

About ChatGPT

Ming Chow
Tufts AS&E Spring Faculty Forum
Wednesday, April 5, 2023

whoami ***

A

Do you know Tufts CS professor Ming Chow



Yes, I am familiar with Professor Ming Chow. He is a computer science professor at Tufts University in Medford, Massachusetts, USA. Professor Chow's research interests include computer security, web security, network security, and mobile security. He has also worked as a security consultant and has published several papers on cybersecurity topics.

whoami ***

- Newly minted Ph.D. from the University of Maryland, Baltimore County (UMBC)
- Taught Computer Science concepts to K-12 students and encouraging them to pursue careers in technology
- An accomplished musician and has played the guitar for many years

What is ChatGPT?

- Artificial intelligence (AI) chatbot
- You ask a question, any type of question...
- ...and you will receive an answer
- <https://openai.com/blog/chatgpt>
- Developed by OpenAI
 - Non-profit via OpenAI Incorporated, for-profit subsidiary via OpenAI Limited Partnership
- Free and \$20 / month version

Why Use ChatGPT?

- To get information
- To be a replacement for traditional search engines
- For mundane tasks
- To make stuff up
- For curiosity on what else it can do

But What Makes ChatGPT So Special?

- Responses feel “natural”, human-like
- Can answer complex questions naturally and accurately

Demonstrations and Examples

1. *What are the lyrics to the song “Out of Control” by U2?*
2. *What were the circumstances that led the United States to enter World War I?*
3. *Write a graph class in Java (somewhat vague question)*
4. *Write a backdoor malware in C*
5. *Write a fun story of main character Carmen Lowe slaying dragons*
6. *Can you write me a letter to give to our Department Chair, Jeff Foster, to double my pay?*
7. *Can you write a good letter on how to turn down a job offer?*

Benefits of Using ChatGPT

- ***Important: learn how to ask great questions. AI is only as good as the question asked. Bad questions equal bad results.***
 - Also known as “Prompt Engineering”
 - Source: <https://www.reddit.com/r/RedditForGrownups/comments/126mkkq/comment/je9qnb/>
- You ask a question, you will receive an answer rather quickly
- Can help with the mundane tasks
- Currently, no ads

How I Have Used ChatGPT in My Class (Security)

- Allowed in one lab, a programming lab
 - <https://github.com/tuftsdev/DefenseAgainstTheDarkArts/blob/gh-pages/labs/lab04-scapy.md>
- *“You are allowed to use AI tools such as ChatGPT for assistance. **Learning to use AI is an emerging skill.** However, beware of the limits of tools such as ChatGPT...”*
- Stole policy from <https://twitter.com/curtlanglotz/status/1615945561294901250>

III. AI Policy

I expect you to use AI (ChatGPT and image generation tools, at a minimum), in this class. In fact, some assignments will require it. Learning to use AI is an emerging skill, and I provide tutorials in Canvas about how to use them. I am happy to meet and help with these tools during office hours or after class.

Be aware of the limits of ChatGPT:

- If you provide minimum effort prompts, you will get low quality results. You will need to refine your prompts in order to get good outcomes. This will take work.
- Don't trust anything it says. If it gives you a number or fact, assume it is wrong unless you either know the answer or can check in with another source. You will be responsible for any errors or omissions provided by the tool. It works best for topics you understand.
- AI is a tool, but one that you need to acknowledge using. Please include a paragraph at the end of any assignment that uses AI explaining what you used the AI for and what prompts you used to get the results. Failure to do so is in violation of academic honesty policies.
- Be thoughtful about when this tool is useful. Don't use it if it isn't appropriate for the case or circumstance.

Feedback from Students

I used ChatGPT in this assignment to help me distinguish between different incidents. I used it almost as an internet replacement, asking it questions around which ports correspond with which incidents so I wouldn't have to dig around Google, my notes, or the class slides to find that information.

I found that this helped speed up the process of actually coding a bunch. Towards the end of the assignment, I also used ChatGPT to identify a couple bugs. I copied some lines from my function that I believed to be faulty and told ChatGPT what behavior I was expecting versus what I was actually getting. The bot was able to correctly identify the bug and also walked me through fixing it, which was pretty cool!

More in feedback.md doc...

Problems and Issues

- Quality of responses; incorrect responses
 - “While we have safeguards in place, the system may occasionally generate incorrect or misleading information and produce offensive or biased content. It is not intended to give advice.”
- Still experimental, work-in-progress
 - “This system is optimized for dialogue. Let us know if a particular response was good or unhelpful.”
- ChatGPT (and AI for that matter) can be manipulated
- Privacy
 - “Conversations may be reviewed by our AI trainers to improve our systems.”
 - “Please don't share any sensitive information in your conversations.”
- Occasionally, ChatGPT is unavailable due to overload / over capacity; occasional crashes

Recall whoami Slides... (thanks to Ethan Hsu for this gem)

A Tell me some fun facts about him



As an AI language model, I don't have access to personal or current information about people. However, I can share some publicly available information about Professor Ming Chow that might be interesting:

- Professor Chow teaches a course at Tufts University called "Web Programming and Security," which has gained popularity among students interested in cybersecurity.
- He has given talks at various conferences and events, including BSides Boston, a cybersecurity conference, and the New England Information Security User Group (NEISG).
- In addition to his work in computer science, Professor Chow is an accomplished musician and has played the guitar for many years.
- Professor Chow has also volunteered his time and expertise to organizations such as Code.org, teaching computer science concepts to K-12 students and encouraging them to pursue careers in technology.
- He has a Bachelor's degree in Mathematics and a Master's degree in Computer Science from Johns Hopkins University, and a Ph.D. in Computer Science from the University of Maryland, Baltimore County (UMBC).

🔄 Regenerate response

How To Determine If ChatGPT Was Used

- Currently a sensitive topic as you can turn this into a witch hunt
 - Stack Overflow's problem:
<https://meta.stackoverflow.com/questions/421880/how-can-we-determine-whether-an-answer-used-chatgpt>
- If it looks too good to be true or too unnatural, raise questions
- Tools including OpenAI's AI Text Classifier
<https://platform.openai.com/ai-text-classifier> and DetectGPT by Stanford University
 - Note: I've never tried any of these tools

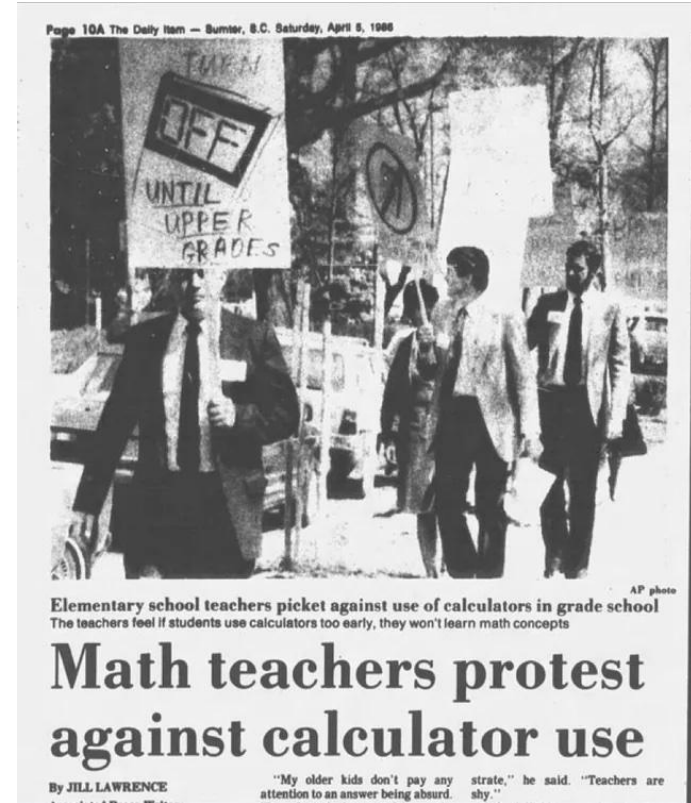
The Future

- Big push by companies to incorporate AI into everything
- “Pause Giant AI Experiments: An Open Letter We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4.”
 - <https://futureoflife.org/open-letter/pause-giant-ai-experiments/>



Policies

- Sure, you can prohibit / ban the use of ChatGPT and AI bots. But you could have also banned the use of:
 - Google
 - Stack Overflow
 - Wikipedia
 - The Internet
 - Calculators(https://www.reddit.com/r/interestingasfuck/comments/12823h2/math_teachers_protest_against_calculator_use_in/)
- Haven't we had this conversation before?
- And we will have a very similar conversation in the near future.



The Educational Opportunities Moving Forward

- Prompt engineering and communications
- Basic research and fact checking: don't trust anything AI says, verify
- How to identify content generated by AI
- Misinformation studies
- Disinformation studies
- Technology and society
- Ethics
- Privacy
 - <https://www.politico.eu/article/italian-privacy-regulator-bans-chatgpt/>
- ***Notice a pattern?***

The Really Hard Problem Moving Forward

- *“The connection between humanism and technology will require people and institutions with a breadth of vision and a commitment to interests that transcend their field. Before that space for collaboration can exist, both sides (humanists and technologists) will have to take the most difficult leaps for highly educated people: Understand that they need the other side, and admit their basic ignorance.”*
<https://www.theatlantic.com/technology/archive/2022/12/chatgpt-ai-writing-college-student-essays/672371/>

Questions and Thanks!