# Day 7 - LLM

UMN CSS Workshop Instructor: Alvin Zhou Presentor: Jiacheng Huang

# **Learning Goals**

- Learn how LLM works
- Practice using LLM to label text and image

Each word is represented by a vector

Each word is represented by a vector

Cat: [0.0074, 0.0030, -0.0105, ..., 0.0002]

Each word is represented by a vector

Cat: [0.0074, 0.0030, -0.0105, ..., 0.0002]

Gorgeous: [0.21, -0.04, 0.11, ..., 0.08]

**Xiangling** = Gorgeous + Cat



Each word is represented by a vector

CAT: [0.0074, 0.0030, -0.0105, ..., 0.0002]

- Words with similar meanings are close in vector space
- Captures semantic and syntactic similarity
- "king" "man" + "woman" ≈ "queen"
- "love" and "like" have similar embeddings

# Words often have multiple meanings

John went to the **bank** to withdraw cash.

He sat on the river **bank**.

### Words often have multiple meanings

John went to the **bank** to withdraw cash.

He sat on the river **bank**.

John picks up a <u>magazine</u>.

Susan works for a magazine.

### Words often have multiple meanings

John went to the **bank** to withdraw cash

He sat on the river **bank** 

Homonyms (two unrelated meanings)

John picks up a magazine.

Susan works for a **magazine**.

Polysemy (two closely related meanings)

### Limitation of traditional word embeddings

Traditional word embeddings:

Each word has a single vector (same vector in every context).

#### Limitation:

Cannot capture **polysemy** (subtle variations of meaning) or **homonyms** (entirely different meanings).

### Embeddings in LLM

Large language models (LLMs) like BERT, GPT:

- Assign different vectors to the same word in different contexts.
- Vectors update dynamically as the model processes the sentence.

#### Example:

- "bank" in "John went to the bank to withdraw cash" (financial)
- "bank" in "He sat on the river bank" (geographic)

### Embeddings in LLM

- "bank" in "John went to the bank to withdraw cash" (financial)
- "bank" in "He sat on the river bank" (geographic)
- → LLM embeddings are very different because the context changes the meaning significantly.

- "magazine" in "John picks up a magazine." (physical object printed publication)
- "magazine" in "Susan works for a magazine." (organization periodical publisher)

LLMs <u>use more similar vectors</u> for polysemous meanings than for homonymous meanings.

### Difference from LLM to Doc2Vec

LLM: The embedding of vector is context dependent, so we can not generate a embedding to work without context.

E.g., Embedding of "cat" 🙅

Embedding of "the big cat that is beautiful"

\*theoretically if the LLM is smart enough they should know the cat in this context refer to Xiangling

### How can I get embedding from LLM?

### **ELMo**

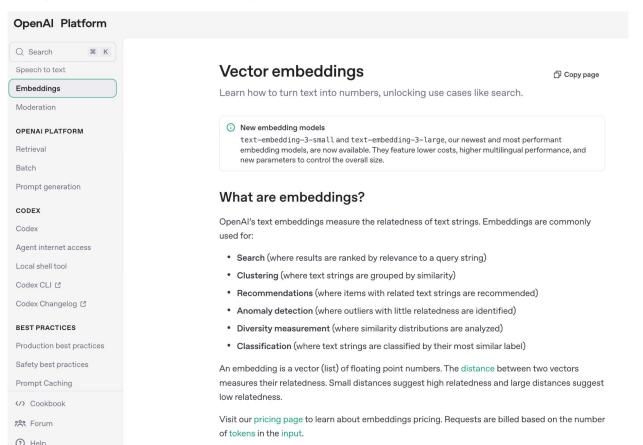
Introduced by Peters et al. in Deep contextualized word representations

Embeddings from Language Models, or ELMo, is a type of deep contextualized word representation that models both (1) complex characteristics of word use (e.g., syntax and semantics), and (2) how these uses vary across linguistic contexts (i.e., to model polysemy). Word vectors are learned functions of the internal states of a deep bidirectional language model (biLM), which is pre-trained on a large text corpus.

A biLM combines both a forward and backward LM. ELMo jointly maximizes the log likelihood of the forward and backward directions. To add ELMo to a supervised model, we freeze the weights of the biLM and then concatenate the ELMo vector  $\mathbf{ELMO}_k^{task}$  with  $\mathbf{x}_k$  and pass the ELMO enhanced representation  $[\mathbf{x}_k; \mathbf{ELMO}_k^{task}]$  into the task RNN. Here  $\mathbf{x}_k$  is a context-independent token representation for each token position.

Image Source: here

### How can I get embedding from LLM?



How does LLM actually work?

How does LLM actually work?

"It predicts the probability of the next word."

How does LLM actually work?

"It leverages the contextual information."

- Sentence → Each word becomes an embedding.
- These word embedding pass through dozens of *transformer* layers (in GPT-3, 96 layers!).
- Each layer adjusts the word's meaning based on surrounding words
  - Update the word's embedding vector
- By the final layer, each word vector has been refined to predict the most likely next word.
  - GPT: Left-to-right (causal)
  - Bidirectional (masked)

### Transformer: Attention is all you need

1. **Attention step:** words "look around" for other words that have relevant context and share information with one another.

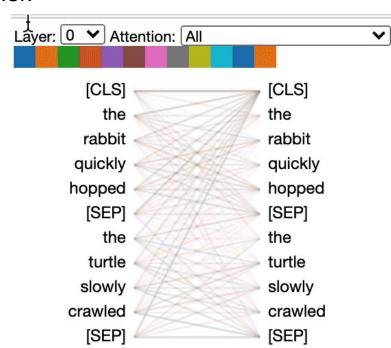
#### **BertViz**

Visualize Attention in NLP Models

**Quick Tour • Getting Started • Colab Tutorial • Paper** 

BertViz is an interactive tool for visualizing attention in <u>Transformer</u> language models such as BERT, GPT2, or T5. It can be run inside a Jupyter or Colab notebook through a simple Python API that supports most <u>Huggingface models</u>. BertViz extends the <u>Tensor2Tensor visualization tool</u> by <u>Llion Jones</u>, providing multiple views that each offer a unique lens into the attention mechanism.

Get updates for this and related projects on Twitter .



### Transformer: Attention is all you need

1. **Attention step:** words "look around" for other words that have relevant context and share information with one another.

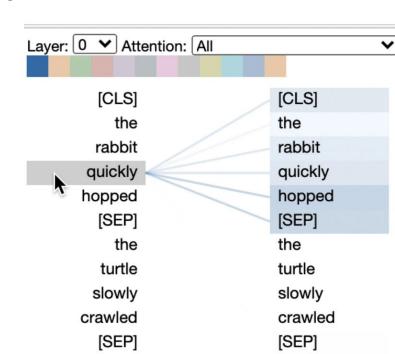
#### **BertViz**

**Visualize Attention in NLP Models** 

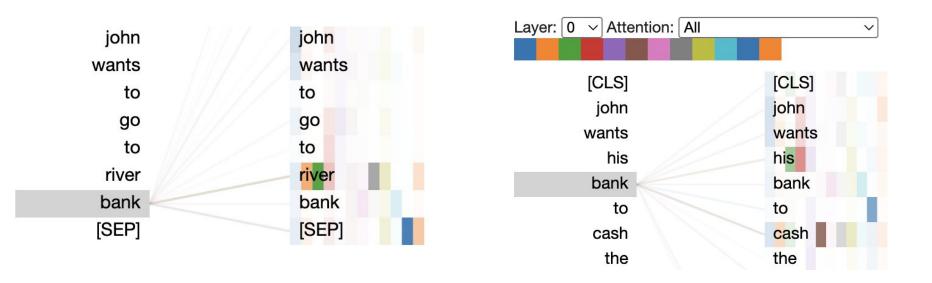
**Quick Tour • Getting Started • Colab Tutorial • Paper** 

BertViz is an interactive tool for visualizing attention in <u>Transformer</u> language models such as BERT, GPT2, or T5. It can be run inside a Jupyter or Colab notebook through a simple Python API that supports most <u>Huggingface models</u>. BertViz extends the <u>Tensor2Tensor visualization tool</u> by <u>Llion Jones</u>, providing multiple views that each offer a unique lens into the attention mechanism.

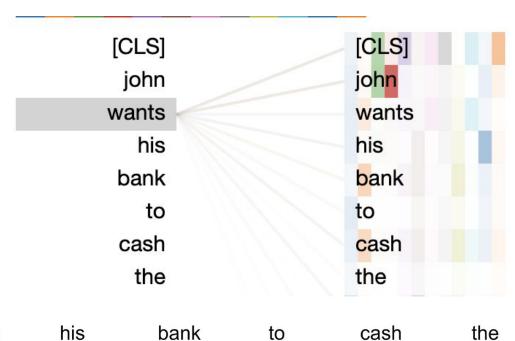
Get updates for this and related projects on Twitter .



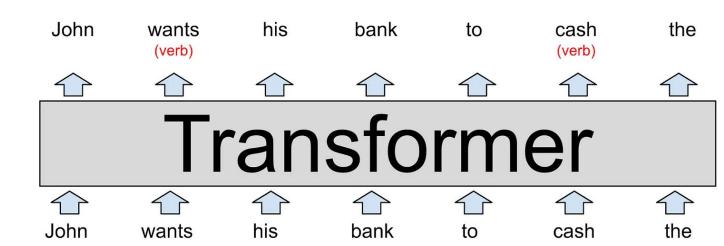
John wants his bank to cash the



John wants his bank to cash the



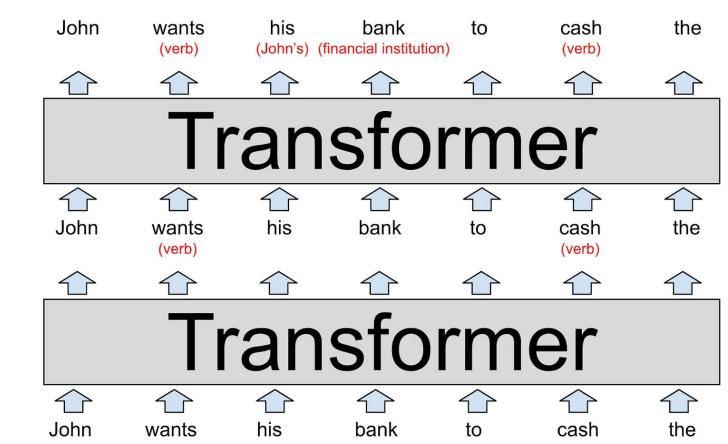
John his bank wants to



### Transformer: Attention is all you need

1. **Attention step:** words "look around" for other words that have relevant context and share information with one another.

2. **Feed-forward step:** each word "thinks about" information gathered in previous attention steps and tries to predict the next word.



"John wants his bank to cash the check."

"John wants his bank to cash the bond."

- "John wants his bank to cash the money order."
- com wante me bank to caen the money order.

### See what's inside the black box: XAI

• <a href="https://huggingface.co/spaces/liujch1998/infini-gram">https://huggingface.co/spaces/liujch1998/infini-gram</a>

https://playground.allenai.org

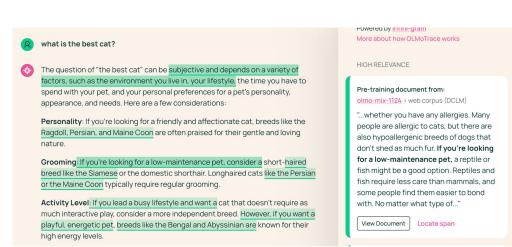
#### ■ Infini-gram: Scaling Unbounded n-gram Language Models to a Trillion Tokens

Jiacheng Liu<sup>1</sup>, Sewon Min<sup>1</sup>, Luke Zettlemoyer<sup>1</sup>, Yejin Choi<sup>1,2</sup>, Hannaneh Hajishirzi<sup>1,2</sup>

<sup>1</sup>University of Washington, <sup>2</sup>Allen Institute for AI

[Web Interface] [API Endpoint] [Python Package] [Docs] [Code] [Paper]

Join our Discord server! Get the latest updates & maintenance announcements, ask the developer anything about infini-gram, and connect with other fellow users.



## LLM can be do a lot of things ...

Textual/ visual analysis Stimuli Simulation Participants

. . . . . .

## LLM can be do a lot of things ...

Textual/ visual analysis

Stimuli

Simulation

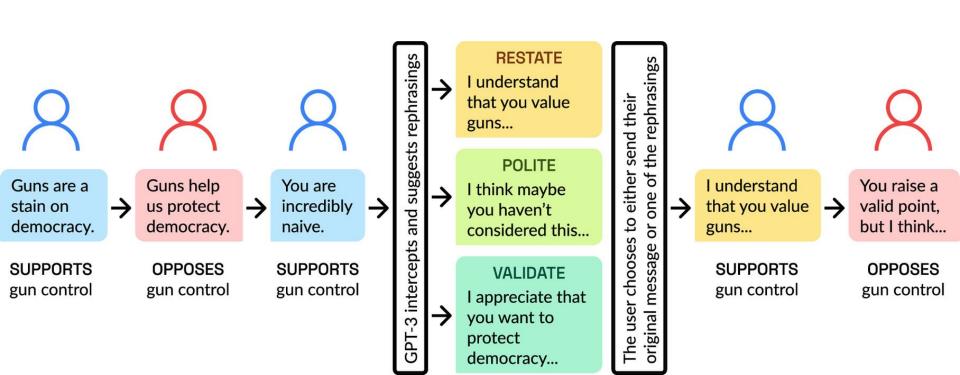
Participants

. . . . . .

Can real-time AI chat suggestions improve online political conversations?

### Hypotheses:

- Al suggested conversations will improve perceived conversation quality.
- Will promote democratic reciprocity—respecting political opponents' rights to speak.
- No expected change in policy attitudes.



#### Al suggestions increased:

- Conversation quality (feeling understood & respected).
- Democratic reciprocity (willingness to hear political opponents).
  - Effects strongest for partners of Al-assisted users.
  - No effect on policy attitude changes.

### Al suggestions increased:

- Conversation quality (feeling understood & respected).
- Democratic reciprocity (willingness to hear political opponents).
  - Effects strongest for partners of Al-assisted users.
  - No effect on policy attitude changes.

#### Mechanism

Al rephrasings → more polite, validating language (text analysis).

## LLM can be do a lot of things ...

Textual/ visual analysis Stimuli Simulation Participants

. . . . . .



Agent-based modeling (ABM): A computational approach to simulate actions & interactions of autonomous agents within an environment.

#### Core Features:

- Agents independent "actors" (e.g., people, animals, firms).
- Rules simple, hand-coded decision rules (e.g., if-then logic).
- Environment spatial or networked setting where agents interact.
- Emergence system-level patterns arise from micro-level behaviors.

#### Micro-level ABM

Focus: Simulation of individual-level interactions based on rule/ mechanism

Outcome: Emergent social patterns from local rules

### **Macro-level ABM**

Focus: Simulation of macro outcomes (like public health, market dynamics)

Outcome: Macro-level patterns (infection rates, herd immunity)

# Let's try to do a ABM together

Neighbor

Neighbor

Schelling's Segregation Model

Agents – students (50% red, 50% blue)

**Environment** – Classroom seating grid

**Rules** – Happy if  $\geq$  2 neighbors are same color.

If unhappy, move to an empty seat with more same-color neighbors.

(Move one by one)

Emergence -

Neighbor

You

# Let's try to do a ABM together

Schelling's Segregation Model

Agents – students (50% red, 50% blue)

**Environment** – Classroom seating grid

**Rules** – Happy if ≥ 2 neighbors are same color.

If unhappy, move to an empty seat with more same-color neighbors.

(Move one by one)

<u>Emergence - Segregated seating patterns.</u>

Neighbor

Neighbor

You

Neighbor

Neighbor

Neighbor

You

#### **Limitations of Traditional ABM:**

- Rules are static
- No long-term memory or self-reflection
- Poor at modeling nuanced social behavior
- Struggles with complex, open-ended interactions

|                             | Micro-Level ABM   | Macro-Level ABM   |  |  |  |
|-----------------------------|---|---|--|--|--|
| Focus                       | Individual-level interactions, specific rules   | System-wide outcomes (public health, market dynamics)   |  |  |  |
| Traditional<br>Outcome      | Emergent patterns (e.g., neighborhood segregation)  | Macro-level trends (e.g., infection curves, herd immunity)  |  |  |  |
| Generative<br>Agents<br>Add | <ul><li>Rich cognitive states (memory, reflection)</li><li>Natural-language social behavior</li><li>Adaptive planning</li><li>Reasoning</li></ul> | <ul><li>Heterogeneous reasoning and compliance</li><li>Realistic social interactions</li><li>Scenario testing with natural language prompts</li></ul> |  |  |  |
| Result                      | More realistic micro-level dynamics that still produce emergent social patterns   | More <b>credible macro projections</b> grounded in nuanced individual behavior  |  |  |  |

# LLM can be do a lot of things ...

Textual/ visual analysis

Stimuli Simulation Participants

. . . . . .

Can Large Language Models (LLMs) accurately predict treatment effects in social science experiments?

70 U.S. survey experiments (476 treatment effects; 105,165 participants)

GPT-4 simulated average participant responses based on demographic prompts

Compared LLM predictions vs. human forecasts vs. actual experimental results

GPT-4 predictions surpassed human forecasters

Even higher accuracy for unpublished studies (no exposure in training data)

GPT-4 have little biases across different subgroups:

 Didn't perform worse for Black participants, for women, or for one political party over another.

GPT-4 have little biases across different subgroups:

- Consistent performance across different subgroups
- Didn't perform worse for Black participants, for women, or for one political party over another.

GPT-4 have little biases across different subgroups:

- Consistent performance across different subgroups
- Didn't perform worse for Black participants, for women, or for one political party over another.

The paper shows consistent accuracy across gender, race, and political affiliation—do you think this suggests low bias?

# LLM can be do a lot of things ...

Textual/ visual Stimuli **Simulation Participants** analysis

. . . . . .

# **Labeling Methods**

Manual Labeling Time-consuming & Expensive

Machine Learning
Technical skills &
Computing power

# **Labeling Methods**

Manual Labeling
Time-consuming &
Expensive

**LLM**Affordable & Easy

Machine Learning
Technical skills &
Computing power

# LabelGenius



## LabelGenius

# Data sharing

Save

https://platform.openai.com/settings/organization/data-controls/sharing https://help.openai.com/en/articles/10306912-sharing-feedback-evals-and-api-data-with-openai

#### Enable sharing of model feedback from the Platform Enable all members of your organization to share feedback and chats with OpenAI to help improve and train our models. If enabled, users can click the "thumbs down" button on model responses in the Playground and choose to share their feedback and content from the current chat. Learn more. Disabled Enabled for all projects Enabled for selected projects Share Logs with OpenAl Turn on sharing with OpenAl for logs from your organization to help us develop and improve our services, including for improving and training our models. Only inference inputs and outputs created after turning this setting on will be shared. You can change your settings at any time to disable sharing inference inputs and outputs. You're enrolled for up to 11 million complimentary tokens per day 1 Disabled Enabled for all projects Enabled for selected projects

## LabelGenius

| Module  | Function                      | Purpose  | Single-<br>theme |   | Modality Support             |
|---|-------------------------------|--|------------------|---|------------------------------|
| CLIP  | classification_CLIP_0_shot    | Perform zero-shot classification with CLIP                   | ✓                |   | Text, Image, Text-Image Pair |
| (Runs locally; no data                            | classification_CLIP_finetuned | Use a fine-tuned CLIP model for classification               | 1                |   | Text, Image, Text-Image Pair |
| sharing required)                                 | finetune_CLIP                 | Fine-tune CLIP on labeled data                               | ✓                |   | Text, Image, Text-Image Pair |
| GPT   | classification_GPT            | Perform text classification with GPT (zero-shot or few-shot) | ✓                | / | Text, Image, Text-Image Pair |
| (Requires data sharing with third-party provider) | generate_GPT_finetune_jsonl   | Prepare JSONL files for GPT fine-tuning                      | ✓                | ✓ | Text                         |
| - · · · ·   | finetune_GPT                  | Fine-tune a GPT model on labeled data                        | ✓                | ✓ | Text                         |
|   | price_estimation              | Estimate the cost of OpenAI API calls                        | -                | - | -                            |
|   |                               |  |                  |   |                              |

## LabelGenius

### Price estimation

#### https://openai.com/api/pricing/

#### OpenAl o4-mini

Our faster, cost-efficient reasoning model delivering strong performance on math, coding and vision

#### Price

Input:

\$1,100 / 1M tokens

Cached input:

\$0.275 / 1M tokens

Output:

#### GPT-4.1

Smartest model for complex tasks

Price

Input:

\$2.00 / 1M tokens

Cached input: \$0.50 / 1M tokens

Output:

\$8.00 / 1M tokens

#### GPT-4.1 mini

Affordable model balancing speed and intelligence

Price

Input:

\$0.40 / 1M tokens

Cached input: \$0.10 / 1M tokens

Output:

\$1.60 / 1M tokens

#### GPT-4.1 nano

Fastest, most cost-effective model for low-latency tasks

Pricing

Input:

\$0.100 / 1M tokens

Cached input:

\$0.025 / 1M tokens

Output:

\$0.400 / 1M tokens

# Prompt

### **Zero-shot prompt**

Does the following tweet relate to politics, yes or no? Tweet: {the focal tweet}

## Prompt

**Zero-shot prompt** 

### **Few-shot prompt**

Does the following tweet relate to politics, yes or no? Tweet: {the focal tweet}

Example1: Tweet: {the focal tweet}. Label :{xxxx}

Example2: Tweet: {the focal tweet}. Label :{xxxx}

Coding Time!

