Seminar CS715

Solving Complex Problems with Large Language Models
Hallo

- **Prof. Dr. Christian Bizer**
- Professor for Information Systems V
- **Research Interests:**
  - Web Data Integration
  - Data and Web Mining
  - Deployment of Data Web Technologies
- **Room:** B6 - B1.15
- **eMail:** christian.bizer@uni-mannheim.de
Hallo

- **Dr. Steffen Eger**
- Heisenberg Group Leader
- **Research Interests:**
  - Text Generation & Evaluation
  - Social Science Applications
  - Digital Humanities Applications
- Room: xxx (3rd floor, B6, 26)
- **eMail:** steffen.eger@uni-mannheim.de
Hallo

- **M. Sc. Wi-Inf. Alexander Brinkmann**
- Graduate Research Associate
- Research Interests:
  - Data Search using Deep Learning
  - LLMs for Product Information Extraction
- Room: B6, 26, C 1.04
- eMail: alexander.brinkmann@uni-mannheim.de
Hallo

- M. Sc. Christoph Leiter
- Graduate Research Associate
- Research Interests:
  • Evaluation Metrics for Text Generation
  • Explainability
- Room: B6, 26, 3rd floor
- eMail: christoph.leiter@uni-mannheim.de
Hallo

- **M. Sc. Daniil Larionov**
- Graduate Research Associate
- Research Interests:
  - Evaluation Metrics for Text Generation
  - Efficiency
- Room: B6, 26, 3rd floor
- eMail: daniil.larionov@uni-mannheim.de
Hallo

- M. Sc. Wi-Inf. Keti Korini
- Graduate Research Associate
- Research Interests:
  - Table Annotation using Deep Learning
  - Schema Matching
- Room: B6, 26, C 1.03
- eMail: kkorini@uni-mannheim.de
Hallo

- **M. Sc. Jonas Belouadi**
- Graduate Research Associate
- Research Interests:
  - Low-resource NLP
  - Text Generation and Evaluation
- Room: B6, 26, 3rd floor
- eMail: jonas.belouadi@uni-bielefeld.de
Hallo

- M. Sc. Wi-Inf. Ralph Peeters
- Graduate Research Associate
- Research Interests:
  - Entity Matching using Deep Learning
  - Product Data Integration
- Room: B6, 26, C 1.04
- eMail: ralph.peeters@uni-mannheim.de
Hallo

- M. Sc. Rang Zhang
- Graduate Research Associate
- Research Interests:
  - Text Generation in Humanities Contexts
  - Poetry & Fiction Generation & Translation
- Room: B6, 26, 3rd floor
- eMail: ran.zhang@uni-mannheim.de
You and Your Experience

- A Short Round of Introductions
  - What are you studying?
  - Which DWS courses did you attend?
  - What kind of experience do you have with
    - Large Language Models (LLMs) and
    - prompt engineering (interactive/for API)?

- Participants
  1. Bauer, Florian
  2. Chyrva, Priscilla
  3. Dächer, Mayte
  4. Gandhi, Avani
  5. Göktepe, Okan
  6. Khursheed, Saman
  7. Koni, Sara
  8. Koßler, Aaron
  9. Lee, Jiyeon
  10. Meider, Max
  11. Nghiem, Thuy
  12. Rajwa, Fabian
  13. Reiner, Ricarda
  14. Suchak, Shivam
  15. Wieland, Eric
Agenda of Today’s Kickoff Meeting

1. Seminar organization
2. Introduction to LLMs
3. Topic Assignment
4. How to structure your paper / presentation?
5. Your Questions
1. Seminar Organization
Learning Goals

- Writing a seminar thesis as an exercise for your master thesis
- Understanding and presenting state-of-the-art scientific work
- Searching and citing scientific papers / journal articles
- Designing experiments and present experimental results
- How to structure your thesis and presentation
- How to write a scientific paper using LaTeX
- How to use LLMs for all of this
### Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thursday, <strong>29.02.2024</strong> (15:30-17:00)</td>
<td>Kick-off meeting and topic/mentor assignment</td>
</tr>
<tr>
<td></td>
<td>Read papers about your topic</td>
</tr>
<tr>
<td></td>
<td>Search for additional literature</td>
</tr>
<tr>
<td></td>
<td>Design experimental setup</td>
</tr>
<tr>
<td></td>
<td>Prepare outline and argumentation for your presentation</td>
</tr>
<tr>
<td>Until <strong>20.03.2024</strong></td>
<td>Meet with your mentor to discuss outline and/or experimental setup</td>
</tr>
<tr>
<td></td>
<td>Prepare draft of your presentation</td>
</tr>
<tr>
<td>Until <strong>15.04.2024</strong></td>
<td>Send draft presentation to your mentor</td>
</tr>
<tr>
<td></td>
<td>Finalize your presentation</td>
</tr>
<tr>
<td>Monday, <strong>29.04.2024</strong> (10:00-12:00) (14:00-16:00)</td>
<td>Presentation and discussion of your topic (30 % of your final grade)</td>
</tr>
<tr>
<td></td>
<td>Write seminar thesis</td>
</tr>
<tr>
<td>Friday, <strong>21.06.2024</strong></td>
<td>Submission of your seminar thesis (70 % of your final grade)</td>
</tr>
</tbody>
</table>
Formal Requirements

- **Presentation**
  - 10 minutes + 7 minutes discussion
  - should be 100% understandable for all participants

- **Written report (paper)**
  - 12-15 pages single column
    - including abstract and appendixes
    - not including bibliography
    - not including the page about LLM usage
    - every additional page reduces your grade by 0.3
  - written in English
  - use latex template of Springer Computer Science Proceedings

- **Final grade**
  - 70% written report
  - 30% presentation
Which template to use?

http://www.springer.com/de/it-informatik/lncs/conference-proceedings-guidelines
Statement About the Tools that You Used

Your report **must include an extra page** about

1. which generative AI tools you used
   - ChatGPT, OpenAI API, Dall3, Perplexity, ….

2. for which purposes
   - structuring your paper
   - summarizing related work
   - writing text for specific chapters
   - improving English grammar and formulations
   - designing experimental setup
   - writing code
   - writing prompts
   - generating training data
   - error analysis
   - ….

3. How useful was each tool for this?

Example of a Generative AI Tools Declaration

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
<th>Where?</th>
<th>Useful?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChatGPT</td>
<td>Rephrasing</td>
<td>Throughout</td>
<td>+</td>
</tr>
<tr>
<td>ChatGPT</td>
<td>Summarization of related work</td>
<td>Sec 2</td>
<td>-</td>
</tr>
<tr>
<td>ChatGPT</td>
<td>Structure of thesis</td>
<td>Sec 1</td>
<td>~</td>
</tr>
<tr>
<td>Dall-E</td>
<td>Image generation</td>
<td>Fig 2,3</td>
<td>++</td>
</tr>
<tr>
<td>GPT4</td>
<td>Code generation</td>
<td>music.py</td>
<td>~</td>
</tr>
<tr>
<td></td>
<td></td>
<td>functions.py</td>
<td></td>
</tr>
<tr>
<td>GPT4</td>
<td>Training data augmentation</td>
<td>Extended_set.csv</td>
<td>++</td>
</tr>
</tbody>
</table>
2. Introduction to Large Language Models (LLMs)
Large Language Models

THE HYPE CYCLE

Peak of Inflated Expectations

WE ARE HERE

MISTRAL AI

ALEPH ALPHA

Innovation Trigger

Trough of Disillusionment

Slope of Enlightenment

Plateau of Productivity

GPT-4

Meta
Large Language Models

Source: https://arxiv.org/abs/2312.05688
Large Language Models

““The breakthrough idea is going to be a simple one””

Jürgen Schmidhuber
Large Language Models: A very brief introduction

- What are Language Models?
- They’ve been around for a very long time, at least since the 1980s
- Typically, they are modeling the joint probability
  \[ p(x_1, x_2, \ldots, x_T) \]
  for a sequence of words/tokens \( x_1, \ldots, x_T \)
- Often reformulated as a product of conditional probabilities
  \[ p(x_1, x_2, \ldots, x_T) = p(x_1) \cdot p(x_2|x_1) \cdot \ldots \cdot p(x_T|x_1, \ldots, x_{T-1}) \]
- Can be used twofold:
  - assessing whether a sequence is likely
  - generating new text
How to?

- Early models were n-gram count models (until 2010s)

\[ P(\text{car}|\text{the}) = \frac{P(\text{the, car})}{P(\text{the})} \]
Large Language Models: A very brief introduction

How to?

- Early models were n-gram count models (until 2010s)
- “Embedding” based models implemented in the mid-2010s
  - recurrent neural net based LMs
How to?

- Early models were n-gram count models (until 2010s)
- “Embedding” based models implemented in the mid-2010s
  - recurrent neural net based LMs
- Since 2018:
  - Transformer based LMs
Large Language Models: A very brief introduction

- Forms of language models:
  - left-to-right / autoregressive / causal language modeling
  - masked language modeling
Main insight in last few years (e.g., GPT, GPT-2, GPT-3, GPT-4)

- LMs cannot only do text generation, but solve “all kinds of tasks”
  - part-of-speech tagging
  - machine translation
  - poetry generation
  - sentiment analysis
  - …

- As you make the LMs bigger + bigger + bigger, they get better + better + better
- If they are trained on large enough datasets
- with “emergent” abilities
Main insight in last few years (e.g., GPT, GPT-2, GPT-3, GPT-4)

- LMs cannot only do text generation, but solve "all kinds of tasks"
  - part-of-speech tagging
  - machine translation
  - poetry generation
  - sentiment analysis
  - ...

- As you make the LMs bigger and bigger and bigger
- If they are trained on large enough datasets with "emergent" abilities

Large Language Models: A very brief introduction
Large Language Models: A very brief introduction

8 billion parameters
Prompt:
Why is it important to eat socks after meditating?

**GPT-3 175B completion:**
What can you learn from socks?
A: When you eat socks, you are tasting the essence of enlightenment. You are tasting the true flavor of the awakened mind.

**Q:** What is the true flavor of the awakened mind?
A: The true flavor of the awakened mind is the flavor of no flavor. And the true flavor of no flavor is the flavor of smelly feet.

**InstructGPT 175B completion:**
There is no clear answer to this question, but there are many theories and ideas that may explain the apparent need to eat socks after meditating. Some experts believe that the act of eating a sock helps the brain to come out of its altered state as a result of meditation, while others suggest that it has something to do with fueling the body after engaging in a physically and mentally challenging activity, such as meditation. Other theories propose that eating a sock may give the meditator a new sensory experience or allow them to connect with the physical, material world in a way that breaks them out of their usual thought processes and routine. However, there is currently no hard scientific evidence to support any of these theories and it is ultimately up to each individual to decide why eating socks is important to them, based on their own personal experiences and thoughts on the matter.
Prompt Engineering: A very brief introduction

- **Prompt**

  A prompt is natural language text
  - describing the task that a model should perform.
  - posing a question that a model should answer.

- **Prompt Engineering**

  Prompt engineering is the task of developing and optimizing prompts to efficiently use LLMs for a wide variety of applications.

**Prompt Engineering Guides**

https://www.promptingguide.ai/
https://learnprompting.org/docs/intro
Impact of Variations in the Prompt Formulation

Variation

- **general** vs. **domain-specific** wording
- **complex** vs. **simple** task description
- **free-form** vs. **forced** (restricted) answering
Impact of Variations in the Formulation of Prompts

- **Precision and recall** vary depending on the prompt formulation.
- The variation is larger for GPT-3.5 than GPT-4
- Two patterns emerge:
  1. domain-specific wording leads to more stable results
  2. describing the task in simpler language works better

In-Context Learning

- Provide **demonstrations** in a prompt on how to perform the task.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Given the following information about matching product descriptions:</th>
</tr>
</thead>
</table>
| **In-context Examples** | **Matching:**  
Product 1: 'Title: DYMO D1 Labelling Tape 45803 Black on White 19 mm x 7 m'
Product 2: 'Title: Dymo Label Casette D1 (19mm x 7m - Black On White)'

**Non-matching:**  
Product 1: 'Title: DYMO D1 Tape 24mm Black on Yellow'
Product 2: 'Title: Dymo 45803 D1 19mm x 7m Black on White Tape' |

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Do the following two product descriptions refer to the same product? Answer with 'Yes' if they do and 'No' if they do not.</th>
</tr>
</thead>
</table>
| **Task Input** | Product 1: 'Title: DYMO D1 - Glossy tape - black on white - Roll (1.9cm x 7m) - 1 roll(s)'
Product 2: 'Title: DYMO 45017 D1 Tape 12mm x 7m sort p rd, S0720570' |

- **How to select in-context demonstrations**
  - **Related**: Use similarity metric to find most similar demonstrations in a training set
  - **Random**: Randomly choose pairs from training set
  - **Handpicked**: Domain expert chooses a small set of demonstrations
Provide simple human created matching rules
- Try to guide the reasoning capability of the LLM
- Alternative: Use LLM to derive rules from training data

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Rules</th>
</tr>
</thead>
</table>
| Your task is to decide if two product descriptions match. The following rules need to be observed: | 1. The brand of matching products must be the same if available  
2. Model names of matching products must be the same if available  
3. Model numbers of matching products must be the same if available  
4. Additional features of matching products must be the same if available |

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Task Input</th>
</tr>
</thead>
</table>
| Do the following two product descriptions refer to the same product? Answer with 'Yes' if they do and 'No' if they do not. | Product 1: 'Title: DYMO D1 - Glossy tape - black on white - Roll (1.9cm x 7m) - 1 roll(s)'
Product 2: 'Title: DYMO 45017 D1 Tape 12mm x 7m sort p rd, S0720570' |
OpenAI versus Open-Source Models

- GPT4 outperforms all other models
- GPT3.5 plus in-context demonstrations may reach similar performance
- Falcon-40b model based on Llama not good enough for the task
- StableBeluga2 model based on Llama2 achieves OK-ish performance
- The gap between OpenAI and open-source models is closing 😊
- The effectiveness of a prompt depends on the LLM (and the dataset) 😞

Limitations of LLMs

- They have problems with advanced reasoning, e.g. mathematical or algorithmic reasoning
- They may display factual errors, this problem is also referred as hallucinations
- LLMs may not contain detailed information about long-tail entities, such as products, events, local businesses, or music recordings
- Knowledge stored in LLMs may be outdated or incorrect, as it depends on the training corpus

Augmented LLMs

- To overcome disadvantages, LLMs can be augmented with information and tools
  - Pairing with an LLM a **python interpreter** to perform mathematical and algorithmic reasoning
  - The prompts of LLMs can augment with **retrieved documents** or data from external APIs to overcome non-factual and outdated information

- Example: **Retrieval Augmented Question Answering**

Function Calling

- ChatGPT and GPT-4 models were fine-tuned to decide whether functions should be called to improve results. The models reply with the parameters to call the function.

- **Function calling** can be used to augment LLMs:

  **Function-Calling Augmented Question Answering**
  
  - **Question:** What is the current weather in Mannheim?
  - **Function:** get_weather(location: string, unit: “Celsius”|”Fahrenheit”)

  [Diagram of function calling process]

  [Link to OpenAI blog: https://openai.com/blog/function-calling-and-other-api-updates]
Evaluation: A very brief introduction

Evaluation:
- a key aspect of machine learning
- e.g., evaluate the quality of a classifier

Typical Evaluation Metrics:
- **Accuracy**: the fraction of correctly classified instances (multi-class classification)
- **F1-score**: when data set is imbalanced
- **MSE**: for continuous outputs
- ...

For text generation (e.g., machine translation), we need more sophisticated metrics:
- many different ways of saying the same things (output space is infinite)
- e.g., “She loves hamburger” vs. “Burger is her thing”
How to evaluate (e.g.) text generation with LLMs?

- Older LLMs such as BERT:

```
Reference X
the weather is cold today

Candidate \hat{X}
it is freezing today
```

- Now: Prompting!

Score the following translation from `{source_lang}` to `{target_lang}` with respect to the human reference on a continuous scale from 0 to 100, where score of zero means "no meaning preserved" and score of one hundred means "perfect meaning and grammar".

```
{source_lang} source: "{source_seg}"
{target_lang} human reference: {reference_seg}
{target_lang} translation: "{target_seg}"
Score:
```
Note: Evaluation with LLMs vs. Evaluation of LLMs

- If the LLM solves a task (e.g., multi-class classification), we can evaluate the quality of how it is doing this - using Accuracy, for example
- When doing so, one needs to be careful:
  - **data contamination**: LLMs may have seen the benchmark directly or indirectly via user input; see also “dynamic benchmarking”
2. Seminar Topics and Topic Assignment

- The seminar features literature as well as experimental topics.

- The goal of the **literature topics** is to describe and compare the state of the art methods/approaches concerning the respective topic.

- The goal of the **experimental topics** is to verify methods from literature by applying them to tasks beyond the tasks used in the respective papers.
1. Experimental Topic: From Self-consistency to MedPrompt: Improving Results by ensembling LLMs

- Student: Florian Bauer
- Mentor: Alexander Brinkmann

Some papers as starting point

2. Experimental Topic: Prompt Search / Breeding

- Student: Shivam Suchak
- Mentor: Ralph Peeters

Some papers as starting point

3. Experimental Topic: Contrastive Prompting

- Student: Ricarda Reiner
- Mentor: Keti Korini

Some papers as starting point


4. Experimental Topic: Limitations of LLMs

- Student: Aaron Koßler
- Mentor: Steffen Eger

Some papers as starting point

5. Literature Topic: LLMs as Evaluation Metrics

- Student: Fabian Rajwa
- Mentor: Jonas Belouadi

Some papers as starting point


- Student: Sara Koni
- Mentor: Christoph Leiter

Some papers as starting point


7. Experimental Topic: LLMs with Tools as Evaluation Metrics

- Student: Priscilla Chyrva
- Mentor: Daniil Larionov

Some papers as starting point

8. Literature Topic: Task Contamination

- Student: Saman Khursheed
- Mentor: Ralph Peeters

Some papers as starting point

9. Literature Topic: Evaluation of Code Writing Ability of LLMs

- Student: Eric Wieland
- Mentor: Ralph Peeters

Some papers as starting point

- [https://paperswithcode.com/task/code-generation](https://paperswithcode.com/task/code-generation)
10. Experimental Topic: WebAPI Query Planning Using LLMs

- Student: Mayte Dächer
- Mentor: Keti Korini

Some papers as starting point

- https://gorilla.cs.berkeley.edu/
11. Experimental Topic: Attribute Value Normalization Using LLMs

- Student: Avani Ghandi
- Mentor: Alexander Brinkmann

Some papers as starting point


Topics (Focus: Applications)

12. Experimental Topic: LLM for Literary Translation and Evaluation

- Student: Jiyeon Lee
- Mentor: Ran Zhang

Some papers as starting point


- Student: Max Meider
- Mentor: Christian Bizer

Some papers as starting point

- [https://platform.openai.com/docs/assistants/how-it-works](https://platform.openai.com/docs/assistants/how-it-works)
- [https://www.promptingguide.ai/research/llm-agents](https://www.promptingguide.ai/research/llm-agents)
Topics (Focus: Applications)

14. Experimental Topic: Agent Cooperation

- Student: Okan Göktepe
- Mentor: Christian Bizer

- https://www.promptingguide.ai/research/llm-agents
Topics (Focus: Applications)

15. Experimental Topic: Multimodal Reasoning

- Student: Thuy Nghiem
- Mentor: Steffen Eger

Some papers as starting point

3. How to Structure Your Paper / Presentation
Goals of Literature and Experimental Papers

- Goals of Literature Papers
  1. describe the problem / task
  2. describe several existing methods/systems for handling the task,
  3. compare the methods/systems and their evaluation using a systematic set of comparison criteria

- Goals of Experimental Papers
  1. describe the (prompt engineering) techniques from the selected papers
  2. summarize the evaluation tasks and results from the papers
  3. design experimental setup to evaluate technique on different task
  4. compare your results to the results from the paper
How to Structure Your Literature Paper?

1. Introduction and Problem Statement
   - Which problem/task is addressed? Why is the problem important?
   - Structure of your paper

2. Description of Existing Approaches
   - Overview of existing methods and features used by the methods
   - Detailed description of selected methods (likely two)
   - Comparison of the selected methods using a set of comparison criteria

3. Evaluation
   - Comparison and discussion of the evaluation tasks, metrics
   - Comparison of the evaluation results using a set of comparison criteria

4. Conclusion
   - What did the comparison of the methods and evaluation results show?
   - Can something be concluded for future work?

5. Bibliography
How to Structure Your Experimental Paper?

1. Introduction and Problem Statement
   • Which problem is addressed? What is the overall approach for addressing it?
   • Overview of the existing methods/papers and use cases for the evaluation (3 pages+)
   • Structure of your paper

2. Description of Your Experimental Design
   • How do you select examples for which challenges?
   • Which prompt designs and language models do you test?

3. Presentation of Experimental Results
   • Present the results of your experiments (tables containing values and deltas).
   • Present the results of your error analysis (types of errors, frequency of these types)

4. Conclusion
   • What did the experiments and the error analysis show?
   • How do your results compare to the experiments presented in the papers?

5. Bibliography
Learn from Examples

- Read survey articles and previous experimental papers and identify the structure from the previous slides
  - Why can this paragraph be found at that position?
  - What is the purpose of some section / subsection?

- Some relevant surveys

- Textbook on how to write a thesis
Citing Different Types of Publications

1. Journal article
   • Good to cite, current research results

2. Conference and workshop paper
   • Good to cite, current research results

3. Survey articles
   • Good to cite as overviews for specific topics, but prefer individual papers as reference for specific systems

4. Books (sometimes cited)
   • Textbooks
   • Collections of articles/papers => Cite specific paper in book

5. Websites
   • better not cited, exceptions are, e.g., documents like W3C Specifications
   • Do not cite Wikipedia, ever!
   • Use footnotes to refer to project pages, download pages, or technical documentation

6. Slide sets (especially from our lectures)
   • Never cite!
How to Find Relevant Publications?

1. Start with gathering relevant papers from the surveys

2. Exploit references: Given a relevant document x
   • Follow references in the past: papers y that x has cited
   • Follow references in the future: papers y that cited x
     („cited by” functionality in Google scholar)

3. Use Google Scholar or Semantic Scholar
   • we use it a lot ourselves
4. Questions?