**Romanian Open-Source Chatbot**

**Candidate: Andrei - Răzvan, JOLDEA**

**Scientific coordinator: Associate Professor Cosmin, CERNĂZANU**

Session: June 2024

**Table of Contents**

**(Arial 20 pt, Bold, Uppercase, Center)**

The abstract is intended to inform about the content of the paper through a brief description of the research of up to one page, the procedures/methods, as well as its results or conclusions. The abstract in Romanian becomes mandatory for works edited in languages other than Romanian and will be written in 12 pt Arial fonts. It will start two blank lines after the heading "ABSTRACT". Before the title, there will be three blank 12 pt. lines.

**ABSTRACT**

**(Arial 20 pt, Bold, Uppercase, Center)**

The English abstract will be on the third page of the manuscript and will synthetically present the paper work. The maximum length of the abstract is one page written with Arial fonts, size 12 pt. The abstract text will begin after two blank lines (size 12pt.) from the “ABSTRACT” title. Before the title there will be left three 12 pt blank lines.

# INTRODUCTION

Over the past few years, the technological landscape has suffered an immense shift due to the emergence of large language models (LLMs). Fuelled by advancements in artificial intelligence (AI) domains such as machine learning (ML), deep learning (DL) and natural language processing (NLP), these models are prevalent in a wide variety of fields, namely healthcare, business intelligence, legal analytics, and even creative arts, encompassing music and literature [1].

While it is true that Large Language Models have impressive capabilities, most of the powerful models are only fluent in the English language, with a few exceptions regarding their multilingual capabilities.

My goal for this thesis was to create a large language model capable of understanding and speaking in Romanian, by finetuning a base model on high quality Romanian data.

A screenshot of a computer

Description automatically generated

Table 1: GPT-4 benchmarks (source: [2]).

A screenshot of a computer screen

Description automatically generated

Table 2: Gemini performance on text benchmarks with external comparisons (source: [3]).

A screenshot of a computer

Description automatically generated

Table 3: Meta Llama 3 Pre-trained model performance (source: [4]).

A screenshot of a computer screen

Description automatically generated

Table 4: Comparison of Mixtral with Llama (source: [5]).

The Massive Multi-task Language Understanding (MMLU) is one of the most well rounded and popular benchmarks when it comes to large language models. It allows researchers to gain insights into the capabilities and limitations of various LLMs, by measuring the performance of these models using a plethora of tasks and evaluation methods [6].

According to tables 1, 2, 3, 4, we can conclude that the best LLMs on the market right now are OpenAI’s GPT-4 and Google’s Gemini Ultra, each with a 5-shot MMLU benchmark score of 86.4% and 83.7%, respectively. It is worth noting that both these large language models, as well as other highly rated models such as GPT-3.5, PaLM 2L or Claude 2 are closed-source models. On the other hand, Meta’s Llama models and Mistral AI’s Mistral and Mixtral models are open source. This is a relevant aspect that we will discuss further in our analysis. Another detail that is of utmost importance for my task is that these results have been achieved on mainly English tasks.

A graph with numbers and a number of text

Description automatically generated with medium confidence

Figure 1: GPT-4 3-shot accuracy on MMLU across languages (source: [2])

From figure 1, one can infer the fact that the performance of GPT-4 decreases steadily in multilingual scenarios, based on the amount of training data that it had been exposed to during training. This is general amongst all other models.

When choosing between a closed source and an open source LLM, one must take into consideration the following criteria:

* Cost: Closed source models often involve subscriptions in order to have access to the model itself or its API.
* Customization: Open source LLMs are highly customazible for any particular task, due to the fact that the underlying architecture and source code are available to the users.
* Technical expertise: Closed source LLMs are typically more user-friendly, providing an easy to use UI
* Transparency: Users can better understand open source models due to their availability
* Collaboration: Open source communities contribute to the development of the field through shared resources and expertise

Another factor of utmost importance is the computation power available. In this case, I have had at my disposal a virtual machine (VM) with 3 NVIDIA Tesla T4 GPUs, each with approximately 16GB of GDDR6 memory, 16 8-core CPUs, 128GB of RAM and over 2T of storage to complete this task.

As stated before, all the afore mentioned models perform best on English use cases, making a Romanian customization difficult. For instance, if we wanted to create a chatbot specialized in a specific field such as medicine, law or business, a retrieval augmented generation (RAG) using text data from the particular field should be enough. However, since our chatbot should be able to communicate in the Romanian language, this process becomes much more difficult, as it must first be ensured that the LLM is consistent in understaning and providing qualitive answers in Romanian. With this in mind, an open source model would be the most logical choice, since it is highly customizable and would not require additional costs.

A table of numbers and letters

Description automatically generated

Table 5: Llama 2 language distribution in pretraining data with percentage >= 0.005% (source: [7])

In table 5, it can be observed the language distribution of the pretraining data for Llama 2. The Romanian language had a 0.03% distribution, which may seem extremely low (and it is) compared to English, for instance, with almost 90%. Even so, my goal could be worse if I was Bulgarian, Danish, Slovenian or Croat, each with a distribution lower than 0.03%.

With all these aspects in mind, it can be concluded that the base model to be used for the finetuning process should respect the following constraints:

* It should be open source.
* It must fit within the available computing resources.
* It must have been exposed to some Romanian data during pretraining

That being said, the large language models that fit these criteria are: Llama-2 7B, Llama-2 13B, Llama-3 8B and Mistral 7B. Altough the official research paper has not yet been released for Llama 3, we can take figure 3 as a reference point and assume that the Romanian language distribution is at least equal to that of Llama 2, but the reasoning capabilities should be much greatear due to its exposure to 15 trillion tokens, compared to Llama 2’s 2 trillion tokens. Therefore, on paper, Llama-3 8B should be the best candidate for this task.

In this paper, I am going to present the techniques, comparisons and results for each of these models, in order to fulfill the task of creating a chatbot that cand follow and express itself in a natural manner in the Romanian language.

1. **Theoretical Foundation**
   1. **The Transformer**
      1. **State of the art**

Recurrent neural networks (RNNs) form a diverse class of artifical neural networks characterized by internal feedback loops. These loops allow for information to flow both forward and backward, unlike traditional feedforward networks, enabling RNNs to process sequential data and model time dependencies [8].

Long Short-Term Memory (LSTM) networks are a specialized type of recurrent neural networks, designed to address the vanishing gradient problem and capture long-term dependencies in data more effectively. Memory cells represent the base of the innovation associated with LSTM. These memory cells are able to retain information over extended periods of time, by selectively remembering or forgetting information based on signals received from input data. Each LSTM unit is composed out of four main components: cell state, input gate, forget gate and output gate [9].

Recurrent neural networks (RNNs), Long Short-Term Memory (LSTM) and gated recurrent units (GRUs) in particular, have been leading approaches in the field of natural language processing (NLP) tasks such as language modelling and machine translation. However, these architectures face a significant challenge when it comes to handling long sequences, namely: as new elements are incorporated, their ability to retain information from the initial elements decreases. This is because the hidden state in each step of the encoder often reflects the most recent input element. If the decoder only relies on the final hidden state, it misses crucial contextual information from the beginning of the sequence. To adress this issue, the attention mechanism was introduced [10, 11].

The attention mechanism allows the decoder to examine all encoder states at each step, instead of focusing only on the last state. What this does, is it enables access to information about every element in the input sequence. The main idea behind attention lies in aggregating information from the whole sequence, by calculating a weighted sum of all past encoder states [11]. In this manner, the decoder is able to assign varying degrees of importance to different parts of the input sequence when predicting each output element. This is an iterative process, allowing the model to learn to focus on the most relevant parts of the input in order to provide an accurate prediction of the corresponding output element [10, 11]. However, a major bottleneck remains: the sequential nature of processing. Both the encoder and the decoder must complete processing the previous step, before moving on to the current step [11]. This approach becomes time consuming and computationally expensive when dealing with large datasets. The Transformer model aims to address this very issue.

The Transformer model architecture follows a unique approach in order to extract features for each word in a sentence. Unlike other traditional models that rely on recurrent units, it leverages a mechanism called „self-attention” [10] which analyses the importance of every other word in the sequence relative to the word being examined. Since the Transformer doesn’t use any recurrent units in order to obtain these features, the activations and weighted sums are very parallelizable, increasing efficiency.

**2.1.2 Model Architecture**

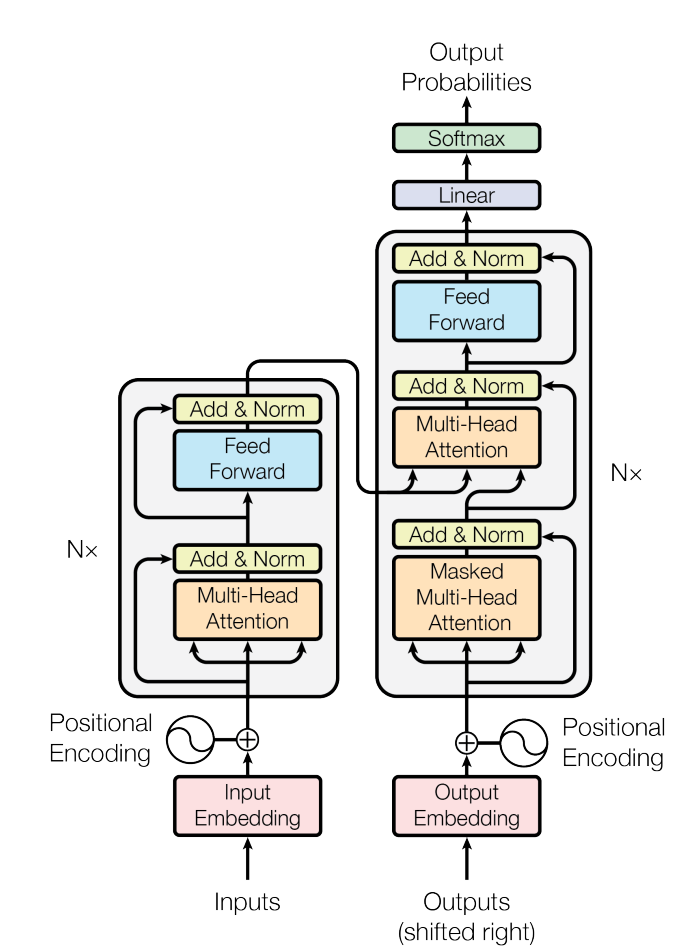


Figure 2: The Transformer - model architecture (source: [10])

Figure 2 depicts the Transformer model architecture, with an encoder model on the left side and a decoder on the right. Many state-of-the-art neural models for sequence translation encompass an encoder-decoder architecture. The encoder acts as an information extractor, processing an input sequence of symbol representations and mapping them to a continuous representation sequence [10, 12]. The decoder, provided with the encoded representation, is tasked with generating an output sequence, one symbol at a time. At every step, the model takes the generated output as additional input for the next one [10, 13].

The encoder model consists of six identical layers, each processing the input through two sub-layers: a multi-head self-attention mechanism that analyses relationships between different parts of the input sequence and a position-wise fully connected feed-forward network which adds non-linearity to the model learning capacity, which is represented by two linear transformations with a ReLU activation funciton, according to (1).

( 1 )

The decoder also uses six identical layers, each with the same two sub-layers as the encoder, with an additional sub-layer: a multi-head attention mechanism that is mainly focused on the output of the encoder, allowing the decoder to understand the context of the input.

Both the encoder and decoder layers incorporate residual connections around each sub-layer. This ensures efficient information flow through the network. In addition, layer normalization is applied after each sub-layer and residual connection for improved training stability.

To prevent information leakage during decoding, a masking mechanism is applied to the decoder’s self-attention sub-layer. This ensures each prediction at the current position considers only the information from preceding positions. This, combined with a one-position shift in the output embeddings, guarantees the model relies solely on previously generated outputs when predicting the next element in the sequence.

„Self-attention, sometimes called intra-attention is an attention mechanism relating different positions of a single sequence in order to compute a representation of the sequence” [10]. The self attention mechanism of the Transformer model introduces three components: queries, values and keys, each corresponding to a distinct role within the self-attention mechanism. As a query, the vector is compared to others to identify relevant information. In its role as a key, it is compared against queries to determine its contribution to the final output based on the weights calculated during the comparison stage.

( 2 )

( 3 )

( 4 )

Each role corresponds to a k×k weight matrix, computed according to equations (2), (3) and (4).

A diagram of a diagram

Description automatically generated

Figure 3: Illustration of the self-attention with key, query and value transformations. (source: [14])

Commonly denoted as , and , these matrices are obtained by applying linear transformations to a single encoded input. This shared origin allows the model to perform self-attention, where the attention mechanism focuses on the input vector itself and its relationship with other elements within the sequence [11, 14].

The Scaled Dot-Product Attention mechanism operates on queries and keys of dimension , and values of dimension . It calculates the compatibility between each query and all keys using the dot product. To address potential instability during training, this value is scaled by the square root of . Furthermore, a softmax function is applied to these scaled values, resulting in weights that represent the relative importance of each value [10, 11, 14].

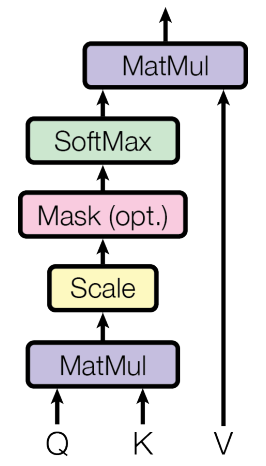


Figure 4: Scaled Dot-Product Attention (source: [10])

In other words, the mechanism employs the , , and matrices to compute attention scores. These scores indicate the significance of other positions (or words) within the sequence in relation to a specific word’s position. For instance, to determine the attention score for the first position (word), the model calculates the dot product of the first query vector with each key vector , , , etc [10, 11].

A crucial aspect of this approach is the scaling factor introduced before the softmax function. This scaling mitigates vanishing gradients, a phenomenon that can hinder training by making it difficult for the model to learn effectively. After obtaining the weights through softmax, the mechanism multiplies them by the value matrix . This selectively emphasizes relevant words (those with greater weights) and reduces the influence of irrelevant words (whose weights and corresponding values in become insignificant) [11, 14].

The matrix of outputs is computed according to equation (5):

( 5 )

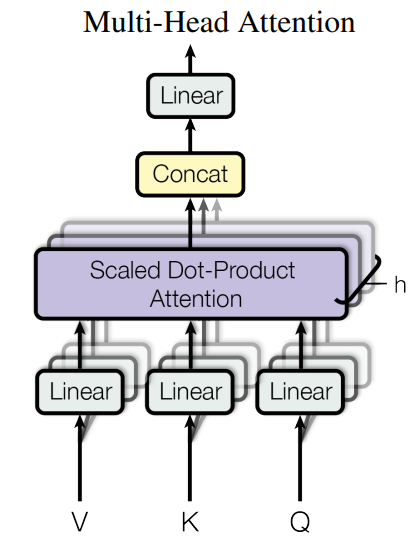


Figure 5: Multi-Head Attention (source: [10])

where

( 6 )

A potential limitation of the previously described approach is its inability to distinguish between sentences with identical words but different word order. Since attention scores are computed for the entire sentence at once, such sentences might receive similar scores. To address this challenge and enhance the model’s ability to differentiate between sentence structures, the Transformer architecture uses multi-head self-attention [11, 14].

Multi-head self-attention involves splitting the word vectors into separate groups, where represents the number of attention heads. Each head independently performs self-attention using its corresponding sub-matrices from the original, , and matrices. This process essentially allows the model to focus on different aspects of the sentence simultaneously through these separate heads, resulting in different output matrices containing attention scores [10, 11, 14].

However, the subsequent layer in the architecture, the feed-forward layer, requires a single input vector for each word. To adjust this, the outputs from each head (individual attention score matrices) are concatenated into a single larger matrix, according to equation (6). Finally, this combined matrix is multiplied by a learnable weight matrix to consolidate the information captured by all the attention heads [11, 14].

One issue that occurs within the self-attention mechanism is its inherent permutation invariance. This means shuffling the order of words in a sentence wouldn't affect the final output of the network. Since word order plays a crucial role in understanding sentence meaning, addressing this limitation is essential [10, 11].

A resolution for this issue is represented by incorporating positional encodings into the input embeddings at the beginning of both the encoder and decoder stacks. These encodings, with the same dimensionality as the embeddings, are added together to provide the model with information about the relative position of each word within the sequence. There are various approaches to implement positional encodings [10, 11].

One approach utilizes a function that maps each word's position in the sentence to a real-valued vector. This allows the network to learn and utilize this positional information during the training process. An alternative approach involves using position embeddings, similar to word embeddings. Here, a unique vector is assigned to each possible position in a sentence. However, this method requires the model to be trained on sentences with all possible lengths beforehand. In contrast, positional encoding empowers the model to generalize to sequences even longer than those encountered during training [11].

( 7 )

( 8 )

The sinusoidal functions from (7) and (8) are applied, according to [10].

It's crucial to incorporate different masks during the training process. These masks serve to selectively exclude irrelevant information from the attention calculations. The encoder mask acts as a filter, preventing padding tokens from influencing the attention calculations within the encoder. The first decoder mask combines two functionalities. It addresses padding tokens similar to the encoder mask, and additionally implements a look-ahead mask. The look-ahead mask ensures the decoder only attends to information from previous positions in the sequence, mimicking a left-to-right reading process and preventing information leakage from future words that could influence the prediction of the current word. The decoder mask is constructed by taking the maximum value between the padding mask and the look-ahead mask. The second mask is a separate padding mask specifically applied within the encoder-decoder attention layer. It prevents the decoder from attending to irrelevant padded tokens within the encoder's output.

After defining the essential components – the encoder, decoder, and final linear-softmax layer – we can now assemble them to form the complete Transformer architecture.

* 1. **Llama 2**

Building upon the success of its predecessor, in February 2023, Meta released Llama 2, an upgraded iteration boasting an increased parameter range of up to 70B and greater logical and thinking capabilities.

As LLM technology advances, researchers are engaging in efforts to enhance the capabilities of these models. A common approach has been to increase model size, under the assumption that larger models equate to better performance. However, recent studies have challenged this notion, emphasizing the critical role of training on vast and diverse datasets rather than solely prioritizing model size.Llama 2 exemplifies this shift in focus by achieving optimal performance through the exclusive use of publicly available datasets [7, 15].

* + 1. **Pretraining**

**A diagram of a diagram

Description automatically generated**

Figure 6: Pretraining of Llama 2 and training of Llama 2-Chat (source: [7])

The foundation of LLaMA 2 lies in its highly curated training dataset. This data is gathered from publicly accessible sources and then preprocessed accordingly. To protect user privacy, the selection process eliminates websites known for collecting large amounts of personal information. To balance out performance and computation efficiency, the corpus leverages approximately 2 trillion tokens, double the context length compared to its predecessor, LLaMA 1, as it can be seen from table 6. Furthermore, to increase the model's knowledge base and mitigate the potential for generating inaccurate information, factual sources are prioritized during the data up-sampling process [7, 16].

Llama 2 builds upon the existing architecture of Llama 1, retaining the base pretraining settings and sticking to the standard transformer architecture. This framework incorporates pre-normalization using RMSProp and the SwiGLU activation function, while also integrating rotary positional embeddings (RoPE) [7, 15, 16]. What differentiates Llama 2 from its predecessor is the inclusion of augmented context length and the adoption of grouped-query attention (GQA) [16]. These features enable Llama 2 to handle extensive contextual information more efficiently during generation.

A table with numbers and text

Description automatically generated

Table 6: Llama 2 family of models (source: [7])

* + 1. **Finetuning**

The fine-tuning process for LLaMA 2 is constructed for dialogue applications. It starts with supervised fine-tuning to establish a foundational version of Llama-2-chat. Afterwards, iterative refinement is implemented using Reinforcement Learning from Human Feedback (RLHF). This RLHF process incorporates techniques like rejection sampling and proximal policy optimization (PPO) to achieve optimal performance in dialogue scenarios [7, 15, 16].

Optimizing LLMs for conversations depends on getting qualitative and diverse third-party SFT data [16]. Additionally, Reinforcement Learning with Human Feedback (RLHF) plays a crucial role. This technique involves gathering data about human preference through binary comparisons to ensure that the finetuned model aligns with human preferences and instructions.

The reward model within the RLHF system is essential in optimizing Llama 2-Chat’s performance in dialogue scenarios. The model outputs scalar scores that indicate the quality of the generated text in terms of helpfulness and safety. To address the potential trade-off between these two aspects, separate reward models are trained for each [7, 16]. These models use a combination of newly collected data and existing open-source datasets in order to enhance generalization and prevent reward errors.

A graph showing different colored lines

Description automatically generated

Figure 7: Training Loss for Llama 2 models (source: [7])

In terms of tokenization, Llama 2 uses the same tokenizer and adopts the same approach as Llama 1, meaning that it utilizes a byte-pair encoding (BPE) algorithm implemented via SentencePiece [7]. Furthermore, all numbers are segmented into individual digits, and bytes are used to decompose unknown UTF-8 characters. This approach maintains a total vocabulary size of 32k tokens, ensuring seamless communication within the context of dialogue applications.

* + 1. **Evaluation**

A table with numbers and text

Description automatically generated

Table 7: Overall performance on grouped academic benchmarks compared to open-source base models (source: [7])

Table 7 showcases the clear performance advantage of Llama 2 models compared to their Llama 1 predecessors. Notably, the LLaMA 2 70B model demonstrates significant improvements in both Massive Multi-task Language Understanding (MMLU) and BIG-Bench Hard (BBH) benchmarks. These improvements translate to roughly 5 and 8 point gains, respectively, when compared to the LLaMA 1 65B model. Furthermore, comparisons between LLaMA 2 models (7B and 34B) and similarly sized MPT models reveal that LLaMA 2 outperforms across various categories, with the exception of coding benchmarks. Similarly, when compared to Falcon models (both 7B and 40B), LLaMA 2 models (7B and 34B) achieve superior performance across all benchmark categories.

A table with numbers and text

Description automatically generated

Table 8: Comparison to closed-source models (source: [7])

Beyond the open-source landscape, table 8 provides some insights regarding the comparison of Llama 2 models with closed-source LLMs. The results indicate that LLaMA 2 70B closely rivals GPT-3.5 on MMLU and GSM8K benchmarks. However, a notable performance gap persists on coding benchmarks. In comparison to PaLM (540B) by Chowdhery and others [17], LLaMA 2 70B demonstrates either comparable or superior performance across most benchmarks. It is important to acknowledge, however, that a substantial performance difference remains between LLaMA 2 70B and more advanced models like GPT-4 and PaLM-2-L [18].

LLama 2 emerges as a leading collection of open-source foundational language models, ranging from 7 billion to 70 billion parameters. These models have garnered recognition for their exceptional performance, scalability and transparency. By relying on publicly available data for training and open-sourcing these models, Meta favorizes advancements within the rapidly evolving landscape of large language models. The open and adaptable nature of the LLaMA 2 framework empowers researchers and developers to accelerate advancements in AI and language modeling.

**2.3 Mistral**

**Bibliography**

[1] Petroșanu, Dana-Mihaela, Alexandru Pîrjan, and Alexandru Tăbușcă. "Tracing the Influence of Large Language Models across the Most Impactful Scientific Works." Electronics 12.24 (2023): 4957.

[2] <https://openai.com/research/gpt-4>

[3] Team, Gemini, et al. "Gemini: a family of highly capable multimodal models." arXiv preprint arXiv:2312.11805 (2023).

[4] <https://ai.meta.com/blog/meta-llama-3/>

[5] Jiang, Albert Q., et al. "Mixtral of experts." arXiv preprint arXiv:2401.04088 (2024).

[6] Ono, Kensuke, and Akira Morita. "Evaluating Large Language Models: ChatGPT-4, Mistral 8x7B, and Google Gemini Benchmarked Against MMLU." Authorea Preprints (2024).

[7] GenAI, Meta. "Llama 2: Open foundation and fine-tuned chat models." arXiv preprint arXiv:2307.09288 (2023).

[8] Grossberg, Stephen. "Recurrent neural networks." Scholarpedia 8.2 (2013): 1888.

[9] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." Neural computation 9.8 (1997): 1735-1780.

[10] Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems 30 (2017).

[11] Muñoz, Eduardo. "Attention is all you need: Discovering the Transformer paper." Towards Data Science (2020).

[12] Cho, Kyunghyun, et al. "Learning phrase representations using RNN encoder-decoder for statistical machine translation." arXiv preprint arXiv:1406.1078 (2014).

[13] Graves, Alex. "Generating sequences with recurrent neural networks." arXiv preprint arXiv:1308.0850 (2013).

[14] Peter Bloem, "Transformers from scratch" blog post, 2019.

[15] Jayaseelan, Nivas. "LLaMA 2: The New Open Source Language Model."

[16] Roumeliotis, Konstantinos I., Nikolaos D. Tselikas, and Dimitrios K. Nasiopoulos. "Llama 2: Early Adopters' Utilization of Meta's New Open-Source Pretrained Model." (2023).

[17] Chowdhery, Aakanksha, et al. "Palm: Scaling language modeling with pathways." Journal of Machine Learning Research 24.240 (2023): 1-113.

[18] Anil, Rohan, et al. "Palm 2 technical report." arXiv preprint arXiv:2305.10403 (2023).

[] Lai, Viet Dac, et al. "Okapi: Instruction-tuned large language models in multiple languages with reinforcement learning from human feedback." arXiv preprint arXiv:2307.16039 (2023).