

# AI & Using AI Tools (in your research)

Yen-Ling Kuo ylkuo@virginia.edu





#### What do you use Al for?

You may already intentionally or unintentionally use AI in your daily life

Coding / Debugging

Generating Excel Functions

Reply Emails

Translate / Fix Grammar Issues

Learning New Knowledge

Extract Abstract / Keywords

Data Analysis

Summary / Rewriting

Generating / Recognizing Images

Tutoring / Teaching

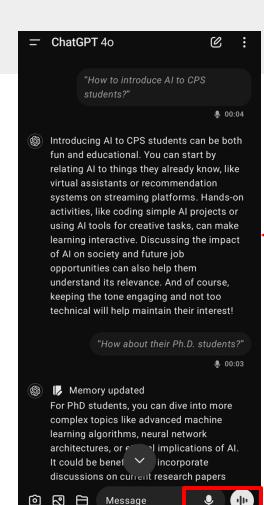
Chat

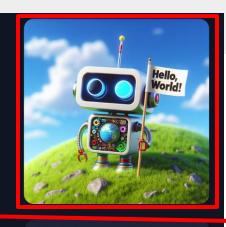
Generating Web Pages

#### Let's try it out (2 min)

- Choose the one you haven't used before, try to ask it some questions
  - o Both app or web version are fine!







#### What's the prompt for this image?

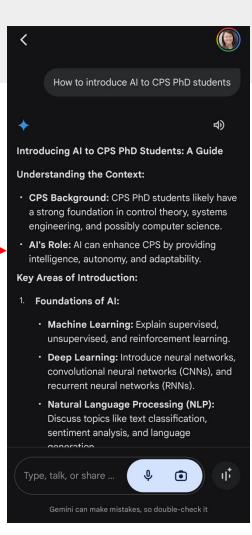
Seems like the prompt for this image is something like "A cute robot holding a 'Hello, World!' sign on a grassy hill with a bright blue sky background."

The image features a small robot with glowing blue eyes and an antenna, standing on a hill, holding a "Hello, World!" sign. There's a bright blue sky with fluffy clouds in the background. It's got a cool vibe—kind of like technology meets nature.



Message Copilot

0



### Today's agenda

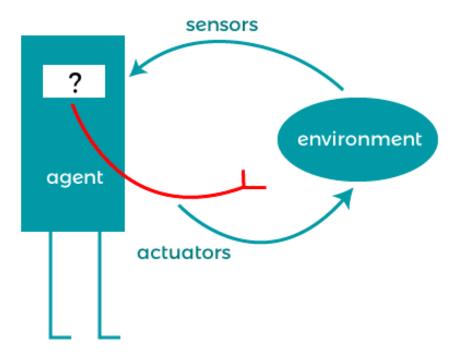
- What is Al? Al agent?
- "Hire" an Al agent
- Machine Learning Pipeline
  - Evaluation
- Issues and appropriate use of AI

#### What is intelligence?

- Linguistic
- Logico-mathematical
- Spatial
- Musical
- Kinesthetic
- Intrapersonal
- Interpersonal

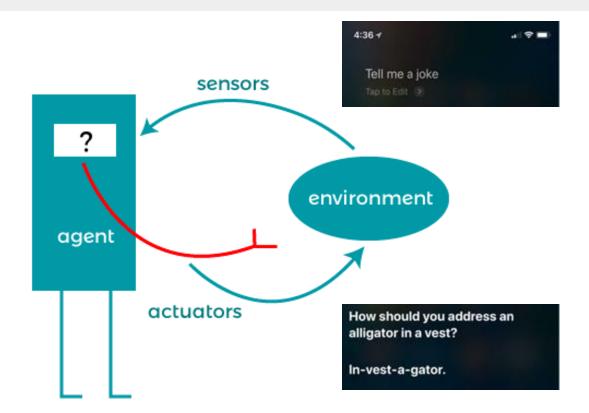
- The ability to solve complex problems
- Learning from experience
- Adaptability
- Self-awareness
- Dealing with incomplete information
- Action under time pressure
- Creativity
- Common sense reasoning etc.

### Agent

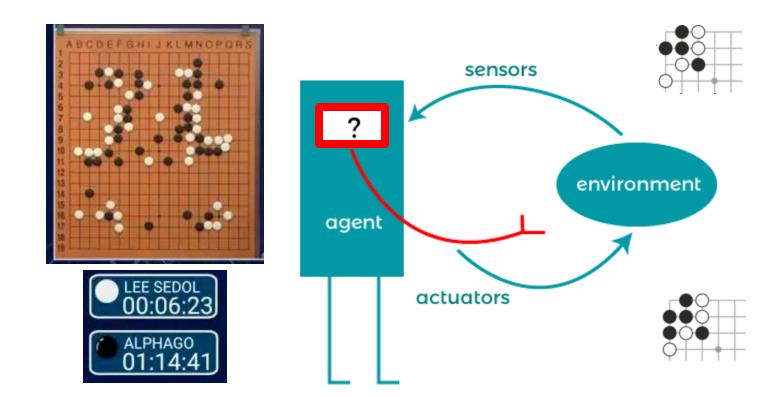


## Agent - Siri





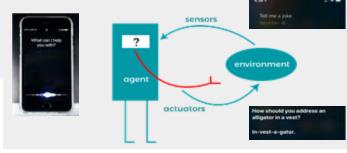
### Agent - AlphaGo



#### Making decisions with rules

```
Welcome to
                                            777777
                                                     AAAAA
                                                    AAAAAAA
  Eliza is a mock Rogerian psychotherapist.
  The original program was described by Joseph Weizenbaum in 1966.
  This implementation by Norbert Landsteiner 2005.
ELIZA: Is something troubling you ?
       Men are all alike.
ELIZA: What is the connection, do you suppose ?
       They're always bugging us about something or other.
ELIZA: Can you think of a specific example ?
       Well, my boyfriend made me come here.
ELIZA: Is it important to you that your boyfriend made you come here ?
       He says I'm depressed much of the time.
ELIZA: I am sorry to hear that you are depressed.
       It's true. I am unhappy.
ELIZA: Can you explain what made you unhappy ?
```

https://web.njit.edu/~ronkowit/eliza.html



```
if the input matches

(first bunch of words) "you" (second bunch of words) "me".

respond with

"What makes you think I" (second bunch of words) "you?"

if the input matches

"You are" (bunch of words).

respond with

"So, I'm" (bunch of words) ", am I?"

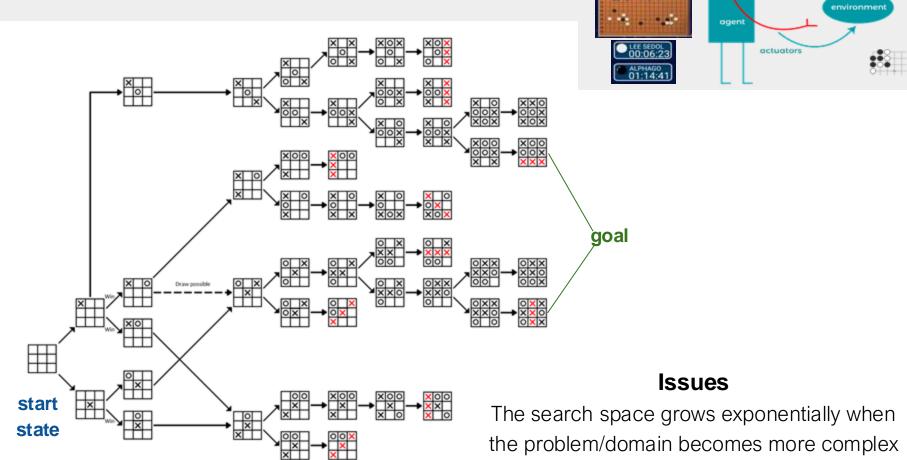
etc.
```

#### **Issues**

Input doesn't match any pattern

Cannot enumerate all rules

### Making decisions by search

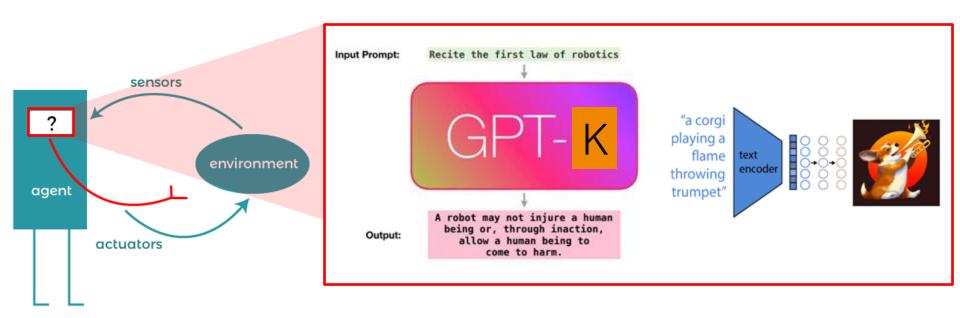


sensors

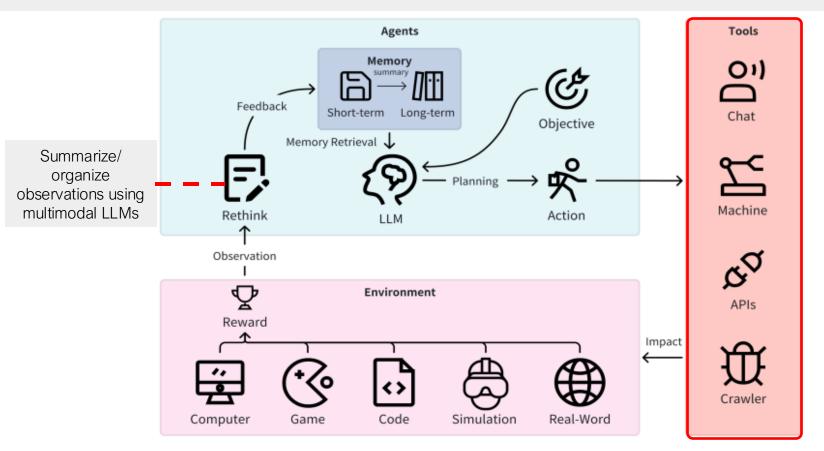
?

#### Making decision with generative models

 Using generative models (mostly Large Language Models) to generate response or take actions – mapping from prompts to desired outputs



#### Connecting LLM-based generative agents with actions/tools

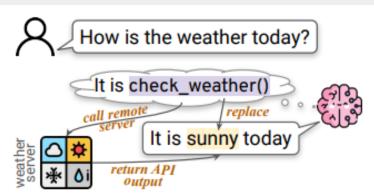


Cheng et al. "Exploring Large Language Model based Intelligent Agents: Definitions, Methods, and Prospects (2024).

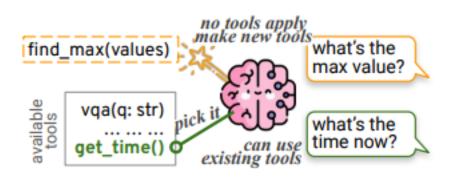
#### Tool use & creation

- Language models often struggle with complex tasks or are unable to solve tasks that require access to info not included in their training data
- Using tools to extend LLM's abilities

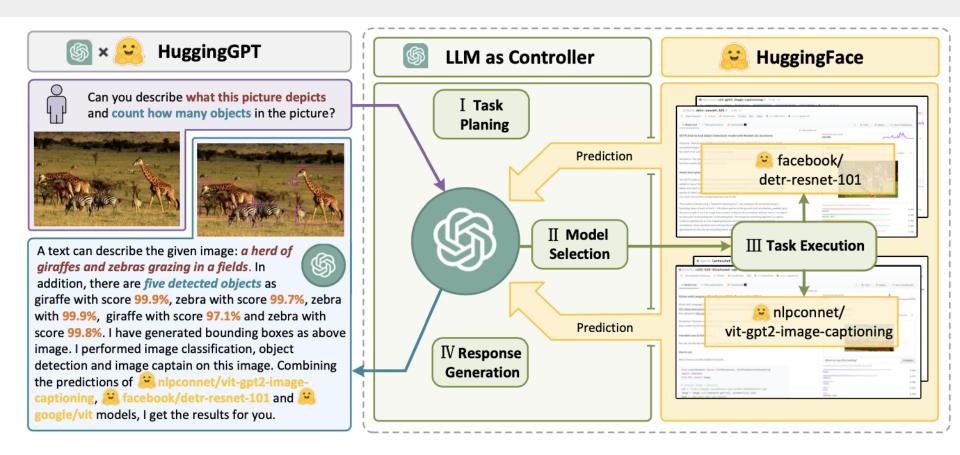
Shift between text-generation mode and tool-execution mode is the key



Use LMs to make tools, e.g., compose frequently-used-together actions into shortcut



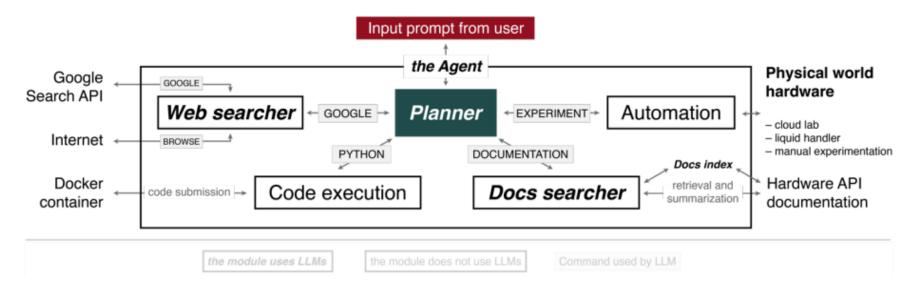
### Example agent: HuggingGPT



Shen et al. "HuggingGPT: Solving ai tasks with chatgpt and its friends in hugging face." NeurIPS 2024.

#### Example agent: Scientific discovery

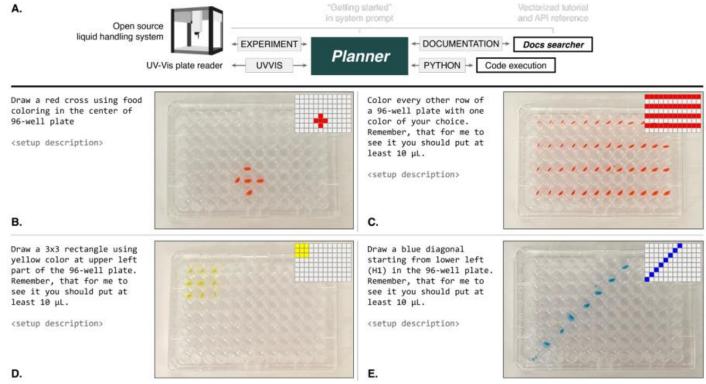
 The LLM agent use tools to browse the Internet, read documentation, execute code, call robotics experimentation APIs



Boiko et al. "Emergent autonomous scientific research capabilities of large language models." (2023).

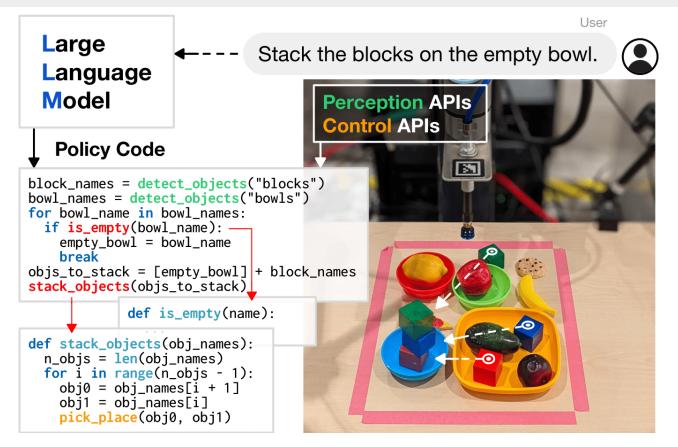
#### Example agent: Scientific discovery (cont.)

The LLM planner control the robotic liquid handler



Boiko et al. "Emergent autonomous scientific research capabilities of large language models." (2023).

#### Example agent: Robotics - Code As Policies

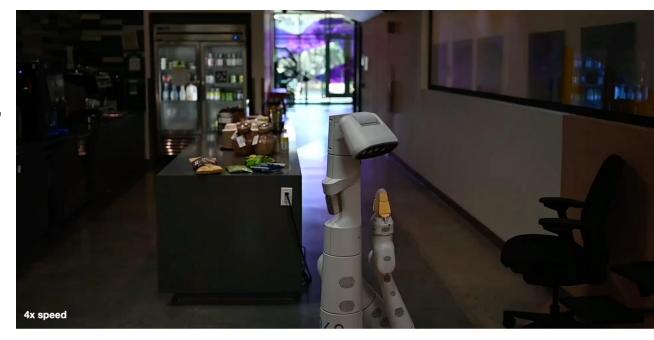


Liang et al. "Code as policies: Language model programs for embodied control." ICRA 2023.

#### Example agent: Robotics - Code As Policies (cont.)

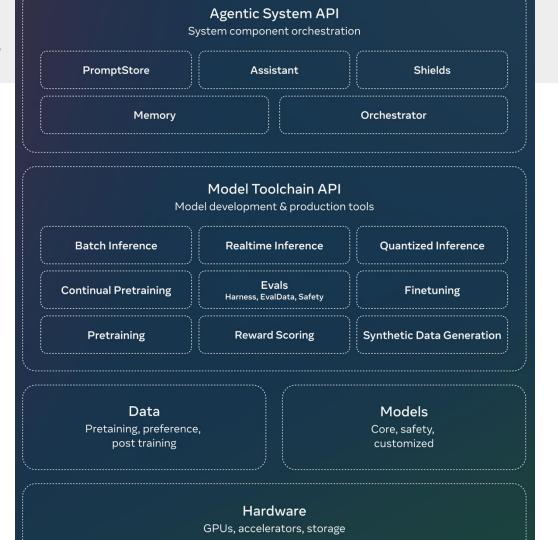
Task:

"Put away the coca cola can and the apple on their corresponding bins"



### **Building Agentic Apps**

• e.g., Llama Stack APIs



#### Today's agenda

- What is Al? Al agent?
- "Hire" an Al agent
- Machine Learning Pipeline
  - Evaluation
- Issues and appropriate use of Al



Onboard

- Pay or not Monthly subscription, API, hosting
  - o Proprietary LLMs: GPT-4o/o1, Claude, Gemini, ...
  - o Opensourced LLMs: Llama 3.1/3.2, Mistral, Phi, Gemma, Vicuna, Qwen
- Model size Edge, cloud (few GPUs, more GPUs)
  - Small: 0.5B, 1.5B, 2B
  - o Medium: 7B, 8B
  - Large: 70B, 405B
- Context length Short/normal/longer novel, book
  - o 8k, 16k, 32k, 128k, 300 pages
- Input/Output General model, fine-tuned model
  - o text, image, speech, pdf, code

#### Different LLMs have different capabilities



Category Benchmark	Llama 3.1 405B	Nemotron 4 340B Instruct	<b>GPT-4</b> (0125)	GPT-4 Omni	Claude 3.5 Sonnet	
General MMLU (0-shot, CoT)	88.6	<b>78.7</b> (non-CoT)	85.4	88.7	88.3	
MMLU PRO (5-shot, CoT)	73.3	62.7	64.8	74.0	77.0	
IFEval	88.6	85.1	84.3	85.6	88.0	
Code HumanEval (0-shot)	89.0	73.2	86.6	90.2	92.0	
MBPP EvalPlus (base) (0-shot)	88.6	72.8	83.6	87.8	90.5	
Math	96.8	92.3 (0-shot)	94.2	96.1	<b>96.4</b> (0-shot)	
MATH (0-shot, CoT)	73.8	41.1	64.5	76.6	71.1	
Reasoning ARC Challenge (0-shot)	96.9	94.6	96.4	96.7	96.7	
GPQA (0-shot, CoT)	51.1	-	41.4	53.6	59.4	

### Different capabilities needed for tool usage





Model	INSTRUCT		PLAN		REASON		RETRIEVE		UNDERSTAND		REVIEW	Overall	
	String	JSON	String	JSON	String	JSON	String	JSON	String	JSON	Choice	Overan	
API-Based													
Claude2	97.7	97.8	87.1	84.9	62.9	62.8	76.5	78.2	74.9	82.0	70.4	78.8	
GPT-3.5	94.1	99.1	86.6	86.6	65.2	70.3	98.3	86.2	82.9	88.1	75.6	84.0	
GPT-4	96.7	95.9	88.9	86.7	65.6	65.1	91.3	86.6	83.2	88.3	94.5	86.4	
Open-Sourced													
LLaMA2-7B	68.7	0.2	47.0	9.1	37.1	7.1	30.3	3.5	36.8	12.1	38.6	27.4	
CodeLLaMA-7B	<u>96.0</u>	0.9	61.4	44.3	28.7	0.9	3.6	1.2	25.4	1.4	40.0	28.6	
AgentLM-7B	80.8	13.1	53.1	15.9	50.1	17.5	70.2	13.8	66.4	26.1	44.8	41.4	
Vicuna-7B	65.3	30.8	13.4	47.8	47.6	<u>49.9</u>	12.4	32.6	66.8	<u>54.2</u>	58.5	44.8	
InternLM-7B	48.4	29.9	67.7	43.1	48.8	25.0	72.1	22.2	70.4	30.2	46.2	45.8	
ChatGLM3-6B	63.3	80.8	46.9	38.5	48.2	24.1	66.5	24.0	79.9	35.6	54.8	51.4	
Mistral-7B	59.7	63.6	<u>77.2</u>	<u>64.9</u>	<u>63.0</u>	15.3	92.6	11.0	79.8	18.1	<u>63.2</u>	56.0	
Baichuan2-7B	68.0	78.0	65.6	39.0	51.3	31.3	73.7	28.5	<u>80.1</u>	39.2	61.4	56.5	
Qwen-7B	28.7	<u>94.2</u>	66.2	63.1	56.4	34.1	89.0	<u>35.3</u>	77.7	46.1	61.6	<u>59.5</u>	

#### What do you ask LLMs? Prompting



Please act as a marketer and create a campaign an introduction to ChatGPT class on March 24. This class will cover the foundation, applications, and architecture to use ChatGPT in business scenarios.

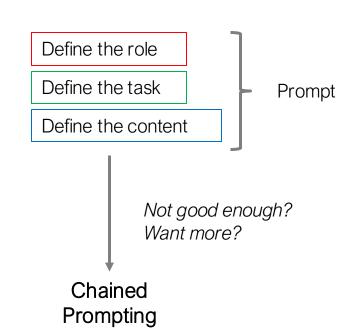


Attention all businesses! Are you looking for a way to take your customer service and engagement to the next level? Look no further than ChatGPT, the powerful language model that can revolutionize the way you interact with your customers.

Join us on March 24th for an exclusive introduction to the ChatGPT class. Our expert instructors will cover the foundations of this cutting-edge technology, as well as its many practical applications for businesses like yours.

You'll learn how ChatGPT can be used to streamline your customer service processes, increase customer satisfaction, and even generate leads and sales. We'll also delve into the architecture behind ChatGPT, giving you a deeper understanding of how this powerful tool works.

Whether you're a small business owner or a large corporation, this class is a must-attend event for anyone interested in harnessing the power of ChatGPT. Don't miss out on this opportunity to learn from the best and take your business to the next level. Register now for the ChatGPT class on March 24th!



Job

Description

Onboard

Candidate Selection

#### Chained prompting



My target audience is the college students studying management. Rewrite the campaign for the college students.



Hey there, college students studying management! Are you interested in learning about the latest technology that can revolutionize the way businesses interact with their customers? Look no further than ChatGPT, the cutting-edge language model that's taking the business world by storm.

Join us on March 24th for an exclusive introduction to the ChatGPT class. Our expert instructors will cover the foundations of this powerful tool and show you how it can be applied in real-world business scenarios.

You'll learn about the many practical applications of ChatGPT, from improving customer service to generating leads and sales. We'll also dive into the architecture behind ChatGPT, giving you a deeper understanding of how it works and how it's being used in the business world today.

As a management student, you know that staying up-to-date with the latest technology is key to success in the business world. That's why you won't want to miss this opportunity to learn about ChatGPT and how it can give you an edge in your future career. Register now for the ChatGPT class on March 24th and take the first step towards becoming a ChatGPT expert!

Job Description Candidate Selection Onboard

Change the tone for a different target audience (TA)

#### Define the follow-up task



Now write 5 keywords for SEO.



- 1. ChatGPT
- 2. Language model
- 3. Business applications
- 4. Artificial intelligence
- 5. Customer service

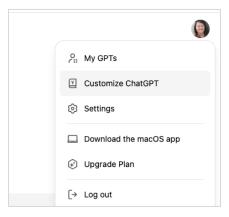


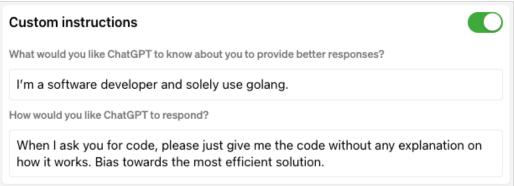
This list of keywords is too technical. Add more business scenarios



- 1. ChatGPT
- 2. Language model
- 3. Business applications
- 4. Artificial intelligence
- 5. Customer engagement
- 6. Lead generation
- 7. Sales optimization
- 8. Marketing automation
- 9. E-commerce

#### Customized your ChatGPT/LLMs





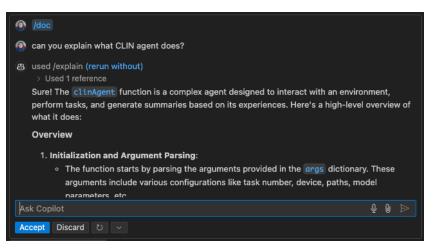
- Role-playing with GPTs
- Awesome ChatGPT Prompts
   <u>https://prompts.chat/</u>
  - Edit them based on your need and copy-paste!

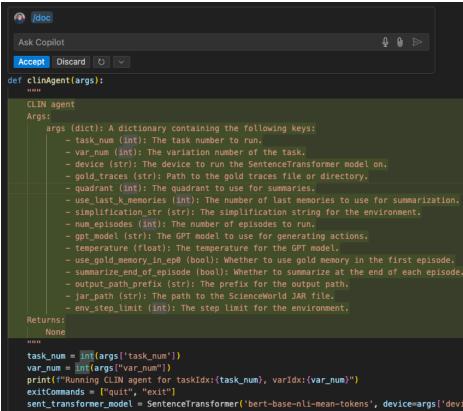
#### Useful Al tools: for creating conference videos

- TTS-Maker (Free): <a href="https://ttsmaker.com/">https://ttsmaker.com/</a>
  - Text to speech service, support different styles and languages
- Groq speech to text: <a href="https://console.groq.com/">https://console.groq.com/</a>
  - Groq is compatible with OpenAl APIs, e.g., whisper
  - Speech to text JSON
- JSON to SRT
  - Converter on Hugging Face Space:
     <a href="https://huggingface.co/spaces/the-walking-fish/Whisper-JSON-to-SRT-Converter">https://huggingface.co/spaces/the-walking-fish/Whisper-JSON-to-SRT-Converter</a>

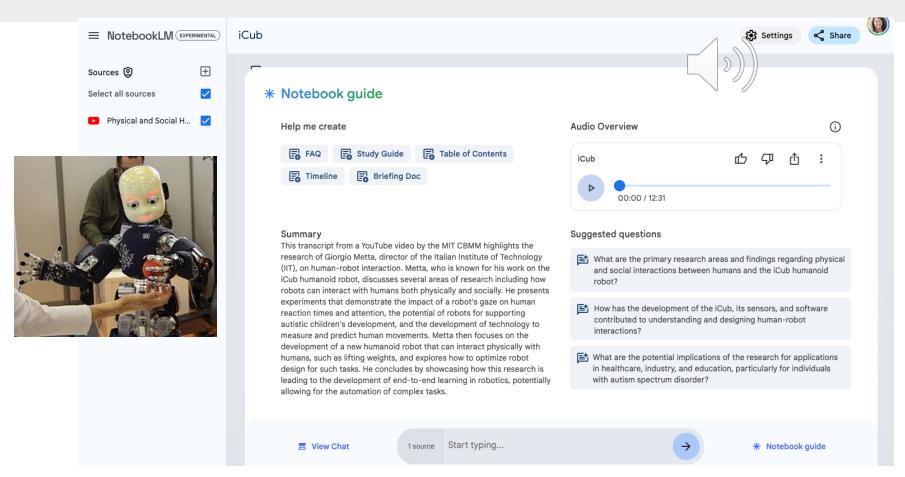
#### GitHub Copilot (<a href="https://github.com/features/copilot">https://github.com/features/copilot</a> )

Free with Education account





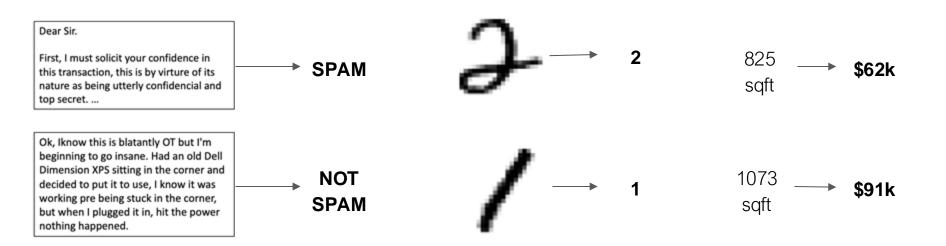
#### NotebookLM (<a href="https://notebooklm.google.com/">https://notebooklm.google.com/</a>)



### Today's agenda

- What is Al? Al agent?
- "Hire" an Al agent
- Machine Learning Pipeline
  - Evaluation
- Issues and appropriate use of Al

#### Learning from data



Set up a goal through data

Learn a model (sometimes blackbox) to map from input to labels/target

### Machine learning basics

Data

Hello Sir ... → SPAM

**→** 

Evaluation

Accuracy

= # correct / # data points

Model

Input heta Output

Learning

Learning rules to update heta

P(input, output), probability table

#### Dataset vs. real-world setting

ObjectNet (<a href="https://objectnet.dev/">https://objectnet.dev/</a>)

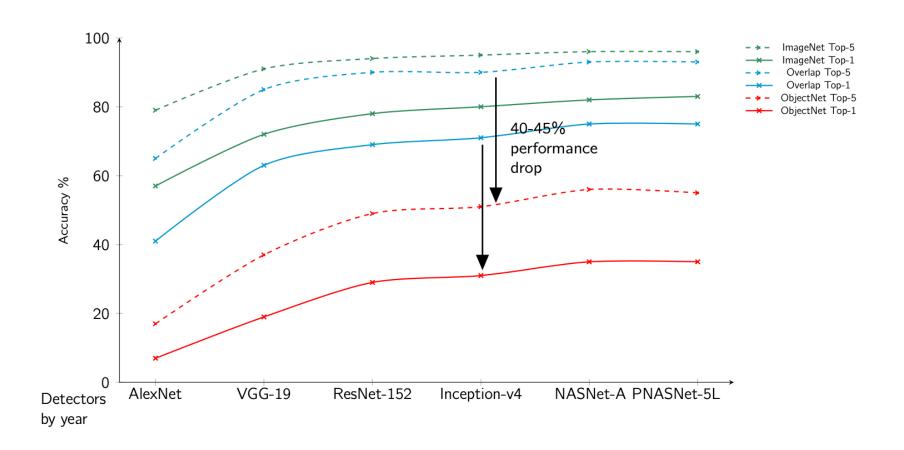






### Overfitting/biasing toward datasets

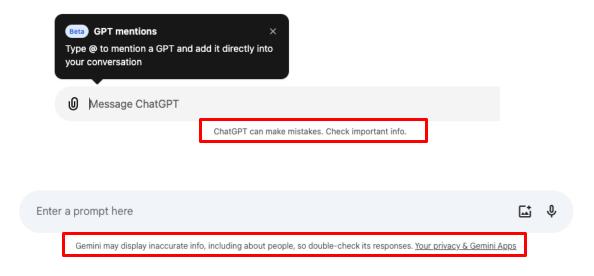
# Thinking about their evaluation when reading a paper



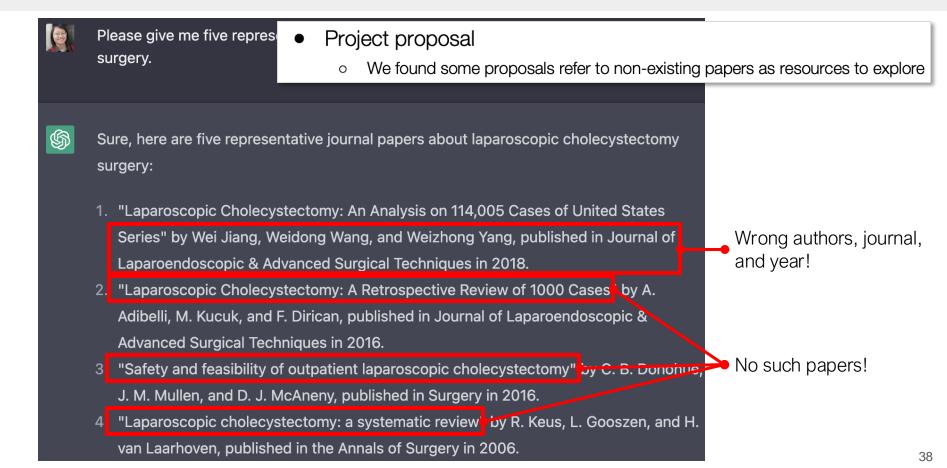
### Today's agenda

- What is Al? Al agent?
- "Hire" an Al agent
- Machine Learning Pipeline
  - Evaluation
- Issues and appropriate use of Al

#### Issues: Al can make mistakes double check it



#### Issues: Hallucination, Factuality



#### Issues: Conference Al policy

#### • ICML 2023 LLM Policy

#### Clarification on Large Language Model Policy LLM

We (Program Chairs) have included the following statement in the Call for Papers for ICML represented by 2023:

Papers that include text generated from a large-scale language model (LLM) such as ChatGPT are prohibited unless the produced text is presented as a part of the paper's experimental analysis.

#### TLDR:

- The Large Language Model (LLM) policy for ICML 2023 prohibits text produced entirely by LLMs (i.e., "generated"). This does not prohibit authors from using LLMs for editing or polishing author-written text.
- The LLM policy is largely predicated on the principle of being conservative with respect to guarding against potential issues of using LLMs, including plagiarism.
- The LLM policy applies to ICML 2023. We expect this policy may evolve in future conferences as we
  understand LLMs and their impacts on scientific publishing better.

#### ACM Policy

#### If I use generative AI software tools, under what conditions must I disclose their use in my Work?

Today's generative AI software tools perform different tasks and it is reasonable to expect that their use and use cases will expand and become more robust over time. Whether disclosure in your published AC Work is necessary depends on how you utilize these tools. The following guidelines should be followed when determining whether and to what extent disclosure must be provided in your Work.

#### Can a generative AI tool be listed as an author?

No, generative AI software tools cannot be listed as authors on ACM Works under any conditions.

#### ACM CHI guideline

#### TL;DR:

- All authors nust have made substantial intellectual contributions to the paper, be aware that the manuscript has been submitted, and are held responsible and accountable for the work.
- All authors must be human beings and identified via PCS at the time of submission.
- Pseudonyms are permitted, as is authorship after death, with permission of next of kin.
- AI tools, communities, and non-humans (e.g., landscapes, animals) cannot be listed as authors, but can appear in the acknowledgements.
- Adding or removing authors once the review process begins is prohibited.
- The use of generative AI tools (such as ChatGPT) is permitted, but all
  authors are responsible for the content created by these tools, and the
  use of the tools must be disclosed.
  - Authors are responsible for plagiarism, misrepresentation, fabrication or falsification of content and/or references by AI tools, and could be sanctioned with penalties, such as a publication ban.
  - AI tools may be safely used to copy-edit author-generated content, but caution is advised in using them for generating content.

#### Issues: Copyright, Ownership

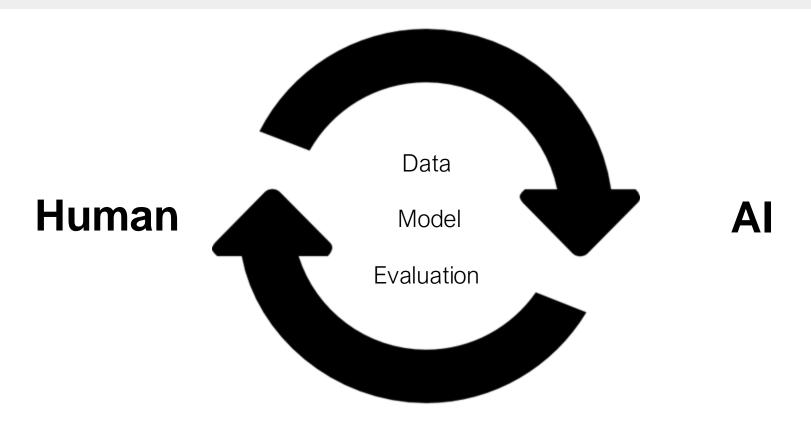
Guided provided by the U.S. Copyright Office

If a work's traditional elements of authorship were produced by a machine, the work lacks human authorship and the Office will not register it. For example, when an AI technology receives solely a prompt from a human and produces complex written, visual, or musical works in response, the "traditional elements of authorship" are determined and executed by the technology—not the human user. Based on the Office's understanding of the generative AI technologies currently available, users do not exercise ultimate creative control over how such systems interpret prompts and generate material. Instead, these prompts function more like instructions to a commissioned artist—they identify what the prompter wishes to have depicted, but the machine determines how those instructions are implemented in its output. For example, if a user instructs a text-generating technology to "write a poem about copyright law in the style of William Shakespeare," she can expect the system to generate text that is recognizable as a poem,

mentions copyright, and resembles Shakespeare's style. But the technology will decide the rhyming pattern, the words in each line, and the structure of the text. When an AI technology determines the expressive elements of its output, the generated material is not the product of human authorship. As a

result, that material is not protected by copyright and must be disclaimed in a registration application.

### A human-Al loop (now/past)



#### Summary: Coworking with AI (more than one AI)

#### Learn it

Understand how it work

#### Use it

Learn what it is good at and bad at

# Cowork with it

Achieve your goal better

