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
- Consultation: Wednesday, 13:30-14:30
Hallo

- **Dr. Steffen Eger**
- Heisenberg Group Leader
- Research Interests:
  - Text Generation & Evaluation
  - Social Science Applications
  - Digital Humanities Applications
- Room: xxx
- eMail: eger.steffen@gmail.com
- Consultation: no fixed office hours, by appointment
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: xxx
- eMail: christoph.leiter@uni-bielefeld.de
Hallo

- M. Sc. Daniil Larionov
- Graduate Research Associate
- Research Interests:
  - Evaluation Metrics for Text Generation
  - Efficiency
- Room: xxx
- eMail: daniil.larionov@uni-bielefeld.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. 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: xxx
- eMail: ran.zhang@uni-bielefeld.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. Schlüter, Maria
  2. Eroglu, Zeynep
  3. Tomori, Flavjo
  4. Jano, Stiliana
  5. Bajri, Deidamea
  6. Delev, Daniel
  7. Wade, Saloni
  8. Arenz, Joel
  9. Hüllen, Kilian
  10. Höppner, Jannis
  11. Nghiem, Thuy
  12. Petra Revesz
Agenda of Today‘s Kickoff Meeting

1. Seminar organization
2. Introduction to LLMs and Prompt Engineering
3. Topic Assignment
4. How to structure your seminar 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
- Designing experiments and present experimental results
- Searching and citing scientific papers / journal articles
- How to structure your thesis and presentation
- How to write a scientific paper using LaTeX
### Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tuesday, 19.09.2023</strong> <em>(10:15-11:45)</em></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>9.10.2023</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>27.10.2023</strong></td>
<td>Send draft presentation to your mentor</td>
</tr>
<tr>
<td></td>
<td>Finalize your presentation</td>
</tr>
<tr>
<td><strong>Monday, 20.11.2022</strong> <em>(10:00-12:00)</em> <em>(14:00-16:00)</em></td>
<td>Presentation and discussion of your topic <em>(30 % of your final grade)</em></td>
</tr>
<tr>
<td></td>
<td>Write seminar thesis</td>
</tr>
<tr>
<td><strong>Wednesday, 31.01.2024</strong></td>
<td>Submission of your seminar thesis <em>(70 % of your final grade)</em></td>
</tr>
</tbody>
</table>
Formal Requirements

- **Presentation**
  - 12 minutes + 8 minutes discussion
  - should be 100% understandable for all participants

- **Written report (paper)**
  - 12-15 pages single column
    - including abstract and appendixes
    - not including bibliography
    - 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
2. Introduction to LLMs and Prompt Engineering
Figure 4: Popularity of ChatGPT and LLMs (in percentage of papers having the words in their abstracts or titles) over time in our dataset.

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
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
● 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 and bigger and bigger
- 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

- with “emergent” abilities
Large Language Models: A very brief introduction

8 billion parameters
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
- If they are trained on large enough datasets
- with “emergent” abilities
Large Language Models: A very brief introduction

**ChatGPT**

**Step 1**
Collect demonstration data and train a supervised policy.

- A prompt is sampled from our prompt dataset.
- A labeler demonstrates the desired output behavior.
- This data is used to fine-tune GPT-3.5 with supervised learning.

**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.
- This data is used to train our reward model.

**Step 3**
Optimize a policy against the reward model using the PPO reinforcement learning algorithm.

- A new prompt is sampled from the dataset.
- The PPO model is initialized from the supervised policy.
- The policy generates an output.
- The reward model calculates a reward for the output.
- The reward is used to update the policy using PPO.
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
- Precision and recall strongly vary depending on the prompt formulation.

- Three patterns emerge:
  1. domain-specific wording leads to more stable results
  2. describing the task in simpler language works better
  3. forcing the model to answer with simple “Yes” or “No” is helpful
In-Context Learning

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

  - **Task Description**
  - **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'

  - **Task Description**
  - **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
Results: In-Context Learning

- Performance increase of ~3% F1 with just small number of examples
- Best performance: **20 related** examples lead to ~8% F1 increase
- Increased performance comes with a **cost increase** of > 100% per gained percentage point of F1
Provide simple human created matching rules

- Try to guide the reasoning capability of the LLM

- Intrinsic understanding of product features necessary
Results – Domain Knowledge

Table 5: Matching Knowledge results

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Shots</th>
<th>P</th>
<th>R</th>
<th>F1</th>
<th>Δ F1</th>
<th>Cost (€) per pair</th>
<th>Cost increase</th>
<th>Cost increase per Δ F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChatGPT-zeroshot</td>
<td>0</td>
<td>71.01</td>
<td>98.00</td>
<td>82.35</td>
<td>-</td>
<td>0.14</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ChatGPT-zeroshot with rules</td>
<td>0</td>
<td>80.33</td>
<td>98.00</td>
<td>88.29</td>
<td>5.94</td>
<td>0.28</td>
<td>100%</td>
<td>17%</td>
</tr>
<tr>
<td>ChatGPT-related</td>
<td>6</td>
<td>80.36</td>
<td>90.00</td>
<td>84.91</td>
<td>2.56</td>
<td>0.68</td>
<td>386%</td>
<td>151%</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>89.58</td>
<td>86.00</td>
<td>87.76</td>
<td>5.41</td>
<td>1.05</td>
<td>650%</td>
<td>120%</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>88.46</td>
<td>92.00</td>
<td>90.20</td>
<td>7.85</td>
<td>1.97</td>
<td>1307%</td>
<td>167%</td>
</tr>
<tr>
<td>ChatGPT-related with rules</td>
<td>6</td>
<td>90.70</td>
<td>78.00</td>
<td>83.87</td>
<td>1.52</td>
<td>0.79</td>
<td>464%</td>
<td>305%</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>90.91</td>
<td>80.00</td>
<td>85.11</td>
<td>2.76</td>
<td>1.17</td>
<td>736%</td>
<td>267%</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>91.11</td>
<td>82.00</td>
<td>86.32</td>
<td>3.97</td>
<td>2.09</td>
<td>1393%</td>
<td>351%</td>
</tr>
</tbody>
</table>

- Matching rules lead to increase in ~9% Precision and ~6% F1
- Similar but not as strong effect as providing related in-context examples
- Rules are cheaper to derive, cost of a query is lower
Multi-Step-Pipelines

**Approach:** Split task into multiple prompts, e.g. for table annotation
1. predict domain/type of complete table
2. perform annotation using reduced set of domain-specific labels

**Advantages:**
1. save token space for large vocabularies
2. simplify the annotation task as the model chooses from smaller set of labels
Impact of the LLM/Prompt Combination

ChatGPT vs GPT4 vs Open Source Models

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Falcon-40b-Instruct</th>
<th>StableBeluga2</th>
<th>ChatGPT-0301</th>
<th>GPT4-0613</th>
<th>delta GPT4/ChatGPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>general-complex-forced-T</td>
<td>24.06</td>
<td>76.29</td>
<td>77.52</td>
<td>91.26</td>
<td>+13.74</td>
</tr>
<tr>
<td>general-simple-forced-T</td>
<td>15.38</td>
<td>72.53</td>
<td>85.22</td>
<td>89.80</td>
<td>+4.58</td>
</tr>
<tr>
<td>domain-complex-forced-T</td>
<td>31.16</td>
<td>70.71</td>
<td>82.35</td>
<td>89.32</td>
<td>+6.97</td>
</tr>
<tr>
<td>domain-simple-forced-T</td>
<td>16.33</td>
<td>68.69</td>
<td>84.48</td>
<td>88.89</td>
<td>+4.41</td>
</tr>
<tr>
<td>Narayan-complex-T</td>
<td>24.56</td>
<td>70.83</td>
<td>83.67</td>
<td>88.24</td>
<td>+4.57</td>
</tr>
<tr>
<td>Narayan-simple-T</td>
<td>3.92</td>
<td>57.89</td>
<td>84.78</td>
<td>85.19</td>
<td>+0.41</td>
</tr>
</tbody>
</table>

- Zero-shot performance of GPT4 is similar to ChatGPT using related in-context examples
- Falcon-40b model based on Llama not good enough for the task
- StableBeluga2 model based on Llama2 already achieves good performance
- The gap between OpenAI and open-source models is closing 😊
- The effectiveness of a prompt depends on the LLM 😞
- So, you always need to compare prompt/LLM pairs
2. Seminar Topics and Topic Assignment

− The seminar features literature as well as experimental topics.

− The goal of the **literature topics** will be to summarize the state of the art concerning the application and evaluation of LLMs.

− The goal of the **experimental topics** will be to verify prompt engineering techniques by applying them to tasks beyond the tasks used in the respective papers.
1. Literature Topic: Explainability of LLMs

- Student: Jannis Höppner
- Mentor: Christoph Leiter

- Some papers as starting point
- Yao et al., Tree of Thoughts: Deliberate Problem Solving with Large Language Models
- Turpin et al., Language Models Don't Always Say What They Think: Unfaithful Explanations in Chain-of-Thought Prompting
- Lanham et al., Measuring Faithfulness in Chain-of-Thought Reasoning
- Radhakrishnan et al., Question Decomposition Improves the Faithfulness of Model-Generated Reasoning
2. Literature Topic: Efficiency of LLMs

- Student: Flavjo Tomori
- Mentor: Daniil Larionov

- Some papers as starting point
- Lee et al., Surveying (Dis)Parities and Concerns of Compute Hungry NLP Research
- Touvron et al., LLaMA: Open and Efficient Foundation Language Models
- Dettmers et al., QLoRA: Efficient Finetuning of Quantized LLMs
- Hsieh et al., Distilling Step-by-Step! Outperforming Larger Language Models with Less Training Data and Smaller Model Sizes
- Gu et al., Knowledge Distillation of Large Language Models
3. Literature Topic: Agent-Based Modeling via LLMs

- Student: Stiliana Jano
- Mentor: Ran Zhang

- Some papers as starting point
- Park et al., Generative Agents: Interactive Simulacra of Human Behavior
- Li et al., CAMEL: Communicative Agents for "Mind" Exploration of Large Scale Language Model Society
- Boiko et al., Emergent autonomous scientific research capabilities of large language models
- Zhuge et al., Mindstorms in Natural Language-Based Societies of Mind
- Wang et al., Interactive Natural Language Processing
4. Literature Topic: LLMs for the Social Sciences

- Student: Saloni Wade
- Mentor: Steffen Eger

- Some papers as starting point
- Ziems et al., Can Large Language Models Transform Computational Social Science?
- Feng et al., From Pretraining Data to Language Models to Downstream Tasks: Tracking the Trails of Political Biases Leading to Unfair NLP Models
- Hartmann et al., The political ideology of conversational AI: Converging evidence on ChatGPT's pro-environmental, left-libertarian orientation
5. Literature Topic: Limitations of LLMs

- Student: Zeynep Eroglu
- Mentor: Steffen Eger

- Some papers as starting point
- Frieder et al., Mathematical Capabilities of ChatGPT
- Borji, A Categorical Archive of ChatGPT Failures
- Wang et al., Large Language Models are not Fair Evaluators
- Schick et al., Toolformer: Language Models Can Teach Themselves to Use Tools
- Bang et al., A Multitask, Multilingual, Multimodal Evaluation of ChatGPT on Reasoning, Hallucination, and Interactivity
6. Literature Topic: LLMs for Education+Science

- Student: Daniel Delev
- Mentor: Steffen Eger

- Some papers as starting point
- Baidoo-Anu et al., Education in the Era of Generative Artificial Intelligence (AI): Understanding the Potential Benefits of ChatGPT in Promoting Teaching and Learning
- Choi et al., ChatGPT Goes to Law School
- Boiko et al., Emergent autonomous scientific research capabilities of large language models
- Meyer et al., ChatGPT and large language models in academia: opportunities and challenges
7. Literature Topic: Multimodality an LLMs

- Student: Thuy Nghiem
- Mentor: Steffen Eger

- Some papers as starting point
- Liu et al., Visual instruction tuning
- Video-LLaMA: An Instruction-tuned Audio-Visual Language Model for Video Understanding
- InstructBLIP: Towards General-purpose Vision-Language Models with Instruction Tuning
8. Experimental Topic: Chain-of-Thought Prompting

- Student: Maria Schlüter
- Mentor: Keti Korini


9. Experimental Topic: Knowledge Generation Prompting

- Student: Deidamea Bajri
- Mentor: Alexander Brinkmann


10. Experimental Topic: Tree of Thoughts Prompting

- Student: Kilian Hüllen
- Mentor: Ralph Peeters

- Besta et al. “Graph of Thoughts: Solving Elaborate Problems with Large Language Models” arXiv preprint arxiv.org/abs/2308.09687 (2023)
11. Experimental Topic: Plan-and-Solve Prompting

- Student: Joel Arenz
- Mentor: Keti Korini

- https://python.langchain.com/docs/modules/agents/agent_types/plan_and_execute
12. Experimental Topic: Data Fusion using LLMs

- Student: Petra Revesz
- Mentor: Alexander Brinkmann

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 technique from the paper
  2. present evaluation task and results from the paper
  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
   - Structure of your paper

2. Description of Experimental Design
   - What is your How to 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 to 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?

- Important
  - Read survey articles!
  - Read conference or journal papers

- Some relevant surveys

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

- **Journal article**
  - Good to cite, current research results
  - Survey articles (very good for an overview)

- **Conference and workshop paper**
  - Good to cite, current research results

- **Books (sometimes cited)**
  - Textbooks
  - Collections of articles/papers => Cite specific paper in book

- **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

- **Slide sets (especially from our lectures)**
  - Never cite!
How to Find Relevant Publications?

- Use Standard Search Engines
- **Use Google Scholar**
  - we use it a lot ourselves
- Search Engines of the University’s library
  - see slides from the library course
- **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)
4. Questions?