
# Chatbots and AI Agents

11-667: LARGE LANGUAGE MODELS: METHODS AND APPLICATIONS

# What to expect on the midterm

- Conceptual questions about the content of the lecture and readings
- Topics you should prepare to be assessed on
  - Transformer architecture
  - Pretraining (data collection and learning objectives)
  - Finetuning techniques and data (alignment, RLHF, PETM)
  - Evaluation (human and automatic)
  - In-context learning
  - Interpretability
  - Applications (search, dialog agents)

# When you think of “chatbot” what comes to mind?

- ChatGPT
- Bard
- character.ai

Implementation

1. Take pre-trained LLM
2. Finetune it on appropriate data
3. Clever prompting

# What distinguishes an AI agent from a chatbot?

- An agent…
  - exists within an environment
  - can take actions that change its environment
  - can converse with other agents within the environment
  - Has a persona
  - Has a goal
  - Has memories of what has previously transpired

General-purpose chatbots (ChatGPT, Bard, etc.) do not exist in an environment they can alter, and they do not have specific goals. All memory is implicit in the conversational history.

# Why care about building AI agents?

- Entertainment / video games
- Modeling real-user behaviour
  - For example, testing a new application with “mock” users could be less expensive than hiring real users to test it out.
- Pre-requisite for *embodied* agents.
  - We can use agents acting in a virtual environment to measure progress toward agents acting in a real one.
- Challenging evaluation platform for natural language understanding and generation

# Case Studies in this Lecture

- Agents in a fantasy text adventure game
  - "Learning to Speak and Act in a Fantasy Text Adventure Game." Urbanek et al. 2021.
- Diplomacy-playing agent
  - "Human-level play in the game of Diplomacy by combining language models with strategic reasoning." Bakhtin et al. 2022.
- Simulated town
  - "Generative Agents: Interactive Simulacra of Human Behavior." Park et al. 2023.

# Agents in a fantasy text adventure game

- Environment:
  - Locations, randomly glued together
  - Each location also has some number of items
- Agents:
  - Each agent is situated in the environment.
  - Each agent possess some number of items
- Agent actions:
  - Emote: {applaud, cringe, cry, etc.}
  - Chat with other agents
  - Perform a physical action (e.g. “put robes in closet” or “eat salmon”)
- Agent, locations, and items have natural language descriptions.

# Agents in a text adventure game

| | |
|---|---|
| **Category:** | Graveyard |
| **Description:** | Two-and-a-half walls of the finest, whitest stone stand here, weathered by the passing of countless seasons. There is no roof, nor sign that there ever was one. All indications are that the work was abruptly abandoned. There is no door, nor markings on the walls. Nor is there any indication that any coffin has lain here... yet. |
| **Backstory:** | Bright white stone was all the fad for funerary architecture, once upon a time. It's difficult to understand why someone would abandon such a large and expensive undertaking. If they didn't have the money to finish it, they could have sold the stone, surely - or the mausoleum itself. Maybe they just haven't needed it yet? A bit odd, though, given how old it is. Maybe the gravedigger remembers... if he's sober. |
| **Neighbors:** | Dead Tree, south, following a dirt trail behind the mausoleum<br>Fresh Grave, west, walking carefully between fallen headstones |
| **Characters:** | gravedigger, *thief, peasant, mouse, bat* |
| **Objects:** | wall, *carving, leaf, dirt* |

(a) Example room created from the room collection and labelling tasks.

# Agents in a text adventure game

| **Character:** | Thief | Gravedigger |
|---|---|---|
| **Persona:** | I live alone in a tent in the woods. I steal food from the townspeople and coal from the blacksmith. The village police can not find me to put me in jail. | I am low paid labor in this town. I do a job that many people shun because of my contact with death. I am very lonely and wish I had someone to talk to who isn't dead. |
| **Description:** | The thief is a sneaky fellow who takes from the people and does so in a way that disturbs the livelihood of the others. | You might want to talk to the gravedigger, specially if your looking for a friend, he might be odd but you will find a friend in him. |
| **Carrying:** | meat, potatoes, coal | shovel |
| **Wearing:** | dark tunic, cloak | *nothing annotated* |
| **Wielding:** | knife | *nothing annotated* |

(b) Example characters annotated via character collection tasks.

# Agents in a text adventure game

| **Character:** | Thief | Gravedigger |
|---|---|---|
| **Persona:** | I live alone in a tent in the woods. I steal food from the townspeople and coal from the blacksmith. The village police can not find me to put me in jail. | I am low paid labor in this town. I do a job that many people shun because of my contact with death. I am very lonely and wish I had someone to talk to who isn't dead. |
| **Description:** | The thief is a sneaky fellow who takes from the people and does so in a way that disturbs the livelihood of the others. | You might want to talk to the gravedigger, specially if your looking for a friend, he might be odd but you will find a friend in him. |
| **Carrying:** | meat, potatoes, coal | shovel |
| **Wearing:** | dark tunic, cloak | *nothing annotated* |
| **Wielding:** | knife | *nothing annotated* |

(b) Example characters annotated via character collection tasks.

Task goal: Can we generate a conversation between the thief and the gravedigger and predict which actions/emotes they will take after each conversational utterance?

# Agents in Diplomacy, a negotiation-based board game

- Seven players compete to control countries (SCs) on a map.
- At each turn, players chat with each-other to decide on their actions.
  - Any promises, agreements, threats, etc. are non-binding.
- Once chatting is over, players may choose to
  - Move their units, waging war if into an already-occupied region
  - Use their units to support other units (which could include the units of a different player)

# Agents in Diplomacy, a negotiation-based board game

- Seven players compete to control countries (SCs) on a map.
- At each turn, players chat with each-other to decide on their actions.
  - Any promises, agreements, threats, etc. are non-binding.
- Once chatting is over, players may choose to
  - Move their units, waging war if into an already-occupied region
  - Use their units to support other units (which could include the units of a different player)


Task goal: An AI agent that follows the same rules and norms as the human agents, and has as good a win-rate as skilled human players.

# Agents in a simulated town

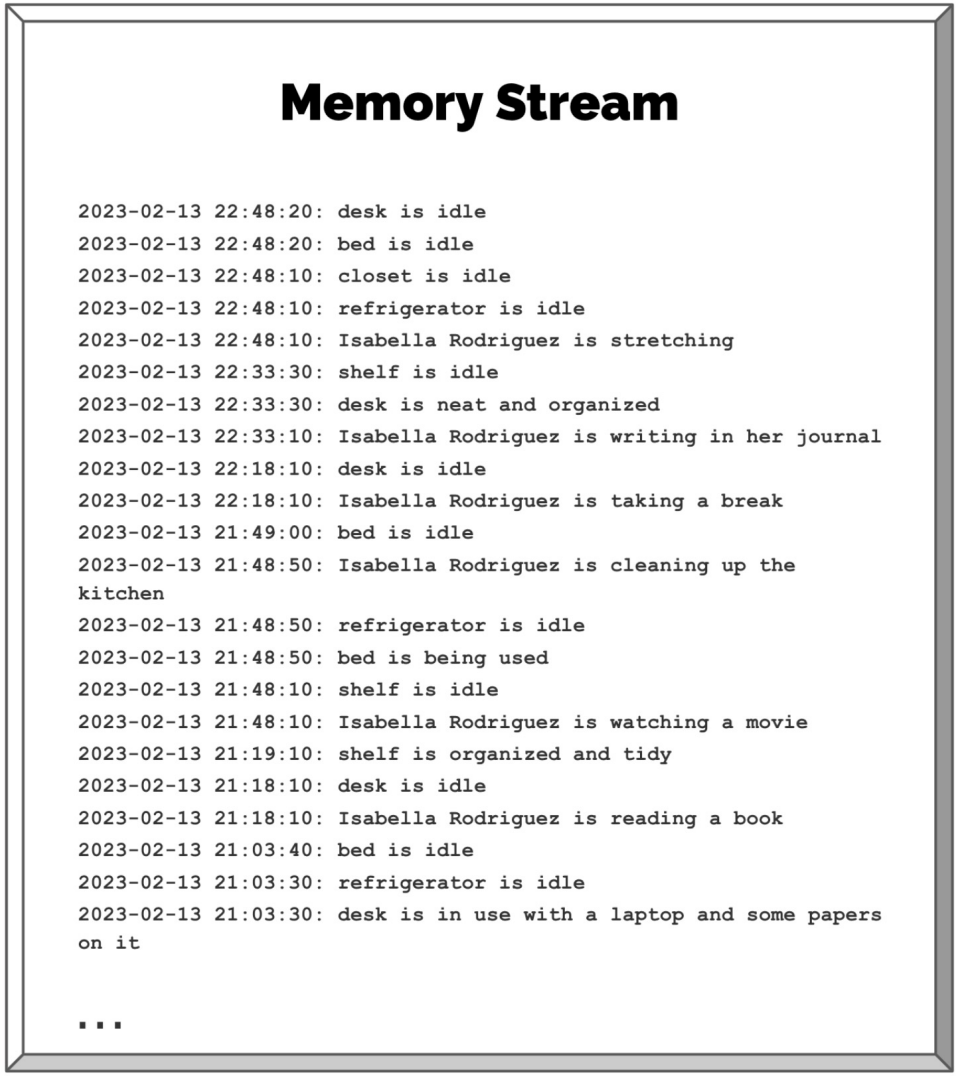
# Agents in a simulated town

- Modeled after the video game the Sims
- 25 agents
  - Each begins the simulation with a pre-defined set of “seed memories”
  - Agents do not have explicit goals

John Lin is a pharmacy shopkeeper at the Willow Market and Pharmacy who loves to help people. He is always looking for ways to make the process of getting medication easier for his customers; John Lin is living with his wife, Mei Lin, who is a college professor, and son, Eddy Lin, who is a student studying music theory; John Lin loves his family very much; John Lin has known the old couple next-door, Sam Moore and Jennifer Moore, for a few years; John Lin thinks Sam Moore is a kind and nice man; John Lin knows his neighbor, Yuriko Yamamoto, well; John Lin knows of his neighbors, Tamara Taylor and Carmen Ortiz, but has not met them before; John Lin and Tom Moreno are colleagues at The Willows Market and Pharmacy; John Lin and Tom Moreno are friends and like to discuss local politics together; John Lin knows the Moreno family somewhat well — the husband Tom Moreno and the wife Jane Moreno.

# Agents in a simulated town

- Modeled after the video game the Sims
- 25 agents
  - Each begins the simulation with a pre-defined set of “seed memories”
  - Agents do not have explicit goals
- At each step:
  - Each agents output a natural language statement of their action
    - “write in journal”
    - “walk to pharmacy”
    - “talk to Joe”
  - Actions and environment state are parsed into memories, reflections, and observations.



# Where can LLMs be used in these systems?

- Dialog with other agents (who may be either human agents or other AI agents)
- Deciding on agent actions
- Choosing what information (from the environment and from the agent's internal state) to condition the conversation and decision-making on.

.

# Where can LLMs be used in these systems?

- Dialog with other agents (who may be either human agents or other AI agents)
- Deciding on agent intents
- Choosing what information (from the environment and from the agent's internal state) to condition the conversation and decision-making on.

Challenges:

- How can we convert world and agent state into natural language?
- How can we convert natural language into agent actions and environment changes?
- Can all these tasks be accomplished with a general-purpose LM or do we need finetuned models?

# Choosing information to condition the conversation and decision-making on.

- In many cases, there will be more information than can fit into an LM context window. Most of this won't be relevant.
  - The Town Sim keeps around a database of memories. Memories are scored by their recency, importance, and relevance to ongoing memory.

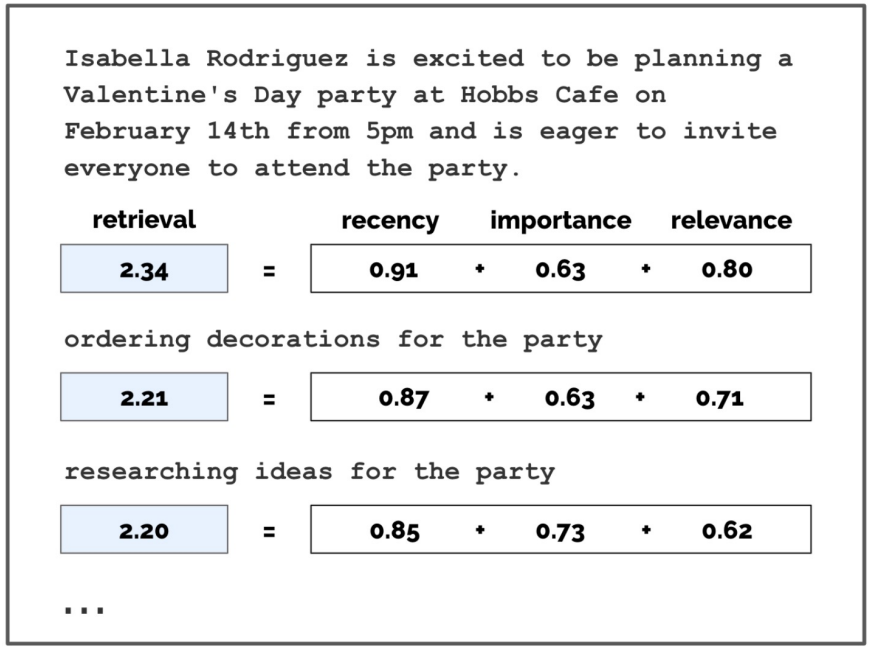
```
On the scale of 1 to 10, where 1 is purely mundane
(e.g., brushing teeth, making bed) and 10 is
extremely poignant (e.g., a break up, college
acceptance), rate the likely poignancy of the
following piece of memory.
Memory: buying groceries at The Willows Market
and Pharmacy
Rating: <fill in>
```

Compute LM sequence embedding of query memory and each memory in database.

Score database memories by dot product with query memory.

# Choosing information to condition the conversation and decision-making on.

- In many cases, there will be more information than can fit into an LM context window. Most of this won't be relevant.
  - The Town Sim keeps around a database of memories. Memories are scored by their recency, importance, and relevance to ongoing memory.



# Choosing information to condition the conversation and decision-making on.

- In many cases, there will be more information than can fit into an LM context window. Most of this won't be relevant.
  - The Town Sim keeps around a database of memories. Memories are scored by their recency, importance, and relevance to ongoing memory.
  - In Diplomacy, the dialog model and intent model see as input:
    - dialogue history (all messages exchanged between player A and the six other players up to time t)
    - game state, action history, and metadata (current game state, recent action history, game settings, A's Elo rating, etc.)
    - For the dialog model: A's intended actions, and the actions A wants its conversational partner to complete.

# Choosing information to condition the conversation and decision-making on.

- In many cases, there will be more information than can fit into an LM context window. Most of this won't be relevant.
  - The Town Sim keeps around a database of memories. Memories are scored by their recency, importance, and relevance to ongoing memory.
  - In Diplomacy, the dialog model and intend model see as input:
    - dialogue history (all messages exchanged between player A and the six other players up to time t)
    - game state, action history, and metadata (current game state, recent action history, game settings, A's Elo rating, etc.)
    - For the dialog model: A's intended actions, and the actions A wants its conversational partner to complete.
  - In the Fantasy Text Adventure, dialog rounds were short enough that all environment information and history fit into max sequence length.

# Deciding on agent intent

- Can we trust an LLM to choose reasonable intents?
  - Fantasy Text Adventure Game
    - Yes, via a finetuned BERT-based ranker
  - Simulated Town
    - Yes, through prompting GPT-3 with an agent's description and memories
    - Hierarchical generation: generate a broad plan first, and then generate smaller steps in the plan
  - Diplomacy
    - No, use a reinforcement learning agent trained through self-play to output an action intent

# Dialog with other agents

- All three examples in our case study use LLMs to generate dialog.
  - Diplomacy and Fantasy Text Adventure finetuned models
  - Simulated Town used instruction-tuned GPT-3 without further finetuning
- When is finetuning especially helpful:
  - If the world state cannot be effectively represented in natural language.
  - When bad dialog can lead to poor outcomes
    - Simulated Town paper notes how their generated dialogs tend to be very formal and stilted, likely due to GPT-3's instruction tuning.
- An LLM is not always the right tool for the job:
  - Example: Settlers of Catan AI agent can do well just with templated text generation

# Takeaways

# Quiz Question

In what kinds of scenarios would a pre-trained LLM without finetuning not be a good choice for outputting agent intents?