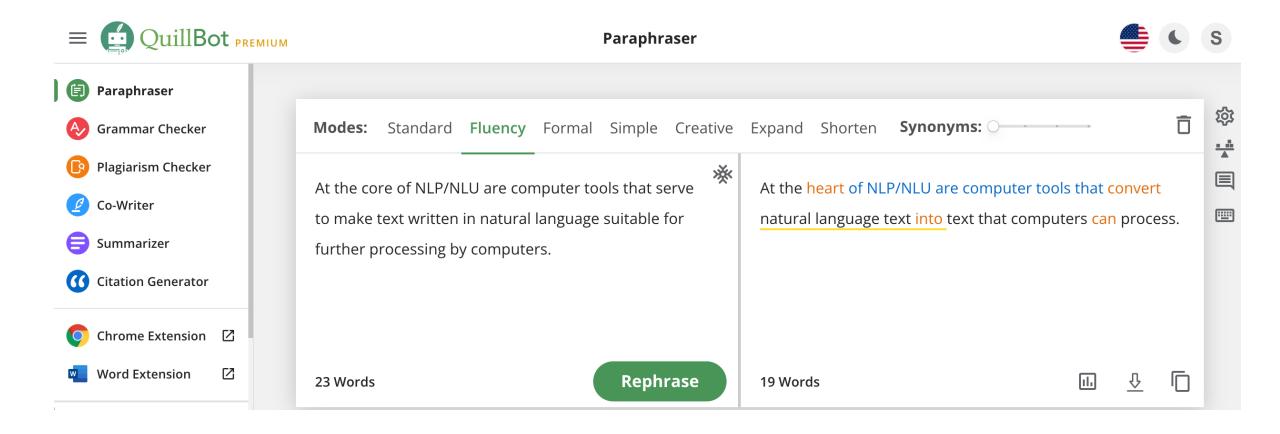
Is GPT-3 a large language model?	~
What makes a language model large?	~
What are the most popular large language models?	~
What are examples of language models?	~
	Povratne informacije

W wikipedia.org https://en.wikipedia.org > wiki > Large_language_model

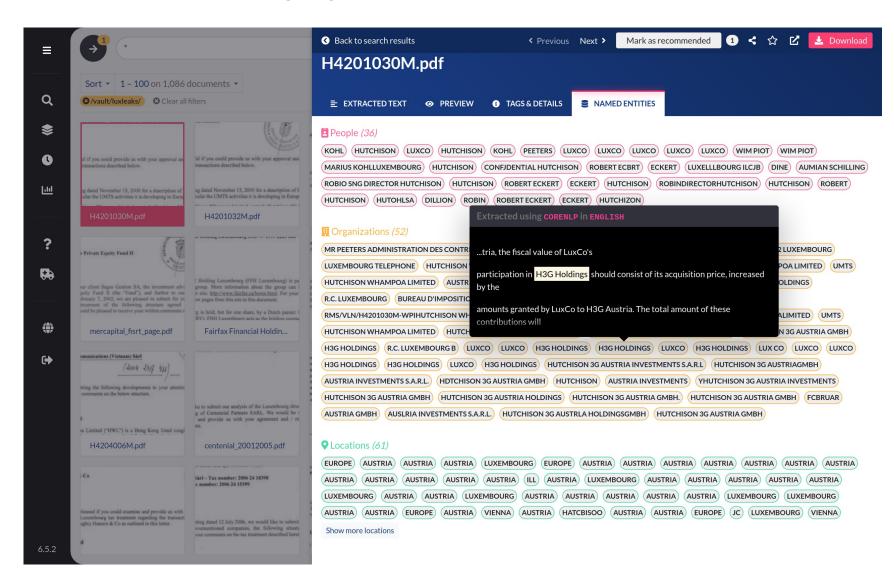
Automatic Translation

\equiv **Google** Translate ••• Sign in え Text **Documents** Websites \rightarrow SPANISH **SERBIAN - DETECTED** ENGLISH SPANISH FRENCH ENGLISH ARABIC \sim \sim У основи NLP/NLU налазе се рачунарски алати који служе да At the core of NLP/NLU are computer tools that serve to make text \therefore X written in natural language suitable for further processing by текст писан природним језиком учине погодним за даљу обраду помоћу рачунара. computers. U osnovi NLP/NLU nalaze se računarski alati koji služe da tekst pisan prirodnim jezikom učine pogodnim za dalju obradu pomoću računara. 69 Γ Ļ < 134 / 5,000 Send feedback

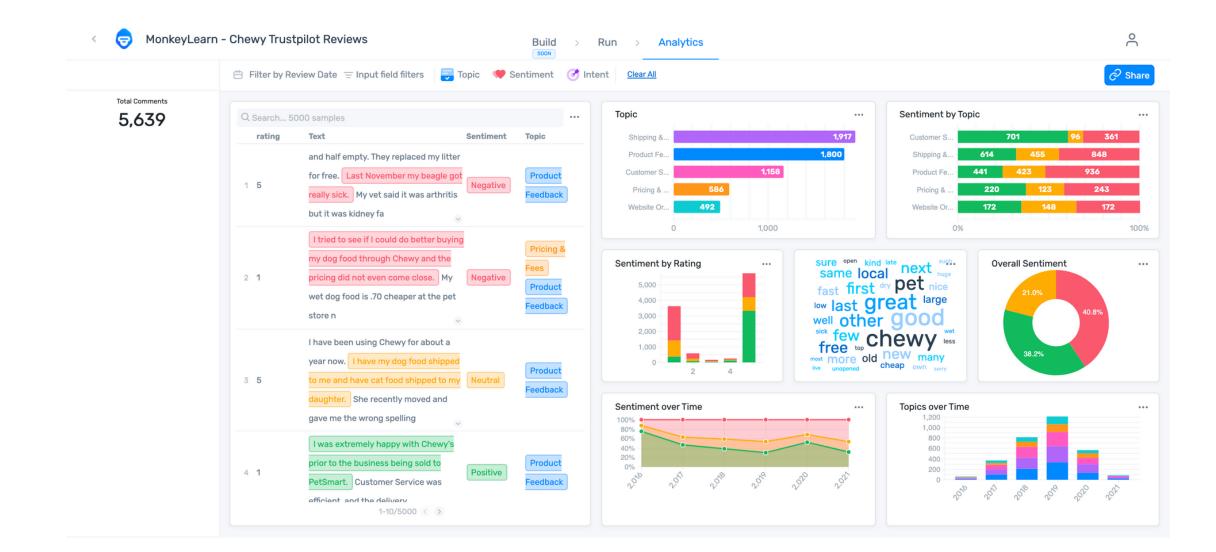
Paraphrasing, shortening and lengthening of text, determining similarities



Knowledge Management: Automatic organization of documents by type, language, names/titles, locations...



Sentiment Analysis



Answering questions and automated interaction with users (chatbots, virtual assistants)

Pretend that you are a hiring manager for an AI position and that you are conducting an interview with a prospective employee. Ask me a question at an expert level.

Ø

As a hiring manager for an AI position, I would like to assess your understanding of state-of-the-art techniques in deep learning. Can you please explain the concept of attention mechanisms in transformer models, and discuss how self-attention is used to capture the dependencies between different positions in the input sequence? Additionally, can you highlight any key advantages and limitations of using transformers for natural language processing tasks?

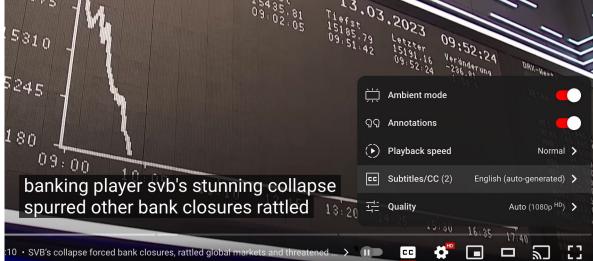
	List top 3 highest grossing movies in a tabular form "movie", "year", "amou	nt" C
8	As my knowledge was last updated in September 2021, here are the top 3 highest-grossing movies up to that point. Please note that these figures min have changed in the meantime.	ght

Movie	Year	Amount (worldwide gross)
Avatar	2009	\$2,847,246,203
Avengers: Endgame	2019	\$2,798,589,794
Titanic	1997	\$2,202,201,882

Automatic Speech Recognition (ASR)

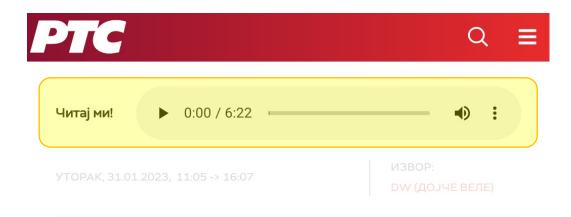


Voice device control (digital assistants)



Automatic captioning of audio-video content

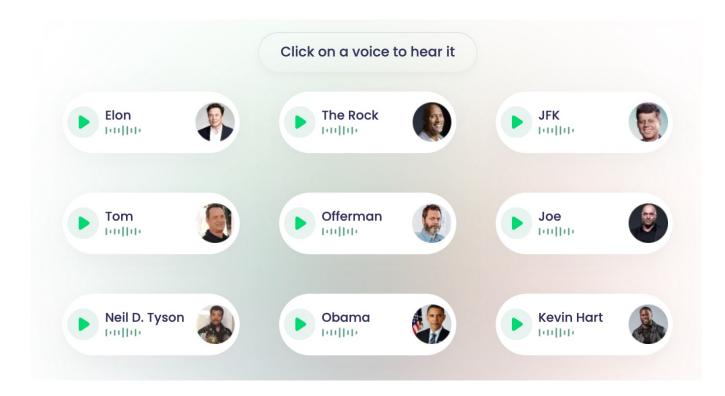
Speech Synthesis (text-to-speech, TTS)



Вештачка интелигенција у школи: ChatGPT ради домаће задатке

Софтвер који користи вештачку интелигенцију ChatGPT пише писмене задатке у школама и решава домаће задатке. Да ли би то требало користити или забранити? Да ли је то помоћ или ризик? И шта раде у немачким школама?

Voice cloning



Generating music (based on textual description)

Caption	Generated audio
The main soundtrack of an arcade game. It is fast- paced and upbeat, with a catchy electric guitar riff. The music is repetitive and easy to remember, but with unexpected sounds, like cymbal crashes or drum rolls.	► 0:00 / 0:30 - ↓
A fusion of reggaeton and electronic dance music, with a spacey, otherworldly sound. Induces the experience of being lost in space, and the music would be designed to evoke a sense of wonder and awe, while being danceable.	► 0:00 / 0:30 🛏 📣
A rising synth is playing an arpeggio with a lot of reverb. It is backed by pads, sub bass line and soft drums. This song is full of synth sounds creating a soothing and adventurous atmosphere. It may be	► 0:00 / 0:30 🛏 📣

► 0:00 / 0:30 - **•**

Slow tempo, bass-and-drums-led reggae song. Sustained electric guitar. High-pitched bongos with ringing tones. Vocals are relaxed with a laidback feel, very expressive.

playing at a festival during two songs for a buildup.















Their combination is particularly interesting!

- Virtual customer support agent. Speech-to-text translation, understanding of questions and generating responses, speech synthesis.
- Virtual actors, TV/podcast hosts, historical figures. Generating text in a specific style, speech synthesis with a cloned voice, generating 3D avatars based on images.
- Al tribute band. Generating text and music in a specific style, speech synthesis (singing) with a cloned voice.
- Automatic sign language generation for any audio or video content. Speech-to-text translation, sign language generation by a 3D avatar.
- Automatic video generation based on text. Generating a sequence of images (storyboard) from textual descriptions, generating a video based on the storyboard.

The limits

produce biased or discriminatory outputs. understanding and analysis.

the model generates output that is not based on the generate high-quality text, they are not capable of input or the task it was trained to perform. In other generating truly original or creative content. words, the model generates output that is not grounded in reality, but rather reflects patterns or information it has learned from the training data.

3. Lack of common sense: LLMs lack the common sense knowledge that humans possess, which can lead to misunderstandings or nonsensical responses in certain situations.

1. Data bias. LLMs are trained on large datasets of **4.** Difficulty with complex reasoning. While LLMs are text, which can be biased towards certain adept at language processing tasks, they can struggle with perspectives or demographics; can sometimes more complex reasoning tasks that require deeper

2. Hallucinations in LLMs. Refer to instances where **5. Inability to generate original content**. While LLMs can

6. Lack of interpretability. LLMs are often described as "black boxes" because it can be difficult to understand how they arrive at their outputs. This lack of interpretability can make it challenging to diagnose and correct errors or biases.

Openness and competition

<u>dealroom.com</u> mapped **250+ generative AI startups**, updated 11 April 2023.

Trends to watch in 2023, according to Forbes:

- Generative Al Infrastructure (where models live: OpenAl, Google, Anthropic, Hugging Face, Stability)
- **Predictive Infrastructure** (Data Management and Data Engineering support for Generative AI training)
- **Generative AI Applications** (mainly content creation, co-writing, marketing)
- **Predictive AI Applications** (i.e. anomaly detection; <u>Abnormal Security</u>, <u>Viz.ai</u>)

GPT-4 Technical Report

OpenAI*

Abstract



Bard can explain why large language models might make mistakes

Meet Bard: your creative and helpful collaborator, here to supercharge your imagination, boost your productivity, and bring your ideas to life.



Bard isn't currently supported in your country. Stay tuned!

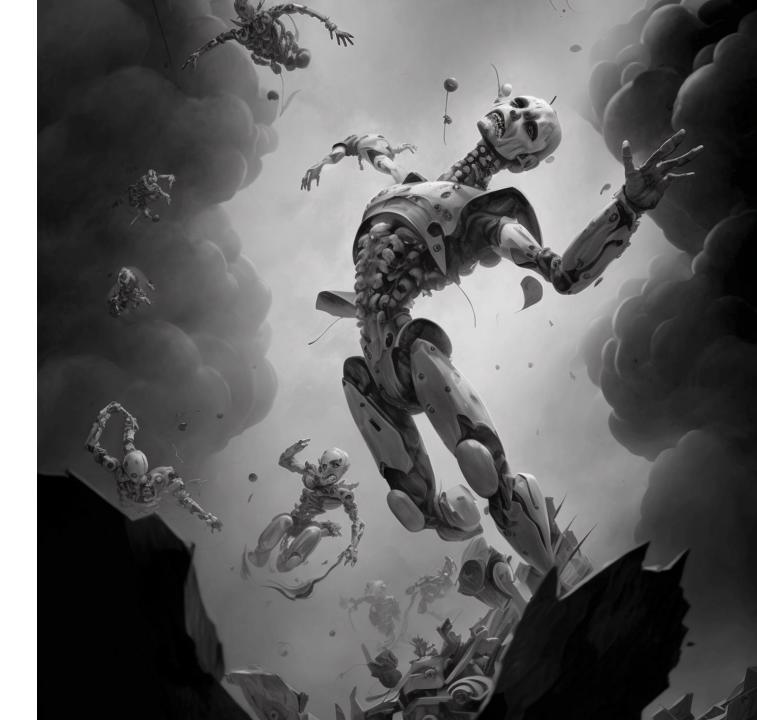
Openness and competition

- A lot is being invested in AI (just this year, Microsoft invested \$10B in OpenAI, while Google invested \$300M in Anthropic), and there will be even more investment in the future.
- In the coming years, there is expected to be an explosion of user AI applications and the creation of ecosystems around large (foundational) models and their APIs.
- Some functionalities will be incrementally **built into software that we already use massively** (office applications, ticketing software, image and sound processing applications), **but there will also be more AI-first software**.

Openness and competition

- Despite the hype, **most (generative) AI systems are currently in early stages of development.** Generative AI models have flaws/limitations and for further progress in the field of AI, solutions are needed that will enable more efficient self-learning (from smaller amounts of data), better reasoning, generalization ability, etc.
- Generative AI models are currently mostly large and demanding the training data and models are measured in gigabytes and terabytes, and the process of training and generating content requires a lot of memory, processing power, and energy.
- That is why they are **usually stored on dedicated computer clusters of large cloud providers** (such as Microsoft Azure, Google Cloud, Amazon AWS) and are typically available via APIs for integration into user applications.
- There is **intense work being done to optimize the models so that they can be executed on weaker hardware**, such as personal computers and phones (for example, open-source models such as **Stable Diffusion** or **LLaMA**).
- At the same time, a new generation of **consumer hardware optimized for AI applications** is being developed (such as **Apple's M-series processors**).

3. Risks and Future Prospects



IS NOT COMING ANYTIME SOON.

(ONCE AND FOR ALL)

SYSTEMS OF ASSOCIATIVE LEARNING (SUPERVISED, SELF-SUPERVISED, **REINFORCED, WHATEVER) LIKE OUR GENERATIVE AIS HAVE KNOWN, INTRINSIC** LIMITATIONS.

The Artificial General Intelligence (AGI)

CHILDREN DO NOT NEED TO READ THE WHOLE INTERNET WHILE THEY PERFECTLY MASTER HUMAN LANGUAGE.

The Artificial General Intelligence (AGI)

THAT ANYTHING THAT PLAYS A ROLE OF A SUBJECT IN A SENTENCE IN SERBIAN LANGUAGE NEEDS TO BE PUT IN THE NOMINATIVE CASE IS NOT **A STATISTICAL FACT. SIMILAR FOR PYTHON.**

The Artificial General Intelligence (AGI)

MORE IMPORTANT, "DO NOT KILL" AND "DO NOT STEAL" ARE NOT STATISTICAL FACTS.

Immediate risks, catastrophic risks

MISUSE OF THE TECHNOLOGY WEAPONIZATION OF AI JOB DISPLACEMENT **BIASES AND DISCRIMINATION PRIVACY VIOLATIONS EROSION OF HUMAN VALUES** DECREASE IN HUMAN CREATIVITY PLAGIARISM AUTOMATED PROPAGANDA

LOSS OF CONTROL INSTRUMENTAL CONVERGENCE EXTINCTION LEVEL EVENT UNEXPECTED CONSEQUENCES UNINTENDED VALUES ALIGNMENT SYSTEM FAILURE Immediate risks, catastrophic risks

WHEN WE INVENTED FAST INTERNET AND SOCIAL MEDIA, MANY STOPPED READING. NOW THAT WE HAVE COME UP WITH GENERATIVE ARTIFICIAL INTELLIGENCE, IS THERE A RISK THAT MANY WILL STOP THINKING?

The future

"Prediction is very difficult, especially about the future."

The future of the Internet

Vector database servers caching LLM embeddings for semantic search? Embeddings Exchange Points (EEP)? Emergent Web Ontologies?

The future of the Security and Privacy

Game Theory, business as usual. It will just be more difficult and more complicated than it already is - if that is possible at all. Automated propaganda: well, we were almost there already, it is only going to become cheaper.

The future of the Education

Creative problem solving and research should be considered a primary criterion for human development, while recognizing that knowledge of facts and their reproduction and recapitulation are of secondary importance only?

The future of work and creativity

The price of true creativity and genuine human intelligence will skyrocket. People might become motivated to discover "the new" again and again and compete against generative Als in what can be discovered and produced beyond recombination strategies.



Regulations and ethical guidelines

Although it has great potential for improving everyday life and work, the social consequences of widespread use of artificial intelligence are not easy to predict...

The EU is working on the AI Regulation (EU AI Act, expected in 2024), which is based on the assessment of the risk of AI application to human rights and society as a whole. For the most risky applications (unacceptable risk), a ban on the use of AI systems is proposed (e.g. systems that manipulate people at a subconscious level, continuous facial recognition and tracking systems in public spaces, social credit scoring). For less risky applications, various restrictions and obligations to provide publicly available information on how models are trained and applied are prescribed.

Serbia received its <u>"Ethical guidelines for the</u> <u>development, application, and use of reliable and</u> <u>responsible artificial intelligence</u> on 23 March 2023.

lilašinerija



