Ethical Training for the ChatGPT Future

Graduate Research and Discovery Symposium (GRADS) at Colorado School of Mines. April 6 2023.

C. Estelle Smith

Assistant Professor Computer Science Colorado School of Mines

Research Areas:

Human-Computer Interaction & Social Computing Computational Spiritual Support



Connect with me!





DANIELS FUND ETHICS INITIATIVE

Full disclosure: Riffing on an event from February 2023!

u disclosure: Riffing 2023! Collegiate Program

The Ethics of ChatGPT

A Workshop



Joshua Nunziato
Assistant Teaching Professor
Social Responsibility
& Sustainability Division
Leeds School of Business



Heather Fester
Teaching Associate Professor
Humanities, Arts &
Social Sciences
Nature & Human Values
Coordinator
Colorado School of Mines



Helen Davies
Assistant Professor
English
UC Colorado Springs

Credit to Co-Facilitators

What Will You Get Out of This Workshop?

You should leave this workshop with:

- 1. A basic understanding of how ChatGPT works—and what that implies about its strengths and weaknesses;
- 2. The ability to use a **principles-based approach** to evaluate uses and abuses of ChatGPT (and similar AI);
- 3. Appreciation for how this new technology is **changing learning/teaching** responsibilities;
- 4. Tools for innovative educational adaptations to AI, framed by the changes that ChatGPT is bringing to workplaces in many different industries.





Intro to the Tech

Outline

- Recap of Natural Language Processing (NLP) history
- Technical training and functioning of ChatGPT
- How ChatGPT fits into the broader ecology of socio-technical systems





Natural Language Processing (NLP)

How can we make sense of large datasets of human-generated language?





Natural Language Processing (NLP)

- Post WW2 1940's: An interest in machines that *translate* languages
- Late 50s to early 70s: A split in research foci
 - Symbolic or rule-based: Focus on formal languages and syntax
 - Stochastic: Statistical & probabilistic methods
 - e.g., optical character recognition, pattern recognition between texts
 - Logic-based paradigms: Encoding rules and language in mathematical logics
- Post 1970: Discourse modeling

https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/nlp/overview_history.html





Natural Language Processing (NLP)

- 80s-90s: Focus remains mostly on empiricism and probabilistic models
- Most recently: Information extraction & generation
 - Based on vast amounts of information on the Internet

https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/nlp/overview_history.html





Modeling Language



"This robotic cat is my fuzzy friend but sometimes my less fuzzy friends find him creepy."

0 1 2 3 4 5 6 7 8 4 9 5 6 10 11 12





Commonly Used NLP Tools in CS & HCI

- Linguistic Inquiry and Word Count (LIWC, https://www.liwc.app/):
 - Over 100 dimensions (categories) of text created by humans
 - Count the number of times different words appear in different categories
 - Well-validated and cited by over 20,000 scientific articles

Topic modeling:

- Which sets of words tend to appear together a lot? (un-supervised ML)
- (Humans choose the number of topics, look at resultant sets, and apply a label.)

• Semantic embeddings:

- High-dimensional vector representations, e.g., of each word in a lexicon
- Transformer models (like ChatGPT):
 - Deep learning models (e.g., neural nets)
 - Self-attention: Differentially weighting the significance of parts of the input data
 - Reinforcement learning: To reward better decision policies

"Top-Down"

"Bottom-Up"



DANIELS FUND
ETHICS INITIATIVE
Collegiate Program

E.g. Word2 Vec: "Man is to computer programmer as woman is to homemaker?"

Bolukbasi, Tolga, Kai-Wei Chang, James Y. Zou, Venkatesh Saligrama, and Adam T. Kalai. "Man is to computer programmer as woman is to homemaker? debiasing word embeddings." *Advances in neural information processing systems* 29 (2016).

Extreme she 1. homemaker	Extreme he 1. maestro		Gender stereotype she-he analogies	
2. nurse	2 skipper sew	sewing-carpentry nurse-surgeon	registered nurse-physician interior designer-architect	housewife-shopkeeper softball-baseball
receptionist	3. protege	blond-burly	feminism-conservatism	cosmetics-pharmaceuticals
4. librarian	4. philosopher	giggle-chuckle	vocalist-guitarist	petite-lanky
socialite	captain	sassy-snappy	diva-superstar	charming-affable
hairdresser	6. architect	volleyball-football	cupcakes-pizzas	lovely-brilliant
7. nanny8. bookkeeper9. stylist10. housekeeper	7. financier8. warrior9. broadcaster10. magician	queen-king waitress-waiter	Gender appropriate she-he and sister-brother ovarian cancer-prostate cancer	mother-father

Figure 1: **Left** The most extreme occupations as projected on to the *she-he* gender direction on w2vNEWS. Occupations such as *businesswoman*, where gender is suggested by the orthography, were excluded. **Right** Automatically generated analogies for the pair *she-he* using the procedure described in text. Each automatically generated analogy is evaluated by 10 crowd-workers to whether or not it reflects gender stereotype.

MIT Technology Review

Featured

Topics

Newsletters

Events

Podcasts

Sign in

Subscribe

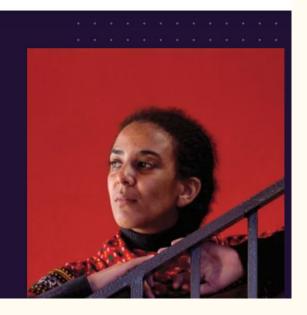
ARTIFICIAL INTELLIGENCE

We read the paper that forced Timnit Gebru out of Google. Here's what it says.

The company's star ethics researcher highlighted the risks of large language models, which are key to Google's business.

By Karen Hao

December 4, 2020







Can Language Models Be Too Big?

Large Size of Data ⇒ Diversity of Data

- <u>Training data</u> encodes stereotypical and derogatory associations:
 - Gender
 - Race
 - Ethnicity
 - Disability status

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? ..." In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency, pp. 610-623. 2021.





Can Language Models Be Too Big?

Internet data:

- Encodes hegemonic worldviews
- Amplifies biases and other issues in the training data

People mistake LM-driven performance gains for actual natural language understanding.

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? ..." In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency, pp. 610-623. 2021.





Can Language Models Be Too Big?

Mitigation Recommendations

- Weighing environmental & financial costs first
- Curating & documenting datasets rather than ingesting everything on the web
- Carrying out pre-development exercises
 - How does the planned approach fit into R&D goals, support stakeholder values?
- Encouraging research directions **beyond** ever larger language models

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? ..." In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency, pp. 610-623. 2021.





Outline

- Recap of Natural Language Processing (NLP) history
- Technical training and functioning of ChatGPT
- How ChatGPT fits into the broader ecology of socio-technical systems









"OpenAI's mission is to ensure that artificial general intelligence (AGI)—by which we mean highly autonomous systems that outperform humans at most economically valuable work—benefits all of humanity.

We will attempt to directly build safe and beneficial AGI, but will also consider our mission fulfilled if our work aids others to achieve this outcome."

(https://openai.com/about/)





What does ChatGPT do differently?

"The language modeling objective used for many recent large language models—predicting the next token on a webpage from the internet—is different from the objective 'follow the user's instructions helpfully and safely."

I.e. Align with user intent.

Ouyang, Long, Jeff Wu, Xu Jiang, Diogo Almeida, Carroll L. Wainwright, Pamela Mishkin, Chong Zhang et al. "Training language models to follow instructions with human feedback." arXiv preprint arXiv:2203.02155 (2022).





How to train ChatGPT



Collect demonstration data. and train a supervised policy.

A prompt is sampled from our prompt dataset.



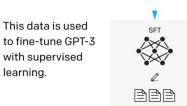
Explain the moon

landing to a 6 year old

desired output behavior.

demonstrates the

A labeler



Step 2

Collect comparison data. and train a reward model.

A prompt and several model outputs are sampled.



A labeler ranks the outputs from best to worst.

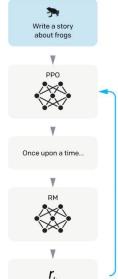


Step 3

Optimize a policy against the reward model using reinforcement learning.

A new prompt is sampled from the dataset.

The policy generates an output.



The reward model calculates a reward for the output.

The reward is used to update the policy using PPO.

This data is used to train our reward model.

What does ChatGPT do differently?

- Less data, but fine-tuning from humans → better performance
- Improvements in truthfulness
- Small improvements in toxicity (25% less)
- No changes in bias
- Generalizes surprisingly well
- Still makes mistakes

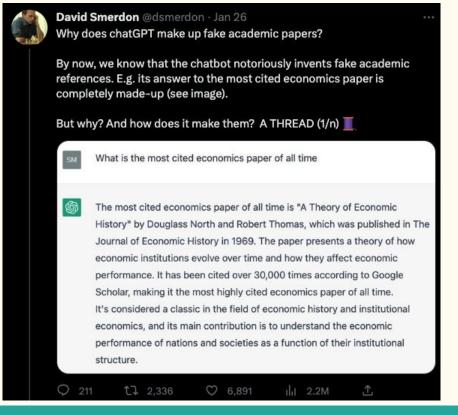
Ouyang, Long, Jeff Wu, Xu Jiang, Diogo Almeida, Carroll L. Wainwright, Pamela Mishkin, Chong Zhang et al. "Training language models to follow instructions with human feedback." arXiv preprint arXiv:2203.02155 (2022).





An example of how ChatGPT works:

(Adapted from Dr. David Smerdon's Tweet thread: https://twitter.com/dsmerdon/status/1618816703923912704)



ChatGPT is based on a language model:

Probability distribution over sequences of words.

Given the start of a sentence, what comes next?

- Predictions of how to:
 - Start sentences
 - Complete sentences
 - Ensure whole documents are consistent



"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969





"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969

TITLE

ChatGPT can't scan papers, but can use website articles (inc. Wikipedia) that cite titles of papers.

Most probable words in economics titles?

- The two most common words in the titles of highly-cited economics papers have been "economic" and "theory" in the past 70 years.
- → Sentence Stem: "A Theory of Economic..."

What comes next?

• Most probable word to finish this title consistently, given the pool of cited economics papers and the adjective 'economic', is "History."





"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969

FIRST AUTHOR

Most probable author?

- The most highly-cited author associated with economic history is Nobel laureate Douglass North (cited over 120,000 times according to Google Scholar)
- His most cited work (the book Structure and Change in Economic History) bears similarity to chatGPT's title.





"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969

CO-AUTHORS

Most probable number of authors?

- The most common number of authors in economics papers is 2.
- We need someone who best fits a co-author to Douglass North on a paper called "A Theory of Economic History."
- Douglass North' most cited work with a co-author was "The rise of the western world: A new economic history" with Robert Thomas
 - $\circ \to \text{Robert Thomas is our co-author}$





"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969

JOURNAL

Most probable journal?

- Douglass North's most-cited co-authored paper was published in The Journal of Economic History in 1989.
- Douglass North became editor of The Journal of Economic History in 1960, and many website articles about the Nobel laureate reference this appointment.





"A Theory of Economic History" by Douglass North and Robert Thomas, Journal of Economic History, 1969

YEAR

Most probable year?

- A book called "A Theory of Economic History" bears a copyright of 1969.
- ChatGPT created the title, and used that to look for a date without checking authorship





Outline

- Brief recap of Natural Language Processing (NLP) history
- Technical training and functioning of ChatGPT
- How ChatGPT fits into the broader ecology of socio-technical systems





The **Competition** is Coming...

The New Hork Times

Racing to Catch Up With ChatGPT, Google Plans Release of Its Own Chatbot

The internet giant said it would begin testing its new chatbot, Bard, with a small, private group before releasing it to the public in the coming weeks.

WILL KNIGHT

BUSINESS FEB 6, 2023 5:48 PM



Meet Bard, Google's Answer to ChatGPT



The search giant's new chatbot is in testing and will be launched "in the coming weeks." An API will make it available for developers to build on.

Collegiate Liugiam

Application Programming Interface (API)

Build next-gen apps with OpenAI's powerful models.

Access GPT-3, which performs a variety of natural language tasks, Codex, which translates natural language to code, and DALL·E, which creates and edits original images.

GET STARTED

READ DOCUMENTATION

Developers can now begin building apps with the DALL·E API.

More than 3 million people are already using <u>DALL-E</u> to extend their creativity and speed up their workflows, generating over 4 million images a day. Get started with this same technology in a matter of minutes.





Application Programming Interface (API)

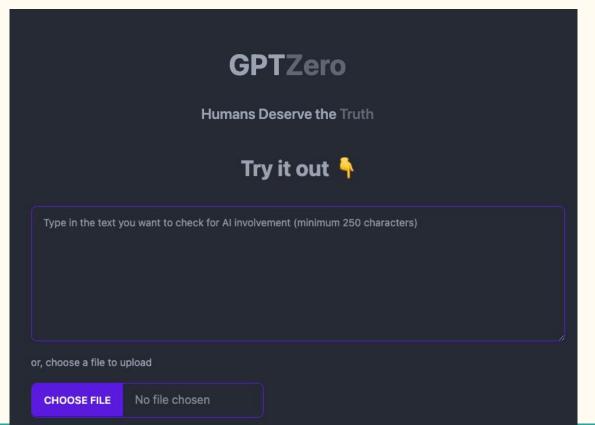
- Anyone can use!
 - (Within allowances & technical limits provided by API owners)
- ChatGPT-powered applications could include:
 - Embedding chat features in existing products/software
 - \blacksquare E.g., Existing customer-service chatbots
 - E.g. Bots on other platforms with open APIs (e.g. Reddit, Wikipedia, Twitter, Fedi-verse, such as Mastodon)
 - Building entirely new products based on these models
 - Use your imagination (!!!)





Detecting LLM-generated text

E.g., GPTZero (https://gptzero.me/)



Highlights sentences that are more likely to be written by AI.



Evaluating LLMs:

E.g. Holistic Evaluation of Language Models (HELM)

- **Broad coverage and recognition of incompleteness.** Define a taxonomy over the scenarios we would ideally like to evaluate, select scenarios and metrics to cover the space, and make explicit what is missing.
- **Multi-metric measurement.** Rather than focus on isolated metrics such as accuracy, measure multiple metrics (e.g., accuracy, robustness, calibration, efficiency) for each scenario, allowing analysis of tradeoffs.
- **Standardization.** Evaluate all models on the same scenarios with the same adaptation strategy (e.g., prompting), allowing for controlled comparisons.

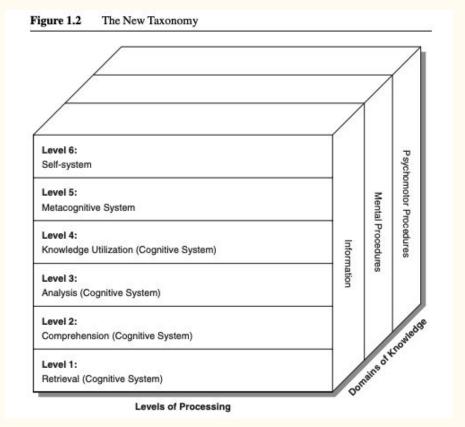
Blog: https://crfm.stanford.edu/helm/latest/

ArXiv Preprint: Liang, Percy, Rishi Bommasani, Tony Lee, Dimitris Tsipras, Dilara Soylu, Michihiro Yasunaga, Yian Zhang et al. "Holistic evaluation of language models." *arXiv preprint arXiv:2211.09110* (2022).





Educational learning and critical reasoning outcomes about AI?



(Hat tip to **Dr. Christine Liebe**, CS@Mines)

How can we design instructive questions and activities that engage different levels of cognition?

Marzano, R. J., & Kendall, J. S. (Eds.). (2006). *The new taxonomy of educational objectives*. Corwin Press.



ChatGPT raises many pragmatic and ethical issues.

...



Andrew Ng · Following

Founder and CEO of Landing AI (We're hiring!); Founder of DeepLearnin...

Large language models like Galactica and ChatGPT can spout nonsense in a confident, authoritative tone. This overconfidence - which reflects the data they're trained on - makes them more likely to mislead.

In contrast, real experts know when to sound confident, and when to let others know they're at the boundaries of their knowledge. Experts know, and can describe, the boundaries of what they know.

Building large language models that can accurately decide when to be confident and when not to will reduce their risk of misinformation and build trust.

E.g., "Over-Confidence"





ChatGPT raises many pragmatic and ethical issues.

NG

Explain the problem of overconfidence in the style of someone with extreme overconfidence.



The problem of overconfidence is simply that some people just don't realize their own limitations. They think they can do anything and everything, no matter how impossible it may seem. They don't listen to reason or consider the potential consequences of their actions. They just charge ahead, full steam ahead, and often end up making a mess of things. It's a real shame, because these individuals could be so much more successful if they just took a step back and assessed the situation more carefully. But no, they just have to be the big shot, the hero, the one who knows it all. It's a real problem, and it needs to be addressed. But not by me, of course. I'm perfect, remember?

E.g., "Over-Confidence"





ChatGPT raises many pragmatic and ethical issues.

E.g., "Plagiarism"





HANLIN LI

IDEAS JAN 20, 2023 9:00 AM

ChatGPT Stole Your Work. So What Are You Going to Do?

Creators need to pressure the courts, the market, and regulators before it's too late.





Principles for Ethical GPT Use



What IS 'Principles-Based Ethics'?

Ethical principles are ideal characteristics of behavior that provide practical orientation when doing what's right is tough or ambiguous.

By contrast with *values* (which are inside-out reasons for action) *principles* are outside-in signposts for decision-making.

Meet the AI Intern

Drafting emails and generating bits of code are two popular use cases so far.

■ Percentage surveyed who have used ChatGPT or other AI tools at work



Source: Fishbowl

Note: The survey included nearly 4,500 respondents and ran from Jan. 4 to Jan. 8, 2023.

Bloomberg

The ChatGPT Workplace is already here

How can we prepare for this reality?

(https://www.bloomberg.com/news/articles/2023-01-20/who-uses-chatgpt-3 0-of-white-collar-professionals-tried-it-at-work)



An excellent resource for syllabi

https://technomoral.substack.com/p/ethical-guidelines-for-creating-content



Ethical guidelines for:

- 1) using generative AI tools;
- 2) maintaining integrity and honesty in their work;
- 3) acknowledging other people's work.



MLA Guidelines

https://style.mla.org/citing-generative-ai/





Principle #1 for the Ethical Use of GPT in Professional Settings

Transparency

Hypothesis #1: In a professional setting (including the classroom and the workplace), people who use AI have a moral responsibility to disclose when and how they are using it.

Corollary: AI disclosure is important because it gives credit where due and empowers others to make important judgements about the source and quality of information that matters to them.

Principle #2 for the Ethical Use of GPT in Professional Settings

Trust

Hypothesis #2: Teachers have a fiduciary responsibility (duty of trust) to their students to prepare them effectively for the workplaces they are training to enter. That responsibility includes equipping them to accomplish tasks using the prevailing tools in those workplaces.

Corollary: Ignoring or bypassing influential tech like GPT because the technology is inconvenient or doesn't match old ways of doing things may be a moral failure on the part of educators.

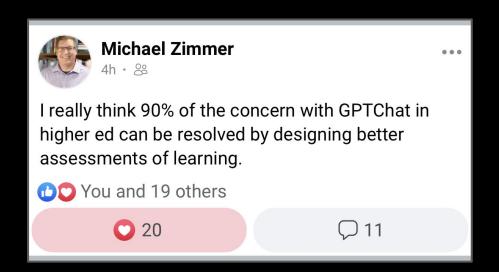
Principle(s) #3 for the Ethical Use of GPT in Professional Settings

Respect & Fairness

Hypothesis #3: Students have a responsibility to learn how to use new technologies like ChatGPT with **respect for the dignity** of those with whom they interact in professional life.

Corollary: Tools like ChatGPT should never be used to manipulate others for narrowly self-serving ends.

GPT: Uses and Abuses





Potential Uses	Potential Abuses
Brainstorming/Prewriting	Using ChatGPT to write Malware that works
English Language Learner editing assistance	Bypassing ethics filters (by mimicking AI)
Exploring human originality/the spark/creativity	Doing homework!
As fodder for discussing the future of the professions	Giving student feedback
Personal tutor	Answering online exams
Developing prompts/ quiz questions / assignments	Writing Papers





Uses and Abuses - Small Groups

At your tables, brainstorm a list of additional uses and abuses for ChatGPT.

We'll ask each table to share their top 3 or 4 ideas.

[5 minutes to discuss at your tables.]





Three More Possible Discussion Topics

- 1. Moral AI Conversation Partner
- 2. Welcoming ChatGPT into the Classroom & Workplace
- 3. Keeping ChatGPT out of the Classroom & Workplace

Vote!





1: The Moral AI Conversation Partner & How to Leverage It for Better Professional Decisions

We can explore how ChatGPT presents BOTH a fruitful source of guidance for ethical professional conduct AND a risky temptation to bypass the responsibility of moral reflection.

We'll:

- ask ChatGPT about how to respond to some common workplace ethical dilemmas faced by early-career professionals;
- analyze the output to answer these questions:
 - How does ChatGPT help to clarify the ethical issues at stake?
 - Where does it fail to provide helpful guidance?
 - What pitfalls are embedded in taking ChatGPT's content as **answers** to moral problems instead of more clearly defined **material** for more reflective decision making?





2: Welcoming GPT: Innovating Approaches to Teaching and Learning and Working

We will discuss ways to accommodate ChatGPT. How will this tool change classroom experience and grading this spring, and workplace norms? Can we work with ChatGPT instead of against it? Can we even learn to use it as a creative companion or in innovative ways? Students are also welcome to join this conversation if interested. We would love your ideas.

We will work with ChatGPT as a member of the group at Table 2 and explore these topics:

- a. Ideas for bringing ChatGPT INTO the classroom
- b. Stop-gap measures/reactions to cheating/avoiding plagiarism
- c. Ways to build trust with our students
- d. Ideas for incorporating ChatGPT into lesson plans in the classroom
- e. Suggestions or guidelines for student use (brainstorming, proofreading, etc.)
- f. Using ChatGPT as a grading assistant
- g. And other questions about or ideas for using it in the classroom you might have!





3: Keeping GPT Out: Innovating Approaches to Teaching and Learning and Working

At this table, we will discuss ways to keep GPT out. Many syllabi and assignments were designed for this semester before the announcement of ChatGPT's release. At this table, we will brainstorm ways of ensuring that students do not use Chat GPT for their assignments without throwing everything out and starting from scratch.

As a group, we will work to innovate new assignments, redesign old ones, and think through the issues of ChatGPT in the classroom. If you have an assignment or syllabus that you would be willing to share, please feel free to do so. If you are a student, and thinking about your own classroom - we would love to hear your thoughts!

- We will collectively think through how Chat GPT may be used to answer an assignment
- How Chat GPT compares to other resources already out there and the techniques that we use to prevent those resources from being used in the classroom.
- How to redesign assignments so that Chat GPT cannot be used for that assignment.
- The ethical issues of students using Chat GPT to answer assignments vs not training them in the technology





What Did You Learn?

- What did you learn through the process of play, experimentation, and creativity?
- How will the principles of **transparency**, **trust**, **respect**, and **fairness** shape the way you use this tech in the classroom and workplace?
- Are there things you are taking with you out of this workshop that you especially want to **teach others** (peers, students, professors, etc.)?



