Contents

List of Figures

List of Tables

List of acronyms

PartI

Background

Chapter 1

Large Language Models (LLMs)

1.1 Introduction

Large Language Models (LLMs) represent a transformative leap in Natural Language Processing (NLP), allowing machines to perform complex language tasks with remarkable accuracy. From generating coherent text to answering nuanced questions, LLMs have pushed the boundaries of what AI can achieve. This chapter delves into the architecture and principles behind LLMs, their development through scaling and training techniques, and the models that have defined this field. It also addresses the challenges these models face and their expanding role in various real-world applications.

1.2 Natural language processing (NLP)

Natural Language Processing (NLP) is a field within artificial intelligence (AI) that concentrates on the interaction between computers and human language. It involves the development of algorithms and models that allow machines to comprehend, interpret, and generate human language in a meaningful context.NLP is crucial for enabling computers to process and respond to human language effectively, as demonstrated by features like Google's predictive text in keyboards and language translation systems that manage multiple languages efficiently (Murugan, 2024) .

1.2.1 Historical development of NLP

The figure below presents a timeline outlining the key developments in Natural Language Processing (NLP) beginning with rule-based approaches in the 1950s and progressing through the rise of statistical methods and early neural networks in the late 1980s. It then highlights the impact of deep learning from the 2000s onward, leading to the development of pre-trained models like BERT and GPT. The timeline concludes with the emergence of large language models (LLMs) from 2019 to the present, marking a significant shift in NLP research and applications.

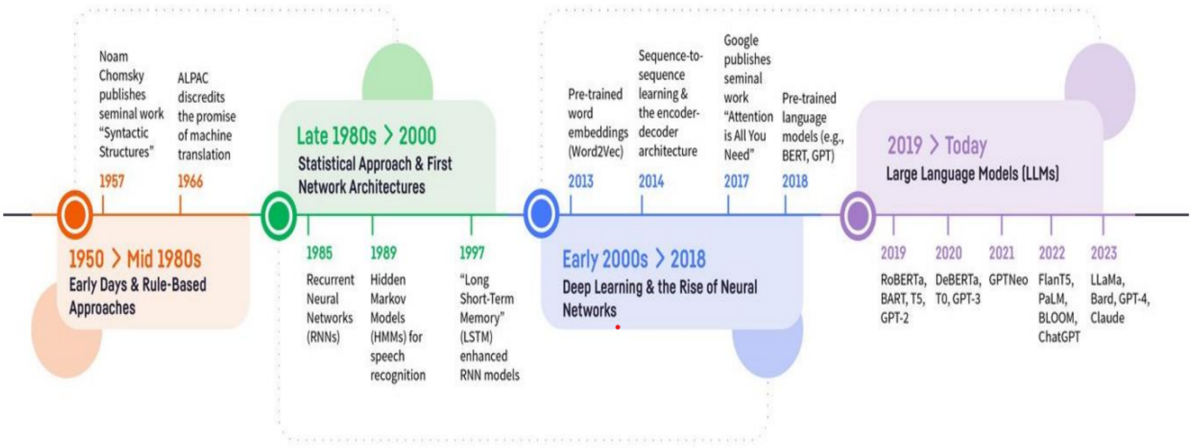

Figure1.1: The Evolution of NLP Murugan (2024).

1.2.2 Importance of natural language processing

- Efficient Data Processing: NLP enables businesses to process and analyze large volumes of unstructured, text-heavy data that would be challenging to handle otherwise..
- Understanding Human Language: NLP can interpret complex language elements, such as acronyms, abbreviations, and context, improving the accuracy of machine learning models..
- Advancements in Technology: Improvements in deep learning and machine learning have made NLP more effective, expanding the types of data that can be analyzed.
- Natural Interactions: NLP allows users to interact naturally with AI chatbots and voice assistants, like Siri, without needing to use specific, predefined language (Gillis etal., 2024).

1.3 Neural Networks in NLP

A neural network, or artificial neural network, is a machine learning algorithm inspired by the human brain. It is a key component of deep learning, a branch of machine learning effective in solving complex problems like image recognition and language processing. Unlike traditional computer programs that use a step-by-step algorithmic approach, neural networks learn from examples, mimicking the way neurons in the human brain operate. They consist of interconnected nodes (processing elements) that work together in parallel to solve specific problems.
A neural network has three basic sections, or parts, each composed of "nodes."
The input layer is the first part, receiving raw data, with each node (or neuron) representing a feature of this data. The hidden layers, which form the intermediate section, perform various transformations and computations, enabling the network to learn complex patterns and relationships. Finally, the output layer, which is the last part, produces the network's output, with the number of nodes corresponding to the desired output classes or regression values (Murugan, 2024).

1.3.1 Basics Concepts in Neural Networks

Weights

Variables on the edges between nodes that are multiplied with node outputs to form the input for the next layer.Weights are crucial for training and tuning a neural network and are often initialized within a range of -1 to 1.

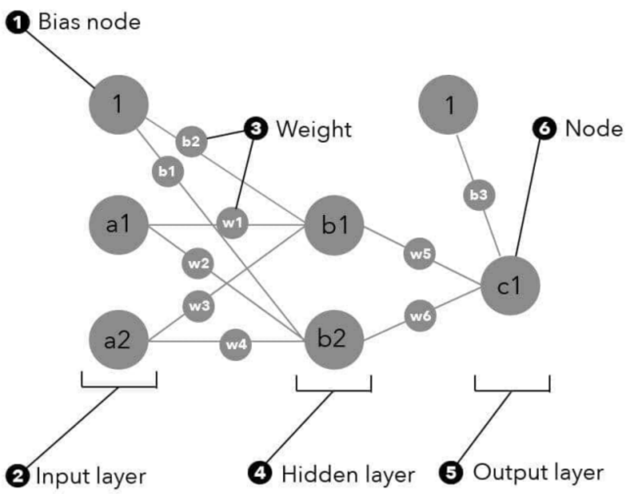

Figure1.2: Artificial Neural Network (ANN).

Biases

Additional nodes in hidden and output layers that connect to every node within their respective layers but not to the previous layer. Biases add a constant value (typically 1 or -1) to the input of a layer, helping shift the activation function and aiding in effective learning.

Activation Functions

These functions introduce non-linearity to the network, enabling it to learn and model complex data patterns. Common activation functions include the sigmoid, hyperbolic tangent (tanh), and rectified linear unit (ReLU).Taylor (2017).

1.3.2 Recurrent Neural Networks (RNNs)

Recurrent neural networks (RNNs) are a type of neural network designed for processing sequential data, such as text or time series, by effectively handling variable-length inputs. An RNN consists of a hidden state h and an optical output y, which operate on a variable sequence x=$(x_1....x_t)$At each time step t, the hidden state h^t of the RNN is updated according to the function $h^{(t)} = f(h^{(t-1)}, x_t)$ where f is a non-linear activation function, such as a logistic sigmoid or a more complex long short-term memory (LSTM) unit. This design allows RNNs to remember past inputs and incorporate them into future outputs, enabling them to recognize patterns that occur at multiple positions within a sequence. Additionally, RNNs utilize parameter sharing across time steps, which helps in generalizing across sequences of varying lengths and learning complex dependencies over time. Despite challenges with long-term dependencies, RNNs are particularly effective for tasks requiring context or sequential understanding, making them valuable for various applications, including time series analysis and natural language processing(Cho etal., 2014) .

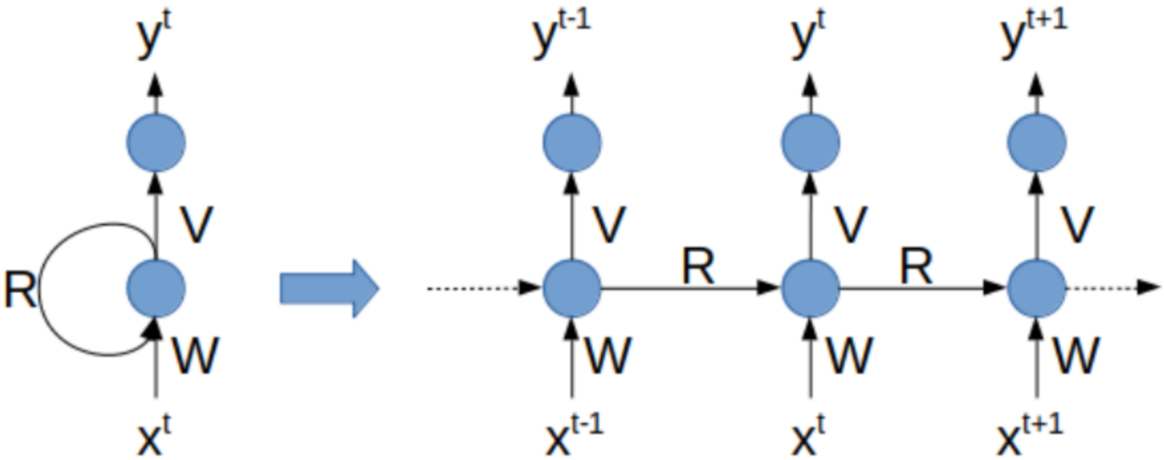

Figure1.3: RNN Architecture.

1.3.3 Long-Short Term Memory (LSTM)

Long Short-Term Memory (LSTM) networks, designed by Hochreiter and Schmidhuber, are an improved version of recurrent neural networks (RNNs) designed to learn long-term dependencies in sequential data, making them suitable for tasks like time series forecasting and language translation They address the limitations of traditional RNNs by introducing a memory cell that maintains information over extended periods. This memory cell is regulated by three gates—input, forget, and output gates—which control the flow of information in and out of the cell as shown in the fig (GeeksforGeeks, 2024).

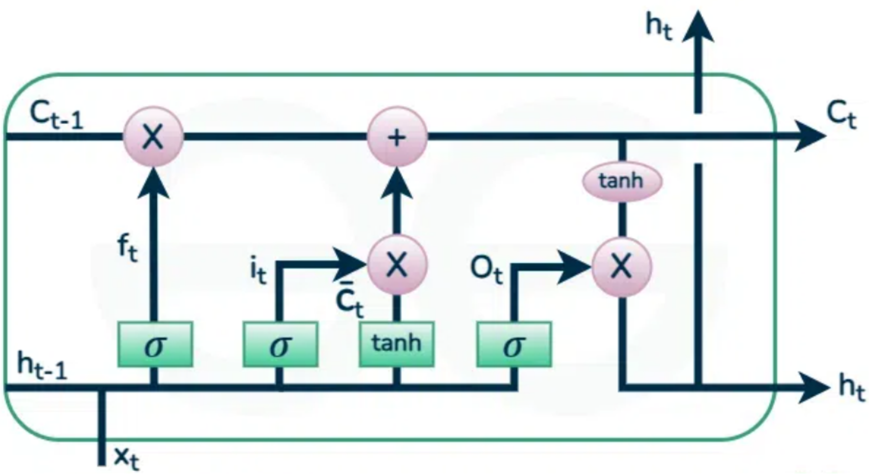

Figure1.4: LSTM Architecture.

Forget Gate: Decides what information to discard from the cell state

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right)$$

Input Gate: Determines what new information to add to the cell state

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right)$$

$$\tilde{C}_t = \tanh\left(W_c \cdot [h_{t-1}, x_t] + b_c\right)$$

Output Gate: Controls what information to output from the cell state

$$o_t = \sigma\left(W_o \cdot [h_{t-1}, x_t] + b_o\right)$$

$$h_t = o_t \odot \tanh(C_t)$$

It is worth mentioning that Bidirectional LSTM networks extend the traditional LSTM architecture by processing data in both forward and backward directions. This approach enables the network to capture dependencies from both past and future contexts, improving its ability to resolve temporal dependencies. Bidirectional LSTMs are particularly effective at handling multidimensional problems, encapsulating spatially and temporally distributed information, and dealing with incomplete data through flexible connection mechanisms (Hochreiter and Schmidhuber, 1997).

1.4 The Transformer Architecture

The Transformer architecture is a deep learning model introduced in June 2017 by Vaswani et al. from Google Brain. Their paper, titled "Attention Is All You Need," presented a groundbreaking approach to processing sequential data through the use of a self-attention mechanism. This innovative method allows the model to assign different levels of importance to various parts of the input, enabling it to capture long-range dependencies much more effectively than earlier models like RNNs and LSTMs.The original Transformer model is structured as a stack of six layers, where the output of each layer i serves as the input to the subsequent layer i+1, continuing this process until the final prediction is reached.It features a six-layer encoder on the left and a corresponding six-layer decoder on the right, both of which work together to transform input sequences into meaningful outputs. Each encoder and decoder consists of six identical layers that allow the model to process and generate language efficiently (Rothman, 2021).

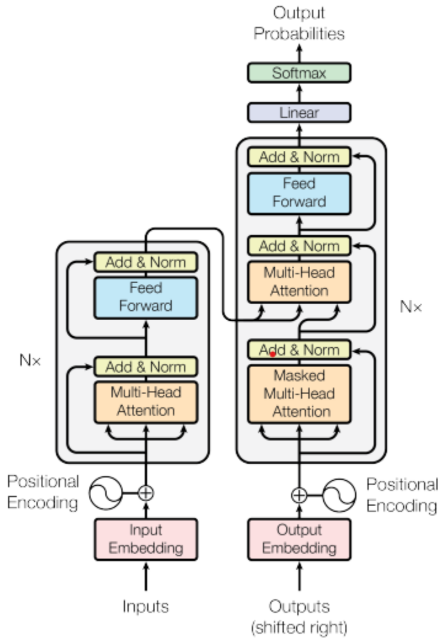

Figure1.5: The Transformer - model architecture..

1.4.1 Encoder and Decoder Stacks

Encoder: Each layer in the encoder consists of two sub-layers:
Multi-head self-attention mechanism: This allows the model to focus on different parts of the input sequence.
Position-wise feed-forward network: A fully connected network applied to each position separately and identically.
Residual Connections: Residual connections are applied around each sub-layer, followed by layer normalization. The output of each sub-layer is computed as Layer Norm(x + Sublayer(x)).
Output Dimension: All sub-layers and embedding layers output vectors of dimension d-model = 512.
Decoder: Similar to the encoder, the decoder also has 6 identical layers, each containing the same two sub-layers: Multi-head self-attention mechanism , Position-wise feed-forward network.
Additional Sub-layer: The decoder includes a third sub-layer that performs multi-head attention over the output of the encoder stack.
Residual Connections and Normalization: Like the encoder, residual connections are applied around each sub-layer, followed by layer normalization.
Masked Self-Attention: The self-attention mechanism in the decoder is modified to prevent positions from attending to subsequent positions, ensuring that predictions

for position i depend only on the known outputs at positions before i (Vaswani etal., 2017).

1.4.2 Self-Attention Mechanism

Self-attention is a mechanism that allows the model to weigh the importance of different words in a sequence relative to each other. This is crucial for understanding context and relationships between words (Vaswani etal., 2017).

1.4.3 Query, Key, and Value Vectors:

Query Vectors (Q): Generated from the input word's embedding and represent the word's role in finding relevant information in other words.
Key Vectors (K): Derived similarly from embedding and serve as a comparison standard for each word.
Value Vectors (V): Contain the actual information to be passed on and are weighted according to relevance determined by the Query and Key comparison (Vaswani etal., 2017)..

1.4.4 Self-Attention Calculation:

The score is computed by taking the dot product of the Query vector of a word with the Key vectors of all other words. This score determines how much focus should be placed on each word when encoding the current word. The scores are scaled and passed through a softmax function, producing a distribution of attention weights.
Each Value vector is weighted by these attention scores and summed to produce the final output of the self-attention layer(Vaswani etal., 2017).

1.4.5 Role of Multi-Head Attention

Multi-head attention enhances the model's ability to focus on different aspects of the input by creating multiple sets of Query, Key, and Value vectors. Each set is processed independently and then combined.
This approach allows the model to attend to information from different representation subspaces at different positions, improving its ability to capture complex relationships(Vaswani etal., 2017).

1.4.6 Positional Encoding:

Since self-attention mechanisms do not inherently capture the order of words, positional encoding is added to the word embeddings to provide information about the relative position of each word in the sequence. These encodings are added directly to the input embeddings, allowing the model to consider both the position and the content of each word during processing(Alammar, 2018).

1.4.7 Transformers in NLP

Transformers have revolutionized the field of Natural Language Processing (NLP) by introducing a powerful and efficient way to handle textual data. This advancement has led to the creation of highly effective models like BERT and GPT, with its deep bidirectional context, excels at understanding and improving performance across various NLP tasks. GPT, on the other hand, is renowned for generating coherent and contextually relevant text, significantly advancing applications such as text generation and translation(Devlin etal., 2019).
Scalability: Transformers efficiently handle large datasets and long sequences, overcoming the limitations of RNNs. This scalability allows for training with billions of parameters, enhancing model capabilities.
Rich Contextual Understanding: The self-attention mechanism in transformers captures relationships between words across the entire sequence, enabling deep contextual understanding and more accurate language processing.
Model Efficiency: Transformers enable parallel processing, which speeds up training and makes them more efficient than sequential models like RNNs. This efficiency supports the rapid development and deployment of advanced language models(Vaswani etal., 2017).

1.5 Emergence of Large Language Models (LLMs)

Large Language Models (LLMs) are advanced artificial intelligence systems designed to process and generate human-like text. They are typically based on transformer architectures and are characterized by their enormous scale, with billions of parameters. LLMs are pre-trained on vast amounts of text data in a self-supervised manner, enabling them to develop a broad understanding of language. They are capable of performing a wide range of tasks with minimal task-specific fine-tuning, often achieving significant performance improvements through few-shot or zero-shot learning(Brown etal., 2020).

1.5.1 Scaling in Large Language Models (LLMs)

Scaling is crucial in the evolution of large language models. The history of scaling shows that increasing both model size and dataset size leads to significant improvements in performance across various NLP tasks. For instance, early work by Brants et al. (2007) demonstrated the benefits of using language models trained on vast datasets, such as 2 trillion tokens, which led to significant advancements in machine translation quality. This was followed by efforts like those of Heafield et al. (2013), who scaled traditional models to Web-scale data, and Jozefowicz et al. (2016), who scaled LSTMs to 1 billion parameters, achieving state-of-the-art results on large benchmarks.The advent of transformer-based models marked a significant shift.Models like BERT, GPT-2, and GPT-3, with their enormous parameter counts—up to 175 billion for GPT-3—demonstrated that scaling up not only the model but also the dataset size yields substantial gains in performance. Researchers like Kaplan et al. (2020) and Hoffmann et al. (2022) studied how scaling affects model performance, proposing power laws that show a predictable relationship between model size, dataset size, and performance. These studies emphasized the importance of scaling for the continued progress of LLMs(Touvron etal., 2023).

1.5.2 Pre-training

Pre-training is a crucial stage in developing Large Language Models (LLMs), where the model learns from extensive unlabeled datasets through a process called self-supervision. This stage allows the model to recognize and internalize a wide range of linguistic patterns, laying the groundwork for fine-tuning on specific tasks.
Several pre-training objectives have been implemented to maximize the effectiveness of this learning process, each offering distinct benefits to the model's performance
Full Language Modeling: Used since GPT-2, this approach trains decoder-only models to predict the next token in a sequence based on previous tokens. This autoregressive method enables models like GPT-3 to generate coherent and contextually relevant text.
Prefix Language Modeling: Employed in encoder-decoder and non-causal decoder-only models, this technique uses a non-causal (considering both past and future tokens) prefix for predicting subsequent tokens, offering more flexibility and enhancing the model's adaptability across various language tasks.
Masked Language Modeling: Popularized by BERT, this method involves masking certain tokens in the input text and training the model to predict them, helping the model understand word context. An extension, span corruption, masks entire

text spans for prediction, further improving contextual comprehension(Wang etal., 2023).

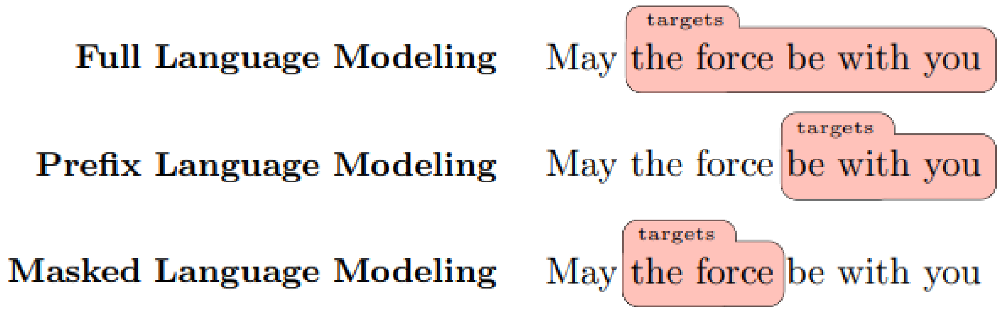

Figure1.6: Training Tokenization in Full, Prefix, and Masked Language Modeling.

1.5.3 Fine-tuning

Fine-tuning has been the most common approach for adapting LLMs to specific tasks. After pre-training on large datasets, these models are further trained on smaller, supervised datasets tailored to the desired task. Fine-tuning updates the weights of the pre-trained model, allowing it to excel at specific tasks like sentiment analysis, machine translation, or question answering. The main advantage of fine-tuning is that it often results in strong performance on task-specific benchmarks. However, it comes with challenges, such as the need for a new large dataset for every task, the risk of overfitting to narrow distributions, and potential poor generalization to out-of-distribution examples(Touvron etal., 2023).

1.5.4 Few-Shot, One-Shot, and Zero-Shot Learning

Few-shot, one-shot, and zero-shot learning represent different paradigms of using LLMs without extensive fine-tuning. These methods involve using pre-trained models to perform tasks with minimal task-specific data.

Few-Shot Learning involves giving the model a few examples (typically 10-100) of the task during inference. This approach reduces the need for large, task-specific datasets and limits the risk of overfitting to narrow data distributions. However, few-shot results are generally not as strong as those from fully fine-tuned models.

One-Shot Learning is similar to few-shot learning but uses only a single example alongside a natural language description of the task. This method mirrors how humans are often instructed for tasks, making it an interesting approach for tasks

where providing multiple examples is impractical.
Zero-Shot Learning requires the model to perform a task based solely on a natural language description, with no examples provided. While this method offers maximum flexibility and robustness, it is also the most challenging for models. Zero-shot performance is often weaker than few-shot or one-shot, but it represents a significant step towards task-agnostic AI, where models can generalize across a wide range of tasks with minimal human intervention(Brown etal., 2020).

1.5.5 Evaluation Datasets and Tasks

Evaluating Large Language Models (LLMs) is essential for determining their effectiveness and limitations in comprehending and generating human language. This evaluation typically falls into two primary categories:

- Natural Language Understanding (NLU):This measures the model's proficiency in comprehending language, encompassing tasks such as sentiment analysis, text classification, natural language inference (NLI), question answering (QA), commonsense reasoning (CR), mathematical reasoning (MR), and reading comprehension (RC).
- Natural Language Generation (NLG):This assesses the model's capability to produce text based on given context. It includes tasks like summarization, sentence completion, machine translation (MT), and dialogue generation.

Benchmarks play a critical role in evaluating LLMs, providing standardized tests to measure their performance across various tasks:

- MMLU: Measures model knowledge from pretraining and evaluates performance in zero-shot and few-shot scenarios across 57 subjects, testing world knowledge and problem-solving abilities.
- SuperGLUE: An advanced benchmark that builds on GLUE, assessing tasks like question answering and natural language inference. It is designed to test deeper aspects of language understanding and requires significant advancements in various learning methodologies.
- BIG-bench: A large-scale benchmark for evaluating LLMs across diverse tasks including reasoning, creativity, ethics, and domain-specific knowledge.
- GLUE: A foundational benchmark for evaluating and analyzing natural language understanding, offering a range of resources for model assessment(HumzaNaveed, 2024).

1.6 Popular Models and Datasets

Large Language Models (LLMs) like GPT-3, GPT-4, and BERT have revolutionized NLP by leveraging vast datasets such as Common Crawl and WebText. These datasets provide a diverse linguistic foundation, enabling models to perform a wide range of tasks with remarkable accuracy and contextual understanding.

1.6.1 GPT-N Models

GPT models are advanced autoregressive language models that generate substantial and complex machine-produced text from minimal input. They leverage deep learning techniques to mimic human text generation by predicting the current value based on preceding values. NLP models initially struggled with tasks outside their training sets due to data restrictions. OpenAI addressed this with GPT-1,introduced in 2018.

- GPT-1, trained on the BooksCorpus dataset, utilized a 12-layer transformer decoder with self-attention. Its pre-training allowed for zero-shot performance on various tasks, demonstrating the potential of generative language models.
- In 2019, GPT-2 improved upon GPT-1 by using a larger dataset and 1.5 billion parameters (compared to GPT-1's 117 million). It excelled in tasks like translation and summarization, enhancing accuracy in recognizing long-distance relationships.
- GPT-3, released later, featured around 175 billion parameters and was trained on the Common Crawl dataset. It could generate human-like text, perform basic math, and write code. Despite its capabilities, its size and cost made it challenging to implement.
- GPT-4, launched in March 2023, advanced further with multimodal capabilities and context windows of up to 32,768 tokens. It incorporates reinforcement learning for better alignment with human input and policy(Yenduri etal., 2023)

1.6.2 BERT

BERT (Bidirectional Encoder Representations from Transformers) is a groundbreaking language representation model that pretrains deep bidirectional representations from unlabeled text by jointly conditioning on both left and right contexts in all layers. This bidirectional approach enables BERT to be fine-tuned with just a single additional output layer for various tasks, such as question answering and language inference, without the need for extensive architectural modifications. BERT has achieved remarkable performance, setting new state-of-the-art results across eleven NLP tasks, including a GLUE score of 80.5%, MultiNLI accuracy of 86.7%, SQuAD v1.1 F1 score of 93.2%, and SQuAD v2.0 F1 score of 83.1%. Its combination of conceptual simplicity and empirical effectiveness makes BERT a powerful and versatile tool for a wide range of natural language processing applications(Devlin etal., 2019).

1.6.3 T5

The T5 (Text-To-Text Transfer Transformer) model represents a unified framework for natural language processing (NLP), designed to address various text processing tasks by treating them as ”text-to-text” problems. This approach involves converting all tasks into a format where both input and output are text, allowing the same model, objective, and training procedure to be applied across different tasks. T5 leverages extensive pre-training on a large, unlabeled dataset, enabling it to develop general-purpose knowledge that enhances its performance on a range of NLP tasks, such as question answering, document summarization, and sentiment classification(Raffel etal., 2023).

1.6.4 LLAMA2

1.6.5 WebText

WebText is a dataset developed by OpenAI to encapsulate a wide variety of high-quality web content. It comprises text sourced from outbound links on popular websites like Reddit, chosen based on their popularity and the quality of their content. Unlike Common Crawl, which indiscriminately includes a broad range of web pages, WebText is more selective, focusing on high-quality, engaging material. Although smaller in size compared to Common Crawl, WebText is curated to ensure the text reflects diverse, well-written content, making it particularly valuable for training language models to produce coherent and contextually appropriate text(Radford etal., 2019).

1.6.6 RuleTaker

RuleTaker is a collection of datasets designed to assess the deductive reasoning capabilities of language models. Each dataset includes a set of facts, rules, and a

Context: Anne is quiet. Anne is not young. Bob is kind. Bob is young. Dave is rough. Dave is round. Dave is smart. Dave is not young. Fiona is quiet. Fiona is not round. Kind, young things are not smart.
Question: Bob is smart.
Expected answer: False

Figure1.7: exammple of RuleTaker dataset

boolean question that the model must use logical reasoning to answer. The datasets feature synthetic subsets requiring various levels of reasoning complexity, with different numbers of deduction steps necessary to reach an answer. Among the datasets are the Bird dataset, which illustrates McCarthy's abnormality problem , the Electricity dataset, which models appliance functions, and the ParaRules corpus, where sentences like “Bob is cold” are paraphrased to “In the snow sits Bob, crying from being cold.” The collection comprises 580,000 training examples, 84,000 validation examples, and 173,000 testing examples(Helwe, 2024).

1.7 Challenges and Limitations

LLMs have greatly advanced NLP, but they also present challenges such as high computational costs, issues with adversarial robustness, and difficulties in interpretability. As these models scale, they encounter new challenges in scalability, privacy, and real-time processing. Ongoing research is exploring multi-modality, transfer learning, and continuous learning, which bring additional complexities and highlight the evolving impact of LLMs in practical applications(HumzaNaveed, 2024).

1.7.1 Computational Cost

Training large language models (LLMs) demands significant computational resources, leading to higher production costs and environmental concerns due to the substantial energy used in large-scale training. Although enhancing computational resources can boost performance, the gains diminish over time when the size of the model and dataset stay constant, adhering to the power law of diminishing returns.

1.7.2 Overfitting

Despite their advanced learning abilities, they can overfit to noisy or unusual patterns in their large training datasets, which may result in generating nonsensical responses. The ongoing discussion about Memorization versus Generalization in

LLMs revolves around finding an optimal balance. Memorization helps the model retain specific details from its training, allowing it to answer precise questions accurately. On the other hand, generalization enables the model to make predictions and generate responses for new, unseen inputs, which is crucial for handling diverse real-world tasks. The challenge is to find the right balance: excessive memorization can lead to overfitting, reducing the model's flexibility and ability to handle novel inputs.

1.7.3 Interpretability and Explainability

The "black-box" nature of LLMs makes it difficult to understand how they make decisions, which is vital for gaining broader acceptance and trust, particularly in sensitive areas. Although these models have advanced capabilities, the lack of transparency into their workings limits their effectiveness and reliability. Efforts are underway to enhance the explainability of LLMs to build user trust and promote responsible use of AI. Understanding how LLMs generate their responses is crucial for ensuring they align with human values and legal standards.

1.7.4 Hallucinations

LLMs sometimes produce "hallucinations," or responses that, despite appearing plausible, are incorrect or do not match the provided information. These hallucinations can be classified into three types:

- Input-conflicting hallucination: When the model generates responses that do not align with the user's input.
- Context-conflicting hallucination: When the model produces content that contradicts information it has previously generated.
- Fact-conflicting hallucination: When the model creates responses that conflict with established knowledge.

1.7.5 Privacy Concerns

As Large Language Models (LLMs) have become more complex and sizable, privacy concerns have intensified, particularly regarding data sharing and potential misuse. Risks include the creation of harmful content, evasion of filters, and issues related to data privacy, especially in areas like e-commerce where safeguarding customer information is vital. When LLMs are trained on private data and then made publicly available, additional privacy risks arise. Since LLMs can memorize phrases from their training data, there's a danger that these phrases could be exploited by malicious actors to retrieve sensitive information, thus threatening personal privacy.

1.7.6 Real-Time Processing

Real-time processing in Large Language Models (LLMs) is crucial for many applications, particularly as mobile AI solutions become more popular and concerns about information security and privacy grow. However, LLMs typically consist of hundreds of layers and millions of parameters, which create significant challenges for real-time processing due to their high computational demands and the limited storage capacity of hardware platforms, especially in edge computing environments. Although efforts such as MobileBERT attempt to lessen memory usage, they still encounter considerable execution overhead because of the extensive number of model layers, resulting in high inference latency.

1.8 Domains of Application

The use of Large Language Models (LLMs) in various downstream tasks has become increasingly prevalent in both AI research and industry, with new applications being identified and explored regularly. These models, which excel at understanding and generating human-like text, are finding valuable applications across diverse fields.

1.8.1 Law

In the legal field, Large Language Models (LLMs) can support the analysis of legal documents by assisting with tasks such as generating initial coding for datasets, identifying key themes, and classifying information accordingly. This synergy between legal professionals and LLMs has been effective in examining legal texts, such as court opinions on theft, enhancing both the efficiency and quality of legal research. Additionally, LLMs have been tested for their capability to generate explanations of legal terms, with a focus on improving factual accuracy by integrating sentences from relevant case law. By incorporating pertinent case law, these enhanced models can produce more accurate and relevant explanations with fewer factual errors. Furthermore, LLMs can be specialized with domain-specific knowledge to tackle legal reasoning tasks and address legal queries effectively (HumzaNaveed, 2024).

1.8.2 Cybersecurity

large Language Models (LLMs) have garnered significant attention in the field of cybersecurity. Recent research has highlighted their potential in addressing software bugs created by human developers and identifying cybersecurity threats. For example, Arora et al. have proposed methods for utilizing LLMs to evaluate cyber threats on social media through sentiment analysis. LLMs are also employed to detect cybersecurity-related information in Open Source Intelligence (OSINT), aiding in the identification of potential cyber threats. Additionally, LLMs have shown promise in detecting scams, such as phishing. Initial tests with models like GPT-3.5 and GPT-4 have demonstrated their ability to recognize common phishing indicators in emails. While LLMs exhibit considerable potential in cybersecurity, improving their reasoning abilities could enhance their effectiveness further, such as in uncovering zero-day vulnerabilities in open-source software by analyzing logic and source code(Helwe, 2024).

1.8.3 Medicine

The integration of Large Language Models (LLMs) into medicine is transforming both healthcare delivery and research. In clinical settings, LLMs are increasingly utilized in decision support systems to offer evidence-based treatment recommendations. By analyzing patient data and medical literature, these models can assist in diagnosing conditions, suggesting relevant tests, and proposing effective treatment options. Additionally, LLMs improve patient interactions through applications like chatbots that answer questions about symptoms and medications, schedule appointments, and provide health advice.

In medical research, LLMs help sift through vast amounts of literature to extract, filter, and summarize relevant information, identify key studies, and predict future research directions. They also play a role in medical education by generating training materials, creating exam questions, explaining complex topics, and offering personalized feedback. Furthermore, LLMs simulate patient interactions, aiding students in honing their clinical skills (HumzaNaveed, 2024).

1.8.4 journalism

Large Language Models (LLMs) offer valuable support to journalists, especially in fact-checking and news verification. They can process and cross-reference large volumes of data with established knowledge bases. Research has demonstrated that LLMs, such as GPT-3.5, can be used to detect fake news by providing rationales that enhance other models like BERT, which can then be fine-tuned for this purpose . In addition to fact-checking, LLMs are useful for analyzing political debates, helping journalists to identify key themes, monitor how discussions evolve, and evaluate sentiments. They can also assist in detecting logical fallacies and underlying motives in political discourse and propaganda . By enhancing their reasoning capabilities, LLMs can uncover deeper insights into propaganda and misinformation, making them a powerful tool for modern journalism(Helwe, 2024).

1.9 Conclusion

This chapter has outlined the evolution and significance of Natural Language Processing (NLP), from early neural networks to advanced Large Language Models (LLMs). We covered key concepts in neural networks and the transformative impact of the Transformer architecture. The exploration of LLMs highlighted their emergence, scaling, and the intricacies of pre-training and fine-tuning. We also discussed various challenges, including computational costs, interpretability, and privacy concerns. Finally, the chapter reviewed the applications of LLMs in fields like law, cybersecurity, medicine, and journalism, showcasing their potential and the ongoing need for further development.

Chapter 2

RAG (Retrieval-Augmented Generation)

2.1 Introduction

Large language models (LLMs) have seen significant advancements but face challenges, particularly in tasks that demand extensive knowledge or deal with queries beyond their training data. These limitations often result in inaccuracies or "hallucinations." To address this, Retrieval-Augmented Generation (RAG) supplements LLMs by retrieving relevant document chunks from external knowledge sources based on semantic similarity. By doing so, RAG helps reduce factual errors, allowing LLMs to produce more accurate content. This has led to the widespread adoption of RAG, particularly in chatbots and other real-world applications, making it a crucial technology in advancing the capabilities of LLMs.

2.2 Fundamentals of Retrieval-Augmented Generation

RAG represents a significant advancement in the capabilities of large language models (LLMs) by integrating external knowledge retrieval with the generation of text. Understanding the individual components of retrieval and generation is essential to appreciate how their synergy improves the overall performance of RAG systems.

2.2.1 Definition of RAG

Retrieval-Augmented Generation (RAG) is a technique that leverages the strengths of pre-trained large language models (LLMs) and external data sources. By merging the generative abilities of LLMs like GPT-3 or GPT-4 with the accuracy of specialized data search mechanisms, RAG systems can generate more sophisticated and contextually relevant responses(Selvaraj, 2024).

2.2.2 Historical Development of RAG

The foundations of Retrieval-Augmented Generation (RAG) can be traced back to traditional information retrieval (IR) systems, Early models primarily relied on keyword matching and simple ranking mechanisms to retrieve relevant documents from databases, establishing a basic framework for information access. The landscape began to shift with the rise of neural networks in the 2010s. Notable innovations like Word2Vec and Transformer-based architectures enabled retrieval methods to incorporate deeper semantic understanding, paving the way for more sophisticated document retrieval processes. A significant advancement occurred with the introduction of dense passage retrieval (DPR) in 2020, which utilized bi-encoder architectures to map both queries and documents into dense vector spaces. The integration of these advanced retrieval techniques with large language models (LLMs) became a focal point as models like GPT-3 gained prominence. Researchers explored how LLMs could be augmented with retrieval capabilities, leading to the development of RAG systems that leverage the strengths of both retrieval and generative capabilities(Gao etal., 2024).

2.2.3 Differences Between RAG and Fine-Tuning

The enhancement of large language models (LLMs) has gained significant interest due to their increasing use. Among the various optimization strategies for LLMs, Retrieval-Augmented Generation (RAG) is often compared to fine-tuning (FT) and prompt engineering. Each method possesses unique attributes,

1. Methodological Characteristics :
   RAG is compared to providing a tailored textbook for information retrieval, making it suitable for precise information retrieval tasks. It excels in dynamic environments with real-time knowledge updates.
   Fine-tuning is likened to a student internalizing knowledge, making it more static and suitable for replicating specific structures, styles, or formats.

2. External Knowledge and Adaptation:
   RAG relies on external knowledge sources and allows for high interpretability but may involve higher latency and ethical considerations regarding data retrieval.

Fine-tuning requires retraining for updates and involves significant computational resources for dataset preparation and training. It enables deep customization of the model's behavior but may struggle with unfamiliar data.

3. Performance:
   RAG consistently outperforms unsupervised fine-tuning in knowledge-intensive tasks, particularly for both previously encountered and new knowledge. LLMs often struggle to learn new factual information through unsupervised fine-tuning.

4. Use Cases and Combination:
   The choice between RAG and fine-tuning depends on specific needs for data dynamics, customization, and computational capabilities. They are not mutually exclusive; their combined use may yield optimal performance and often requires multiple iterations to refine the results (Gao etal., 2024).

2.3 Types of RAG Systems

The RAG research field is continuously evolving, with three main stages: Naive RAG, Advanced RAG, and Modular RAG.

2.3.1 Naive RAG

Naive RAG, a foundational approach in Retrieval-Augmented Generation, operates on a straightforward "Retrieve-Read-Generate" paradigm. This method involves three primary steps:

- Indexing: Raw data is cleaned, extracted, and converted into a uniform text format. It's then segmented into smaller chunks and encoded into vector representations using an embedding model. These vectors are stored in a vector database for efficient similarity searches.

- Retrieval: When a user query is received, it's encoded into a vector and compared to the indexed chunks. The top K most similar chunks are retrieved and included in the prompt for the language model.

- Generation: The query and retrieved chunks are combined into a prompt, which is fed to a large language model. The model generates a response based on the provided context and its internal knowledge.

While Naive RAG offers a basic framework, it faces several challenges in

- Retrieval Issues: The retrieval process can be imprecise, leading to the selection of irrelevant or missing information.
- Generation Challenges: The language model may hallucinate, generating content not supported by the retrieved context. It may also produce irrelevant, toxic, or biased outputs.
- Augmentation Difficulties: Integrating retrieved information into the generation process can be challenging, leading to disjointed or redundant responses.

To address these limitations, more sophisticated RAG techniques have emerged, which we will explore in the next section.

2.3.2 Advanced RAG

Taking aim at the shortcomings of Naive RAG, Advanced RAG introduces specific improvements to enhance retrieval quality. This approach utilizes pre-retrieval and post-retrieval strategies.

Pre-retrieval Strategies:

- Enhanced Indexing: Advanced RAG tackles indexing issues through a sliding window approach, finer segmentation of data, and inclusion of metadata. Additionally, it optimizes the retrieval process by employing various methods.
- Query Optimization: This stage focuses on refining the user's initial query to make it clearer and more suitable for retrieval. Techniques like query rewriting, transformation, and expansion are commonly used.

Post-Retrieval Strategies:

- Re-ranking Chunks: After relevant information is retrieved, Advanced RAG prioritizes the most relevant content by re-ranking the retrieved chunks and placing them strategically within the prompt.
- Context Compression: To avoid overwhelming the LLM with too much information, post-retrieval efforts focus on selecting the most essential parts of the retrieved context, highlighting critical sections, and compressing the data to be processed.

By addressing indexing issues and refining the query and retrieved information, Advanced RAG aims to improve the overall accuracy and relevance of the generated response.

2.3.3 Modular RAG

Modular RAG represents the latest evolution in RAG, offering greater adaptability. it introduces specialized modules and innovative patterns to enhance retrieval and processing capabilities.

New Modules

- Search Module: Adapts to specific scenarios by leveraging LLM-generated code and query languages to search across various data sources.
- RAG Fusion: Employs a multi-query strategy to expand user queries, uncover both explicit and implicit knowledge, and improve retrieval results.
- Memory Module: Leverages the LLM's memory to guide retrieval and create an unbounded memory pool, aligning the text more closely with data distribution.
- Routing Module: Navigates through diverse data sources, selecting the optimal pathway for a query based on its specific needs.
- Predict Module: Reduces redundancy and noise by generating relevant context directly through the LLM.
- Task Adapter Module: Tailors RAG to various downstream tasks by automating prompt retrieval and creating task-specific retrievers.

New Patterns

- Flexible Module Arrangement: Modular RAG allows for the substitution and reconfiguration of modules to address specific challenges, surpassing the fixed structures of previous RAG paradigms.
- Innovative Retrieval Strategies: Techniques like Rewrite-Retrieve-Read, Generate-Read, and Recite-Read leverage the LLM's capabilities to refine queries, generate content, and retrieve information from model weights.
- Hybrid Retrieval: Combines keyword, semantic, and vector searches to cater to diverse queries, improving retrieval relevance.
- Dynamic Module Interaction: Frameworks like Demonstrate-Search-Predict and ITERRETGEN demonstrate the dynamic use of module outputs to enhance each other's functionality.

- Adaptive Retrieval: Techniques like FLARE and Self-RAG evaluate the necessity of retrieval based on different scenarios, allowing for a more flexible and efficient approach.

2.4 Core Components of RAG

The core components of Retrieval-Augmented Generation (RAG) systems consist of a retrieval mechanism, a generation process, and augmentation techniques. These elements work together to enhance the model's ability to access relevant external information, generate coherent and contextually appropriate responses, and improve overall performance in knowledge-intensive tasks.

2.4.1 Retrieval Mechanism

RAG systems combine parametric memory (a pre-trained language model) with non-parametric memory (a retrieval mechanism). The retrieval mechanism allows RAG models to access external information sources (e.g., Wikipedia), and this process is central to improving the model's ability to generate factual and accurate outputs (Lewis etal.).

- Traditional Techniques:
  Classical retrieval methods include **TF-IDF and BM25**, which rely on sparse vector representations based on term frequencies. These methods use exact keyword matching, making them limited in semantic understanding.

- Modern Retrieval Approaches:
  Dense Passage Retrieval (DPR): This approach utilizes dense vector representations learned by neural models like BERT to encode both the query and document. It allows for a more semantic understanding of the content, making retrieval more effective. DPR, for example, computes the similarity between the query and documents using Maximum Inner Product Search (MIPS), which finds the closest passages based on the dense vector space.

- Implementation in RAG:
  In RAG, dense retrieval methods are often paired with techniques like **Maximum Inner Product Search** (MIPS), which efficiently matches query and document embeddings. This enables the system to return the most relevant documents for subsequent generation (Karpukhin etal., 2020).

2.4.2 Generation Process

The generation in RAG occurs through a combination of retrieved passages and the input query.
Large Language Models (LLMs) like BART or T5 are utilized for this generation, leveraging their advanced capabilities in understanding and producing human-like text. The retrieval component supplies external context, which the generator conditions on to formulate a response.This context is crucial, as it enriches the LLM's understanding, enabling it to incorporate real-time, relevant information. Moreover, the generation process benefits from the LLM's ability to synthesize information, allowing it to create responses that are not only coherent but also informed by the latest data, thus improving accuracy and relevance in knowledge-intensive tasks (Lewis etal.).
Two models have been proposed in RAG:

- **RAG-Sequence** uses the same document to generate the entire sequence of output. It marginalizes over the top K retrieved documents to produce a final answer.
- **RAG-Token** allows different tokens in the output sequence to be generated based on different documents, making it more flexible when combining information from various

2.4.3 Augmentation Techniques

The augmentation of the retrieval process in Retrieval-Augmented Generation (RAG) systems focuses on improving how queries are refined and how relevant information is retrieved for downstream generation tasks. Key augmentation methods include.

- **Query Augmentation:** In traditional retrieval pipelines, user queries are often under-specified or ambiguous, leading to poor retrieval performance. Query augmentation involves dynamically rewriting the user's query to better match the documents in the knowledge base. This can be done by leveraging large language models (LLMs) to generate tailored queries or synthetic questions and answers (QAs) that better align with the search objective
- **Synthetic QA Generation:** Instead of using raw document chunks, retrieval is enhanced by generating and embedding synthetic QA pairs from documents. This helps to capture the semantic essence of long texts more effectively, reducing noise and improving retrieval precision. These synthetic QAs can be

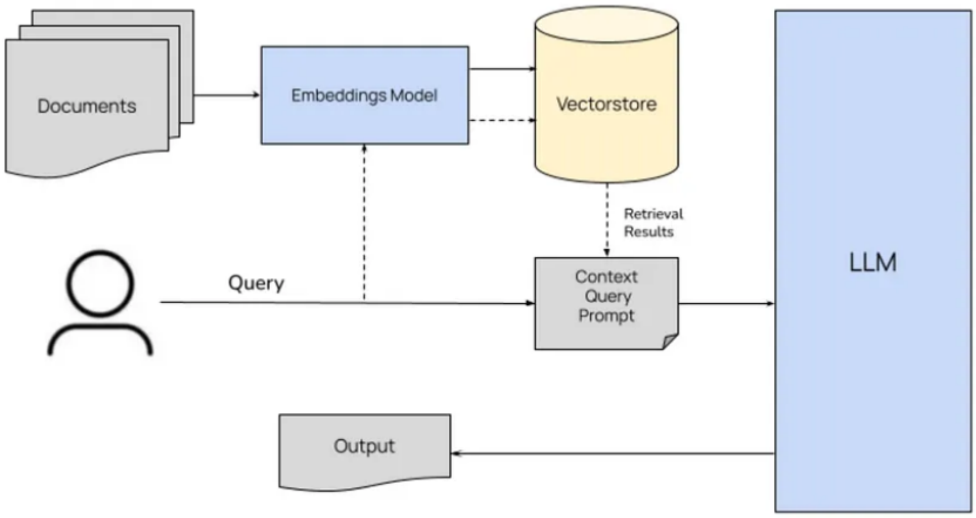

Figure2.1: Rag architecture

used to rewrite the user query, making it more specific to the task at hand (Mombaerts etal., 2024).

2.5 Training and Fine-Tuning RAG Models

Training and fine-tuning are essential steps in enhancing the performance of RAG models by optimizing both the retriever and generator components leading to more coherent, relevant, and accurate responses.

2.5.1 Training the Retriever

A powerful technique for improving retrieval relevance involves training the retriever model using **contrastive learning**. This approach aims to maximize the similarity between query and relevant document embeddings while minimizing the similarity between query and irrelevant document embeddings. By training the model on numerous positive (relevant) and negative (irrelevant) pairs, the retriever learns to effectively distinguish between relevant and irrelevant information(Reimers and Gurevych, 2024).

2.6 Task and Evaluation

The rapid development and increasing use of Retrieval-Augmented Generation (RAG) models in NLP have made their evaluation a critical area of research within the LLM community. This section covers the primary downstream tasks associated with RAG, the datasets used, and the methods for evaluating RAG systems (Zhou etal., 2020).

2.6.1 Factuality

- Fact-Checking Benchmarks: Using datasets like FEVER and SQuAD to evaluate the model's ability to identify and correct factual errors.
- Adversarial Testing: Creating adversarial examples to test the model's robustness against misleading information.
- Contextual Understanding: Assessing the model's ability to understand the context of a query and provide accurate answers.

2.6.2 Robustness

- Noise Injection: Introducing noise into the retrieved documents to test the model's ability to handle imperfect information.
- Adversarial Attacks: Evaluating the model's resilience to attacks that aim to manipulate its outputs.
- Domain Adaptation: Testing the model's ability to adapt to new domains and data distributions.

2.6.3 Fairness

-
- Bias Detection: Identifying and quantifying biases in the training data and model outputs.
- Fairness Metrics: Using metrics like demographic parity and equalized odds to evaluate the model's fairness.
- Mitigation Techniques: Implementing techniques like debiasing and fairness constraints to mitigate biases.

2.6.4 Objective Metrics:

- Accuracy: Precision, recall, and F1-score for evaluating the correctness of the generated responses.
- Consistency: Measuring the consistency of the model's outputs across different queries and contexts.
- Coherence: Assessing the coherence and fluency of the generated text.

2.6.5 Subjective Metrics

- Human Evaluation: Using human raters to evaluate the quality of the generated responses.
- User Studies: Conducting user studies to gather feedback on the user experience

2.7 Limitations

While RAG has gained significant traction across diverse applications, it still faces certain limitations in terms of effectiveness and efficiency(Zhao etal., 2024).

2.7.1 Noisy Retrieval Results

- Retrieval Quality: The quality of retrieved information can be affected by factors like indexing techniques, query formulation, and the underlying dataset.
- Hallucinations: Noisy or irrelevant information can lead to the generation of hallucinated or factually incorrect responses.
- Contextual Understanding: The LLM may struggle to understand the context of the retrieved information, especially if it's poorly formatted or contains inconsistencies.

2.7.2 Extra Overhead

- Computational Cost: Retrieval and processing additional information can increase computational costs, especially for large-scale models and complex queries.

- Latency: Retrieval and processing can introduce latency, impacting the real-time performance of RAG systems.
- Complexity: Implementing and deploying RAG systems requires careful consideration of various factors, including data preparation, model selection, and system architecture.

2.7.3 Interaction of Retrieval and Generation

- Aligning the goals of the retriever and generator is challenging.
- Optimizing the interaction between the two components requires careful design and tuning.
- The impact of various factors, such as metric selection and hyperparameter tuning, on RAG performance is still not fully understood.
-

2.7.4 Long Context Generation:

- Context Length Limits: LLMs have limitations on the amount of context they can process at once.
- Information Loss: Long documents may be truncated or summarized, leading to loss of important information.
- Computational Cost: Processing long contexts can be computationally expensive.

2.8 Conclusion

This chapter provided an overview of Retrieval-Augmented Generation (RAG), highlighting its significance in natural language processing. We discussed the key concepts of retrieval and generation, emphasizing the advantages of their combination in enhancing language model capabilities. The historical development of RAG was explored, along with its core components, including the retrieval mechanism, generation process, and augmentation techniques. Additionally, we examined various downstream tasks and evaluation targets, illustrating RAG's versatility in applications like open-domain question answering and fact verification. Overall, RAG represents a promising advancement in knowledge-intensive tasks, paving the way for further research and innovation in the field.

Bibliography

Jay Alammar. The illustrated transformer. https://jalammar.github.io/illustrated-transformer/, 2018. Accessed: 2024-08-28.

TomB Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, JaredD Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, etal. Language models are few-shot learners. *Advances in neural information processing systems*, 33:1877–1901, 2020.

Kyunghyun Cho, Bart VanMerriënboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. Learning phrase representations using rnn encoder-decoder for statistical machine translation. *arXiv preprint arXiv:1406.1078*, 2014.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, pages 4171–4186. Association for Computational Linguistics, 2019. URL https://arxiv.org/abs/1810.04805.

Yunfan Gao, Yun Xiong, Xinyu Gao, Kangxiang Jia, Jinliu Pan, Yuxi Bi, YiDai, Jiawei Sun, Meng Wang, and Haofen Wang. Retrieval-augmented generation for large language models: A survey. *arXiv preprint arXiv:2312.10997v5*, 2024.

GeeksforGeeks. Deep learning - introduction to long short term memory, 2024. URL https://www.geeksforgeeks.org/deep-learning-introduction-to-long-short-term-memory/. Accessed: August 2024.

AlexanderS. Gillis, Ben Lutkevich, and EdBurn. Natural language processing (nlp), 2024. URL https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP. Accessed: 2024-08-22.

Chadi Helwe. *Evaluating and Improving the Reasoning Abilities of Language Models*. PhD thesis, Institut Polytechnique de Paris, Palaiseau, France, July 2024. URL https://theses.hal.science/tel-04654171. Thèse de doctorat préparée à Télécom Paris, École doctorale n°626, École doctorale de l'Institut Polytechnique de Paris (ED IP Paris), Spécialité de doctorat: Informatique, Données, IA.

Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Computation*, 9(8):1735–1780, November 1997.

Shi Qiu Muhammad Saqib Saeed Anwar Muhammad Usman Naveed Akhtar Nick Barnes AjmalMiani HumzaNaveed, Asad UllahKhan. A comprehensive overview of large language models. *arXiv preprint arXiv:2307.06435*, April 2024. Version 9, 9 Apr 2024.

Vladimir Karpukhin, Barlas Oguz, Sewon Min, Patrick Lewis, Ledell Wu, Sergey Edunov, Danqi Chen, and Wen-tau Yih. Dense passage retrieval for open-domain question answering. *arXiv preprint arXiv:2004.04906*, 2020.

Patrick Lewis, Ethan Perez, Aleksandra Piktus, Fabio Petroni, Vladimir Karpukhin, Naman Goyal, Heinrich Küttler, Mike Lewis, Wen-tau Yih, Tim Rocktäschel, Sebastian Riedel, and Douwe Kiela. Retrieval-augmented generation for knowledge-intensive nlp tasks.

Laurent Mombaerts, Terry Ding, Florian Felice, Jonathan Taws, Adi Banerjee, and Tarik Borogovac. Meta knowledge for retrieval augmented large language models. *arXiv preprint arXiv:2408.09017v1*, 2024. URL https://arxiv.org/abs/2408.09017v1.

Mohana Murugan. Natural language processing (nlp). https://doi.org/10.13140/RG.2.2.13534.04169, 2024. PresentationPDF Available on ResearchGate.

Alec Radford, Jeffrey Wu, Dario Amodei, Jack Clark, Miles Brundage, Ilya Sutskever, etal. Language models are unsupervised multitask learners. *OpenAI Blog*, 1(8):9, 2019.

Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and PeterJ. Liu. Exploring the limits of transfer learning with a unified text-to-text transformer. *arXiv preprint arXiv:1910.10683v4*, September 2023. Editor: Ivan Titov.

Nils Reimers and Iryna Gurevych. Semantic search - sentence transformers, 2024. URL https://sbert.net/examples/applications/semantic-search/README.html. Accessed: 2024-11-01.

Denis Rothman. *Transformers for Natural Language Processing: Build innovative deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, RoBERTa, and more.* Packt Publishing Ltd, 2021. ISBN 1800568630, 9781800568631.

Natassha Selvaraj. What is retrieval augmented generation (rag)?, 2024. URL https://www.datacamp.com/blog/what-is-retrieval-augmented-generation-rag. Updated Jan 30, 2024.

Michael Taylor. *Make Your Own Neural Network: An In-depth Visual Introduction For Beginners.* CreateSpace Independent Publishing Platform, Scotts Valley, CA, 2017. Paperback edition, October 4, 2017.

Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, etal. Llama: Open and efficient foundation language models. *arXiv preprint arXiv:2302.13971*, 2023.

Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, AidanN Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In *Advances in neural information processing systems*, pages 5998–6008, 2017.

Thomas Wang, Adam Roberts, Daniel Hesslow, Teven LeScao, HyungWon Chung, IzBeltagy, Julien Launay, and Colin Raffel. What language model architecture and pretraining objective work best for zero-shot generalization? *arXiv preprint arXiv:2302.03072*, 2023.

Gokul Yenduri, MRamalingam, ChemmalarG Selvi, YSupriya, Gautam Srivastava, Praveen KumarReddy Maddikunta, Deepti Raj, RutvijH Jhaveri, BPrabadevi, Weizheng Wang, AthanasiosV Vasilakos, and ThippaReddy Gadekallu. Gpt (generative pre-trained transformer) – a comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions. *Journal of Artificial Intelligence Research*, 82:123–157, 2023. doi: 10.1016/j.jair.2023.01.007.

Penghao Zhao, Hailin Zhang, Qinhan Yu, Zhengren Wang, Yunteng Geng, Fangcheng Fu, Ling Yang, Wentao Zhang, and Bin Cui. Retrieval-augmented generation for ai-generated content: A survey. *arXiv preprint arXiv:2402.19473*, February 2024. URL https://arxiv.org/abs/2402.19473v1. Accessed: [add the date you accessed the paper].

Yujia Zhou, Yan Liu, Xiaoxi Li, Jiajie Jin, Hongjin Qian, Zheng Liu, Chaozhuo Li, Zhicheng Dou, Tsung-Yi Ho, and PhilipS. Yu. Trustworthiness in retrieval-augmented generation systems: A survey. *arXiv preprint arXiv:2409.10102*, September 2020. URL https://arxiv.org/abs/2409.10102v1. Accessed: [add the date you accessed the paper].