



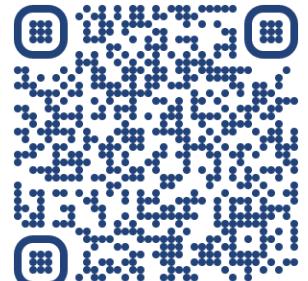
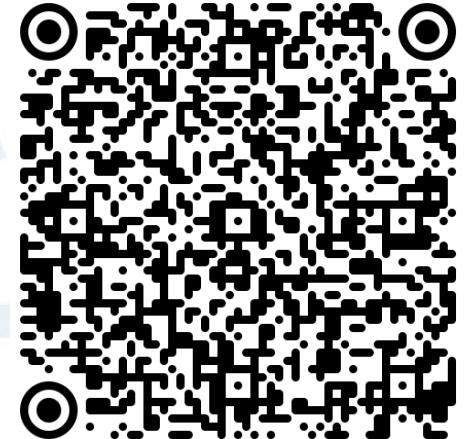
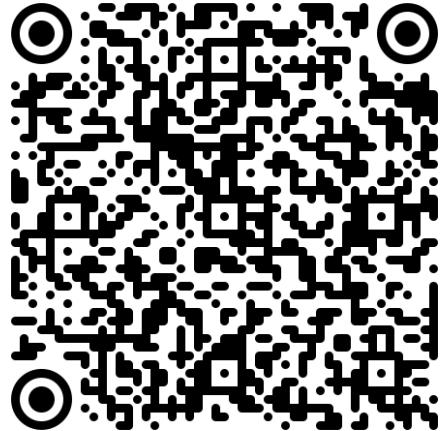
HOGESCHOOL
ROTTERDAM

Generatieve AI

*“Hoe kan het gebruik van
Gen-AI valide en veilig
worden geïntegreerd?”*

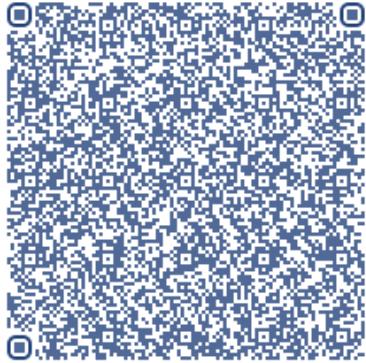
Een open-source product gemaakt door
het HR-brede programma voor AI &
Ethiek <http://hr.nl/ai>

[Rob van der Willigen](#)

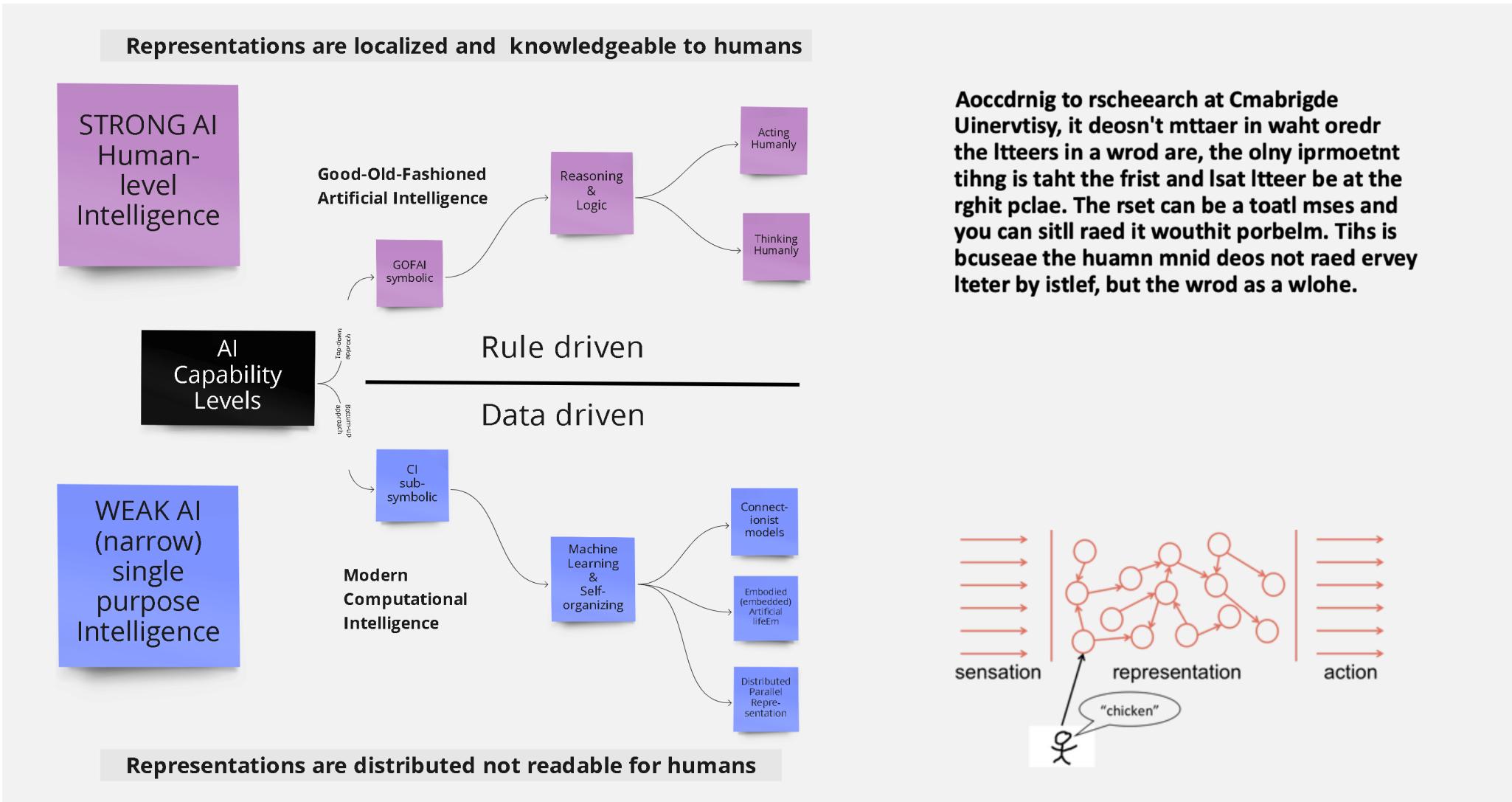


hr.nl/ai

AI-taxonomie is complex



https://www.researchgate.net/publication/359424818_Designing_Neural_Networks_Through_Sensory_Ecology_Biology_to_the_rescue_of_AI_Produced_by_Living-Lab_AIRA_Hub_voor_Data_Responsible_AI_Hogeschool_Rotterdam_Lunch-Lezing_Creating-010_FEB_2022



Generative AI according to Google

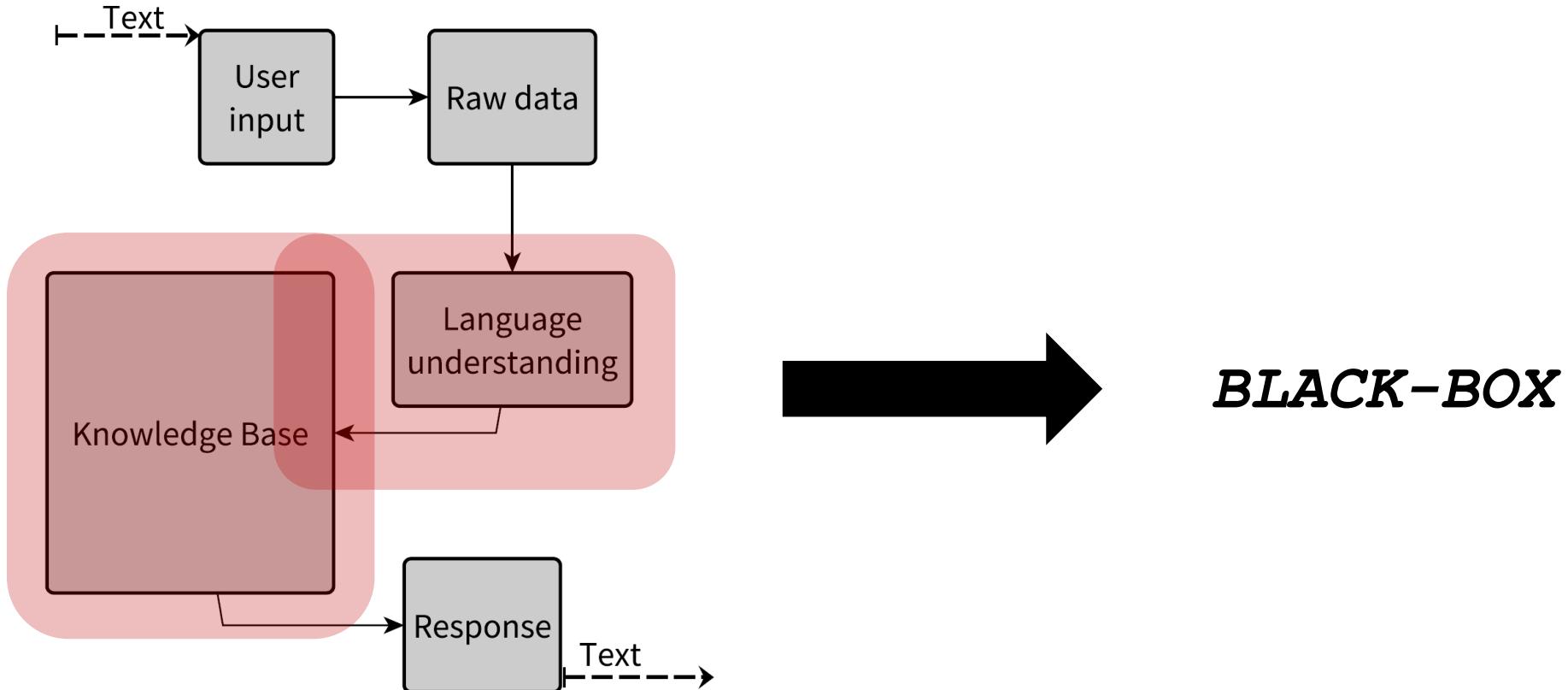
Machine learning (ML) model that can take what it has learned from multimodal-examples it has been provided to create new content, such as text, images, music, and code.

These models learn through observation and pattern matching, also known as training.

Generative AI models are neither information databases nor deterministic information retrieval systems, because they are prediction engines.

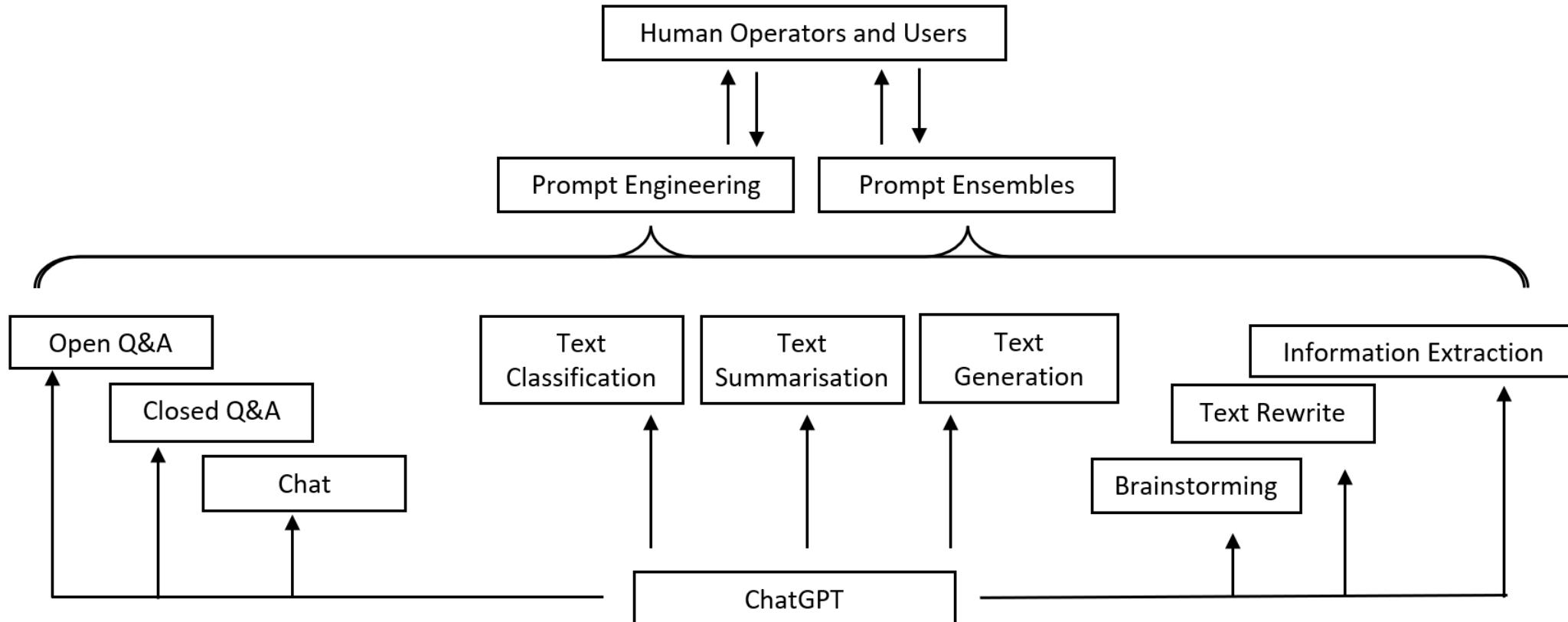
TALIGE IMPLEMENTATIE
*Gen-AI worden
gerepresenteerd door
Conversationele Agenten
== **Chatbots***

ChatGPT is een Conversationele *tekst-in/tekst-uit* AI-agent



Sánchez-Díaz, X., Ayala-Bastidas, G., Fonseca-Ortiz, P., & Garrido, L. (2018).
A knowledge-based methodology for building a conversational chatbot as an
intelligent tutor. https://doi.org/10.1007/978-3-030-04497-8_14

ChatBot Use-Cases



Conferences > 2023 IEEE International Confe... ⓘ

ChatGPT and Generative AI Guidelines for Addressing Academic Integrity and Augmenting Pre-Existing Chatbots

Publisher: IEEE

Cite This

PDF

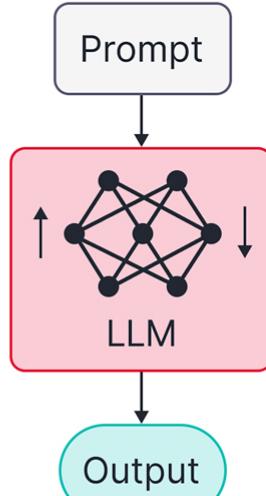
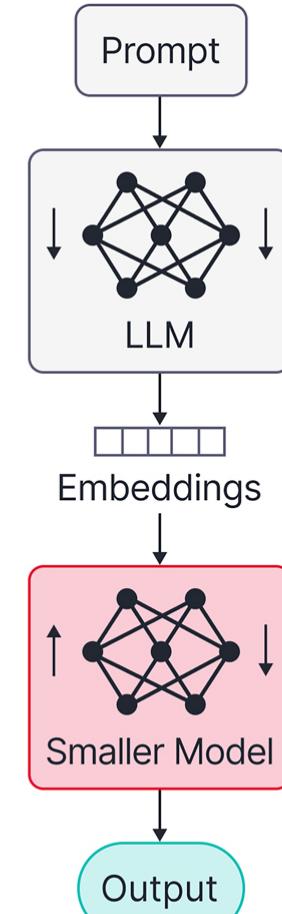
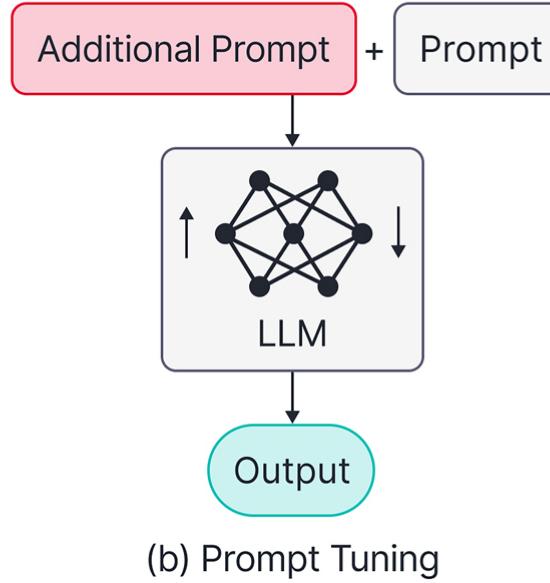
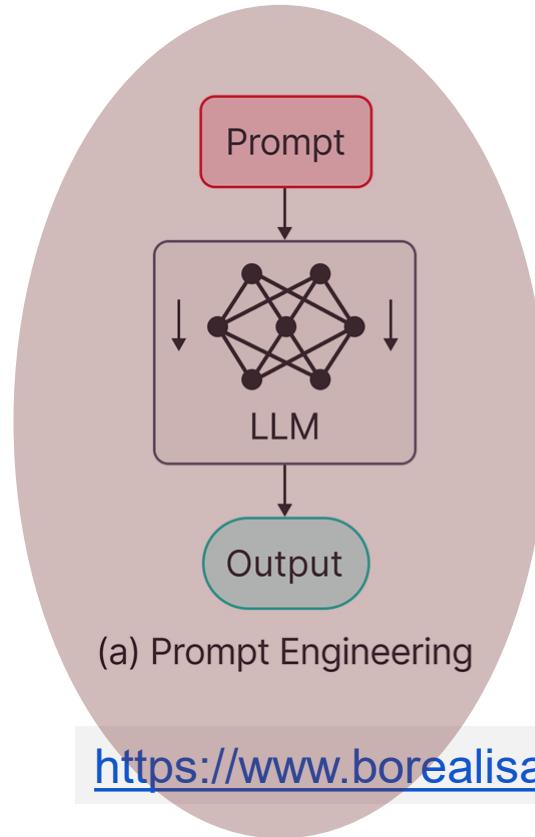
Daswin De Silva ; Nishan Mills ; Mona El-Ayoubi ; Milos Manic ; Damminda Alahakoon [All Authors](#)

635
Full
Text Views

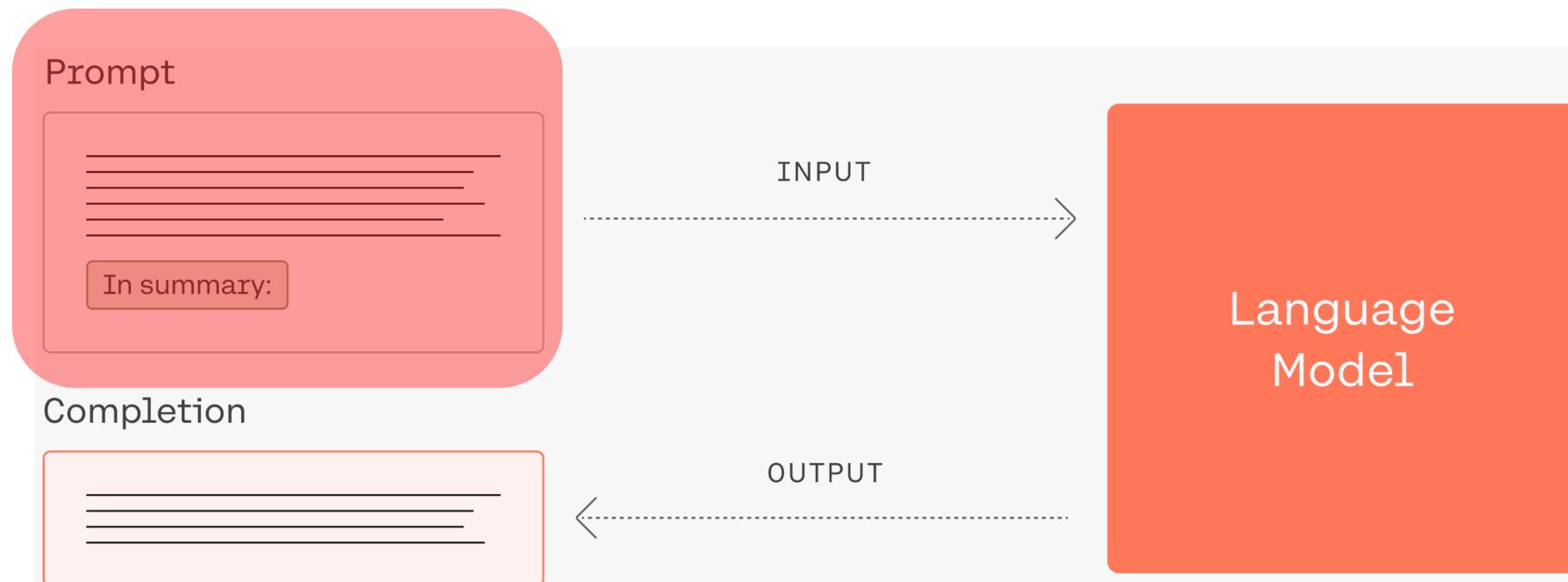


*Hoe kun je optimaal
gebruik maken
van Gen-AI Chatbots:
ChatGPT, Bard & Copilot*

Vier manieren om Chatbots te benutten



*Conversationele AI-agenten worden aangestuurd via “**prompts**”*



<https://docs.cohere.com/docs/prompt-engineering>



<https://docs.cohere.com/docs/introduction-to-large-language-models>

PROMPT-ENGINEERING

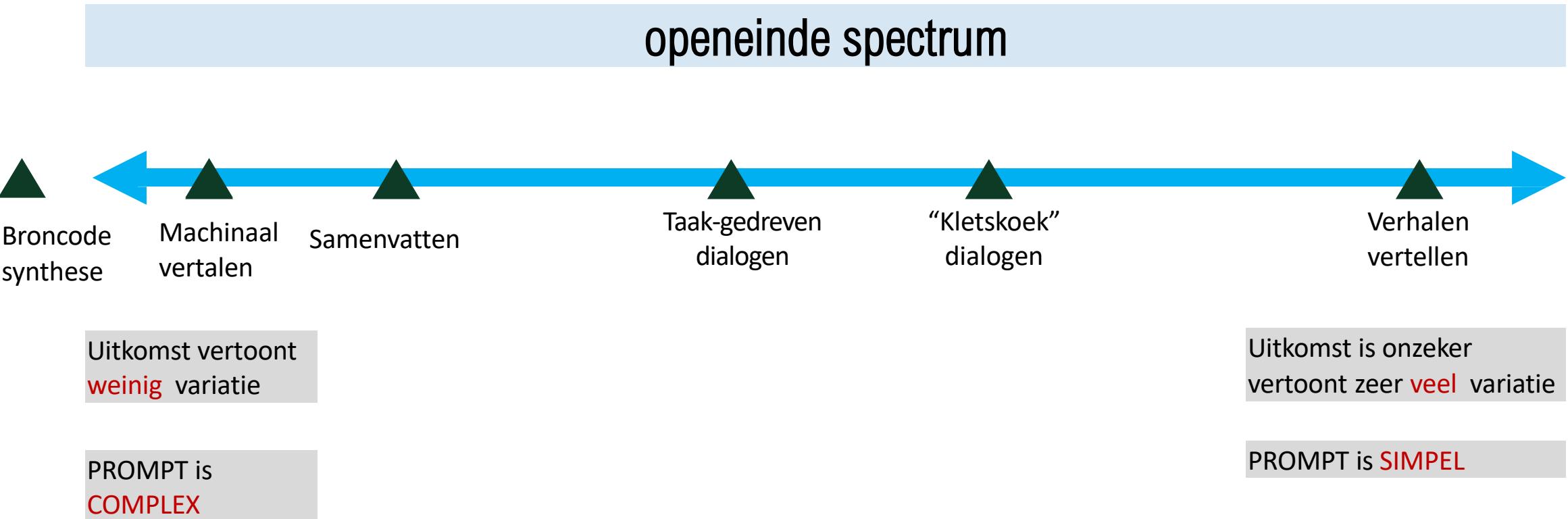
Het creatieve proces van het schrijven van een effectief ***prompt-recept*** wordt in het Engels "***prompt engineering***" genoemd.

Het schrijven van prompt-recepten

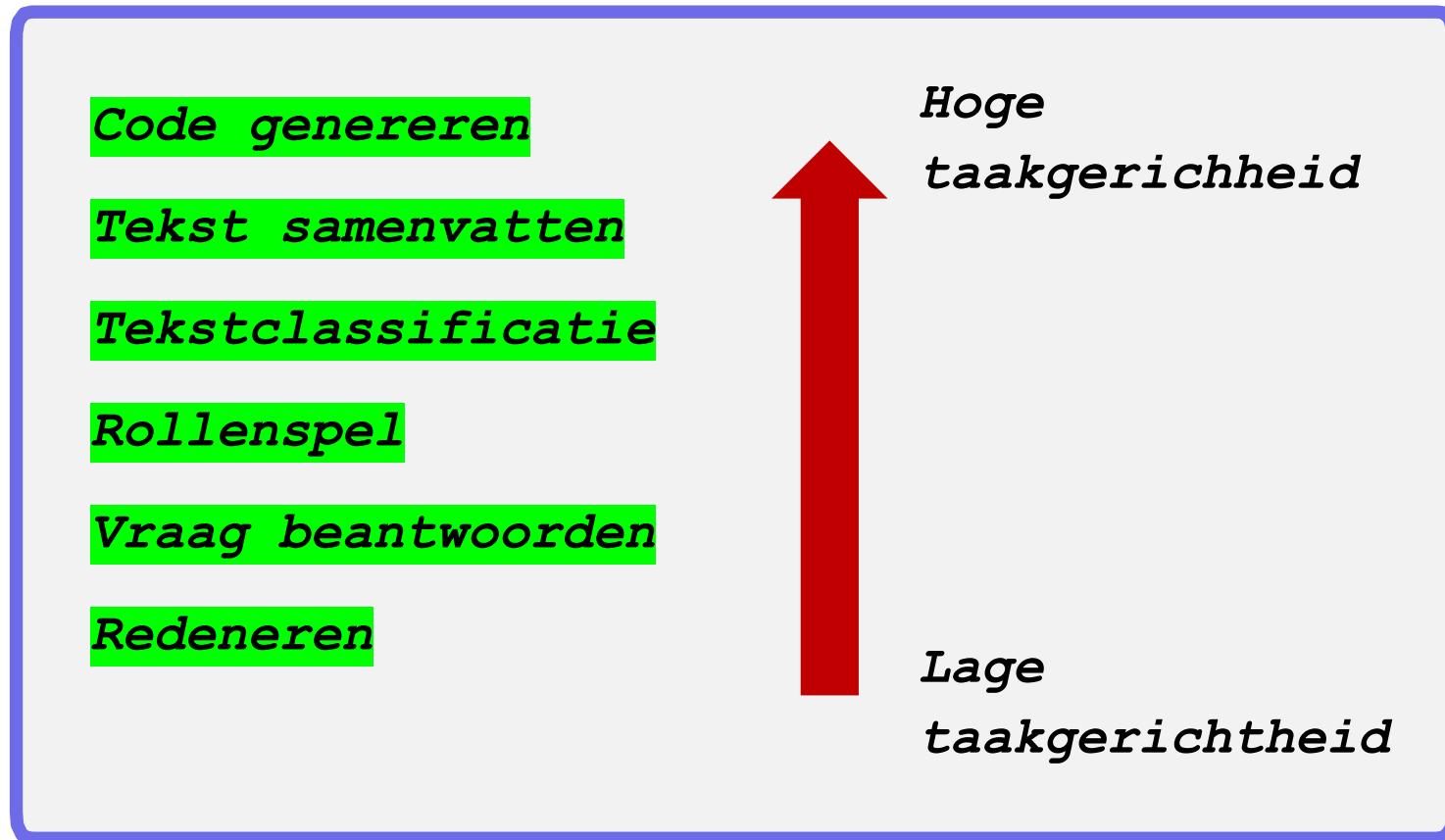
---pseudo-Code---

is een talige manier van het programmeren van "bevroren" voorgetraind taalmodellen.

Prompt Taxonomie



Taakgerichtheid van prompts



Wat is het belang van Prompt Recepten Schrijven?

*Sturen van de mate van taakgerichtheid door
reduceren van variatie in het antwoord zodat de
kans groter wordt dat de uitkomst correct is.*

Prompt Recept Structuur

Een prompt is opgebouwd uit de volgende elementen:

Instructie(s)

Context

Invoergegevens

Uitvoer-indicator

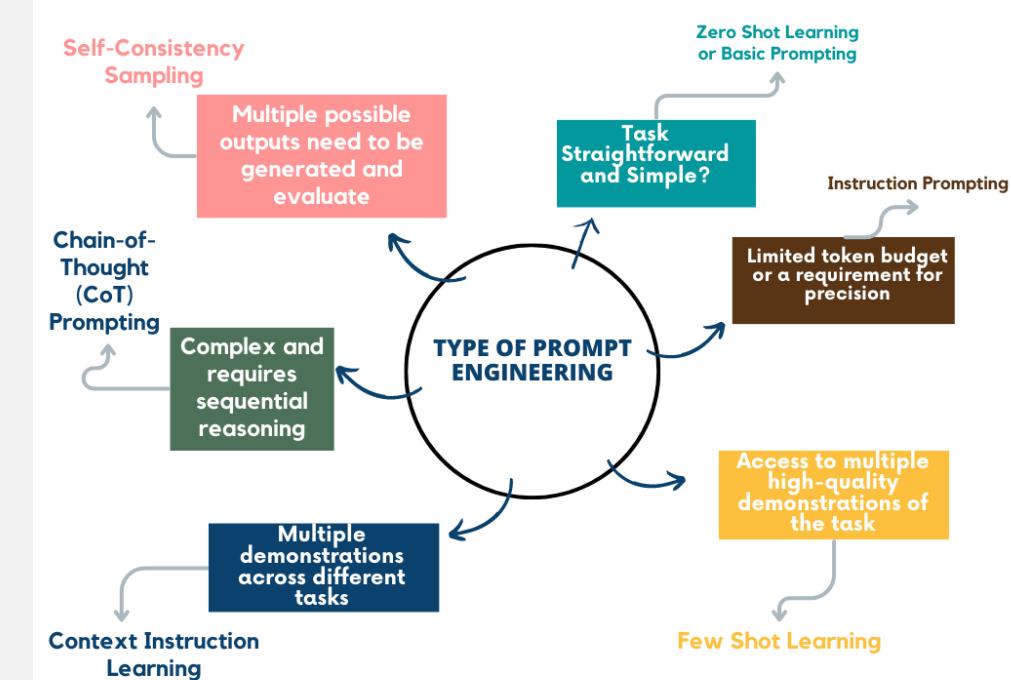
Classificeer de onderstaande tekst als neuraal, negatief of positief

Text: Ik vond het eten wel zoso.

Sentiment:

Prompt recept ontwerptechnieken gebaseerd op fine-tuning van het onderliggende taal-model

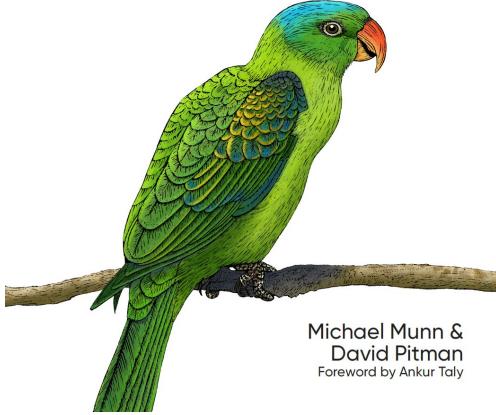
Few-shot prompts (**In Context Leren**)
Chain-of-thought (**CoT**) reasoning
Self-Consistency Sampling
Knowledge Generation Prompting
ReAct



*Hoe kun je veilig & FAIR
gebruik maken
van Gen-AI Chatbots:
ChatGPT, Bard & Copilot*

Explainable AI for Practitioners

Designing and Implementing
Explainable ML Solutions



Michael Munn &
David Pitman
Foreword by Ankur Taly

Interpretability

- Dependent on model architecture
- Computationally fast
- Can be inferred from the model alone

Linear and logistic regression

Decision rules

Generated linear models and generalized additive models

Decision trees

TCAVs

Example-based

Integrated Gradients and its relatives

LIME

Sampled Shapley

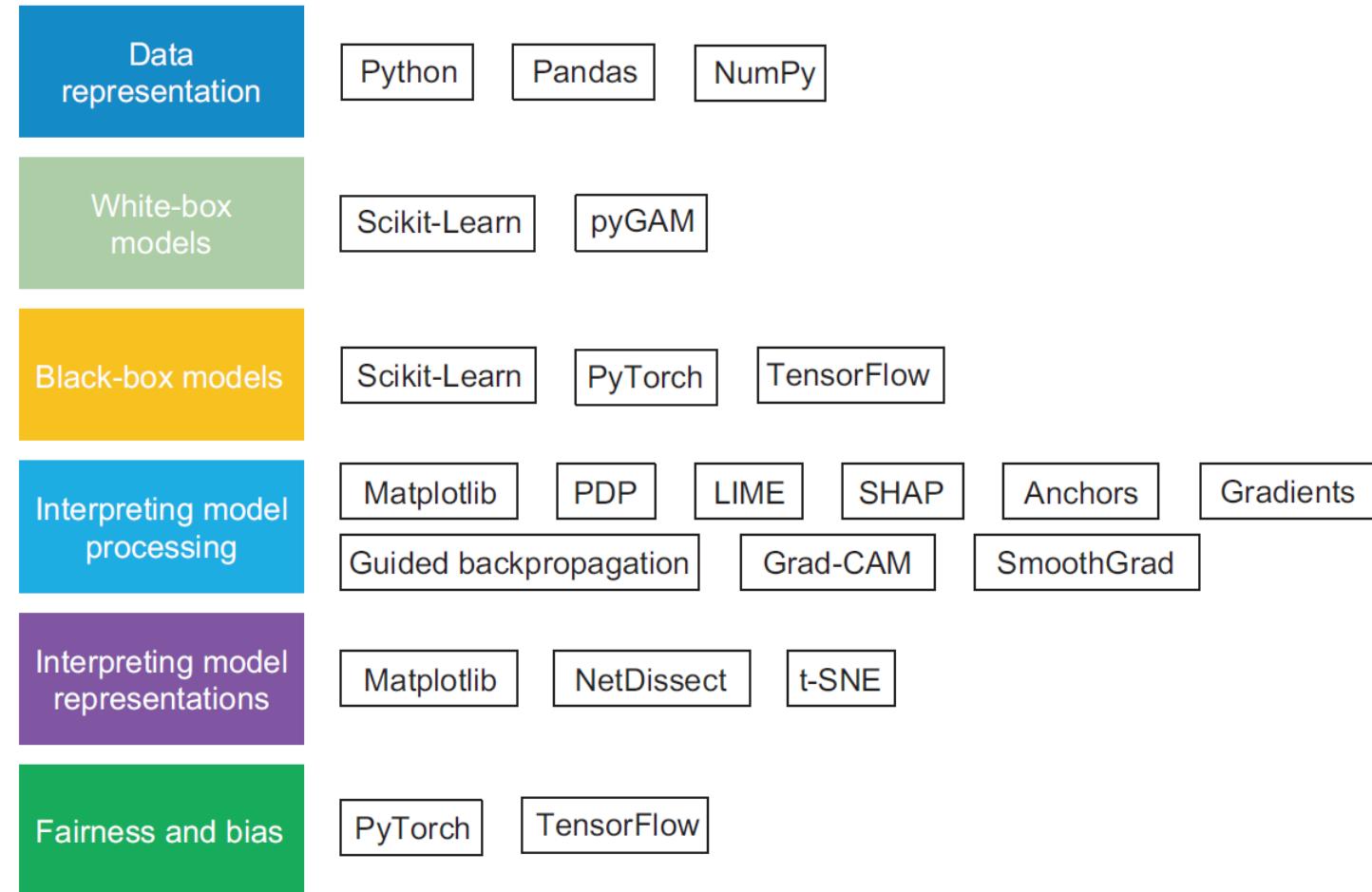
Explainability

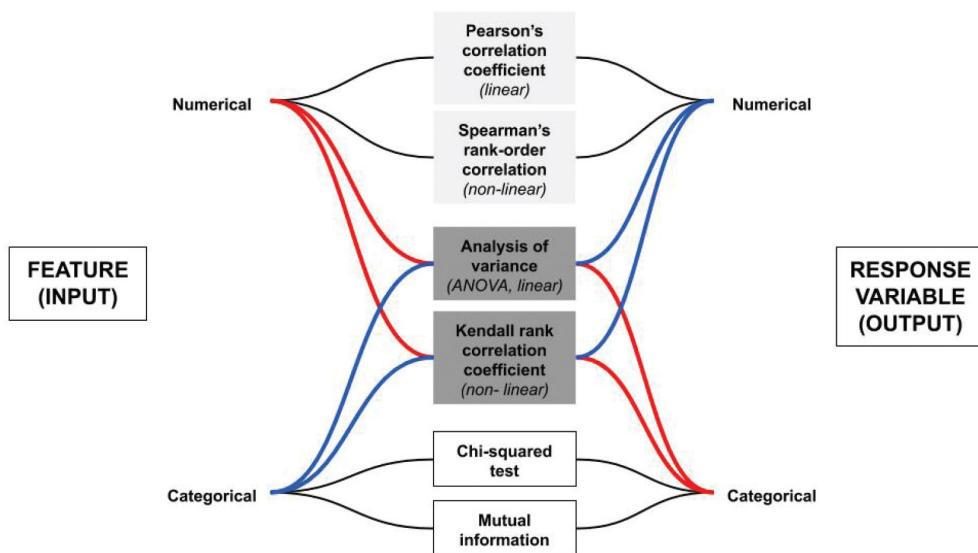
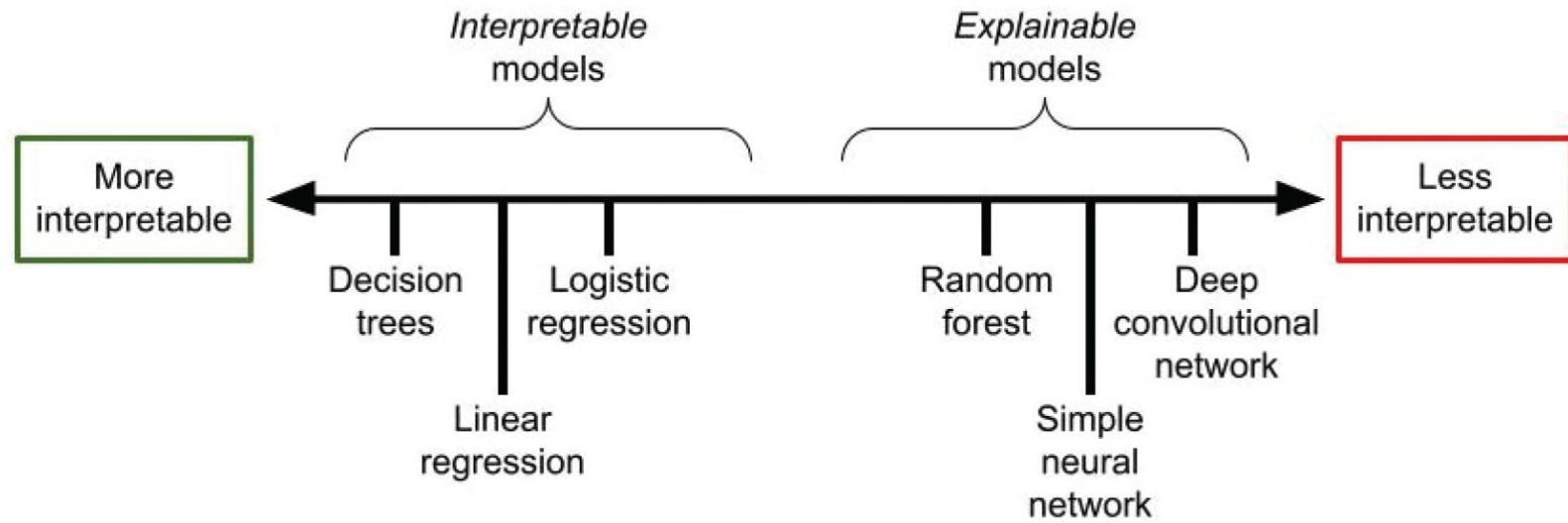
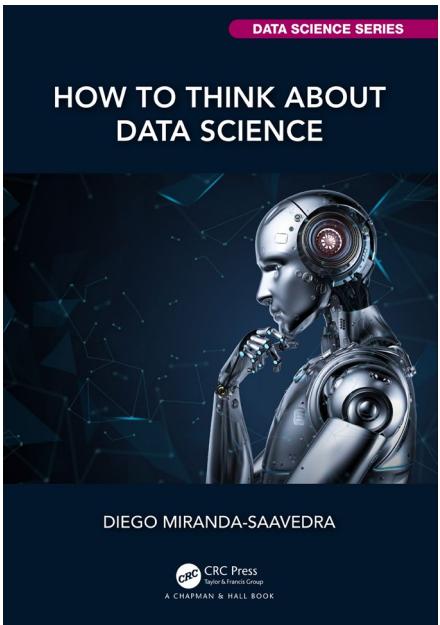
- Model-agnostic
- Computationally intensive
- Based on feature values and predictions

Interpretable AI

Ajay Thampi

MANNING





*Hoe kun je
<gevoelige / private > data
beschermen +
Dialog effectief &
unbiased sturen*

Context

Waarom is RAG nodig als ik al vragen kan stellen over teksten via Gen-AI?

Gen-AI applicaties gebaseerd op grote taalmodellen (LLMs) verwijzen naar elke vorm van machinaal-lerende (ML) kunstmatige intelligentie (AI) die gebruikt maakt van natuurlijke taal verwerkende (NLP) algoritmen.

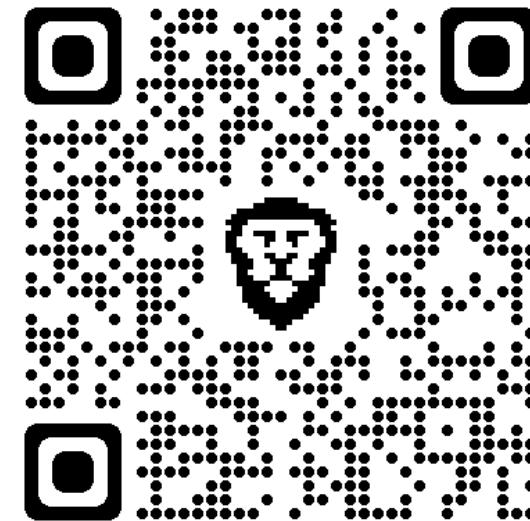
Eindgebruikers kunnen online gebruik maken deze conversationele agenten (Chatbots zoals Bard, Co-Pilot, en ChatGPT) via webbrowser userinterfaces. Hierdoor is het mogelijk om via zelf-geschreven, textuele instructies (zogenaamde prompts), content te genereren, in de vorm van tekst, broncode, afbeeldingen, video's, muziek etc.

LLMs worden tijdens hun trainingfase gevoed met publiekelijk beschikbare content, in de vorm van boeken, video's, audio opnames, databases, artikelen, websites, en open source-broncode. Zo leren LLMs output te creëren die sterk lijkt op door mensen gemaakte, authentieke content. Op het moment dat eindgebruikers gebruik maken van op LLM-gebaseerde gen-AI userinterfaces dan is het onderliggende taal model bevroren en kan niet meer worden getraind. De Engelse term "pre-trained" wordt veelal gebruikt om dit aan te geven. Het onderliggende taalmodel van de ChatGPT interface is GPT-4 hetgeen staat voor: 4de generatie "Generative Pre-trained Transformer".

Een groot nadeel van de huidige generatie LLMs is dat ze feitelijk functioneren als algemene (lees general-purpose) kennisbanken, waarvan de hoeveelheid beschikbare gegevens niet uitbreidbaar (lees, bevroren) en niet op één enkele locatie in het model is opgeslagen, maar over verschillende locaties is verspreid (lees, gedistribueerd). Met andere woorden, de in LLMs opgeslagen kennis is voor eindgebruikers zowel onveranderbaar als ook onherkenbaar waardoor taalmodellen niet eenvoudig doelgericht zijn te bevragen over een specifiek en actueel kennisdomein. Het is dus niet mogelijk om te bepalen welke informatie het LLM benut om antwoorden te genereren, waardoor waarheidsvinding (fact-checking) moeilijk uitvoerbaar is.

Deze tekortkomingen kunnen worden tegengegaan door gebruik te maken van Retrieval-Augmented Generation (RAG). Deze op natuurlijke taal generatie (NLP) gebaseerde AI-technologie kun je opvatten als een onderzoeks- en schrijversduo. Stel je voor dat je een journalist bent die verslag doet van een natuurramp. Je doet dan eerst onderzoek naar de gebeurtenis, verzamelt relevante artikelen of weer rapporten en gebruikt deze informatie om dit specifieke nieuwsverhaal te schrijven.

RAG doet iets soortgelijks maar dan voor grote-taalmodellen. De retriever-component represeneert de journalist die relevante informatie verzamelt, en de generator-component is de schrijver die deze informatie gebruikt om een voor mensen begrijpelijke en waardevolle nieuwsverhaal te schrijven.



 [Leer-je-eigen-documenten-bevragen-met-generatieve-AI](#) Private

main · 1 branch · 0 tags

[Edit Pins](#) [Unwatch](#) [Fork](#)

[Go to file](#) [Add file](#) [Code](#)

 robvdw Update README.md 28933dd · 29 minutes ago  36 commits

 Notebooks Update Another copy of AzureLangchainRAG+colab_V01.ipynb 3 hours ago

 Samples Create Sample.pdf 32 minutes ago

 LICENSE Initial commit 4 days ago

 README.md Update README.md 29 minutes ago

 rag_retrieval_generation.png figures added 1 hour ago

 rag_visual-explaining.png figures added 1 hour ago

[README.md](#)

Leer-je-eigen-documenten-bevragen

Context & Doelen

RAG implementatie met Azure + LangChain + OpenAI
1. Begrijpen wat RAG wel en niet kan Wat is RAG
2. Veiligheidsmaatregelen nemen
3. LangChain installeren en configureren
4. Azure OpenAI API key aanvragen
5. Jupyter Notebook installeren
6. DEMO DEMO .



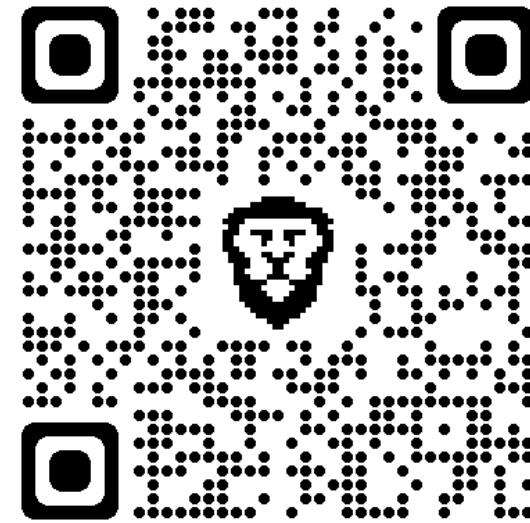
Deze GitHub Repository geeft inzicht hoe je met behulp van Generatieve-AI (Gen-AI) je eigen documenten kunt bevragen.

Disclaimer: deze tekst is door het gebruik van "gezond verstand" tot stand gekomen.
 Artificiële intelligentie [AI] is gebruikt ter verificatie van de gebruikte bronnen + vertaling van Engelstalige teksten.

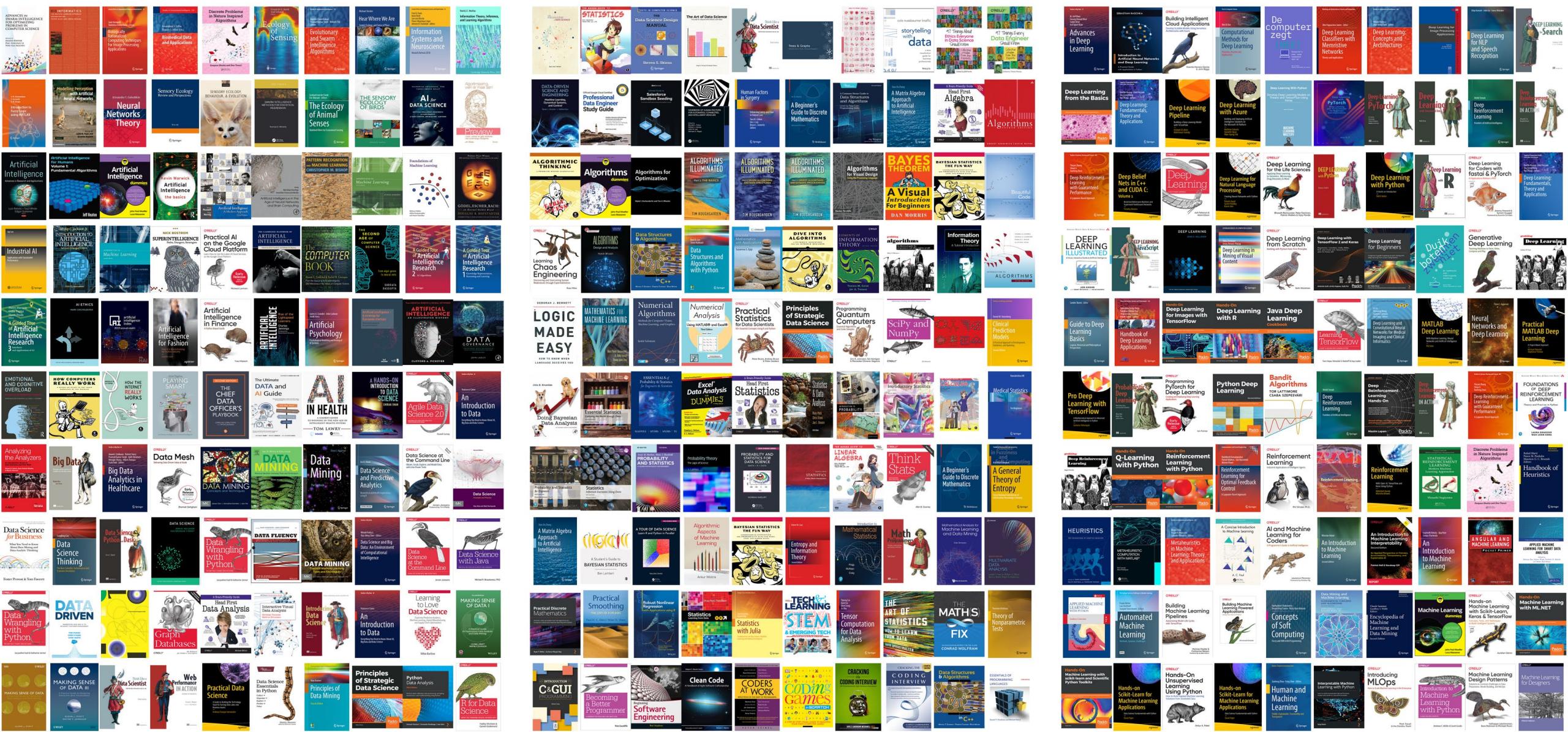
Dit is een data product gemaakt door het [PROMETHEUS DATA SCIENCE LAB](#) van de Hogeschool Rotterdam.

Views since 15 juni 2023:  61

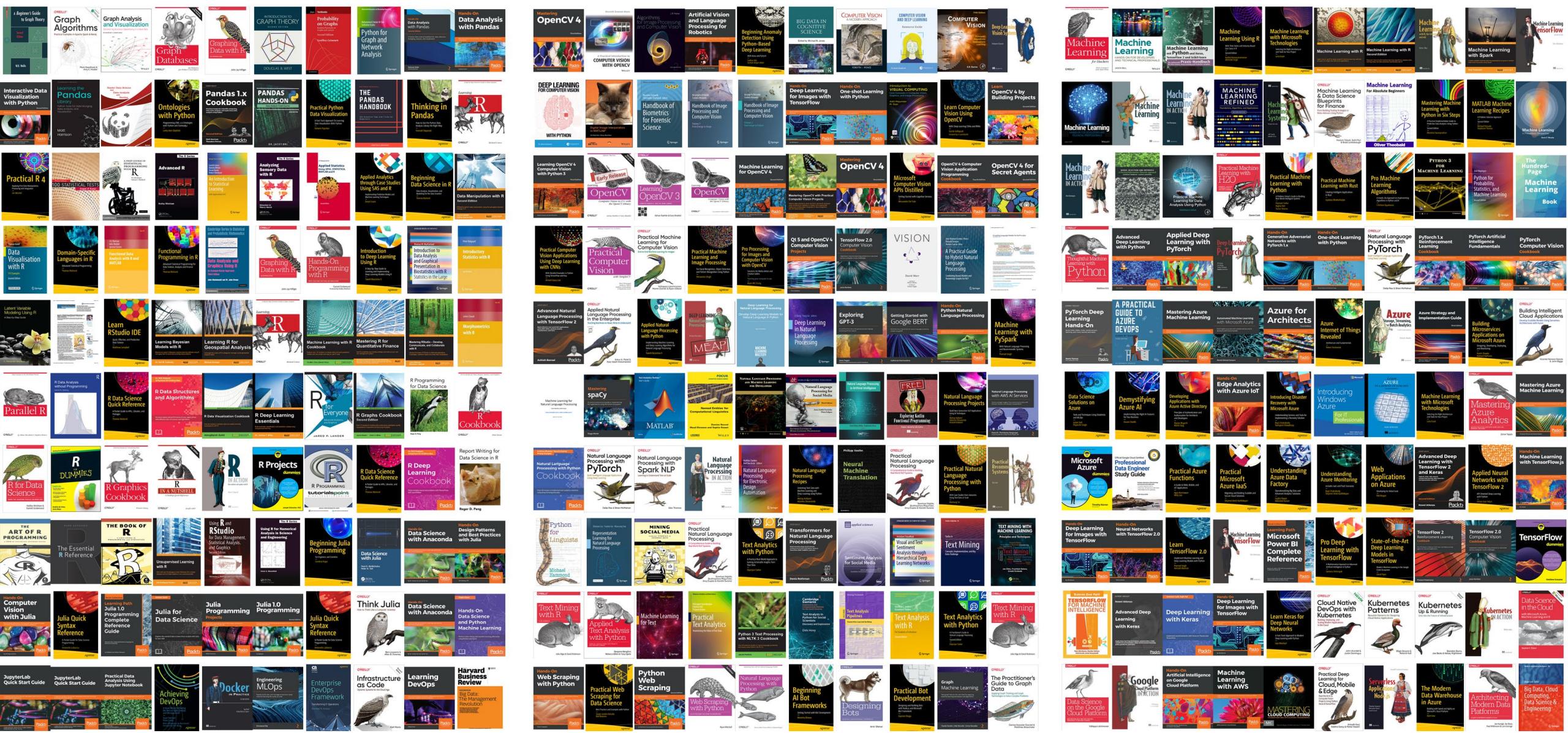
Uniques visitors since 15 juni 2023:  32



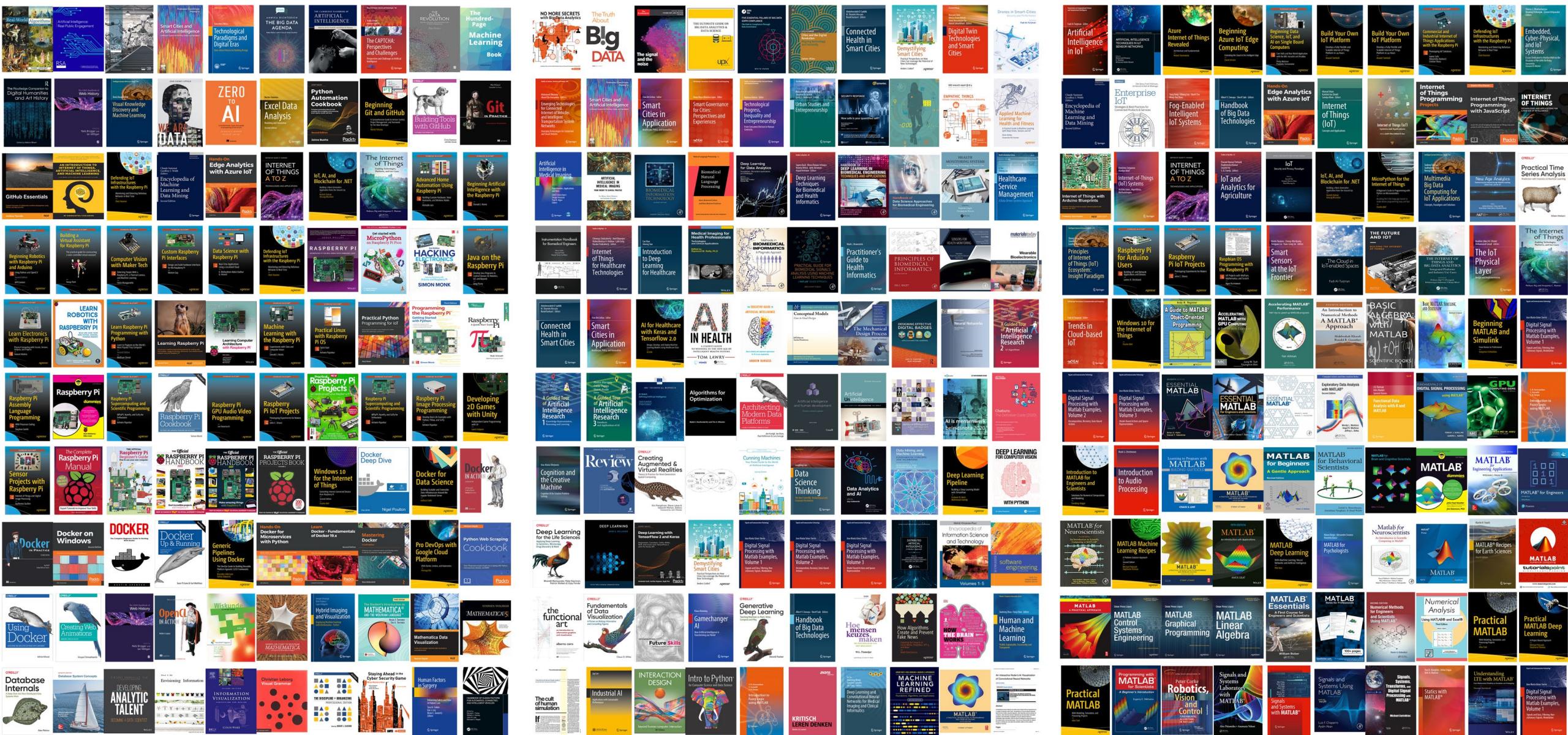
{Studied Materials: books}



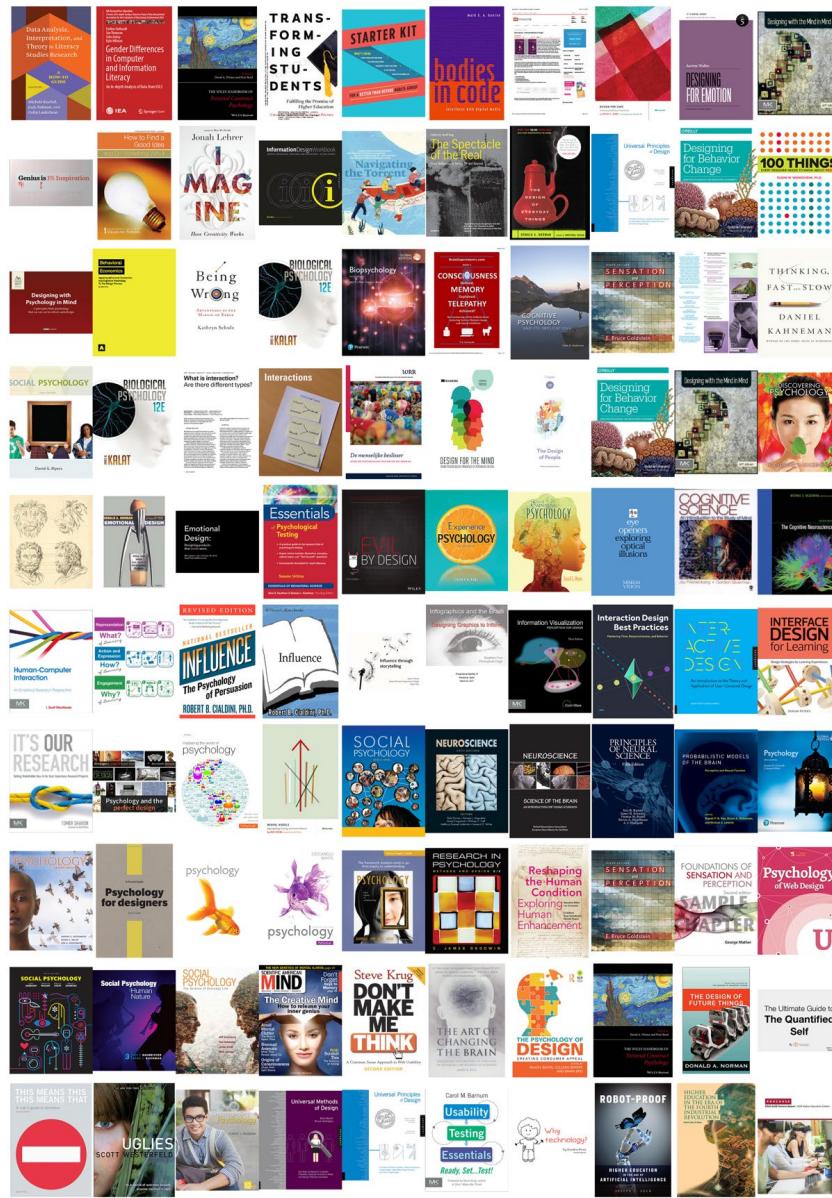
{Studied Materials: books}



{Studied Materials: books}

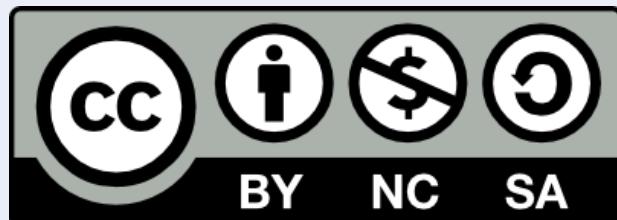


{Studied Materials: books}



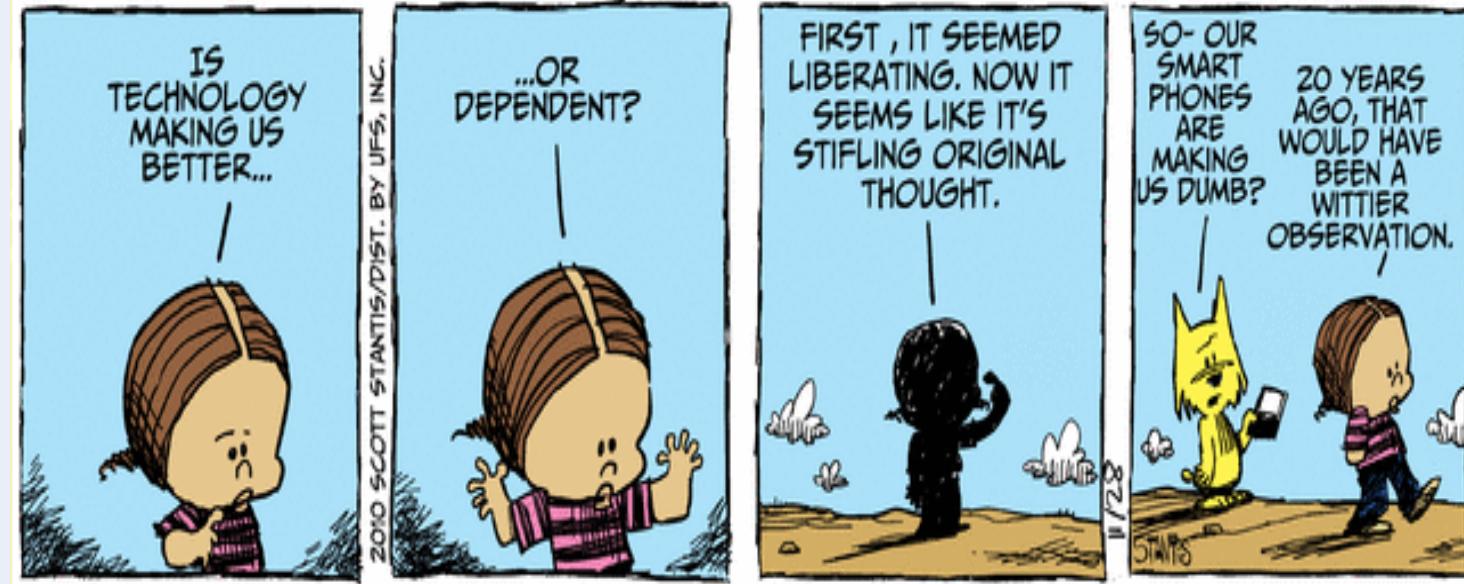
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

These materials are licensed under a Creative Commons Attribution-Share-Alike license.
You can change it, transmit it, show it to other people. Just always give credit to RFvdW.



This seminar was developed by:
Prometheus Data Science lab in het
kader van het HR-brede AI & Ethisiek

Rob van der Willigen
Oktober 2023



Creative Commons License Types		
	Can someone use it commercially?	Can someone create new versions of it?
Attribution	①	②
Share Alike	①②	Yup, AND they must license the new work under a Share Alike license.
No Derivatives	①③	
Non-Commercial	②③	Yup, AND the new work must be non-commercial, but it can be under any non-commercial license.
Non-Commercial Share Alike	①②③	Yup, AND they must license the new work under a Non-Commercial Share Alike license.
Non-Commercial No Derivatives	①②③④	

SOURCE
<http://www.masternewmedia.org/how-to-publish-a-book-under-a-creative-commons-license/>