Implementation of language models within an infrastructure designed for Natural Language Processing

Bartosz Walkowiak, and Tomasz Walkowiak

Abstract—This paper explores cost-effective alternatives for resource-constrained environments in the context of language models by investigating methods such as quantization and CPU-based model implementations. The study addresses the computational efficiency of language models during inference and the development of infrastructure for text document processing.

The paper discusses related technologies, the CLARIN-PL infrastructure architecture, and implementations of small and large language models. The emphasis is on model formats, data precision, and runtime environments (GPU and CPU). It identifies optimal solutions through extensive experimentation.

In addition, the paper advocates for a more comprehensive performance evaluation approach. Instead of reporting only average token throughput, it suggests considering the curve’s shape, which can vary from constant to monotonically increasing or decreasing functions. Evaluating token throughput at various curve points, especially for different output token counts, provides a more informative perspective.

Keywords—language model deployment; quantization; Llama-2; E5 model; ONNX; llama.cpp; CLARIN-PL

I. INTRODUCTION

Artificial Intelligence is nowadays the focus of interest of researchers and commercial developers. Many of those interested do not have access to many GPU units needed to run large language models like GPT-3 [1] or Llama-2 [2]. Methods such as quantization and model implementations using the CPU instead of the GPU come to the rescue. However, the question arises as to how much it costs to reduce the model to run on limited resources.

CLARIN-PL [1] is the Polish branch of the CLARIN ERIC [2] research infrastructure. As part of an international project, it must follow trends in AI and use the latest technologies in the field of NLP. To deliver these state-of-the-art technologies, efficient and scalable tools are used.

The article discusses two problems: the computational performance of language models in inference and the building of infrastructure for processing text documents by language models.

We introduce here a distinction between large and small language models (LLM and SLM). By LLM, we refer to generative models of general purpose like GPT-3 or Llama-2. By SLM we mean classical transformer-based models such as BERT [3] and T5 [4]. SLM are characterized by their smaller size but also their specialization, as they are fine-tuned for specific tasks.

The paper is organized as follows: Section II discusses technologies and research connected with the topics covered in this article. Section III provides a closer look at the architecture and technologies used in CLARIN-PL. Section IV then describes how the SLM and LLM models could be implemented. The implementation methods are validated through experiments performed on various aspects, including model formats, data precision formats, and runtime environments (GPU and CPU). The next section, Section V, is dedicated to the technical aspects of implementing the models, specifically the techniques used to deploy the models as services.

II. RELATED WORKS

A very popular and well-known public repository with many language models is Huggingface. This repository together with the comprehensive Transformers library [5] it supports can be used to process all the most popular SLMs: BERT [3], T5 [4], RoBERTa [6], BART [7], and also LLMs: GPT-3 [1] and Llama-2 [2]. The Transformers library can be used for an inference, as well as for teaching models. The library supports several learning frameworks, with two of the most popular: PyTorch and TensorFlow. Models can also be converted to ONNX [8], an open-source machine-independent standard, or to GGML [9], which enables large models and high performance on commodity hardware.

Another issue is the runtime environment, the model can use the GPU and benefit from its high performance. However, GPU resources are very often limited, and the ability to run only on the CPU is important. An excellent example of CPU inference supporter is llama.cpp [10], which uses GGML format and with which models such as Llama-2, among others, can be used without access to the GPU.

There are production inference servers widely used by industry like Triton Inference Server [11] and TensorFlow
Serving [12], but they are general-purpose servers for deep model execution and do not have model-specific optimizations. Recently, several serving systems are proposed to optimize Transformer-based LLMs [13]–[17].

Another important model-running technique that is gaining interest and development is quantization [18], [19], or more generally, the choice of model precision. What precision we choose affects, on the one hand, how much graphics card memory we will need, that is, in extreme cases, the possibility of running the model. On the other hand, precision, especially in the case of LLM, affects the quality of the results.

The basic precision of the model involves the use of the float32 type so the values are represented by 32 bits, divided between exponent, mantissa, and sign. Other float types used include float16, but also bfloat16 (brain floating point), which differ in the ratio of exponent and mantissa length from the standard float16. Going even lower in precision, choices include float8 E4M3 (4-bit exponent and 3-bit mantissa) and float8 E5M2 (5-bit exponent and 2-bit mantissa). The difference in the way the bits are distributed between exponent and mantissa is the realization of the problems of range (exponent) versus precision (mantissa), because the number of values represented is constant and it is up to us to decide how large a range they will be distributed over.

Typically, models are learned and distributed with a precision of 32 bits and can be quantized in two ways. The first is on-the-fly quantization (implemented by the Transformers library [5]), and the second way is to convert the model beforehand and load the already quantized model (the method used in llama.cpp [10]).

Numerous open-source workflow engines are available for general data pipelining purposes. Apache Airflow [20] or Prefect [21] stand out as popular choices. However, in the field of NLP, the primary focus revolves around libraries such as spaCy [22] and Stanza [23]. Within the context of the CLARIN-PL Language Technology Center (LTC) [24], three solutions have emerged: Weblicht [25], CLARIN-BE [26], and the one detailed in the next chapter.

### III. CLARIN-PL LANGUAGE TECHNOLOGY CENTER

The aim of CLARIN is to develop and maintain a framework that facilitates the exchange, application, and enduring availability of linguistic resources and NLP tools to support research in the fields of humanities and social sciences. The CLARIN-PL Language Technology Center (LTC) [27] realizes this goal in Poland, providing effective and user-friendly NLP tools for the social sciences and humanities. This requirement is fulfilled with a complete processing pipeline of the language tools available via the REST API and web-based interface. The solution ensures flexibility and low processing times. Some tools use models that take longer to load than to process the input file, in which case the tool is run as a service with the required models preloaded into memory [28].

CLARIN-PL LTC is based on the microservice architecture [29] that isolates individual services from each other, so each service runs its own process. Services are interconnected by two techniques, one is the message broker, which is RabbitMQ [30], and the other is the shared file system. The broker is responsible for message queuing and is also used for easy horizontal scaling, which allows the system to dynamically adapt to the current load. The message communication mechanism is lightweight, using only basic commands such as; start, finish, and progress of tasks. This mechanism is implemented using the AMQP protocol [31]. AMQP was not used for data exchange because the size of the input/output data can be very large, which can block message queues. That is why the shared file system is used.

This architecture is deployed on a Kubernetes [32] cluster instance. This solution allows for easy containerization, each NLP tool being deployed as a single pod. The automatic scaling of the number of pods is provided by KEDA HPA [33], which scales up or down the number of instances of a given tool depending on the length of the queue of pending jobs on the broker. The entire infrastructure is implemented using the HELM chart [34] tool, which simplifies and automates the generation of multiple similar services.

Implementing a new NLP worker is possible in languages such as Python, Java, and C++ and is based on a library that is responsible for communication. The developer has to implement functions that process the data (the input/output path and input options are passed as parameters to this function).

The orchestration of related tools in the processing chain is provided by the Language Processing Management Notation [35], which enables improved performance through the use of parallel processing. This means that the processing of a corpus (usually provided as a zip archive) can be parallelized between multiple instances of a given tool. Furthermore, the number of instances scales horizontally, so the response to a high load is to increase the number of processing nodes.

In summary, CLARIN LTC provides a configurable and powerful tool that, using well-known technologies and automation mechanisms, enables the launch of more than 100 different language tools.

### IV. LANGUAGE MODELS DEPLOYMENT

As mentioned in the Introduction, contemporary NLP is based on small and large language models, especially transformer-based ones. Such models require large computing resources, especially graphics cards are an important aspect. Since hardware resources are always limited, there is a question how to effectively implement such models. Therefore, we performed a set of numerical experiments with a classifier built on a deep language model (Section IV-A) and a chat-like generative large language models implemented (Section IV-B) in different ways and on GPU and CPU.

#### A. Small language models

The small language models (like BERT or RoBERTa) could be implemented directly by Transformers library or using ONNX format, in both cases they can be run on CPU or GPU. In GPU tests we used NVIDIA GeForce RTX 3090 GPU with 24GB, whereas in CPU tests we used AMD Ryzen Threadripper PRO 3955WX 16-Core processor (4.4 GHz). For
evaluation we used the E5 base model [36]. It is a general-purpose, multilingual sentence embedding model. The model was initialized from xlm-roberta-base and continually trained on a mixture of multilingual datasets in a contrastive manner with a weak supervision. We tested the effectiveness of the model inference for sequences of 512 tokens, and for different size of batches (ranging from 1 to 8). The experiments were carried out in 200 iterations and the results were subsequently averaged. The summarized findings can be observed in Table I.

<table>
<thead>
<tr>
<th></th>
<th>Transformers</th>
<th>ONNX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>batch size</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>GPU</td>
<td>12.8</td>
<td>8.5</td>
</tr>
<tr>
<td>CPU (4)</td>
<td>423</td>
<td>414</td>
</tr>
<tr>
<td>CPU (8)</td>
<td>214</td>
<td>196</td>
</tr>
<tr>
<td>CPU (16)</td>
<td>152</td>
<td>143</td>
</tr>
</tbody>
</table>

The results show that the ONNX implementation outperforms Transformers in terms of inference speed for both CPU and GPU scenarios. However, the difference is significantly larger in the CPU context. Furthermore, the results show that the use of batches accelerates the average inference time, but the effectiveness of batch usage is limited. Therefore, it is crucial to choose the batch size carefully.

B. Large Language Models

Large generative language models have become an essential component of many text-based user interface applications. However, their size (number of weights) is much larger than that of typical language models, ranging from 7 billion to 70 billion weights in case of Llama-2 [2]. Additionally, their typical usage relies on autoregressive generation of responses, wherein the network takes as input the query and the preceding responses generated by the network itself and produces the next token based on the estimated probability. This process iterates, generating successive output tokens. Due to this operational mechanism and the number of weights, the response generation process is time consuming and strongly influenced by the length of the output text.

Therefore, it is crucial to implement such models effectively in production systems. To assess the feasibility of implementing Large Language Models (LLMs), a series of numerical experiments were conducted using the Llama 7B Chat model provided by Meta. The model was converted into the Transformers library format and implemented in three different formats: a 32-bit float, a 16-bit float, and a quantized 8-bit integer.

In the initial step, the GPU inference time was analyzed with respect to response length. All experiments were carried out in identical setups. They were as follows; maximal number of tokens 1024, topₚ 0.5, temperature 1, top_k 50, and repeat penalty 1.1. Twenty-five diverse queries were developed, ranging from straightforward ones regarding the number of animal legs to complex biographies of historical figures. Each query was repeated 10 times and the results are presented in Figure 1.

The first noticeable aspect is the distinct characteristics of the curves. In the f32 format, the curve takes on a logarithmic shape, whereas in the case of f16, we observe a consistent rate of text generation for texts up to approximately 200 tokens, followed by a logarithmic decrease. On the contrary, the speed of text generation remains constant for q8 format, regardless of the length of the generated text. This difference is likely attributed to implementation variances.

A surprising finding, although consistent with other studies [37], is that 8-bit quantization yields worse results compared to 16-bit or even 32-bit floating point models. On the basis of
the conducted experiments, it is recommended to implement the f16 model on the GPU.

The next experiment evaluated the performance of the Llama model on the CPU using the default implementation in the Transformers library, which utilizes 32-bit floats. These experiments, similar to the previous case, were conducted on a computer equipped with a 16-core CPU. The results are presented in Figure 2 indicating very long text generation times. For instance, generating a text of 540 tokens would take more than 43 minutes. It shows the impracticality of such an implementation.

Next, we investigate the use of the llama.cpp library [10], which leverages the GGML format [9] to execute large-language models on the CPU. We explored formats similar to those employed in the Transformers library. We also tried to analyze the results for the q4 models, but the quality of the result obtained from the model was not acceptable. The generated texts were unreadable, consisting of tokens from different languages. The results (for formats f32, f16, and q8) are presented in Figure 3. As we can observe, the text generation speeds surpass the implementation in the Transformers library when running on the CPU (2). The shape of the curves remains independent of the format used. An exponential increase in speed is noticeable for short texts, after which the speed stabilizes and remains nearly constant regardless of the length of the text. A closer examination of the code and time dependencies revealed that the generation time comprises two components: model loading (with a constant time factor) and the token generation process with a constant speed. The process of loading the model cannot be omitted during text generation because the model retains context information and has to be reloaded. This phenomenon does not occur with the Transformers library. The best results, characterized by the speed, were achieved with the q8 format. Therefore, it is recommended for CPU implementations.

An interesting phenomenon, unrelated to the processing time, is the length of the generated texts. Despite using the same settings in the text generation process and the same queries, this llama.cpp implementation generates significantly shorter texts than the Transformers library. This can be seen by observing the very rare points on the right sides of the graphs in Figure 3, much rarer than in Figures 1 and 2.

An important aspect to note is the variation of speed as a function of the length of the output text, so comparisons of model performance should be reported for a few selected output text length ranges. Therefore, the summary of Llama-2 performance results presented in Table II shows the average speed across four slots for texts of various lengths: 5-20, 100-200, 400-500, and 800-1000. In the case of the llama.cpp implementation, we do not report results for the last slot due to the limited number of results in this range, as discussed earlier. It is worth noting that the best GPU implementation (Transformers f16) is only 2.74 times faster (for longer texts) to 5.13 times faster (for texts up to 20 tokens) than the llama.cpp q8 implementation. This difference is smaller than in the case of BERT models, where the processing time on the GPU differs 11-21 times compared to the CPU time (16 core cases).

<table>
<thead>
<tr>
<th>Model implementation</th>
<th>Speed [token/s]</th>
<th>Mem [GB]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5-20</td>
<td>150-200</td>
</tr>
<tr>
<td>Trans. f32 (GPU)</td>
<td>21.56</td>
<td>8.50</td>
</tr>
<tr>
<td>Trans. f16 (GPU)</td>
<td>32.20</td>
<td>32.66</td>
</tr>
<tr>
<td>Trans. q8 (GPU)</td>
<td>4.92</td>
<td>5.09</td>
</tr>
<tr>
<td>Trans. f32</td>
<td>0.54</td>
<td>0.38</td>
</tr>
<tr>
<td>llama.cpp f32</td>
<td>1.99</td>
<td>2.63</td>
</tr>
<tr>
<td>llama.cpp f16</td>
<td>3.51</td>
<td>5.02</td>
</tr>
<tr>
<td>llama.cpp q8</td>
<td>6.27</td>
<td>8.93</td>
</tr>
</tbody>
</table>

V. Implementing Language Models

A. Infrastructure remarks

In CLARIN-PL, as elsewhere, it is important to manage a limited resource such as the GPU, especially one with high computing power. In the CLARIN LTC case, the problem was raised by the number of available resources, not their power. Kubernetes allows GPU resources to be assigned to a single pod. The solution we used was techniques such as Multi-Instance GPU (MIG) [38] and Time Slicing [39], both of which are supported by the NVIDIA A100 cards. MIG helps when there are not enough GPU instances. It is a technique that logically divides the graphics card, and the card can be split into different parts. The available parts can be 10, 20, 30, or even 40 GB of memory, allowing for a lot of flexibility. The second method allows the GPU to be oversubscribed, but this has the disadvantage of not isolating between resource-using...
services; one service can starve others. For the time being, these technologies also have the major disadvantage of not being observable in terms of memory consumption rates.

The techniques described in Section II for dealing with GPU limitations are extended by the technique of implementing several models in a single pod. This implementation bypasses the limitation that one GPU resource can be allocated to one pod. This technique, combined with the memory release mechanism, contributes to efficient memory usage. It is worth noting that models running in a single pod are separated from each other because they are run in separate processes.

B. Small Language Models as a Service

In CLARIN LTC we have implemented models such as T5 [4] used for keyword identification [40] and text devulgarisation [41], but also Sentence-BERT [42] and E5 [36] for embedding generation. The important thing about these models is that they process text of limited length (typically up to 512 tokens), this strong certainty was used in the design of the architecture. The assumption of a small size also applies to the resulting files; an embedding vector of 512 or 768 (embedding), text of a similar size to the input (devulgarisation), or a keyword list limited to a maximum of five (keyword detection). Based on these facts, communication with the services is done via the AMQP protocol, but unlike regular CLARIN-PL workers, the transmission of input/output data is also done via the AMQP protocol (rather than via a shared drive). As can be seen, the service architecture is strictly tailored to the characteristics of the language model and uses their features to operate effectively. See the list of services in Table III.

TABLE III: Small language models deployed in CLARIN-PL LTC

<table>
<thead>
<tr>
<th>service name</th>
<th>task</th>
</tr>
</thead>
<tbody>
<tr>
<td>sbert-distiluse-base-multilingual-cased-v1 [42]</td>
<td>embeddings gen</td>
</tr>
<tr>
<td>sbert-paraphrase-multilingual-mpnet-base-v2 [42]</td>
<td>embeddings gen</td>
</tr>
<tr>
<td>e5-multilingual-e5-base [4]</td>
<td>embeddings gen</td>
</tr>
<tr>
<td>t5-voicelab-vlt5-base-keywords [40]</td>
<td>keywords deter</td>
</tr>
<tr>
<td>t5-DEPOTxT5-base [41]</td>
<td>devulgarization</td>
</tr>
<tr>
<td>t5-utterance-rewriting-v2-plt5-large</td>
<td>paraphrasing</td>
</tr>
<tr>
<td>t5-plt5-large-poquad-dst-v2</td>
<td>dialogue state trk</td>
</tr>
</tbody>
</table>

The conversion of the models to the ONNX format was carried out using the HuggingFace Optimum\(^3\) library. However, when using this library, it should be noted that it may not include some elements of the conversion. For example, in the case of Sentence-BERT, elements such as the pooling layer or the additional dense layer are omitted from the Optimum library and had to be additionally stored in PyTorch format. For T5 models, on the other hand, prompts and additional parameters, often used in this type of models, must be stored separately.

In addition to the limitations to GPU access, the memory of graphics cards is also not infinite. To make better use of the available memory, a memory release mechanism has been introduced. It works as follows, when a model is not used for a certain period (the length of this period can vary from model to model), then the model is removed from the card’s memory and reloaded when it is needed again.

We are using the KEDA HPA [33] automatic scaling features to scale up or down the number of service instances of a given model depending on the length of the queue of pending jobs on the RabbitMQ broker.

SLM models can be used inside CLARIN-PL services (Section III) via the AMQP protocol (the service library has been extended with dedicated functions) as well as outside the system via the REST interface.

\(^3\)https://huggingface.co/docs/optimum
C. Generative Deep Model as a Service

We have also implemented large language models such as Llama-2 [2] and RWKV [43]. Their implementation is very similar to what was mentioned for SML, but it needs to be adapted to the specifics of LLMs. The main difference is that LLM models running in chat mode require context and, therefore, access to the conversation history. To achieve this, the worker’s input includes the conversation history in JSON format. Additionally, the requests sent to the model have been expanded to include parameters such as temperature and top_p, as well as the ability to choose between two response modes. In single mode, the response is returned when the entire response is generated. In streaming mode, on the other hand, parts of the response (tokens) are returned as they are generated. The LLM services are exposed to the outside world as REST services4, and for the streaming mode, we utilize the Server Side Events mechanism [44].

People are also direct users of LLMs, so we built a dedicated application with a web-based user interface (Figure 4) to communicate with the services. Since an LLM running in chat mode requires context and access to the conversation history, we implemented an infrastructure in which each conversation thread is stored in a separate record in the database. This approach allows for fast access and ensures security.

The user interface allows the model to be used in two modes: chat mode and instruction mode. In chat mode, the model has access to the conversation history, and in instruction mode, the input is split into an instruction and text, allowing for specific tasks to be performed. When chat mode is used, the client that continues the conversation in the thread sends a new input, thread ID, and parameters. The conversation context, retrieved from the database, is prefixed to the new input, and such a query with parameters is passed to the model. The application interface for the different models is unified; regardless of whether Llama-2 or RWKV is selected, the requests sent are the same, differing only in the “model” parameter in the request body.

VI. CONCLUSIONS

As demonstrated in Section II, there are numerous implementations of language models to choose from, together with various techniques to support model deployment. We conducted tests on some of these implementations to run models in inference mode on both GPU and CPU. In addition, we explained the differences and characteristics of runtime environments and precision formats. These results enabled us to identify the most suitable solutions.

We showcased the implementation of small language models at the CLARIN-PL Language Technology Center. This approach relies on the ONNX format and utilizes AMQP for inter-service communication, facilitating efficient and scalable integration with other CLARIN-PL services. For LLM, we employed a Transformer 16-bit implementation for GPU and GGML 8-bit for CPU. Furthermore, we provided a demonstration of the user interface for auto-generative language models.

Fig. 4: CLARIN-PL chat interface (https://chat.clarin-pl.eu/)

The smallest precision we encountered involved storing information using only 4 bits, imposing significant size limitations and resulting in substantial information loss.

The phenomenon of observing different shapes in the curves during experiments leads to the conclusion that reporting only the average speed of tokens per second, which has been the standard practice in many previous works [10], [17], [18], is not entirely informative. This is because the curve can exhibit various shapes, including constant, monotonically increasing, or monotonically decreasing functions. A more effective approach is to report the average number of tokens per second at several points along the curve, specifically for low, medium, and high numbers of output tokens.

REFERENCES


