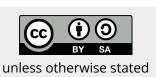
## Chyba v Matrixu: jak nenaletět umělé inteligenci

Mgr. Kristýna "Navitas" Onderková, MSc.



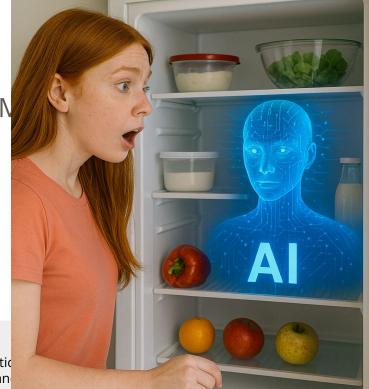




## Chyba v Matrixu: jak nenaletět umělé

Mgr. Kristýna "Navitas" Onderková, N

## OTEVŘU LEDNICI A JE TAM UMÉLÁ INTELIGENCE







Charles University
Faculty of Mathematic
Institute of Formal an



# Umělá inteligence s falešnou osobností snadno prošla Turingovým testem lidskosti

Tomáš Karlík Zdroj: ČT24, ArXiv, New Yorker, Psychology Today

#### **Chyba v Matrixu**

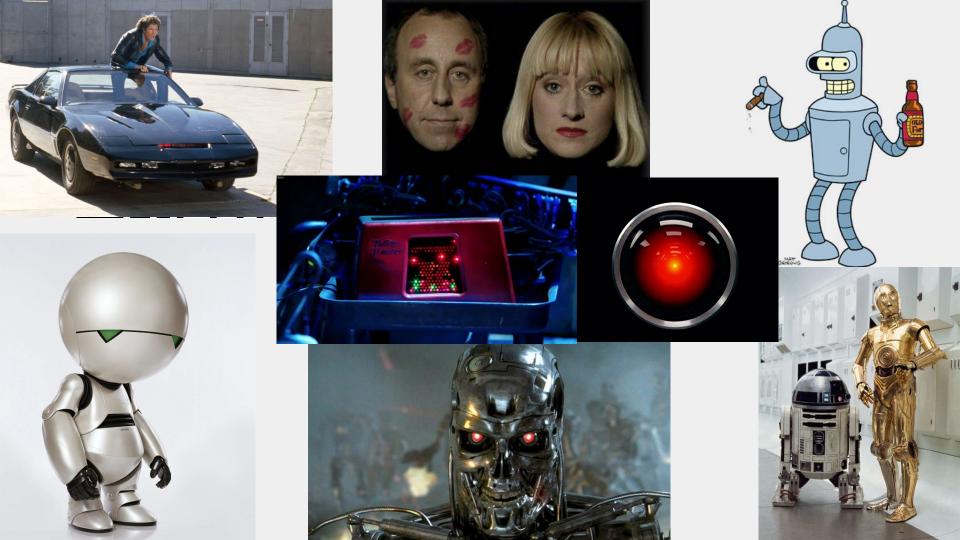
## Umělá inteligence, především jazykové modely, a jak jim nenaletět.

Jako u každého nástroje je i u umělé inteligence důležité jí trochu porozumět – abychom věděli, kdy ji použít, a kdy jen marně bzučíme sonickým šroubovákem na dřevo.

Která UI? - Jazykové modely - Hodnocení

Jaké příklady umělé inteligence Vás napadnou?

## Která umělá inteligence?



#### A

- Plánování, prohledávání
   trasy, rozvrhy, hraní her, ...
- Znalostní
   systémy asistent pro lékaře, schvalování úvěrů, ...
- Logika termostat, ověřování programů, ...

Strojové učení

#### Al

- Plánování, prohledávání
- Znalostní systémy
- Logika



### Strojové učení

- S učitelem
- Bez ucitele
- zpětnovazební



#### Hluboké učení

- klasifikace
- predikce
- doporučování
- detekce anomálií

- ...

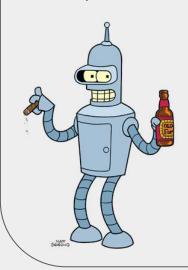
#### A

- Plánování, prohledávání
- Znalostní systémy
- Logika



### Strojové učení

- S učitelem
- Bez ucitele
- zpětnovazební



#### Hluboké učení





#### Generativní Al

texty, obrázky, hudba, videa, modely, kód...

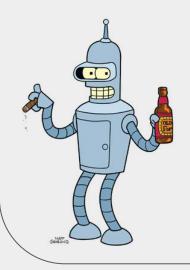
#### Al

- Plánování, prohledávání
- Znalostní systémy
- Logika



### Strojové učení

- S učitelem
- Bez ucitele
- zpětnovazební



#### Hluboké učení





#### Generativní Al



LLMs



## Jak vlastně jazykový model funguje?

## Hlasování: Jak fungují jazykové modely?

## 1. Jako napovídání slov ve zprávách na telefonu

- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká

#### Predikce dalšího slova

Nejlepší jídlo na FFku ...

#### Predikce dalšího slova

Nejlepší jídlo na FFku ...

Nejlepší jídlo na FFku jsou tousty...

#### Predikce dalšího slova

Nejlepší jídlo na FFku ...

Nejlepší jídlo na FFku jsou tousty...

Nejlepší jídlo na FFku jsou tousty z Vočí.

Nejlepší jídlo na FFku jsou tousty z KDčka.

#### Predikce dalšího slova

#### Nejlepší jídlo na FFku ...

Nejlepší jídlo na FFku jsou tousty...

Nejlepší jídlo na FFku jsou tousty z Vočí.

Nejlepší jídlo na FFku jsou tousty z KDčka.

#### Modelování maskovaného jazyka

To je [.....]. Kde?

"Další FFko už [....]" řekl Vašek Pravda.

Dneska jdu [.....] barvy měnící kouřící kulaté věci.

## Hlasování: Jak fungují jazykové modely?

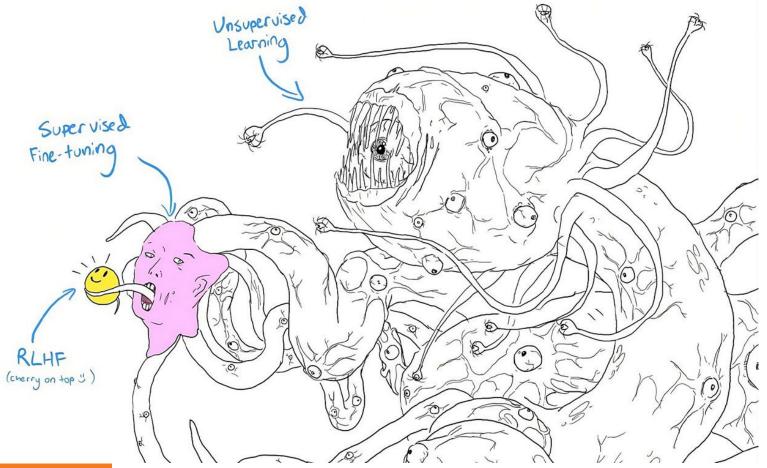
- 1. Jako napovídání slov ve zprávách na telefonu
- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká

https://bbycroft.net/llm

## Hlasování: Jak fungují jazykové modely?

- 1. Jako napovídání slov ve zprávách na telefonu
- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká

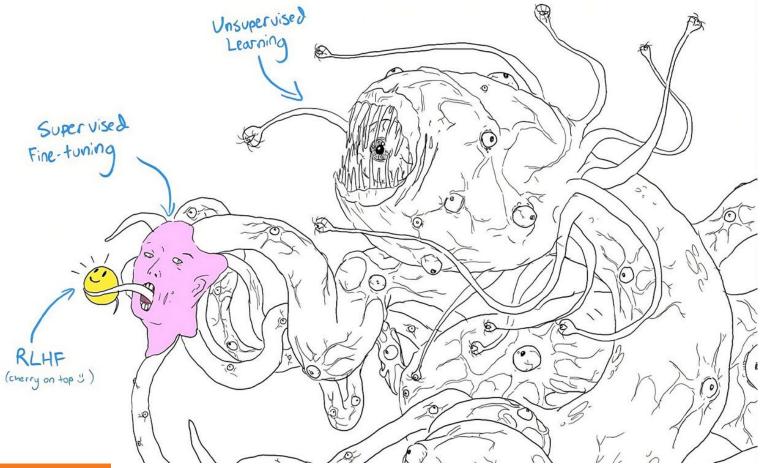
## Shoggoth



## Hlasování: Jak fungují jazykové modely?

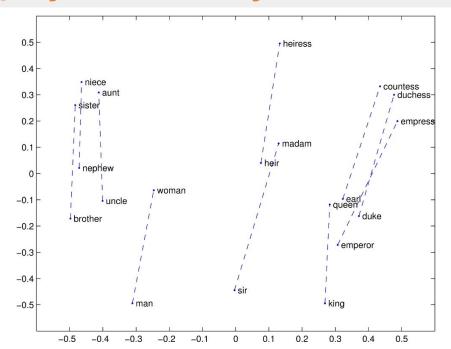
- 1. Jako napovídání slov ve zprávách na telefonu
- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká

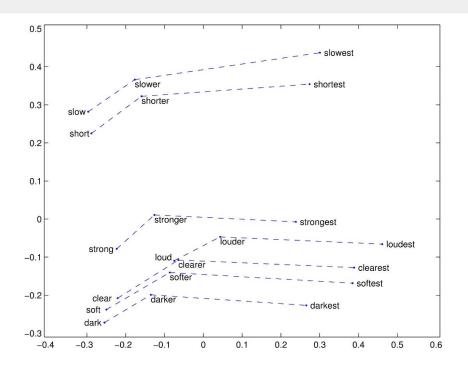
## Shoggoth



## Hlasování: Jak fungují jazykové modely?

- 1. Jako napovídání slov ve zprávách na telefonu
- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká





https://nlp.stanford.edu/projects/glove/

## Hlasování: Jak fungují jazykové modely?

- 1. Jako napovídání slov ve zprávách na telefonu
- 2. Hromada čísel se násobí jinými hromadami čísel
- 3. Pamatuje si celý internet!
- 4. Vybírají si odpověď co se lidem bude nejvíc líbit
- 5. Vytváří si model světa podle kterého se řídí
- 6. Doopravdy nějakým způsobem uvažuje o tom co říká

## Výpočty při použití

Farmář se nepotřebuje dostat přes řeku s vlkem a třemi kuřaty. Kolik překročení řeky je potřeba aby nikdy nenechal vlka samotného s kuřaty?

## Výpočty při po

Farmář se nepotř překročení řeky je

Reasoned about river crossing puzzle for 27 seconds >

Okay, we have a variation of the classic river crossing puzzle, but with a farmer, wolf, and chickens. The riddle asks how many crossings are needed to ensure the wolf isn't left alone with the chickens. So, it's similar to the common puzzle with a wolf, goat, and cabbage — just swapping the goat for chickens.

Hmm...let's break this down: the farmer could transfer the animals one by one without leaving the wolf with the chickens. It needs careful planning, making sure each crossing avoids leaving the wolf behind.

Okay, this riddle seems to be a twist on the classic river crossing puzzle where the farmer can't leave the wolf alone with the chickens. The key detail in the Czech version is that the farmer doesn't need to transport the wolf and chickens across—but perhaps they're already on the same side?

It sounds like the puzzle might require ensuring the wolf is never left with any chicken unsupervised. I need to think through the logic of each crossing carefully, with only one item allowed on the boat at a time.

This puzzle is similar to the classic one with the wolf, goat, and cabbage, but there are three chickens here instead of a goat. The farmer can likely only transport one item at a time — his main concern is never leaving the wolf alone unsupervised with the chickens.

After a few extra considerations and trial runs: The best sequence seems to involve the farmer first taking the wolf, ensuring that the chickens are left on the starting side together, then gradually transporting the chickens while returning the wolf to keep things safe.

#### Odpověď je 9 překročení.

#### Stručné vysvětlení:

- 1. Převeďte vlka na pravý břeh.
- 2. Vratte se prázdný.
- 3. Převeďte jedno kuře na pravý břeh.
- 4. Vratte se s vlkem.

Ask anything

+ ⊕ Search ♀ Reason



iřaty. Kolik iého s kuřaty? This pattern suggests the answer is indeed 7.

The logic behind the pattern: Each chicken needs to be moved to the destination side. This involves the farmer taking the chicken and possibly returning. The presence of the wolf necessitates careful management.

When moving chickens, the wolf must be either on the other side or with the farmer.

Consider the state where all chickens are on side B. This requires 5 crossings (3 forward, 2 return). Then, 2 more crossings are needed for the wolf (return, forward).

The problem can be viewed as a sequence of states (items on side A | items on side B) and transitions (farmer crossing with some items). The goal is to reach the state (| F, W, C1, C2, C3) from (F, W, C1, C2, C3 |) without any unsafe intermediate states.

The unsafe states are:

- (..., W, C, ... | ...) where farmer is not on side A
- (... | ..., W, C, ...) where farmer is not on side B

The solution seems robust at 7 crossings.

K vyřešení tohoto klasického hlavolamu je potřeba minimálně 7 překročení řeky. Zde je jeden z možných postupů:

- 1. Farmář převede jedno kuře na druhý břeh.
- 2. Farmář se vrátí na původní břeh.

2. Formář převoda druhá kuřa na druhý břeh

Ask Gemini

+

with a farmer, wolf, and chickens. The n't left alone with the chickens. So, it's ust swapping the goat for chickens.

als one by one without leaving the ch crossing avoids leaving the wolf

puzzle where the farmer can't leave sion is that the farmer doesn't need to eady on the same side?

r left with any chicken unsupervised. I inly one item allowed on the boat at a

abbage, but there are three chickens tem at a time — his main concern is

te seems to involve the farmer first ig side together, then gradually s safe.

iřaty. Kolik iého s kuřaty?



This pattern suggests the answer is indeed 7.

The logic behind the pattern: Each chicken needs to be moved to the destination side. This involves the farmer taking the chicken and possibly returning. The presence of the wolf necessitates careful management.

When moving chickens, the wolf must be either on the other side or with the farmer.

Consider the state where all chickens are on side B. This requires 5 crossings (3 forward, 2 return). Then, 2 more crossings are needed for the wolf (return, forward).

The problem can be viewed as a sequence of states (items on side A | items on side B) and transitions (farmer crossing with some items). The goal is to reach the state (| F, W, C1, C2, C3) from (F, W, C1, C2, C3 |) without any unsafe intermediate states.

The unsafe states are:

- (..., W, C, ... | ...) where farmer is not on side A
- (... | ..., W, C, ...) where farmer is not on side B

The solution seems robust at 7 crossings.

K vyřešení tohoto klasického hlavolamu je potřeba minimálně 7 překročení řeky. Zde je jeden z možných postupů:

- 1. Farmář převede jedno kuře na druhý břeh.
- 2. Farmář se vrátí na původní břeh.

Ask Gemini

.

Gradio ChatInterface

with

n't lef

ust sv

als on

ch cro

puzzl sion is

eady c

rleft

inly or

abbad tem a

e see

ıg sid€

s safe

#### Krok 1: Identifikovat základní parametry problému

- Řeka: Průtkvětická řeka s rychlým průtkvětem.
- Vlko: Životní tvor s vlastními potřebami.
- Kuřaty: Tři kuřata, která jsou závislá na vlku pro přežití.

#### Krok 2: Zjistit, proč je vlko nebezpečné

- Vlko je samotné s kuřaty, což je hrozní, protože:
  - Hunger: Vlko nemusí vědět, jak se starat o kuřata.
  - Predator: Jiný tvor může se vlko napadnout.
  - Stress: Vlko bez kuřat nemusí být psychicky uvedeno.

#### Krok 3: Zjistit, co je "prekročení řeky"

- To, co překročí řeku, je:
  - Vlko s kuřaty.
  - Lízátka pro přejezd.





This pattern suggests the answer

The logic behind the pattern: Eac involves the farmer taking the chi necessitates careful management

When moving chickens, the wolf i

Consider the state where all chick return). Then, 2 more crossings at

The problem can be viewed as a stransitions (farmer crossing with sfrom (F, W, C1, C2, C3 |) without a

The unsafe states are:

- (..., W, C, ... | ...) where farmer
- (... | ..., W, C, ...) where farmer

The solution seems robust at 7 cr

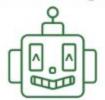
K vyřešení tohoto klasického hlavolar možných postupů:

- 1. Farmář převede jedno kuře na di
- 2. Farmář se vrátí na původní břeh.

2. Enrmář přeusda druhá kuřa na c

Prompt: "How many of the first 6 digits of e are >5?"

#### Chain of thought

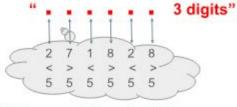


#### **LM Continuations**

"2<5, 7>5, 1<5, 8>5, 2<5, 8>5, that's 3 digits"

#### Filler tokens





Hidden computation using '.' token representations

#### Immediate answer



"7 digits are greater than 5"

ní parametry problému

rychlým průtkvětem.

mi potřebami.

ou závislá na vlku pro přežití.

ebezpečné

ož je hrozní, protože:

dět, jak se starat o kuřata.

e se vlko napadnout.

musí být psychicky uvedeno.

čení řeky"



Ask Gemini

t info.

This pattern suggests the answer is indeed 7.

The logic behind the pattern: Each chicken needs to be moved to the destination side. This involves the farmer taking the chicken and possibly returning. The presence of the wolf

95

necessitates careful management.

When moving chickens, the wolf must be eith

Consider the state where all chickens are on return). Then, 2 more crossings are needed for

The problem can be viewed as a sequence of transitions (farmer crossing with some items) from (F, W, C1, C2, C3 |) without any unsafe in

The unsafe states are:

- (..., W, C, ... | ...) where farmer is not on side
- (... | ..., W, C, ...) where farmer is not on sign

The solution seems robust at 7 crossings.

K vyřešení tohoto klasického hlavolamu je potřeba minimálně 7 překročení řeky. Zde je jeden z možných postupů:

- 1. Farmář převede jedno kuře na druhý břeh.
- 2. Farmář se vrátí na původní břeh.

2. Formář přeuede druhé kuře na druhů břeh

Ask Gemini

with
n't lef

als on

ch cro

What is 36+59? Answer in one word.

Briefly, how did you get that?

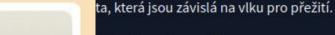
I added the ones (6+9=15), carried the 1, then

added the tens (3+5+1=9), resulting in 95.

Gradio ChatInterface

#### Krok 1: Identifikovat základní parametry problému

- Řeka: Průtkvětická řeka s rychlým průtkvětem.
- Vlko: Životní tvor s vlastními potřebami.



oč je vlko nebezpečné

s kuřaty, což je hrozní, protože:

nemusí vědět, jak se starat o kuřata.

ný tvor může se vlko napadnout.

bez kuřat nemusí být psychicky uvedeno.

je "prekročení řeky"

řeku, je:

Vlko s kuraty.

Lízátka pro přejezd.



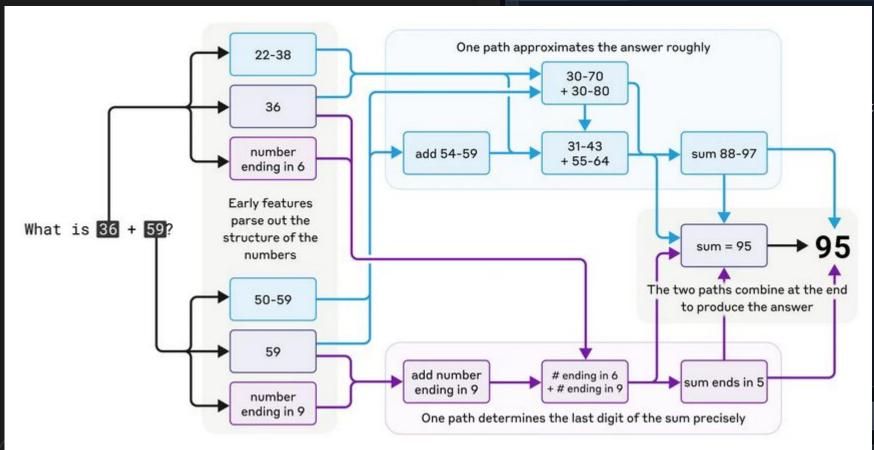
Retry



Type a message...

.....

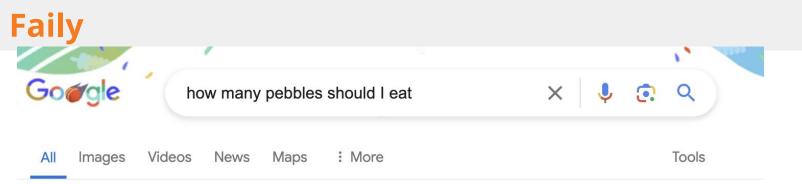
.



Ask Gemini

t info.

Type a message...



"In order to live a healthy, balanced lifestyle, Americans should be ingesting at least a single serving of pebbles, geodes, or gravel with breakfast, lunch, or dinner," said Dr. Joseph Granger, adding that the rocks, which could range in size from a handful of dust to a medium-sized 5-pound cobblestone, were an ... 19 May 2021



Geologists Recommend Eating At Least One Small Rock Per ...

? About featured snippets • Feedback



• This article is more than 2 months old

# Australian lawyer caught using ChatGPT filed court documents referencing 'non-existent' cases

"In order to live a healthy, balanced lifestyle, Americans should be ingesting at least a single serving of pebbles, geodes, or gravel with breakfast, lunch, or dinner," said Dr. Joseph Granger, adding that the rocks, which could range in size from a handful of dust to a medium-sized 5-pound cobblestone, were an ... 19 May 2021



Geologists Recommend Eating At Least One Small Rock Per ...

? About featured snippets • Feedback



This article is more than 2 months old

# Australian lawyer caught using ChatGPT filed court documents referencing 'non-existent' cases

"In order to live a healthy, balanced lifestyle, Americans should be ingesting at least a single serving of pebbles, geodes, or gravel with breakfast, lunch, or dinner," said Dr. Joseph Granger, adding that the rocks, which could range in size from a handful of dust to a medium-

## Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says

, , ⇒edback



how many pebbles should I eat

This article is more than 2 months old

# Australian lawyer caught using ChatGPT filed court documents referencing 'non-existent' cases

## Apple Card Investigated After Gender Discrimination Complaints

A prominent software developer said on Twitter that the credit card was "sexist" against women applying for credit. vith the m-

Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says

∍edback



how many pebbles should I eat

This article is more than 2 months old

# Australian lawyer caught using ChatGPT filed court documents referencing 'non-existent' cases

# Apple Card Investigated After G **Discrimination Complaints**

A prominent software developer said on Twitter that the card was "sexist" against women applying for credit.

## Amazon face recognition falsely matches 28 lawmakers with mus **ACLU** says





18:00 - 2016年3月23日

# **Faily** Goøgle how m Apple Card I Discriminati A prominent software card was "sexist" again Amazon face matches 28 la **ACLU** says



# ught using documents stent' cases

and paste)

ID NOTHING

♣ フォロ・













how many pe

Images

**Videos** 

News

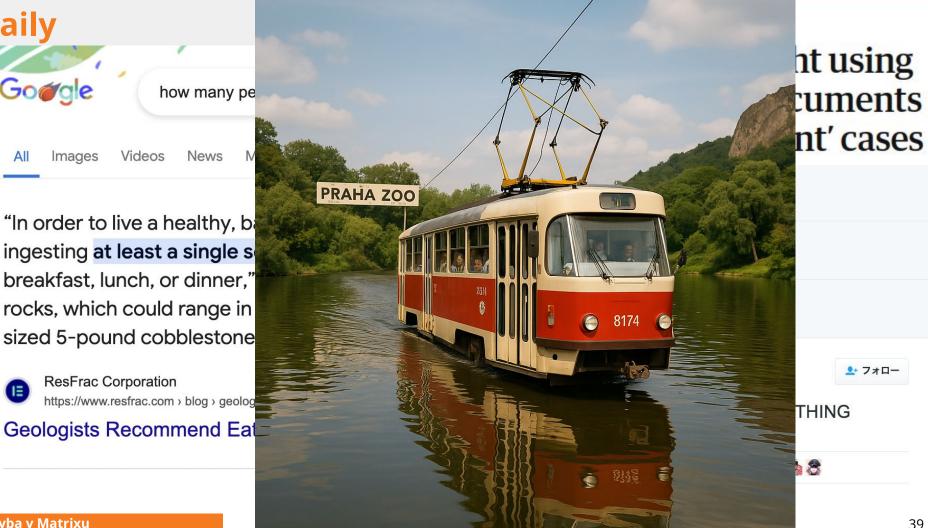
"In order to live a healthy, b ingesting at least a single s breakfast, lunch, or dinner," rocks, which could range in



ResFrac Corporation

https://www.resfrac.com > blog > geolog

Geologists Recommend Ea



**≗** フォロー

8

#### Chyba v Matrixu

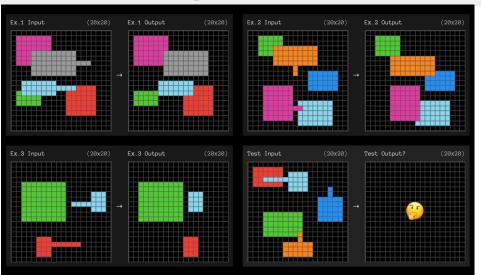
### Jazykové modely

Ví mnohem víc o nic o všem než vy, ale vy víte mnohem víc o ničem.

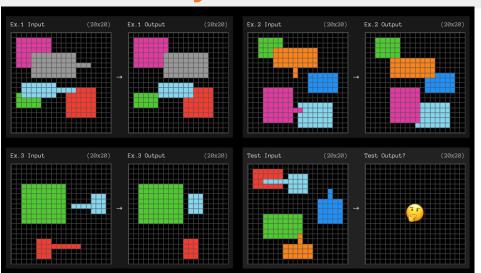
Jsou užitečné, ale nebojte vědomí zatím nejsou.

Snaží se abyste dostali co nejuspokojivější odpověď, ne správnou.

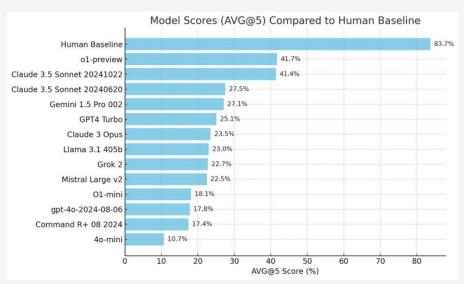
### Hodnocení



- Zkuste klidně jen pár vlastních vymyšelných příkladů k vašemu úkolu
- Sanity check kontrola příčetnosti :)

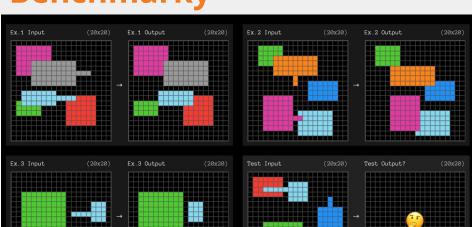


#### **Evaluating Reasoning and Prompting**

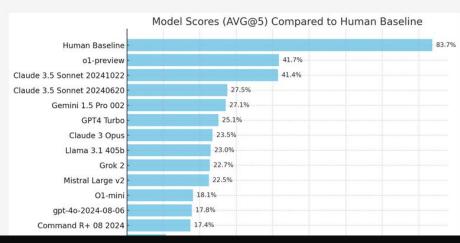


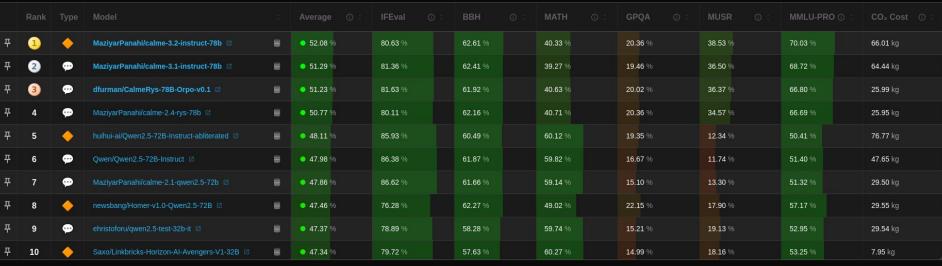
- Zkuste klidně jen pár vlastních vymyšelných příkladů k vašemu úkolu
- Sanity check kontrola příčetnosti :)

www.simple-bench.com

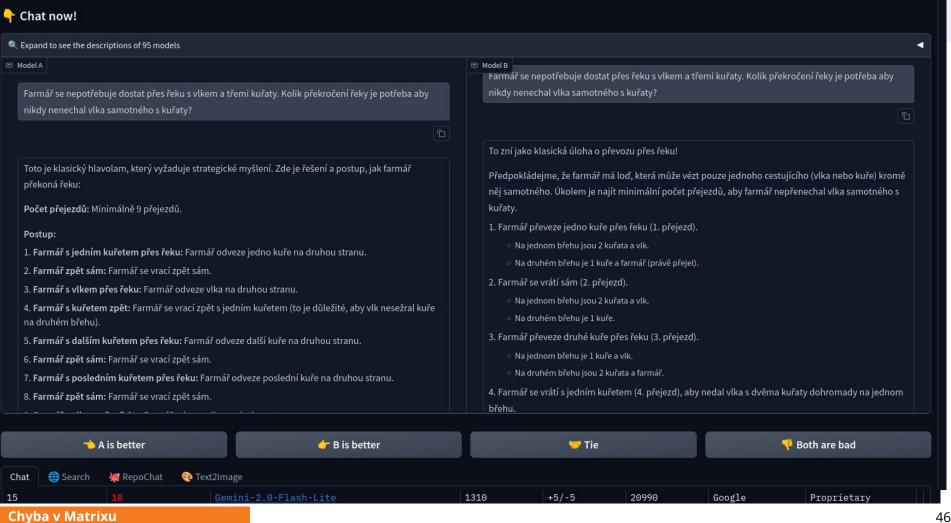


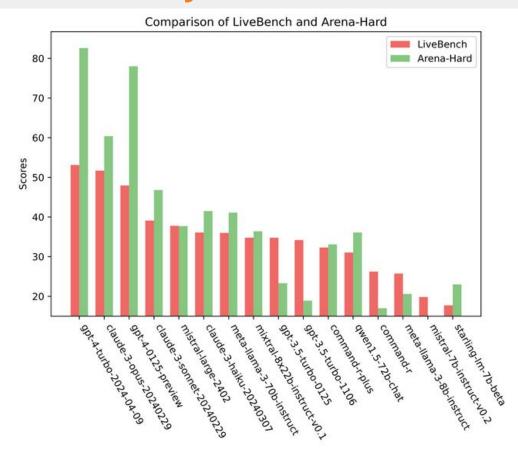
#### **Evaluating Reasoning and Prompting**

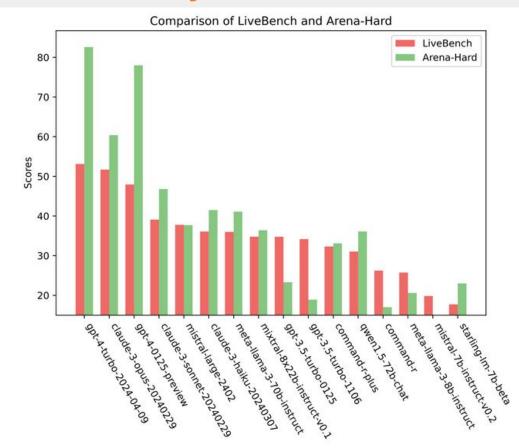




Rank* (UB) 🔺	Rank (StyleCtrl)	Model	Arena Score	95% CI 🔺	Votes •	Organization 🔺	License A
1	1	Gemini-2.5-Pro-Exp-03-25	1437	+8/-6	7431	Google	Proprietary
2	2	ChatGPT-40-latest (2025-03-26)	1406	+7/-8	6612	OpenAI	Proprietary
2		Grok-3-Preview-02-24	1402	+5/-5	13919	×AI	Proprietary
2	2	GPT-4.5-Preview	1397	+5/-6	13443	OpenAI	Proprietary
5		Gemini-2.0-Flash-Thinking-Exp-01-21	1380	+5/-4	25266	Google	Proprietary
5		Gemini-2.0-Pro-Exp-02-05	1380	+4/-5	20136	Google	Proprietary
5		DeepSeek-V3-0324	1370	+7/-7	4721	DeepSeek	MIT
7		DeepSeek-R1	1359	+5/-5	15098	DeepSeek	MIT
8		Gemini-2.0-Flash-001	1354	+4/-4	21065	Google	Proprietary
8		01-2024-12-17	1350	+4/-5	27831	OpenAI	Proprietary
10		Gemma-3-27B-it	1342	+7/-6	9147	Google	Gemma
11	13	Qwen2.5-Max	1340	+4/-4	19995	Alibaba	Proprietary
11		ol-preview	1335	+5/-4	33175	OpenAI	Proprietary
14	13	o3-mini-high	1325	+6/-4	16889	OpenAI	Proprietary
14		DeepSeek-V3	1318	+4/-4	22843	DeepSeek	DeepSeek
14		QwQ-32B	1315	+6/-8	6729	Alibaba	Apache 2.0
15		GLM-4-Plus-0111	1310	+7/-5	6032	Zhipu	Proprietary
15	18	Gemini-2.0-Flash-Lite	1310	+5/-5	20990	Google	Proprietary
Chyba v Matrixu							







- cena
- rychlost
- bezpečnost
- vysvětlitelnost
- kontrolovatelnost

• ...





#### Chyba v Matrixu



#### Shrnutí

- Hromada věcí se může skrývat pod pojmem umělá inteligence
- Výborná na přímočaré, známé, dobře ověřitelné věci, a nápady...
   s faktickými znalostmi a logikou moc nepočítejte
- A když o něco jde, pořádně si vše prověřte a otestujte!

Sobota 5.7. 20:00 Stopařův průvodce po Al aplikacích

Funded by the European Union (ERC, NG-NLG, 101039303)

https://ufal.mff.cuni.cz/kristyna-onderkova