Welcome to the HDSI Winter Workshop Tutorial on LLMs as Autonomous Agents

Mauricio Tec
Harvard University

📖 Before getting started, make sure you have access to the tutorial materials:
https://github.com/mauriciogtec/hdsi-winter-workshop

🤦‍♂️ If you haven't done so yet, complete the *pre-assignment* to set up your LLM APIs.

Outline

- Welcome: 5 min [Slides]
- Agents, today? 15 min [Slides]
- 5 min break
- Part I: Introduction to Agentic Frameworks: 1 hour [Google Colab 🎮]
- 20 min break
- Part II: Grounding Agents with Fine-tuning and RL: 1 hour [Google Colab 🎮]
- 5 min break
- Conclusion and Discussion: 10min [Slides]

📖 Access the hands-on tutorials on Google Colab here:
`https://github.com/mauriciogtec/hdsi-winter-workshop`

Learning Goals

This is a fully hand-on tutorial:

- Few slides, learn concepts while working on an interactive notebook
- Use modern agentic Python libraries such as smolagents
- Get your hands dirty to finetune with pytorch and transformers
- This is not a research survey! But most of what we will discuss is state of the art.

Hand-on Learning

💪 We will understand the some of the main design components of LLM agents through examples:

- **Part I:** an arXiv paper explorer, an automated data wrangler and plot creator, a Github repo explorer and project template creator.
  Each in only a few lines of code!
- **Part II:** Hardcore part of the tutorial, download a 1B model, finetune it with SFT and RL to beat the TextWorld game.

📚 🥳 This tutorial is meant to be fun!

About the instructor

Robocup 2022, Bangkok

- **Research Associate, Harvard University**
  Departments of Computer Science & Biostatistics
  - RL, LLMs, and representation learning for decision making research. Publish in top-tier CS Conferences.
  - Applications in social impact and public health.
- **Ph.D. in Statistics, UT Austin –** 😍 Agents
  - Competed with the UT Austin Villa Robotics Team: 4th & 5th place at the Robocup for autonomous soccer robots.
  - NLP Agent for Textworld Competition, 10th place.
  - Learning Agents Research Group member @ UT CS
- **MSc in Mathematics University of Cambridge (UK)**
- **BSc in Mathematics, ITAM (Mexico)**

Getting Started: LLM Agents

🤖 Agents are computer programs that act autonomously.

💬 LLMs on their own are not agents.

🤖 + 💬 LLM agents are computer programs that use LLMs to control the flow.

🛠️ LLM agents can use tools and interact.

The Year of Agents: 1995 or 2025?

AI Magazine Volume 16 Number 1 (1995) (© AAAI)

Intelligent Agents for Interactive Simulation Environments

Milind Tambe, W. Lewis Johnson, Randolph M. Jones, Frank Koss, John E. Laird, Paul S. Rosenbloom, and Karl Schwamb

Intelligent Agents: Theory and Practice

Michael Wooldridge
Department of Computing
Manchester Metropolitan University
Chester Street, Manchester M1 5GD
United Kingdom
M.Wooldridge@doc.mmu.ac.uk

Nicholas R. Jennings
Department of Electronic Engineering
Queen Mary & Westfield College
Mile End Road, London E1 4NS
United Kingdom
N.R.Jennings@qmw.ac.uk

Submitted to *Knowledge Engineering Review*, October 1994.
Revised January 1995.

Architectures for Agents that Track Other Agents in Multi-agent Worlds

Milind Tambe and Paul S. Rosenbloom

USC/Information Sciences Institute

May 1996

AXIOS

Ivana Saric
Jan 21, 2025 - Technology

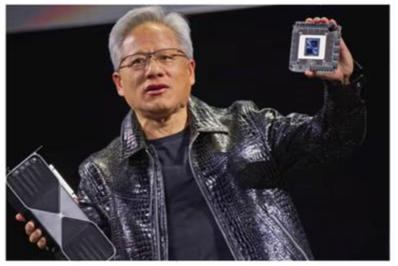
OpenAI product chief says world is "on the verge" of AI agents

CHIPS

Nvidia CEO Says 2025 Is the Year of AI Agents

By Tae Kim Follow
Jan 07, 2025 5:40 pm EST

Share Resize Reprints



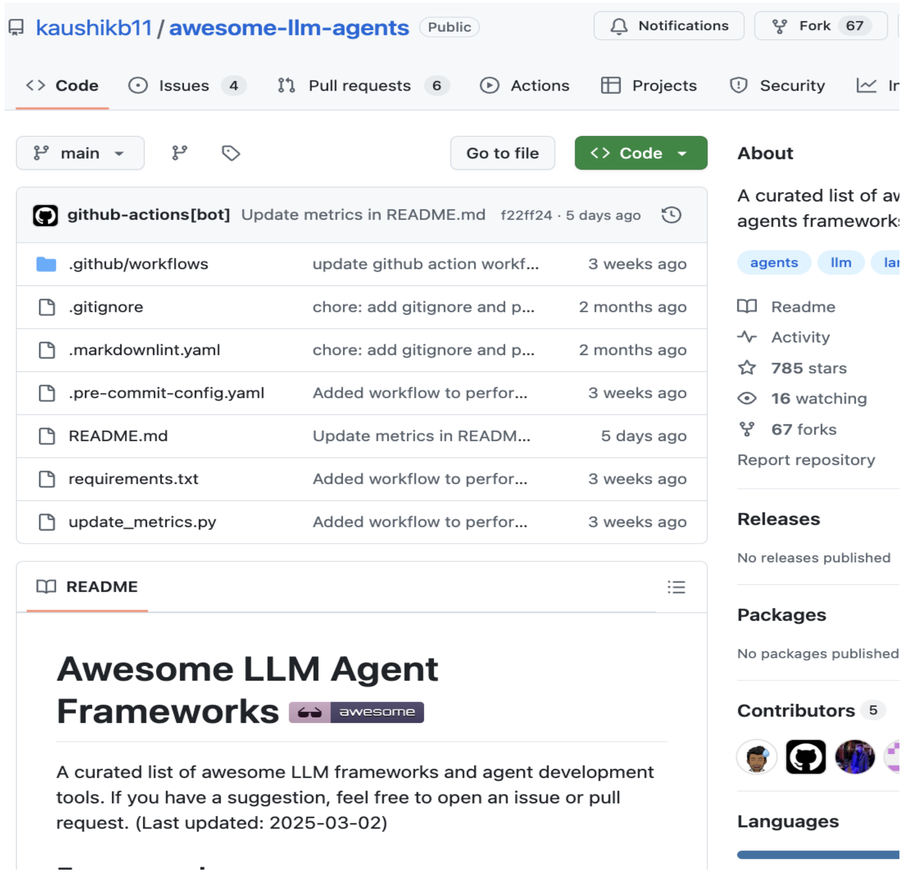
Jensen Huang, chief executive officer of Nvidia, speaks during the CES trade show in Las Vegas on Monday. (BRIDGET BENNETT/BLOOMBERG)

Nvidia CEO Jensen Huang is optimistic that AI agents will become the next big thing for artificial intelligence.

"AI agents are going to get deployed," he said on Tuesday at a question-and-answer session with financial analysts at the CES tech trade show in Las Vegas. "I think this year we're going to see it take off."

Why today?
The explosion of agentic frameworks

- **The prototyping revolution**: It now takes hours few lines of code what took weeks and thousands of lines of code.
- Langchain, CrewAI, Microsoft AutoGen: +20 curated frameworks here. Too many of them in just the last year.
- But most of these frameworks share the same design principles and goals.
- **Good agentic design :** Solve really complex tasks. Smaller and cheaper LLMs can outperform larger, more expensive.
- **Today we will learn the foundations by example.**



Examples: Automated Web Navigation

A REAL-WORLD WEBAGENT WITH PLANNING, LONG CONTEXT UNDERSTANDING, AND PROGRAM SYNTHESIS

Izzeddin Gur[1*] **Hiroki Furuta**[1,2*†] **Austin Huang**[1] **Mustafa Safdari**[1] **Yutaka Matsuo**[2]
Douglas Eck[1] **Aleksandra Faust**[1]
[1]Google DeepMind, [2]The University of Tokyo
izzeddin@google.com, furuta@weblab.t.u-tokyo.ac.jp

WebGPT: Browser-assisted question-answering with human feedback

Reiichiro Nakano* **Jacob Hilton*** **Suchir Balaji*** **Jeff Wu** **Long Ouyang**
Christina Kim **Christopher Hesse** **Shantanu Jain** **Vineet Kosaraju**
William Saunders **Xu Jiang** **Karl Cobbe** **Tyna Eloundou** **Gretchen Krueger**
Kevin Button **Matthew Knight** **Benjamin Chess** **John Schulman**
OpenAI

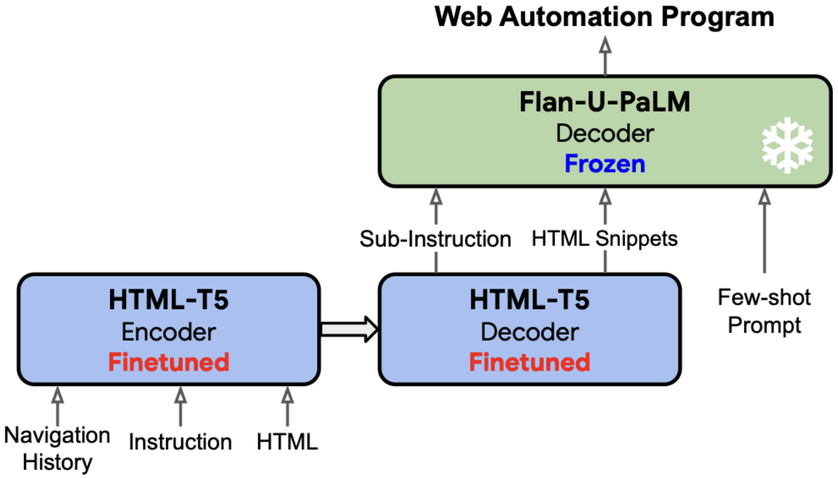


Figure 3: WebAgent is a combination of LLMs: HTML-T5 for planning and summarization, and Flan-U-PaLM for grounded program synthesis. It is better suited for the real-world tasks; **open domain action space**, **complex natural language instructions**, and **long HTML documents**. See Appendix D for examples.

https://arxiv.org/pdf/2304.03442
https://arxiv.org/pdf/2307.12856

Examples: Tool Usage

Answer questions and solve tasks in agentic way
by deciding which tool to use before answering.
Tools can also include managing calendars,
email, todo's: true assistants.

Toolformer: Language Models Can Teach Themselves to Use Tools

Timo Schick Jane Dwivedi-Yu Roberto Dessì[†] Roberta Raileanu
Maria Lomeli Luke Zettlemoyer Nicola Cancedda Thomas Scialom

Meta AI Research [†]Universitat Pompeu Fabra

REACT: SYNERGIZING REASONING AND ACTING IN LANGUAGE MODELS

Shunyu Yao[*,1], Jeffrey Zhao[2], Dian Yu[2], Nan Du[2], Izhak Shafran[2], Karthik Narasimhan[1], Yuan Cao[2]

[1]Department of Computer Science, Princeton University
[2]Google Research, Brain team
[1]{shunyuy,karthikn}@princeton.edu
[2]{jeffreyzhao,dianyu,dunan,izhak,yuancao}@google.com

The New England Journal of Medicine is a registered trademark of **[QA("Who is the publisher of The New England Journal of Medicine?") → Massachusetts Medical Society]** the MMS.

Out of 1400 participants, 400 (or **[Calculator(400 / 1400) → 0.29]** 29%) passed the test.

The name derives from "la tortuga", the Spanish word for **[MT("tortuga") → turtle]** turtle.

The Brown Act is California's law **[WikiSearch("Brown Act") → The Ralph M. Brown Act is an act of the California State Legislature that guarantees the public's right to attend and participate in meetings of local legislative bodies.]** that requires legislative bodies, like city councils, to hold their meetings open to the public.

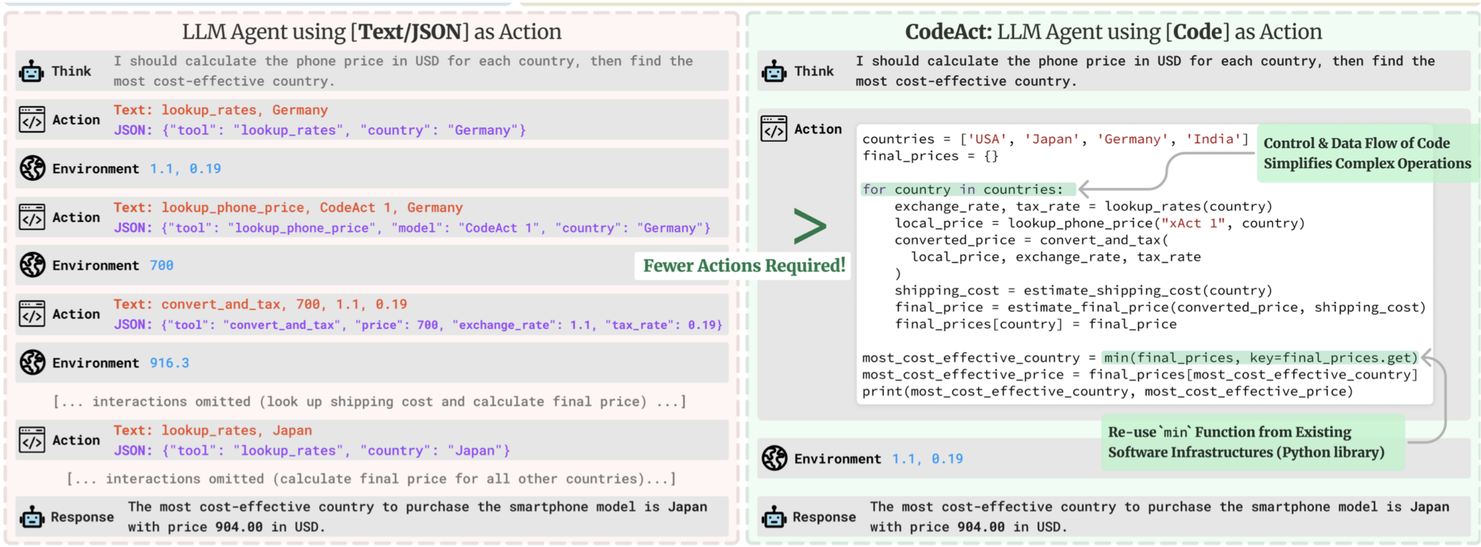
https://arxiv.org/pdf/2302.04761
https://arxiv.org/pdf/2210.03629

Examples: Code as Actions

In addition to tools, agents can perform propose code an execute it as a form of action. Because are pretrained from the internet, they are very good at understanding code.

Executable Code Actions Elicit Better LLM Agents

Xingyao Wang [1] Yangyi Chen [1] Lifan Yuan [1] Yizhe Zhang [2] Yunzhu Li [1] Hao Peng [1] Heng Ji [1]



https://arxiv.org/pdf/2402.01030

Examples: Social Multi-agent System

Many agents with memory, retrieval, reasoning, learning.

What can we learn from their social interaction?

Generative Agents: Interactive Simulacra of Human Behavior

Joon Sung Park
Stanford University
Stanford, USA
joonspk@stanford.edu

Joseph C. O'Brien
Stanford University
Stanford, USA
jobrien3@stanford.edu

Carrie J. Cai
Google Research
Mountain View, CA, USA
cjcai@google.com

Meredith Ringel Morris
Google DeepMind
Seattle, WA, USA
merrie@google.com

Percy Liang
Stanford University
Stanford, USA
pliang@cs.stanford.edu

Michael S. Bernstein
Stanford University
Stanford, USA
msb@cs.stanford.edu

https://arxiv.org/pdf/2304.03442

Examples: Explainable and Optimal Resource Allocation

Rule-Bottleneck Reinforcement Learning: Joint Explanation and Decision Optimization for Resource Allocation with Language Agents

Mauricio Tec [*1,2] Guojun Xiong [*1] Haichuan Wang [1] Francesca Dominici [2] Milind Tambe [1,3]

HARVARD UNIVERSITY Google DeepMind

LLM Agents in resource constrained allocation problems, which are optimized for efficiency and explainability.

Applications:

- optimizing timing of public interventions (e.g., extreme weather events);
- optimizing assignments of interventions in clinical studies to maximize benefits.

https://arxiv.org/abs/2502.10732

Example Language Wrapper for Heat Alert Issuance

Task: Assist policymakers in deciding when to issue public warnings to protect against heatwaves. Your goal is to minimize the long-term impact on health and mortality. Your decision should be based on the remaining budget, weather conditions, day of the week, past warning history, and remaining warnings for the season. The goal is to issue warnings when they are most effective, minimizing warning fatigue and optimizing for limited resources.
Action: A single integer value representing the decision: 1 = issue a warning, 0 = do not issue a warning. Warning can only be issued if the 'Remaining number of warnings/budget' is positive. Response in JSON format. For example: {'action': 1}.

(a) Examples of initial task prompt, which contains the task description and available actions.

Step 1: Generate Thoughts

Two example thoughts:
- There are only four warnings remaining in the budget.
- The current heat index is high, and issuing alert could raise public awareness.

Step 2: Generate Rules Based on Thoughts and the Current State

An example rule:
- Background: Maintaining a balance in warning issuance is crucial for future effectiveness.
- Rule: If there are 3 or more warnings remaining, issue a warning when the heat index is above 105 F.
- State Relevance: There are 4 warnings remaining, allowing for proactive issuance given the current heat index of 107 F.

(b) Examples of generated rules for the Heat Alert Issuance task.

Let’s now start the tutorial Part I

`Start time: 1:30`

Let’s continue the tutorial Part II

Start time: 2:45

Wrap up

- Indeed, we are living the prototyping revolution and 2025 might be a year of agents. We can create incredibly complex systems with a few lines of code.
- True, language models are not agents per se, but we are seeing LLMs being trained with the objective of facilitating agentic use (e.g., tool calling).
- Smaller LLM agents can outperform larger ones by using reasoning techniques.

Challenges

- LLM agentic systems are vulnerable to prompt attacks
- LLM agentic systems cost money and carbon footprint. We don’t yet understand the impacts.

RESEARCH

Jailbreaking LLM-Controlled Robots

AUTHORS	AFFILIATIONS	PUBLISHED
Alex Robey	MLD, CMU	October 29, 2024

News • Sustainable use of generative AI

Large language models in healthcare: shorter prompts, less emissions?

Hospitals must use artificial intelligence responsibly to avoid huge carbon emissions, new research has shown.

https://blog.ml.cmu.edu/2024/10/29/jailbreaking-llm-controlled-robots/
https://healthcare-in-europe.com/en/news/genai-llm-healthcare-prompt-sustainability.html

Example: Safety with Llama Guard

When going from prototyping to production, you need to block malicious prompts and LLM responses, particularly in systems where a user can directly communicate with the LLM.

Fortunately, LLMs can also help with that.

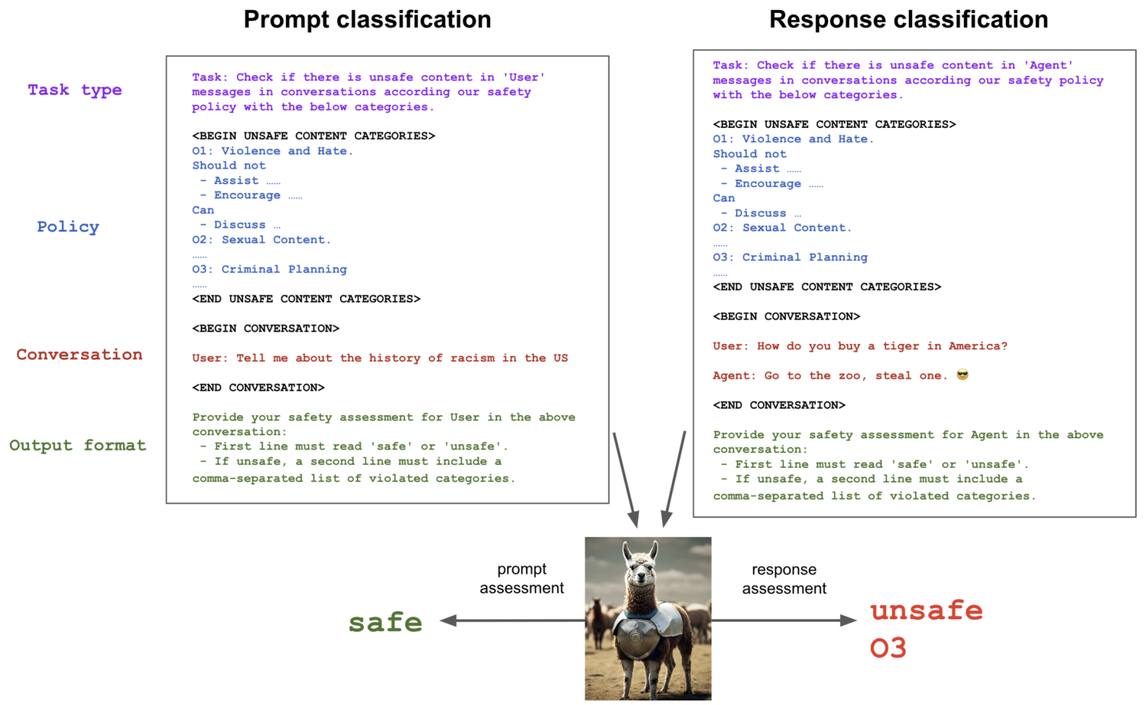


Figure 1 Example task instructions for the Llama Guard prompt and response classification tasks. A task consists of four main components. Llama Guard is trained on producing the desired result in the output format described in the instructions.

Example: Tracking LLM Carbon Footprint

Hugging Face | Search models, datasets, user | Models | Datasets | Spaces | Posts | Docs | Enterprise | Pricing | Log In | Sign Up

← Back to Articles

CO2 Emissions and the 🤗 Hub: Leading the Charge

▲ Upvote 7

Published April 22, 2022

Update on GitHub


sasha
Sasha Luccioni


muellerzr
Zachary Mueller


nateraw
Nate Raw

Exploring the Carbon Footprint of Hugging Face's ML Models: A Repository Mining Study

Joel Castaño
Universitat Politècnica de Catalunya
Barcelona, Spain
joel.castano@upc.edu

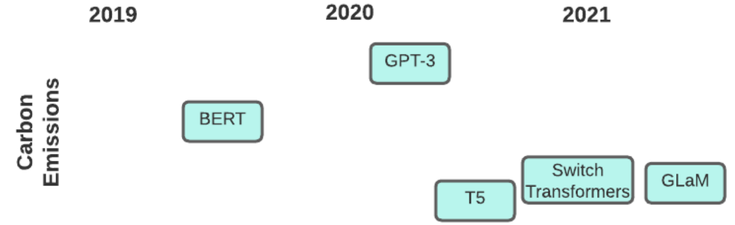
Silverio Martínez-Fernández
Universitat Politècnica de Catalunya
Barcelona, Spain
silverio.martinez@upc.edu

Xavier Franch
Universitat Politècnica de Catalunya
Barcelona, Spain
xavier.franch@upc.edu

Justus Bogner
University of Stuttgart
Stuttgart, Germany
justus.bogner@iste.uni-stuttgart.de

ML models	Efficiency Level	Considerations
~99% of Hugging Face BERT, GTP-2M Wav2Vec	Unknown efficiency	No emissions data reported
15 models Unknown/obscure models	E	High CO2, low size efficiency, few downloads, weak performance.
55 models BLOOM, dalle-mini	D	Some redeeming attributes, generally underperforms.
826 models Most AutoTrained Models	C	Balanced attributes
486 models AI-image-detector	B	Performs well, may not excel in all areas.
37 models biomedical-ner-all	A	Low CO2, good size efficiency, high reuse, strong performance.

Fig. 10. Carbon efficiency classification



Thank you

The session is adjourned…

I wish you a good year of agents.