What AI Can and Cannot Do

Demystifying what AI is and what it can and cannot do to help in the contexts of research and industry.

By Lois Wong, AI Librarian

THE UNIVERSITY OF CHICAGO | THE UNIVERSITY OF CHICAGO Library

Agenda

1. What is AI?
2. Overview of AI Tools
3. Activity: What AI Struggles With
4. Activity: What AI Does Well
5. Best Practices while Using AI
6. GenAI Resources at UChicago

Introduction

- Lois Wong
- AI Librarian since Sep 2025
- BA Linguistics, UC Berkeley
- MS Computer Science, Johns Hopkins
- Spent a year working on Apple's internal AI Education team

Ice Breaker

Go around the room and share your

- Name
- Where you're from
- Current degree

What is AI?

What is AI

1. AI as a technology vs AI as a product
2. Current critiques/concerns
3. Basic Terminology

What People Mean When They Say "AI"

AI as a Technology

- The idea/science/ engineering of simulating human intelligence
- Still developing, final form not reached
- Anyone can contribute to and influence what it becomes (not limited to technical fields)
- You can't really opt in/out

AI as a Product

- The application of AI technologies, can be called AI Applications or AI Tools
- Specific tools like ChatGPT or Perplexity
- You don't get much of a say in its development/what it becomes (unless you're part of the company/entity developing it)
- You can opt in/out

AI as a Technology vs AI as a Product

- Point of confusion: when people exclusively think of AI as a product
- Instead of considering what one can make of it, it's easy to think of it as a static entity we have no say in the development of
- Reality is that both forms of AI exist and being able to distinguish the connotation of AI is being discussed is important

Current Critiques of AI

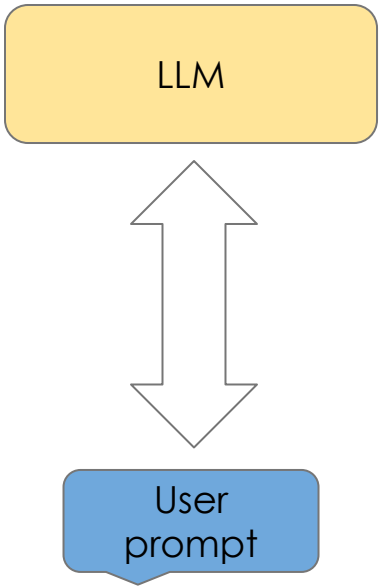
1. **Environmental Impact:** "One query to ChatGPT uses approximately as much electricity as [...]one light bulb for about 20 minutes," – Jesse Dodge
2. **Ethics:** AI applications/ outputs often reflect human biases
3. **Privacy:** AI models are trained on large amounts of data (some personal)
4. **IP Concerns:** tensions between companies who need training data vs IP of authors and artists; questions on consent, attribution, and compensation

AI Terminology

Basic Terminology

- **AI or ML Model -** general term for computer programs that learn from data to make predictions, generate content, or classify information
  - Lots of math/stat and is trained on lots of data
- **LLMs/LMs/SLMs -** takes an input in *natural language* (prompt) and produces a relevant output (response) also in natural language
  - Parameter count: LLM - billions ; SLM - millions/hundreds of millions
  - This is cool because it's like talking to a person
- **AI applications / tools / assistants -** specific products that usually has a model in their architecture and have a user-friendly interface
- **LM APIs -** Application Programming Interface with the models (like a usb port that allows you to connect your project to a model)

Interacting directly with the model via OpenAI's API

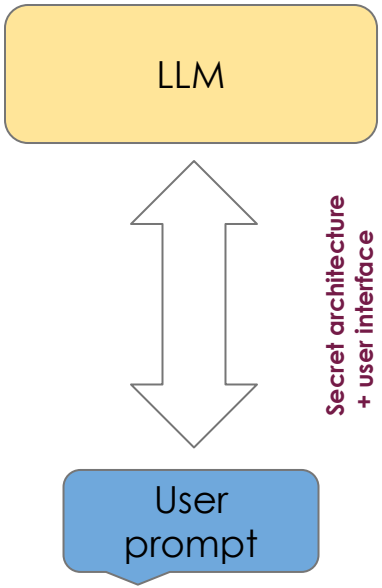


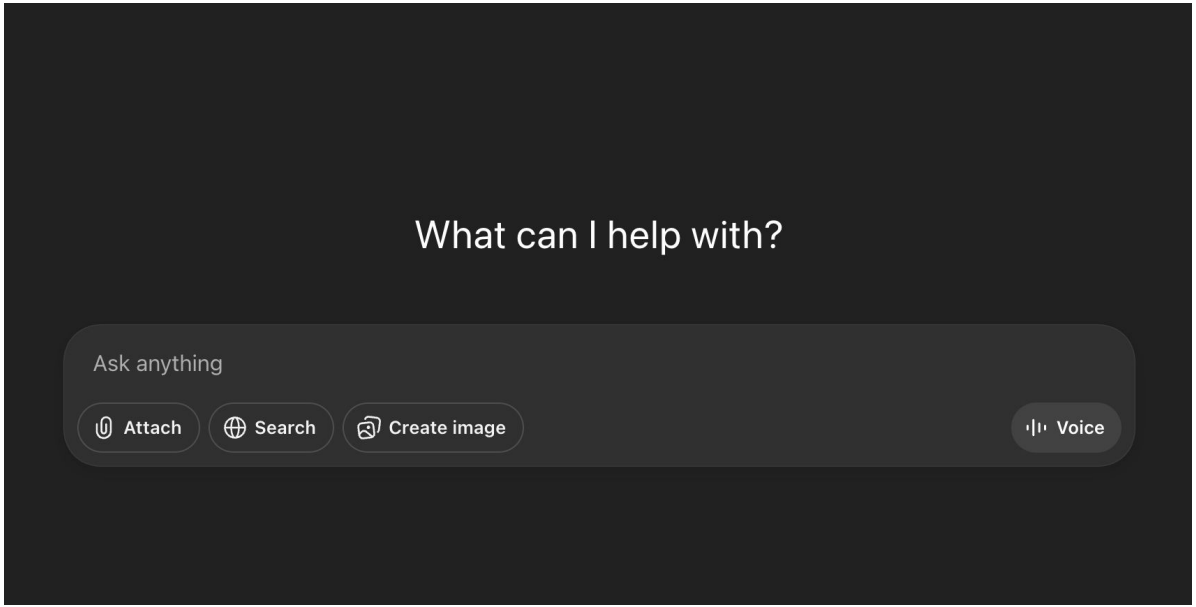

```python
import openai
from openai import OpenAI
import numpy as np

client = OpenAI(
  api_key= "secret"
)

response = client.chat.completions.create(
        model="gpt-4o-mini",
        messages=[
            {"role": "system", "content": "You are a helpful assistant"},
            {"role": "user", "content": "what's up"}
        ],
        #max_tokens=1000,
    )
chatgpt_response = response.choices[0].message.content
print(chatgpt_response)
```

Interacting with the model via OpenAI's User Interface





What AI Can and Cannot Do

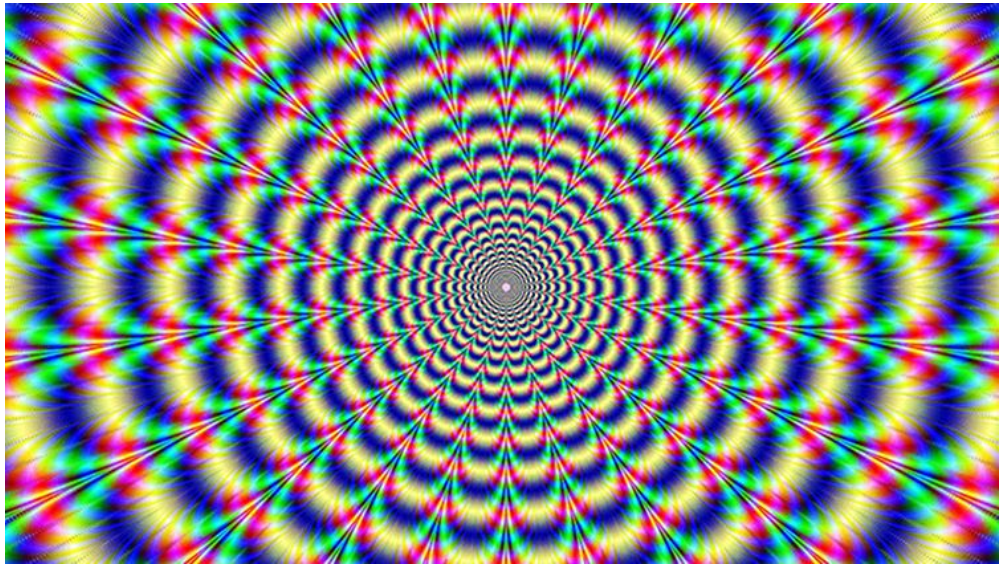
1. **What it cannot do**
    a. Activity - Lit Review
2. **What it can do**
    a. AI in the methods section of research papers
    b. Example - Content Marketing
    c. Brief introduction to prompt engineering
    d. Overview of AI tools

Example of where AI Falls Short

Hallucination

AI cannot reliably output ‘true’ information

Generative AI is prone to "hallucination": catch-all phrase for responding with inaccurate or false information



https://chat.openai.com/share/9b0706f2-2d16-45d1-8707-77356fbe1323

Slides from Taylor Faires, Pulling the Wool Over AI

Hallucination

Example: Lit Review on the role of nature in Macbeth

- **Rosenberg, Marvin. "The Masks of Macbeth."** In this influential work, Rosenberg explores the psychological and symbolic dimensions of Macbeth. He delves into the concept of masks worn by the characters, emphasizing how they reveal and conceal elements of human nature. Rosenberg's analysis provides valuable insights into the complex interplay between the internal and external aspects of the characters, shedding light on the role of nature as a reflection of their inner struggles.
- **Nevo, Ruth. "Forms of Expansion: Recent Studies in Shakespeare."** Nevo's critical examination encompasses various aspects of Shakespearean works, including Macbeth. Her exploration of the play delves into the thematic significance of nature and its impact on character development. Nevo's work serves to contextualize the broader trends in Shakespearean scholarship, offering a lens through which to understand the evolving interpretations of the natural world in Macbeth.
- **Foakes, R. A. "Nature in Shakespearean Tragedy."** Foakes provides a broader perspective by examining the thematic treatment of nature across several Shakespearean tragedies. In relation to Macbeth, Foakes discusses the broader context of nature as a recurring motif in Shakespeare's works and its unique manifestation in Macbeth. This comparative approach contributes to a more comprehensive understanding of the thematic nuances specific to Macbeth.
- **Orgel, Stephen. "Macbeth and the Imperial Theme."** Orgel's analysis focuses on the imperial theme within Macbeth, exploring the connection between political ambition and the disruption of the natural order. His work sheds light on the broader societal implications of the characters' actions and ambitions, emphasizing how the natural world serves as a reflection of the political and social dynamics within the play.

Evaluate its output: which of these sources exist?

https://chat.openai.com/share/9b0706f2-2d16-45d1-8707-77356fbe1323

Slides from Taylor Faires, Pulling the Wool Over AI

Hallucination

Example: Lit Review on the role of nature in Macbeth

- **Rosenberg, Marvin. "The Masks of Macbeth."** In this influential work, Rosenberg explores the psychological and symbolic dimensions of Macbeth. He delves into the concept of masks worn by the characters, emphasizing how they reveal and conceal elements of human nature. Rosenberg's analysis provides valuable insights into the complex interplay between the internal and external aspects of the characters, shedding light on the role of nature as a reflection of their inner struggles.
- **Nevo, Ruth. "Forms of Expansion: Recent Studies in Shakespeare."** Nevo's critical examination encompasses various aspects of Shakespearean works, including Macbeth. Her exploration of the play delves into the thematic significance of nature and its impact on character development. Nevo's work serves to contextualize the broader trends in Shakespearean scholarship, offering a lens through which to understand the evolving interpretations of the natural world in Macbeth.
- **Foakes, R. A. "Nature in Shakespearean Tragedy."** Foakes provides a broader perspective by examining the thematic treatment of nature across several Shakespearean tragedies. In relation to Macbeth, Foakes discusses the broader context of nature as a recurring motif in Shakespeare's works and its unique manifestation in Macbeth. This comparative approach contributes to a more comprehensive understanding of the thematic nuances specific to Macbeth.
- **Orgel, Stephen. "Macbeth and the Imperial Theme."** Orgel's analysis focuses on the imperial theme within Macbeth, exploring the connection between political ambition and the disruption of the natural order. His work sheds light on the broader societal implications of the characters' actions and ambitions, emphasizing how the natural world serves as a reflection of the political and social dynamics within the play.

Only this one is real!

https://chat.openai.com/share/9b0706f2-2d16-45d1-8707-77356fbe1323

Slides from Taylor Faires, Pulling the Wool Over AI

Hallucination

Shakespearean scholar, but no article by this name exists

- **Nevo, Ruth. "Forms of Expansion: Recent Studies in Shakespeare."** Nevo's critical examination encompasses various aspects of Shakespearean works, including Macbeth. Her exploration of the play delves into the thematic significance of nature and its impact on character development. Nevo's work serves to contextualize the broader trends in Shakespearean scholarship, offering a lens through which to understand the evolving interpretations of the natural world in Macbeth.

Shakespearean scholar and real article, but not by this author

- **Foakes, R. A. "Nature in Shakespearean Tragedy."** Foakes provides a broader perspective by examining the thematic treatment of nature across several Shakespearean tragedies. In relation to Macbeth, Foakes discusses the broader context of nature as a recurring motif in Shakespeare's works and its unique manifestation in Macbeth. This comparative approach contributes to a more comprehensive understanding of the thematic nuances specific to Macbeth. 1, 2, 3, 4

Shakespearean scholar but this record didn't exist

- **Orgel, Stephen. "Macbeth and the Imperial Theme."** Orgel's analysis focuses on the imperial theme within Macbeth, exploring the connection between political ambition and the disruption of the natural order. His work sheds light on the broader societal implications of the characters' actions and ambitions, emphasizing how the natural world serves as a reflection of the political and social dynamics within the play.

https://chat.openai.com/share/9b0706f2-2d16-45d1-8707-77356fbe1323

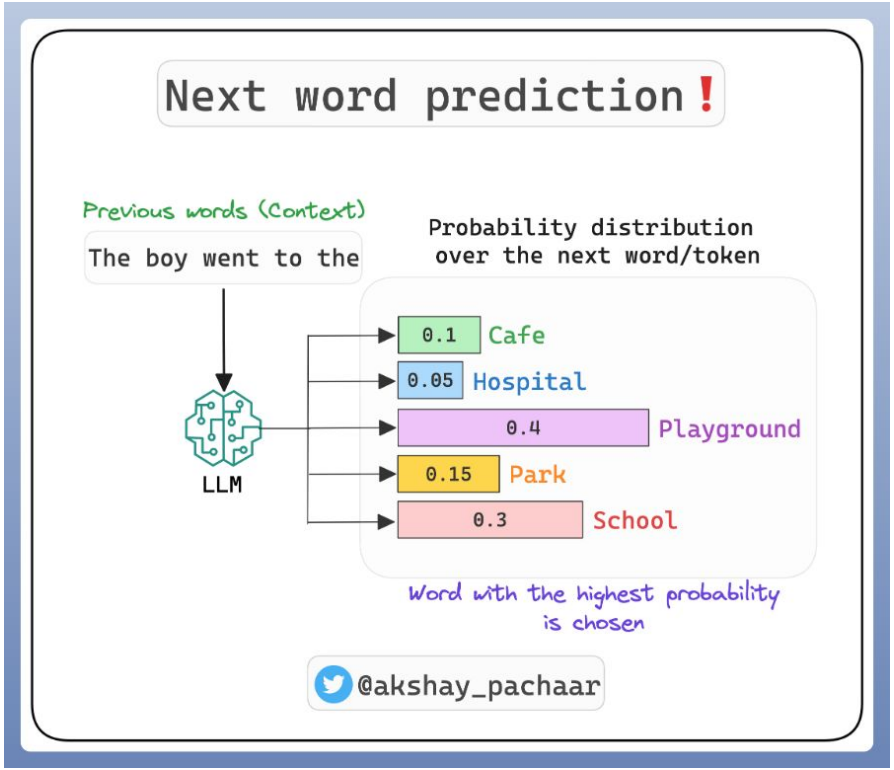
Slides from Taylor Faires, Pulling the Wool Over AI

Exercise: Can we make AI Hallucinate?

1. Use any AI tool (Perplexity, ChatGPT, Phoenix AI)
2. Ask for recommendations on any topic of choice
   a. Recommend a paper, item of clothing, apartment complex, etc.
3. Try to find hallucination
   a. Pay attention to the process you take to verify the output
   b. E.g. check Google Scholar or library catalogue

Why Does AI Hallucinate?

- Simply put, LM outputs are determined by predicting the next word in a sequence
- It doesn't "know" facts, it only generates what it thinks is most likely based on its training data and context
- Note: a lot of training data are not trustworthy (e.g. Reddit posts)



Example of where AI is Helpful

Examples of AI - Research Methods

Topic Modeling: Find themes/topics in large amounts of text data

Word embeddings: Bolukbasi et al. finds gender bias in word embeddings in "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings"

Classification: Buolamwini et al. shows that facial gender classification has the highest error rate among darker-skinned women and lowest among lighter-skinned men in "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification"

Examples of AI - Research Methods

Simulation

- Slater et al.'s "A Virtual Reprise of the Stanley Milgram Obedience Experiments" uses simulation to do what would otherwise be unethical
- An experiment to see how people would react shocking to virtual humans

Data Augmentation: "artificially generating new data from existing data" to increase data diversity and quantity (for cases where you have less data than you need)

Data Imputation: filling in missing values in datasets

https://aws.amazon.com/what-is/data-augmentation/ ; https://milvus.io/ai-quick-reference/what-are-the-limitations-of-data-augmentation

Example - Content Marketing

- **Context**: I used to work in developer relations at an AI startup in San Francisco

- **Novita AI**: AI infra company that hosts open source LLMs and provides API access to them for a lower cost than OpenAI

Sharing an announcement

Qwen3.5-397B-A17B is now live on Novita AI

- Write a marketing email to share the news
- Write a version for C-level audiences and a separate one for developers
- Convert to a LinkedIn Post
- Convert to an X post
- Write a blog post

Activity: Screen share

Prompt Engineering

Terms that people like to use (but refer to very intuitive concepts)

- **In context learning** - provide examples within the prompt so the model picks up the pattern
  - *Translate English to French.*
  - *English: "Good morning" → French: "Bonjour"*
  - *English: "Thank you" → French: "Merci"*

- **Zero/one/few-shot learning** - give it zero/one/a few examples of the desired output

Prompt Engineering

Terms that people like to use (but refer to very intuitive concepts)

- **Personas** - tell the model who to be to shape tone and priorities
  - *You are a marketing professional with 10 years of experience in consumer tech. Write a product description for a new fitness smartwatch aimed at busy professionals.*
- **Chain-of-thought** - ask it to show its work (like math problems)
  - *Solve this problem step by step and explain your reasoning:*
  - *If a train travels 60 miles per hour for 2.5 hours, how far does it go?*

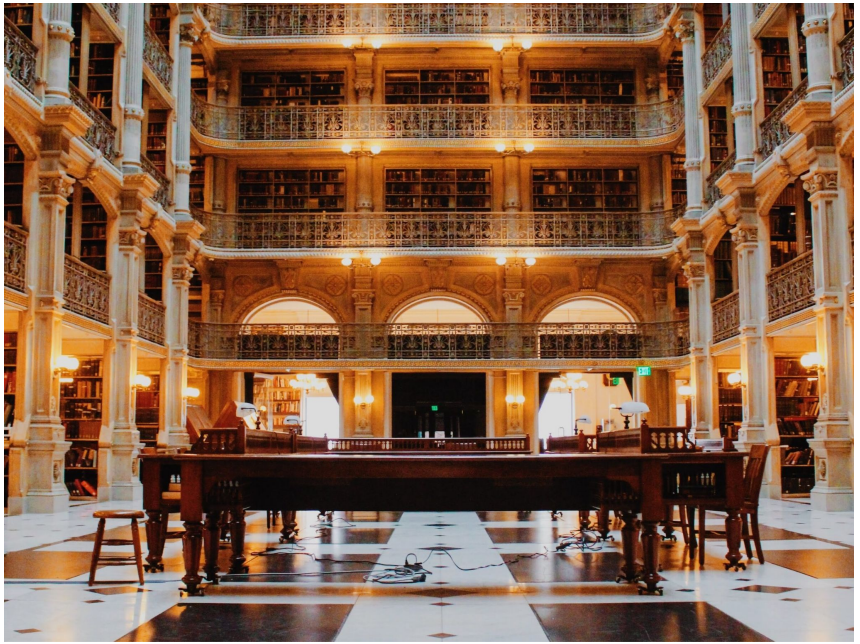
Don't overthink it, it's like talking to a person

Break

Best Practices for Using AI

What each AI tool is good at

- **Gemini:** deep research, lit review
- **Perplexity:** good for looking things up (*recommend additional sources given my current work*). Deep research mode gives you more peer reviewed/serious sources.
- **Claude:** for coding
- **ChatGPT:** for writing
- **Notebook LM:** podcasts and notes
- **Phoenix AI:** connect data sources for RAG (e.g. papers you're citing in a Box, GDrive, or OneDrive folder)
    - Ask which page of this paper or which source discusses x topic
    - Great for papers you've read before



What Happens When You Use AI Tools?

- "When the service is free, you are the product" (source unknown)
- Your prompts and uploaded data are (usually) stored, analyzed, and used to further train AI models
- This exchange is what allows companies to offer powerful technology at minimal to no cost
- Be careful with sensitive, proprietary, and personal data: never assume privacy and confidentiality

Whenever you use AI tools, it's important to realize that anything you share, whether it's original ideas, documents, or creative work, might be incorporated into future versions and AI outputs.

What Happens When You Use AI Tools?

- As a response to those concerns among others, UChicago has taken some steps to protect our community's data while still providing access to helpful AI resources
- How many of you have heard of Phoenix AI?
- Phoenix AI is a Walled Garden of the same models that power ChatGPT

phoenixai.uchicago.edu

What is a Walled Garden?

- Secure and controlled environment where AI tools can be used safely
- Any prompts/data you input does not leave UChicago
- Further trained on a curated dataset to promote safety and accuracy
- Allows us to reap the benefits of AI without exposing ourselves or our data to unnecessary risks

AI Tools at UChicago

UChicago negotiated contracts and license agreements with these vendors (similar to enterprise plan). If you access these services through your UChicago account, you will get the additional data and privacy protections that don't come with the free plan.

- **Phoenix AI**
- **Microsoft Copilot**
- **GitHub Copilot Business**: Coding Assistant
- **NotebookLM:** Study tool, access through UChicago workspace

https://genai.uchicago.edu/generative-ai-tools

Best Practices for External AI Tools

- Review platform policies when uncertain especially before sharing valuable or sensitive data
- Mask sensitive data: use placeholders instead of actual data (e.g., “[Client Name]”)
- Treat every prompt like it could be seen by someone else

Recent oversight: ChatGPT conversations were indexed by Google and appeared in search results last year (summer 2025)

Best Practices for Responsible AI Use

How do we effectively and responsibly use AI?

- **Verify everything**, no matter how confident the LM seems
- **Cite/log AI usage**: always be prepared to answer questions on how you use(d) AI in your work
- **Keep original drafts** if you use AI to proofread your papers
- Always check with your professor/boss re. appropriate AI usage

GenAI at UChicago

AI Tool	Status	Purpose/Reason	Enterprise Supported/Pay/Free	Restrictions
BoxAI	Approved up to SRDS high protection level.	General Use	Enterprise Supported	Can be used for sensitive information with IRB approval.
Copilot	Approved up to SRDS high protection level.	Various purposes to support Microsoft Products	Enterprise Supported	Can be used for sensitive information with IRB approval.
Sonix AI	Approved up to SRDS low protection level.	Transcription service	Paid	Only for non-sensitive information.
claude.ai	Approved up to SRDS low protection level.	General Use	Paid	Only for non-sensitive information; not to create website
ChatGPT 3.5	Approved for data that is made publicly available by its source.	General Use	Free	
ChatGPT 4.0	Approved for data that is made publicly available by its source.	General Use	Free	

https://genai.uchicago.edu/generative-ai-tools

Thank You!

Questions?