The Transformer Blueprint: A Holistic Guide to the Transformer Neural Network Architecture

Jean de Dieu Nyandwi

2023-06-17

Table of contents

# Introduction

Invented in 2017 and first presented in the ground-breaking paper “Attention is All You Need” ([Vaswani, 2017](https://arxiv.org/abs/1706.03762)), the transformer model has been a revolutionary contribution to deep learning and arguably, to computer science as a whole. Born as a tool for neural machine translation, its prowess has proven to be far-reaching, extending its applicability beyond Natural Language Processing (NLP) and cementing its position as a versatile, general-purpose architecture.

In this comprehensive guide, we will dissect the transformer model to its core, thoroughly exploring every key component from its attention mechanism to its encoder-decoder structure. Not stopping at the foundational level, we will traverse the landscape of large language models that leverage the power of the Transformer, delving into their unique design attributes and functionalities. Further expanding the horizons, we will explore the applications of transformer models beyond NLP and probe into the current challenges and potential future directions of this influential architecture. Additionally, a curated list of open-source implementations and supplementary resources will be provided for those intrigued to explore further.

Without bells and whistles, let’s dive in!

# Neural Networks Before Transformers

The designers of transformer neural architecture were interested in finding an architecture that could work for sequence to sequence modelling. It wasn’t that there weren’t existing sequence modelling architectures, it’s just that they had many drawbacks. What are other kinds of neural networks that be used for sequence modelling? What are their drawbacks? Let’s seek the answers to those questions as we motivate transformers along the way.

## MultiLayer Perceptrons(MLPs)

Let’s start with [multilayer perceptrons(MLPs)](https://en.wikipedia.org/wiki/Multilayer_perceptron), one of the classic neural networks. MLPs are not super powerful themselves but you will find them integrated in almost any other architecture(surprisingly even in transformer). MLPs are basically a sequence of [linear layers](https://pytorch.org/docs/stable/generated/torch.nn.Linear.html) or fully connected layers.

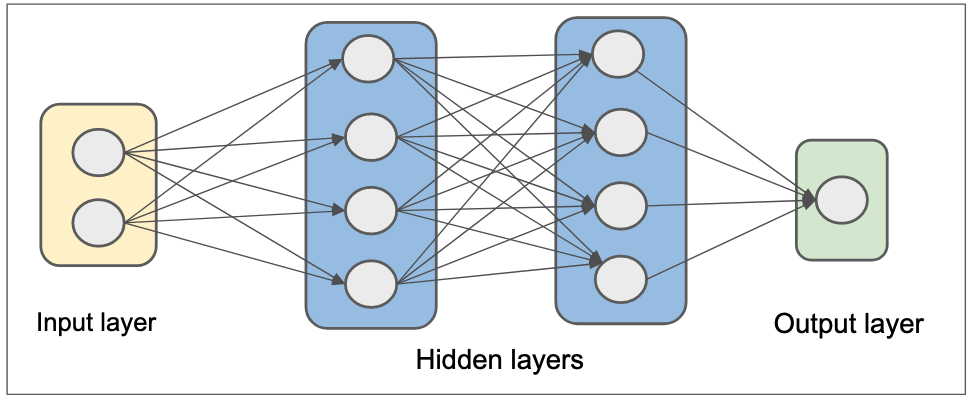


Figure 1: Multilayer Perceptrons(MLPs).

MLPs have long been used to model different kinds of data way before the AI community find best architectures for various modalities but one thing for sure, they are not suitable for sequence modelling. Due to their feedforward design, they can not preserve the order of information in a sequence. Sequence data lose meaning when the order of the data is lost. Thus, the inability of MLPs to preserve order of information make them unsuitable for sequence modelling. Also, MLPs takes lots of paramaters which is another undesired property a neural network can have.

## Convolutional Neural networks

Convolutional neural networks(CNNs or ConvNets) are a class of neural network architectures that are most known for processing images and other modalities such as texts and videos.

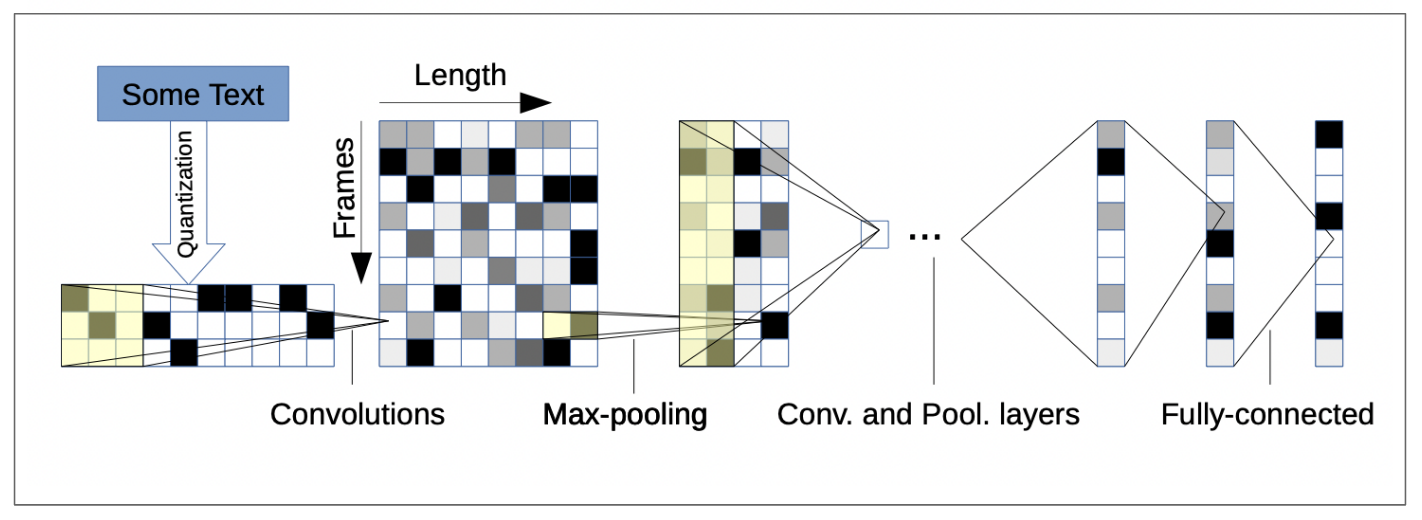


Figure 2: Convolutional neural networks for text understanding[(Zhang et al., 2016)](https://arxiv.org/abs/1502.01710).

ConvNets have so far been successful in small scale and large scale visual recognition but not quite successful in sequence modelling. They are easy to parallize(good for GPUs), due to their locality(computations are bundled in local parts of the input data), they require many layers to handle long-term dependencies. As opposed to images that have fixed length, most sequential data have variable length, something that neither ConvNets or MLPs can handle.

## Recurrent Neural Networks

Unlike MLPs or ConvNets, recurrent neural networks(RNNs) were designed with sequence in mind. RNNs have feedback loop in their design, a key element in their ability to model sequential data. Another desirable property of RNNs is that they can handle variable length data.

There are fundamental problems in how RNNs are wired. Firstly, due to their sequential design, they are likely to be unstable for long-term sequences. Secondly, they can not parallized which limit their scalability on modern machine learning accelerators(like [GPUs](https://en.wikipedia.org/wiki/Graphics_processing_unit)).

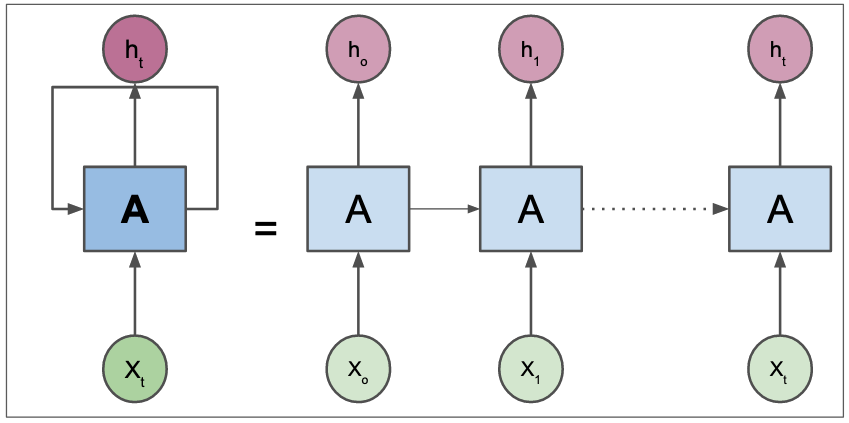


Figure 3: Recurrent neural networks(RNNs).

Recurrent networks have many variations. One of their famous version is Long Short Term Memories(LSTMs). LSTMs can handle long-term sequences. They have a cellstate(horizontal straight line in figure below) and gates which all smooth the flow of information.

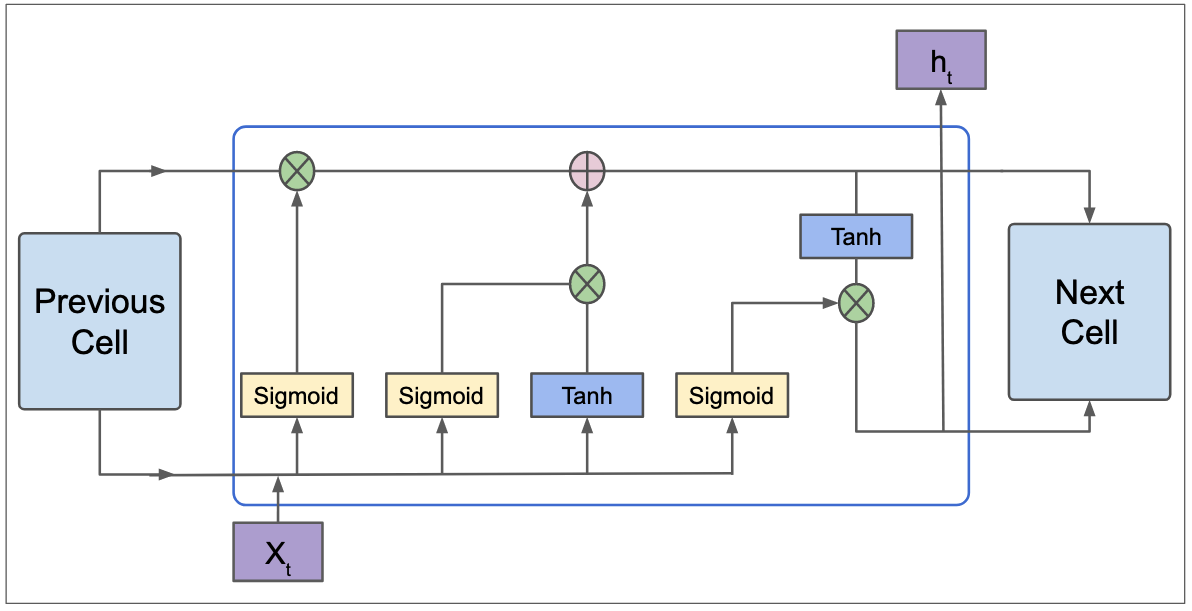


Figure 4: Long Short Term Memories(LSTMs).

Another slightly efficient version of LSTMs is [gate recurrent Units(GRUs)](https://en.wikipedia.org/wiki/Gated_recurrent_unit). LSTMs works great for basic sequence modelling problems but they are still limited in how far they can go. As we previously said, they can not parallized which means they can not be scaled. Also, even if they can preserve the order of information, they can not reason about the global context of the data they are processing. Context is important. Take an example in machine translation(the task that motivated transformer), context of sentence being translated is as important as the order.

All we have been doing basically is to motivate the transformers. So far, we have seen that prior neural networks were either not suitable for sequence modelling or not parallizable or not stable or limited in context length, all of which are primary desirable traits of sequence neural architectures.

Now that we have the right background, let’s dive in the transformer architecture.

# Transformer Architecture

Transformer is a neural network architecture that can process sequential data such as texts, audios, videos, and images(as a sequence of image patches). Transformer does not use any recurrent or convolution layers. It’s fundamental layer is called ***Attention***. It also contain other basic layers such as fully-connected layers, normalization layer(LayerNorm most[(Lei Bai et al., 2016)](https://arxiv.org/abs/1607.06450)), embedding layer, and positional encoding layer. We will see what each of those layers performs in next sections.

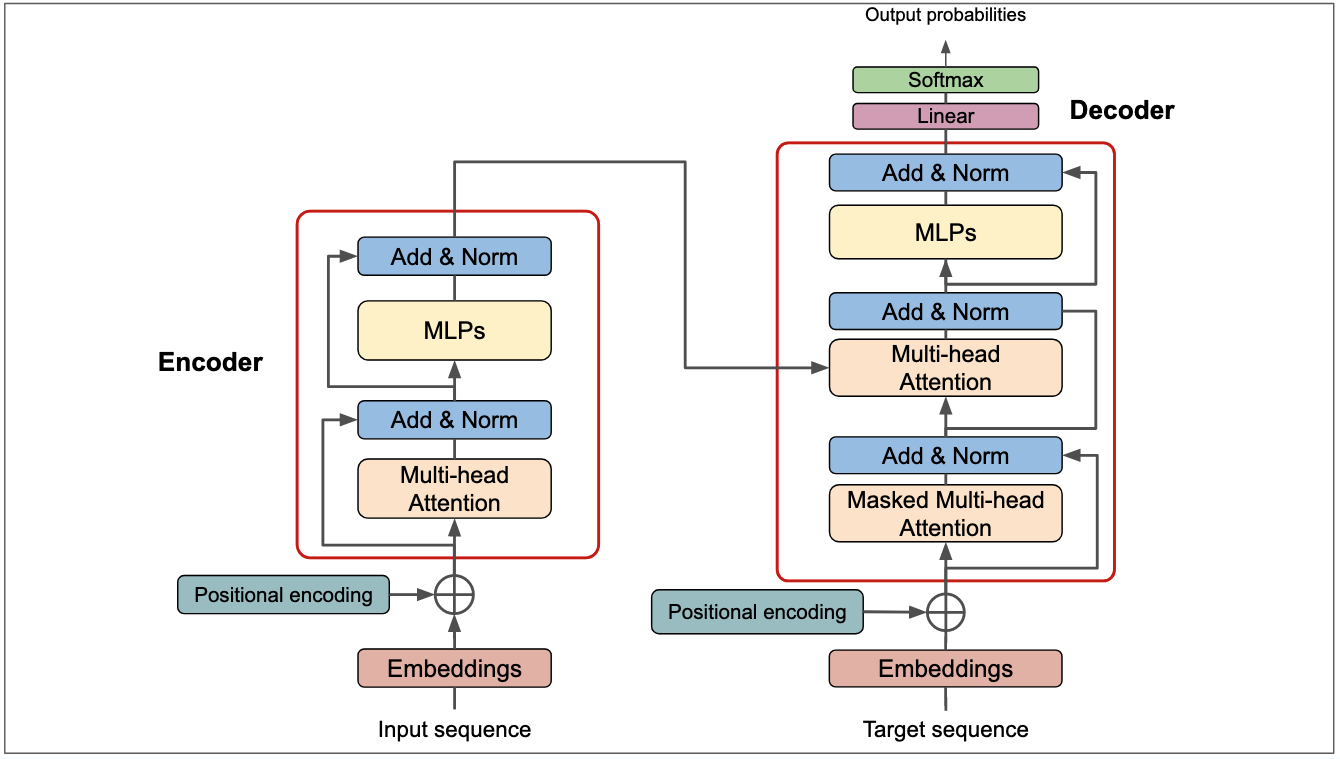


Figure 5: Transformer Architecture. Adapted from [(Vaswani, 2017)](https://arxiv.org/abs/1706.03762).

As we alluded to in the beginning, transformer was initially introduced for machine translation, a task that demands processing two sequences(both input and output are sequences). Thus, the transformer model had two parts: encoder for processing the input and decoder for generating the output. More about encoder, decoder, and other layers are discussed below.

## Encoder

Encoder is one of the main blocks of the transformer architecture that is right at the input of input sequence. Encoder transforms input sequence into compressed representation. In the orginal transformer architecture, the encoder was repeated 6 times(this depends on overall size of architecture, it can be changed). Each encoder block has 3 main layers which are multi-head attention(MHA), layer norm, and MLPs(or feedforward according to the paper).

Multi-head attention and MLPs are referred to as sub-layers in the transformer paper. Between sublayers, there are layer normalization and dropout and residual connections in between(refer to diagram for correct flow of those layers).

The number of encoder layers was 6 as said previously. The more the number of encoder layers, the larger the model, and the more the model is likely to capture the global context of the input sequences hence resulting in better task generalization.

## Decoder

The decoder is pretty much the same as encoder except additional multi-head attention that operated over the output of the encoder. The goal of the decoder is to fuse encoder output with the target sequence and to make predictions(or to predict the next token).

The attention that takes the target sequence in decoder is masked to prevent the current token(being processed) from attending to subsquent tokens in the target sequence. If the decoder had access to a full target sequence, this would basically be cheating and can result in model that can not generalize beyond the training data.

Decoder is also typically repeated the same times as encoder. In the orginal transformer, the number of decoder blocks were also 6 blocks.

## Attention

### What Really is Attention?

Attention is the principal element of transformer architecture. In essence, attention is a mechanism that can allow the neural network to pay more attention to the part of input data that contains meaningful information and pay less attention to the rest of the input.

The attention mechanism was used in various tasks long before the introduction of transformer architecture. The idea of attention first appeared in neural machine translation(NMT) approach that used attention to find the set of positions in input sentence where the *most relevant information is concentrated*([Bahdanau et al., 2015](https://arxiv.org/abs/1409.0473)). Because their attention based NMT could align and translate jointly or simultaneously, it surprisingly performed well than previous approaches. As you can see in the image below, the network was able to find the correct order of words in a translated sentence, a feat that prior neural machine translation approaches struggled to achieve.

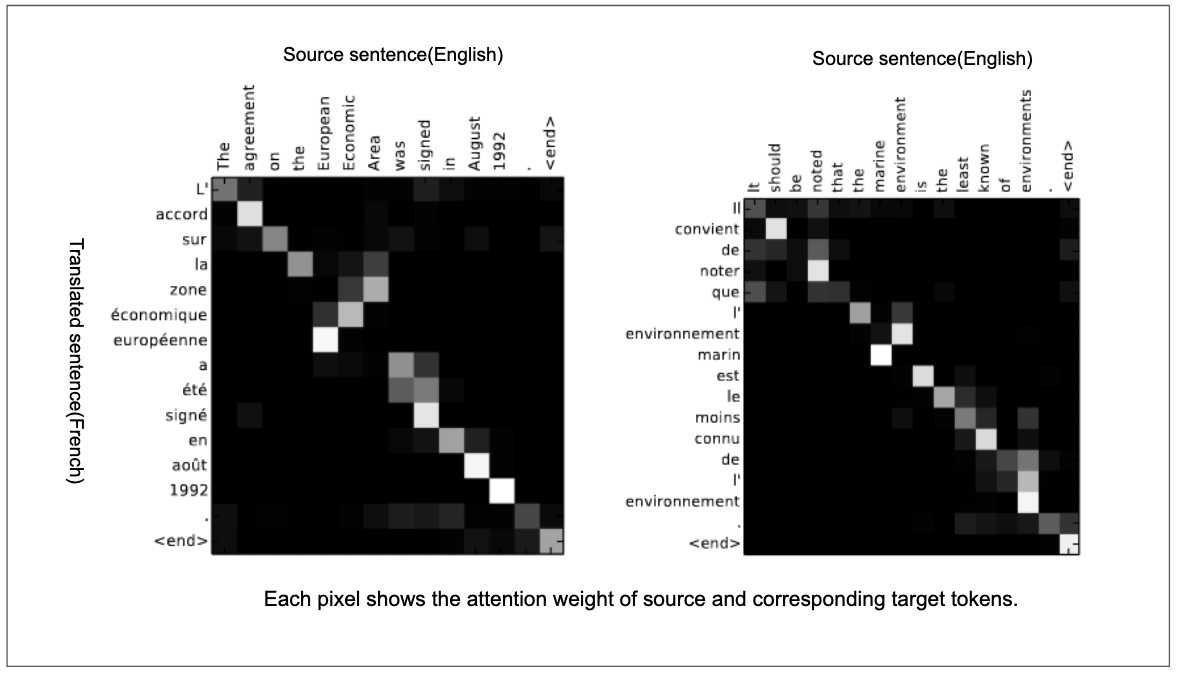


Figure 6: Aligning the source sentence and target sentence in neural machine learning translation([Bahdanau et al., 2015](https://arxiv.org/abs/1409.0473)). The x-axis and y-axis shows the source sentence and translated sentence respectively. Each pixels indicates the attention weights of source(input) token with its corresponding target token. The diagonal attention represents words that are in corresponding order(ex: the agreement on the -> L’ accord sur la). Attention can figure out the correct word order(ex: European Economic Area -> zone économique européenne).

What’s going on in the image above? Can you spot something? The order of words was reversed in translated sentence wherever is make sense in target language. Thus, when translating a sentence, attention can give the model the ability to not only translate the sentence correctly, but to also translate it in the right order based on the context. In brief, attention can identify and preserve the context when translating one language to another.

Another earlier work that used attention is found in neural image captioning([Xu et al., 2015](https://arxiv.org/abs/1502.03044)). In this work, the authors used ConvNets for features extraction and RNNs with attention mechanism to generate a caption that aligns best with the input image. The image belows(taken from the paper) shows where the model roughly attends to.



Figure 7: Generating caption with neural captioning model. The white regions show where the model is focusing when generating caption A woman is throwing a frisbee in a park”. Image from ([Xu et al., 2015](https://arxiv.org/abs/1502.03044)).

On a global level, integrating attention mechanism in image captioning model helps the model to attend to correct objects when generating caption.

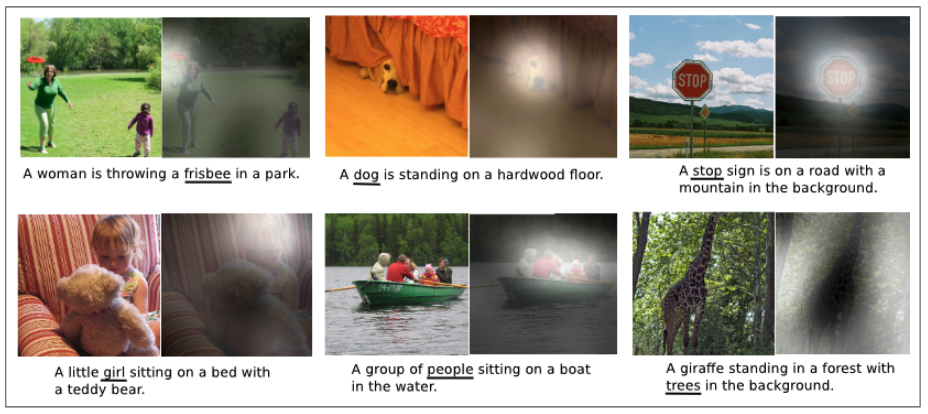


Figure 8: The model can attend to key objects when generating captions. ([Xu et al., 2015](https://arxiv.org/abs/1502.03044))

Both the examples we used above demonstrate the effectiveness of attention. Attention is merely this magic mechanism that allows the neural network to focus to part of input data that contains meaningful information and focus less on rest of the input data.

Now that we understand what attention really is, let’s look at the inputs of attention function in transformer architecture: querry, keys, and values.

### Attention Function: Query, Key, Value

Intuitively, attention is really *“focus on most important part of the input data”*. Technically speaking, attention measures the *similarity* between two vectors and return the *weighted similarity scores*. A standard attention function takes three main inputs which are query, key, and value vectors. Before breaking down the attention function, let’s try to understand what keys, values, and queries stand for.

Query, keys, and values are terms commonly used in search engines and database systems. To understand those terms, let’s take a simple example.[[1]](#footnote-61) Let’s say you are searching papers that are based on ***attention*** on ArXiv. The ***query*** is ideally what you will put in the search box. Internally, the ArXiv may organize papers by a set of predefined ***keys***. Before ArXiv gives you papers that you asked for, it will compare your ***query*** to those predefined set of keys and return papers that best match with query and keys correspondence. ***Values*** merely refers to all papers in the database. As a disclaimer, we are using this example to understand the meaning of query, keys, and values in search and database systems context. It’s not an attempt to show how ArXiv system works.

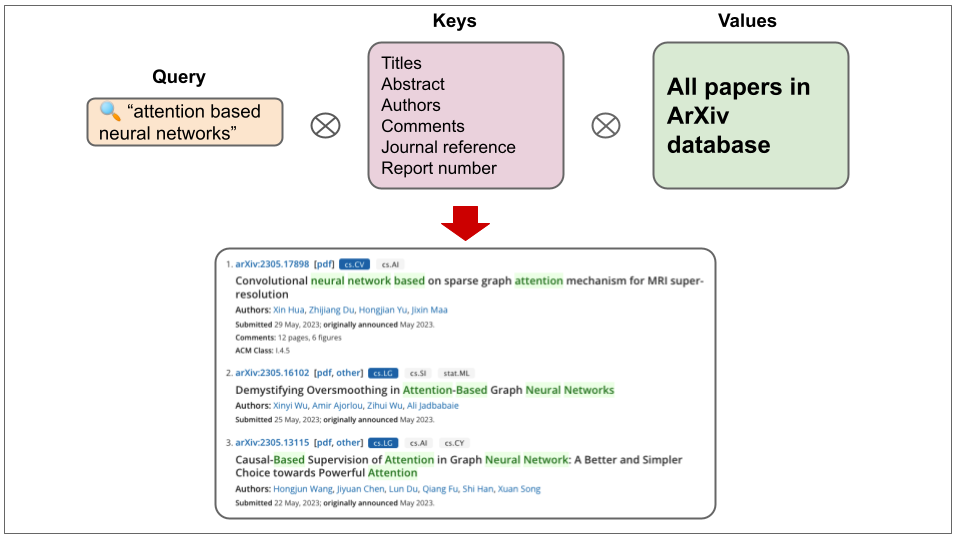


Figure 9: Example demonstrating query, keys, and values in ArXiv paper search system.

With such intuitive understanding of query, keys, and values in mind, let’s move to the mathematical representation of the attention function.

From the function above, , , are query matrix, key matrix, value matrix respectively. We compute the dot product of query and keys divide the product by a scaling factor of . The scaling factor is used to avoid the scenarios where large values of would result in small gradients. Then, we normalize the dot product into a probability distribution with softmax(this basically give us weighted sum) and by multiplying it with values, we get weighted values.

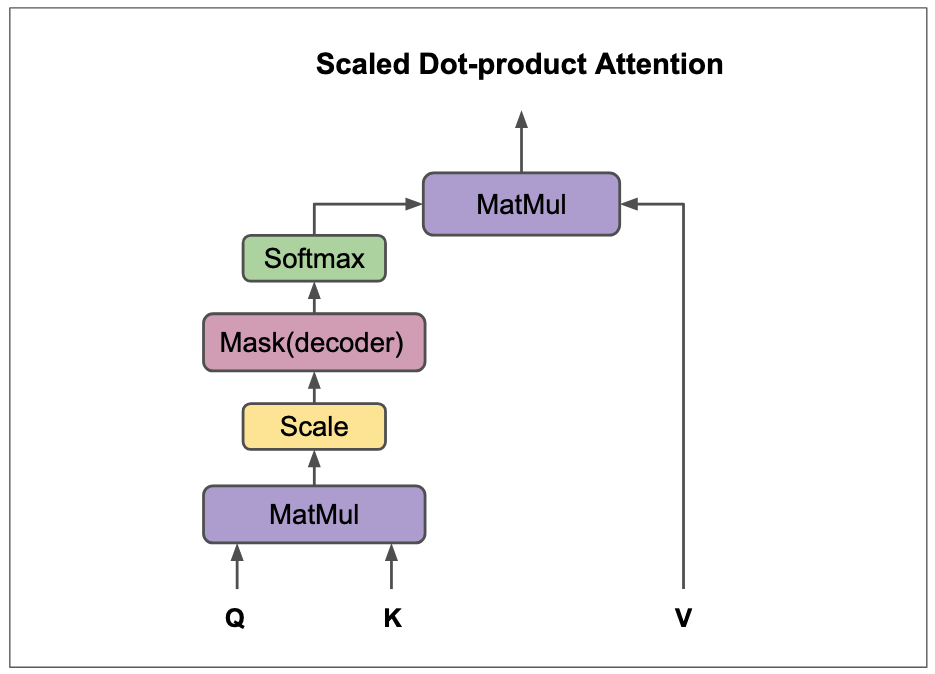


Figure 10: Graphical representation of dot-product attention. Figure adapted from [(Vaswani, 2017)](https://arxiv.org/abs/1706.03762).

The kind of attention described above is called scaled-dot product attention, a modified dot-product attention([Luong et al., 2015](https://arxiv.org/pdf/1508.04025.pdf)). There are other kinds of attention such as additive attention([Bahdanau et al., 2015](https://arxiv.org/abs/1409.0473)), content-based attention([Graves et al., 2014](https://arxiv.org/abs/1410.5401)), location-based attention([Luong et al., 2015](https://arxiv.org/pdf/1508.04025.pdf)), and general attention([Luong et al., 2015](https://arxiv.org/pdf/1508.04025.pdf)). Each of those attention types can either be applied globally(to the whole input data), hence global attention, or locally(sub-parts of the input data), hence local attention.

You may have heard that transformer is parallizable and you may be wondering where it comes from. Transformer parallization comes from attention function. Provided that both query, keys, and values are matrices, attention can be performed in two main matrix multiplies and hence no loops or any recurrent operation involved. Computing attention is resonably faster for GPUs. For bigger models(in order of billions parameters) and massive training data(in order of billion/trillions tokens), attention is can be expensive since it takes quadratic [time complexity](https://en.wikipedia.org/wiki/Time_complexity) from the fact that each token attends other tokens.

One last thing before we conclude this section: if the queries, keys, and values are derived from same source, the attention applied to them is called ***self-attention***. If they come from different source, we say ***cross-attention***.

### Multi-Head Attention

What we decribed above is a single attention layer. In practice, you typically would not get sound results with just one attention layer. Instead, people tend to compute multiple attention layers in parallel and concatenate the results. In nutshell, that is multi-head attention. Multi-head attention is basically multiple independent attentions computed over linearly projected QKV vectors. In the figure below of multi-head attention, the concatenated attention values are linearly projected to the model dimension.

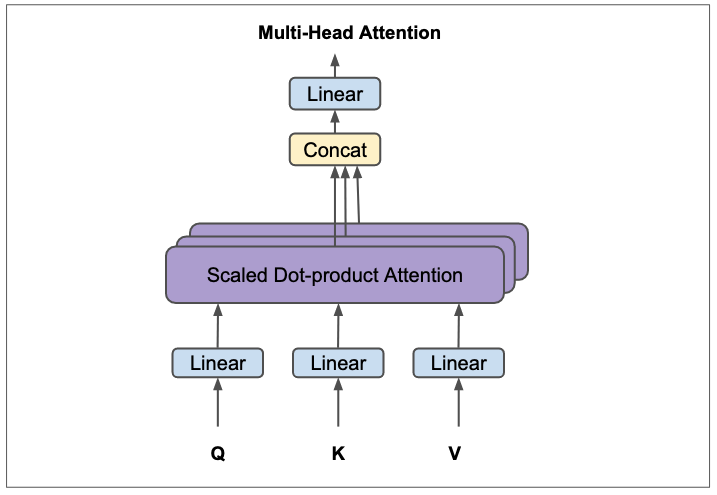


Figure 11: Multi-Head attention. Figure adapted from [(Vaswani, 2017)](https://arxiv.org/abs/1706.03762).

As explained by the designers of the transformer architecture, computing multiple attentions in parallel allows the model to *“jointly attend to information from different representation subspaces at different positions.”“*([(Vaswani, 2017)](https://arxiv.org/abs/1706.03762)). A surprising thing about multi-head attention is that it doesn’t increase the overall computation cost because the dimension of each head is oneth of number of heads(i.e, heads in base transformer is 8) of the overall model dimension(ie, 512). So, if the dimension of the model( in the paper) is 512, the number of heads in multi-head attention are 8, each head is thus .

Multi-head attention can be seen as depth-wise separable convolution([Chollet, 2017](https://arxiv.org/abs/1610.02357)) in ConvNets. Depth-wise separable convolution is a special type of convolution that splits input tensor into multiple channels, operate on each channel independently, concatenate the individual outputs and and feed the results to a pointwise convolution(1x1 convolution which is equivalent to a linear projection).

## MLPs

MLPs or Multilayer Perceptrons[[2]](#footnote-78) are one of the two sublayers in both encoder and decoder. MLPs in the transformer are made of two linear layers with ReLU activation in between and they are applied to each position independently and identically.

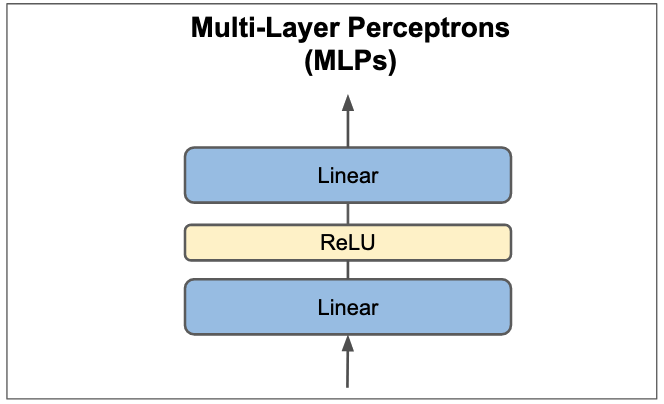


Figure 12:Multi-Layer Perceptrons().

## Embeddings and Positional Encoding Layers

The Transformer architecture incorporates two embedding layers: one located in the encoder to handle the input or source sequence, and another in the decoder for the target or output sequence. These embedding layers convert input or output tokens into dense vectors of a fixed size, essentially mapping each token in a sequence to a specific dense vector. Utilizing embeddings is a standard practice in language modeling due to the semantic depth they provide. With these embedded token vectors, those bearing similar semantic meanings tend to align in the same direction.[[3]](#footnote-83).

The size of the embeddings in the base transformer is 512(this is the dimension of the whole model). As a side note here, transformer architecture maintains the same dimension across the whole network and it is 512 for base model. This is what referred to as previously.

Positional encodings serve as integral components in the initial stages of both the encoder and decoder within a Transformer model. They are used to preserve the order of tokens in a sequence. One might question the necessity of these positional embeddings. This stems from the inherent permutation invariance of the attention mechanism, whereby modifying the order of tokens does not alter the output weighted values[[4]](#footnote-85). Consequently, the attention mechanism, on its own, lacks awareness of the token order. As the Transformer architecture does not incorporate any other recurrence methods, positional encodings are introduced to equip the model with positional awareness of the tokens in the sequence. In essence, without positional encodings, a Transformer would indeed exhibit permutation invariance. However, such a design would fall short for tasks where sequence order holds significance, as is the case for most NLP tasks.

For encoding positional information in a sequence, the designers of transformer used sinusoidal functions of different frequencies. They also experimented with learned positional embeddings, but it did not make a difference in the results.

## Residual Connections, Layer Normalization, and Dropout

Residual connections are at the heart of neural network design and they are one of the popular ingredients in modern deep learning. Since when deep residual networks proved substantial performance in computer vision([He et al., 2015](https://arxiv.org/abs/1512.03385)), residual connections have been used in almost most neural networks not just in vision but in other modalities as well. In fact, it is almost impossible to see a neural network model that does not use residual connections in present times. Residual connections alleviate unstable gradient problems and they help the model to converge faster.

One of the transformer authors, Ashish Vaswani once said that “redisual connections carry positional information to higher layers, among other information.” Take a look at the image below!

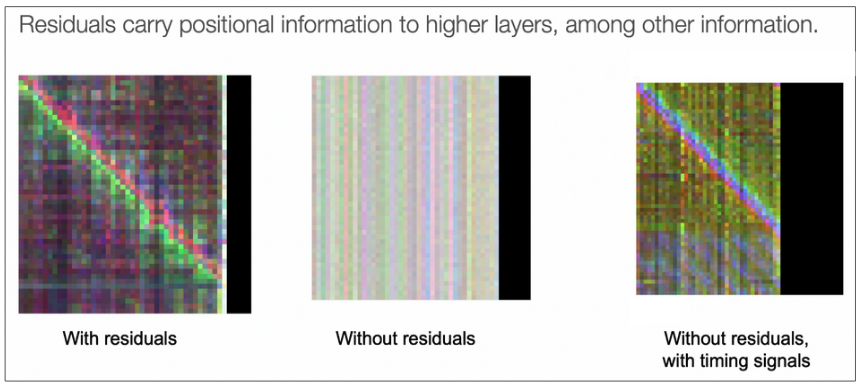


Figure 13: Residual connections carry signals to higher layers which improves the training of transformer model. The smooth diagonal in first image(with residuals) shows the effectiveness of residual connections. Image by Ashish Vaswani in CS224N.

Layer normalization[(Lei Bai et al., 2016)](https://arxiv.org/abs/1607.06450) is also one of the most used normalization techniques in modern neural networks. Layer normalization significantly reduces the training time by normalizing the activations of a layer with the layer mean and variance. Unlike batch normalization[(Ioffe and Szegedy, 2015)](https://arxiv.org/abs/1502.03167) that normalizes each layer with mean and variance computed over the mini-batch, layer norm just normalizes each layer with the mean and variance of each activation. Layer normalization maintains similar behavior during both training and testing phases, unlike batch normalization which exhibits different behaviors in these two stages.

There are two ways to place layer normalization in transformer architecture. The first option is called Post layer normalization(Post-LN) where layer normalization is placed between residual blocks(or after each sublayer(multihead-attention and MLPs) but after addition). The second option is called Pre layer normalization(Pre-LN) where layer normalization is placed before each sublayer inside the residual block. The standard transformer architecture uses Post-LN, but in the [updated codebase that trained the orginal transformer](https://github.com/tensorflow/tensor2tensor/commit/f5c9b17e617ea9179b7d84d36b1e8162cb369f25)[[5]](#footnote-93), it was found that to be Pre-LN. This mismatch between paper and codes makes it hard to trace back the actual position of layer normalization in initial transformer but from the commit history, it looks like Pre-LN was used later. The authors could have updated the paper but they probably didn’t mind since no one knew this would turn out to be one of the influential and reference papers in neural network design.

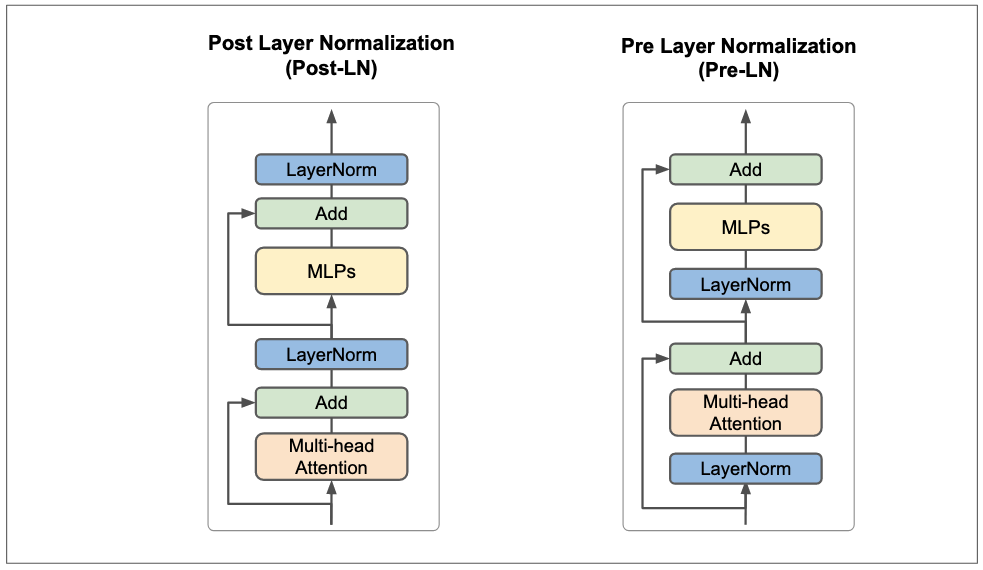


Figure 14: Post layer normalization(Post-LN) and Pre layer normalization(Pre-LN).

Thus, it’s not exactly clear where the layer normalization should be and this is an active research question. A recent study on the impacts of Pre-LN and Post-LN([Xiong et al., 2020](https://arxiv.org/abs/2002.04745)) showed that placing layer normalization before multi-head attention and MLPs(Pre-LN) improves the training and converge much faster than layer normization placed after multi-head attention and MLPs. The study also claimed that with Pre-LN, you don’t need to be smart at choosing learning-rate scheduler since Pre-LN have better initializations. Neither of Pre-LN an Post-LN is perfect. Another quite recent study introduced ResDual([Xie et al., 2023](https://arxiv.org/abs/2304.14802)) which basically alleviates issues of Pre-LN and Post-LN by introducing additional residual connection with layer normalization.

Where you should place layer normalization continue to be a question but this should be less of a question. As many people have noted, transformer seems to be a universal architecture. The orginal vanilla transformer(with few tweaks like yes LN) is the one that is still behind most novel works in language modelling, visual recognition, and multimodal learning depsite millions number of works that claims to improve the transformer. Thus, we should aim to keep the universality of this architecture. We will see this more in efficient transformers toward the end of the article.

Before we wrap up this section, let’s talk about dropout([Srivastava et al., 2014](https://www.cs.toronto.edu/~rsalakhu/papers/srivastava14a.pdf)) in the transformer architecture. Layer normalization can acts as a regularizer as a side effect but you still need other forms of network regularizations to deal with overfitting. Dropout is applied to the output of each sublayer(before addition and normalization). It is also applied to the sum of the embeddings and the positional encodings in both encoder and decoder stacks. For other regularization techniques used in training transformer and other training details, check out the [paper](https://arxiv.org/abs/1706.03762) for more.

## Linear and Softmax Layers

The linear layer after decoder takes the decoded activations and project them to the size of the vocabulary. This linear layer will basically produce logits. The softmax layer will take those logits and turn them into next-token probabilities. The next predicted token will be basically the argmax of softmax output.

# Visualizing Attention

Attention can capture the overall context from an input sequence, which often leads to better performance of the model. By visualizing attention, we can see which parts of the input sequence have significant influence on the model’s output. This helps us better understand how the inner workings of Transformer neural networks.

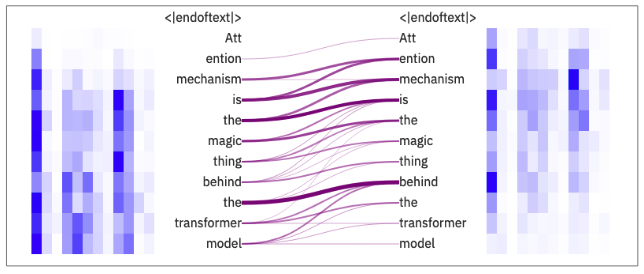


Figure 15: Visualizing attention with [ExBert](https://huggingface.co/spaces/exbert-project/exbert).

The figure above depicts the attention heads on 8 layer of GPT-2([Radford et al., 2019](https://d4mucfpksywv.cloudfront.net/better-language-models/language_models_are_unsupervised_multitask_learners.pdf)). From the figure, it’s clear that even in the early layers of the transformer, most tokens attend to each other.

A number of tools that visualize attention have evolved overtime to help the AI community understand what’s going inside the transformer model. One of the most famous tools is BertViz([Vig Jesse, 2019](https://aclanthology.org/P19-3007.pdf))[[6]](#footnote-110). [ExBert](https://huggingface.co/spaces/exbert-project/exbert) that we used to make the above visualization is also an excellent and simple tool for visualizing the attention on most transformer based models such as GPT-2 and BERT([Devlin et al., 2018](https://arxiv.org/abs/1810.04805)).

# The Pros and Cons of Attention Mechanisms

The attention mechanism has ushered in a significant shift in the approach to sequence modelling and other modalities that can be framed as sequences. When compared with other sequence networks such as recurrent networks and 1D convolutions, attention offers numerous advantages. These are briefly discussed below:

* **Long-term Dependencies**: Traditional Recurrent Neural Networks (RNNs), including variants like Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), are prone to the issue of long-term dependencies, where the model’s ability to retain information weakens over time. Attention mechanisms help mitigate this problem by enabling the model to directly access any point in the input sequence, thereby preserving the overall context.
* **Parallelization**: Unlike RNNs, which require sequential computation, attention-based models, such as Transformer architectures, can process all tokens in the input sequence in parallel. This makes them more computationally efficient and scales better with sequence length.
* **Interpretability**: Attention provides a certain degree of interpretability, as it highlights the parts of the input that the model considers most important for producing a particular output. The “attention map” can help us understand what the model is “thinking.”
* **Global Context**: In Convolutional Neural Networks (CNNs), the receptive field is typically local and depends on the kernel size, potentially leading to the loss of broader context. However, with attention, each output token can take into account information from every token in the input sequence, thus preserving the global context.
* **Improved Performance**: Attention-based models, especially those that utilize Transformer architectures, have achieved state-of-the-art performance in many NLP tasks, outperforming their RNN and CNN counterparts. They have also pushed envelope in other modalities such as computer vision, speech recognition, robotics, multimodal learning, etc…

In the figure below, we summarize the properties of attention-based models versus other deep neural network architectures.

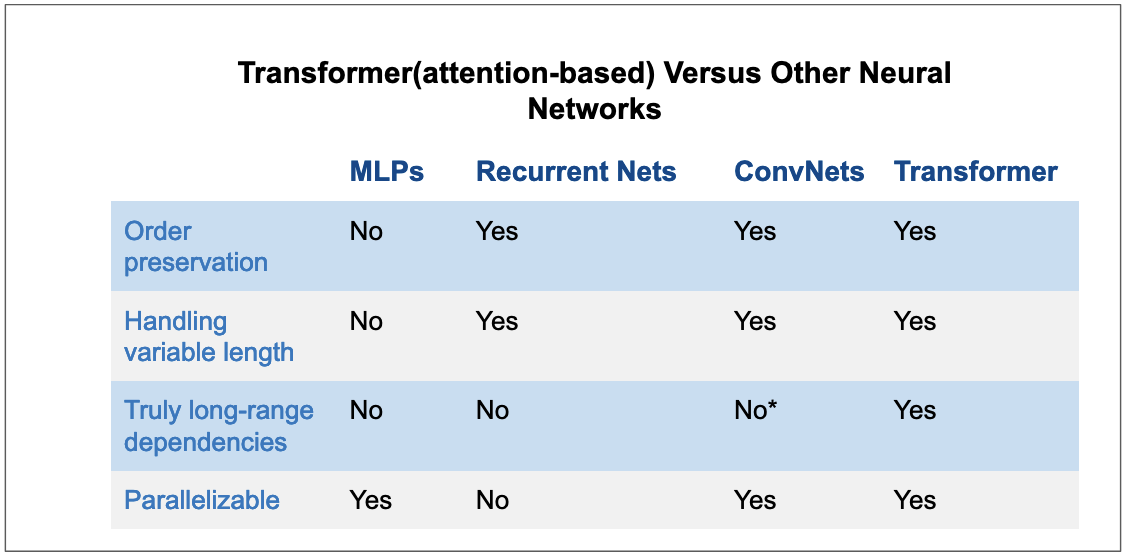


Figure 16: Attention versus other recurrent network architectures. Tranformer possesses nearly all good traits of neural networks. ConvNets are close to transformer but they require many layers to achieve long-range dependencies.

Despite the multitude of advantages they offer, as everything else in life, attention mechanisms also come with their fair share of challenges. For instance, in several types of attention, both memory consumption and computational cost can scale quadratically with sequence length. Various strategies, such as [sparse attention](https://openai.com/research/sparse-transformer) or local attention, have been proposed to alleviate these issues but none of them are used in practice([Tay et al., 2022](https://arxiv.org/abs/2009.06732)).

While Transformers offer the advantage of parallelization during training, the nature of the inference process may still necessitate a sequential approach, contingent on the specific task. Due to their autoregressive nature, Transformers generate outputs one token at a time, continuing this iterative process until the desired output sequence is fully produced.

Furthermore, while attention offers a certain level of interpretability, it is far from perfect. Although it provides some insights into the model’s functioning, fully deciphering complex models based solely on attention maps can be, to say the least, a daunting task, if not almost impossible.

# Large Language Transformer Models

## Evolution of LLMs

Large Language Models (LLMs) have revolutionized human interaction with machine learning systems. Natural language interfaces, such as [ChatGPT](https://openai.com/blog/chatgpt) and [Bard](https://blog.google/technology/ai/bard-google-ai-search-updates/), are powered by robust LLMs. These models have paved the way for executing natural language downstream tasks on-fly or through zero-shot learning. Such tasks, in the past, necessitated the gathering of a downstream or task-specific dataset.

At the core of these LLMs, one finds a fundamental Transformer model, it’s fundamentaly a transformer model that we have seen with little tweaks here and there. In this section, we will delve into the compressed evolution of Large Language Models. Moreover, we will explore the development of vertical LLMs, specifically designed and trained for particular applications.

Transormer base model has 65M parameters but since then, language models got bigger and bigger(in order of billions) and hence the name large language models. Below is a quick overview of popular large language models.



Figure 17: Overview of popular LLMs. Layers are number of stacked encoders/decoders or both for encoder-decoder models, width is the dimension of the model, heads are number of attention layers in multi-head attention, params are number of parameters. N.B, the numbers of GPT-2 are not exactly clear.

The training process for most large language models (LLMs) follows a broadly similar pattern. In the initial pretraining phase, LLMs are exposed to vast volumes of curated textual data, sourced from a diverse range of materials such as books, articles, code snippets, and websites. This vast dataset is essential for the models to gain a comprehensive understanding of the world, enabling them to create rich representations and generate contextually relevant responses. The general public holds high expectations for LLMs’ performance across various domains. To meet these expectations, the pretraining data must encompass a wide spectrum of topics and disciplines([Yang et al., 2023](https://arxiv.org/abs/2304.13712)).

The actual training of LLMs occurs in an [unsupervised](https://en.wikipedia.org/wiki/Unsupervised_learning) fashion, with a specific focus on [self-supervised learning(SSL)](https://en.wikipedia.org/wiki/Self-supervised_learning). This approach eliminates the need for labelled data, a crucial feature considering the near-impossibility of labeling the entirety of online content.

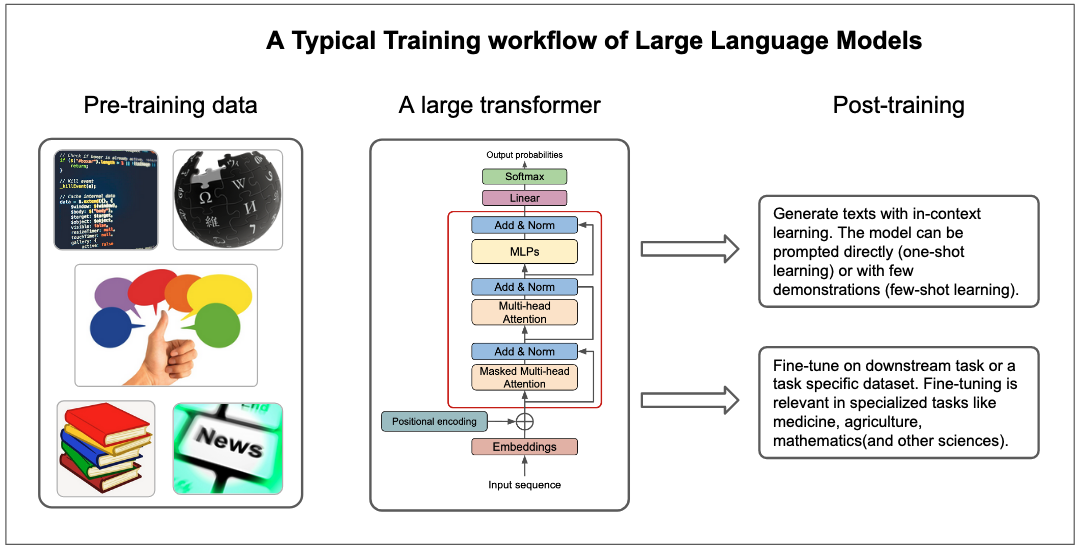


Figure 18: A typical training workflow of large language models. LLMs are typically trained on large unlabelled dataset. After, they can be used directly via prompt engineering or they can be fine-tuned further on specialized tasks.

However, training models on unlabelled data requires the clever implementation of training objectives since there is no ground truth for reference. Most LLMs, therefore, utilize the next-token prediction (NTP) as a common training objective. In essence, the LLMs are taught to accurately predict the next token in a sequence, gradually enhancing their understanding and generating capabilities. Another commonly used training objective is [masked language modelling(MLM)](https://huggingface.co/docs/transformers/main/tasks/masked_language_modeling). Masked language models are trained to predict a masked token in a sequence. This objective was popularized by BERT([Devlin et al., 2018](https://arxiv.org/abs/1810.04805)).

After pretraining phase, the models can be used to generate texts via techniques like zero-shot learning or few-shots learning. In zero-shot learning, a model is prompted to perform a task(or answer a given question) without any demontrations of how the task is done. In few-shots learning, a model is given a number of demonstrations of how the task is done before it can be asked to perform that task. Zero-shot learning and few-shot learning are examples of [in-context learning](https://en.wikipedia.org/wiki/Few-shot_learning_(natural_language_processing)). In-context learning(ICL) refers to the ability of LLMs to generate coherent texts using semantic prior knowledge([Wei et al., 2023](https://arxiv.org/abs/2303.03846)) and without any parameter updates([Akyurek et al., 2023](https://arxiv.org/abs/2211.15661)). Prompting large language models(also known as [prompt engineering](https://en.wikipedia.org/wiki/Prompt_engineering)) is a relatively new field itself and there are other prompt engineering techniques such as chain of thoughts(CoT)([Wei et al., 2022](https://arxiv.org/abs/2201.11903)).

In-context learning tends to excel at tasks that are considered simple but falls short for tasks that can not be described easily in prompts. Complex tasks requires more than clever prompts. In the words of Karpathy, “reaching top tier performance(on complex tasks) will include finetuning, especially in applications with concrete well-defined tasks where it is possible to collect a lot of data and”practice” on it.”[[7]](#footnote-136). Thus, for LLMs to get good performance on specialized tasks like mathematics, medicine, scientific fields(like chemistry), people typically finetune base LLMs on downstream datasets. We will see examples of this in the section of vertical LLMs.

Now that we’ve briefly introduced Large Language Models (LLMs), it’s time to examine some of the most popular LLMs, focusing specifically on their design choices: whether they function as encoders, decoders, or employ a combined encoder-decoder architecture.

## Encoder, Decoder, Encoder-decoder LLMs

The standard transformer model has encoder-decoder and this has to do with the task it was meant to perform which is machine translation where you have to process both input sentence and its target translation. Since the transformer, AI research community came up with different variations of the architecture for different tasks. Depending on the task, some transformer models maintained encoder-decoder structure, some used decoder only or encoder only. Let’s start with the latter.

### Encoder-only LLMs

Encoder-only LLMs use the encoder part of the standard transformer model. Encoder-only LLMs are typically used for NLP discriminative tasks such as text classification and sentiment analysis.

BERT([Devlin et al., 2018](https://arxiv.org/abs/1810.04805)) is one of most popular encoder-only language models. BERT is one of the earliest works that showed that you can pretrain a transformer(encoder) on large unlabeled text dataset and finetune the same architecture on various downstream tasks with additional task-specific head. The pretraining objectives for BERT was masked language modelling(MLM) and next sentence prediction(NSP)[[8]](#footnote-139). With masked language modeling, we mask a given percentage(15% as noted in the paper) of input tokens and the goal is to predict the masked tokens. In next sentence prediction, for two sentences making up the input sequence, the goal is to predict whether or not two sentences are in a correct order at random.

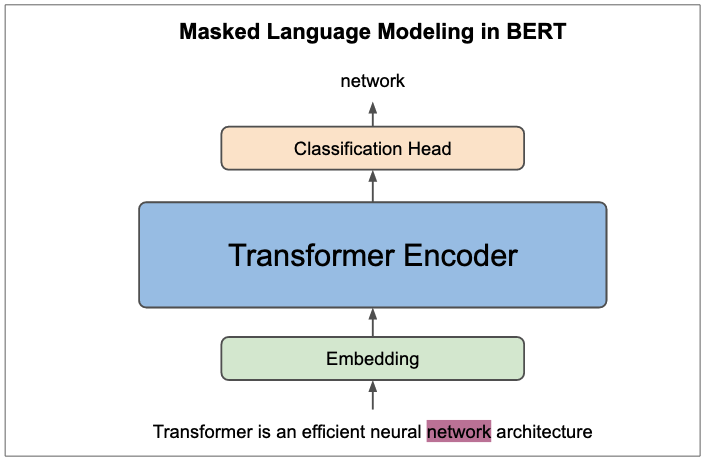


Figure 19: Masked language modelling(MLM) in BERT. In the sentence example shown in the figure, the objective of training BERT is to predict the masked word “network”. In next sentence prediction objective, the workflow is roughly the same but instead of predicting the masked tokens, we predict if two sentence pairs separated by SEP token are in correct order.

BERT is a truly revolutionary technique that improved SOTA on ubiquitous number of NLP downstrea tasks. It also inspired other efficient bidirectional architectures for NLP pretraining such as RoBERTa([Liu et al., 2019](https://arxiv.org/abs/1907.11692)) standing for Robustly optimized BERT approach. One of the main design choices that RoBERTa introduces is not using next sentence prediction objective.

### Decoder-only LLMs

Decoder-only LLMs are based on the decoder part of standard transformer. In transformer architecture, decoder is highly similar to encoder except that the self-attention in decoder is masked to prevent the model to look at subsequent tokens when generating current token.

Decoder LLMs are trained with next token prediction objective[[9]](#footnote-145). As a result, they can only generate one token at time or autoregressively. Overally, decoder models are used in generative tasks.

The most popular decoder models are GPT(Generative Pretrained Transformer) models family, most notably GPT-3([B.Brown et al., 2020](https://arxiv.org/abs/2005.14165)) and GPT-4([OpenAI, 2023](https://arxiv.org/abs/2303.08774)). GPT-3 and GPT-4 are direct scale-up of the early GPT model([Radford et al., 2018](https://s3-us-west-2.amazonaws.com/openai-assets/research-covers/language-unsupervised/language_understanding_paper.pdf)). As any other large language model, GPT models are trained on massive amount of unlabelled data(in order of billions to trillions tokens). Due to the large-scale pretraining and suitable training objective, GPT models develops impressive in-context learning capabilities where they can perform a range of NLP downstream tasks without gradient updates or task-specific fine-tuning([B.Brown et al., 2020](https://arxiv.org/abs/2005.14165)). In fact, GPT models can perform tasks like text classification, summarization, question answering ***on-fly*** by just prompting the model in zero-shot or few-shot settings[[10]](#footnote-149). This remarkable feat of in-context learning has often been called “emergent abilities” of large language models([Wei et al., 2022](https://arxiv.org/abs/2206.07682)).

GPT models are not the only models based on decoder. In fact, most famous LLMs are decoders. Examples include PaLM([Chowdhery et al., 2022](https://arxiv.org/abs/2204.02311)), BLOOM([Le Scao et al., 2022](https://arxiv.org/abs/2211.05100)), Chinchilla([Hoffmann et al., 2022](https://arxiv.org/abs/2203.15556)), LLaMA([Touvron et al., 2023](https://arxiv.org/abs/2302.13971)), and many others.

### Encoder-Decoder LLMs

Encoder-decoder LLMs looks like the standard transformer. They are generally used in tasks that demands processing two sequences(i.e, input and target are both sequences) such as machine translation. Encoder-decoder style is not widely used compared to other model styles we have seen. The most famous models of this kind are T5([Raffel et al., 2019](https://arxiv.org/abs/1910.10683)), BART([Lewis et al., 2019](https://arxiv.org/abs/1910.13461)), UL2([Tay et al., 2022](https://arxiv.org/abs/2205.05131)), FlanT5([Chung et al., 2022](https://arxiv.org/abs/2210.11416)), mT5([Xue et al., 2020](https://arxiv.org/abs/2010.11934)), etc…

Encoder-decoder style is also used in multimodal learning, most notably vision-language pretraining(VLP). Works like SimVLM([Wang et al., 2021](https://arxiv.org/abs/2108.10904)) and PALI-X([Chen et al., 2023](https://arxiv.org/abs/2305.18565)) employs encoder for learning joint image and text representations and decoder for generating the output.

## Vertical LLMs

Most of LLMs that we outlined above are typically referred to as foundational LLMs. Foundational models are typically trained on massive amount of data with self-supervision and they can be fine-tuned to a wide range of downstream tasks([Bommasani et al., 2022](https://arxiv.org/abs/2108.07258)).

Vertical LLMs are a class of LLMs that are adapted to specific applications. Foundational LLMs can generalize to simple tasks like sentiment analysis but they don’t perform well on complex tasks or tasks that require a domain expertize. For example, a foundational LLM is unlikely to perform well on medical question answering task because it doesn’t have expertize in medicine. More examples: a foundational LLM is unlikely to perform well on legal question answering task because it doesn’t have expertize in law. This is also true in other fields such as finance, physics, chemistry, etc…Vertical LLMs are designed to address this issue. They are trained on a specific domain and they can perform well on tasks that require expertize in that domain. Foundational models aim to be generalists but most of the time, we care about models that can do one thing very well.

Examples of recent vertical LLMs include MedPaLM([Singhal et al., 2022](https://arxiv.org/abs/2212.13138)) and [Med-PaLM 2](https://blog.google/technology/health/ai-llm-medpalm-research-thecheckup/), ClinicalGPT([Wang et al., 2023](https://arxiv.org/abs/2306.09968)), FinGPT([Yang et al., 2023](https://arxiv.org/abs/2306.06031)), BloombergGPT([Wu et al., 2023](https://arxiv.org/abs/2303.17564)), etc…

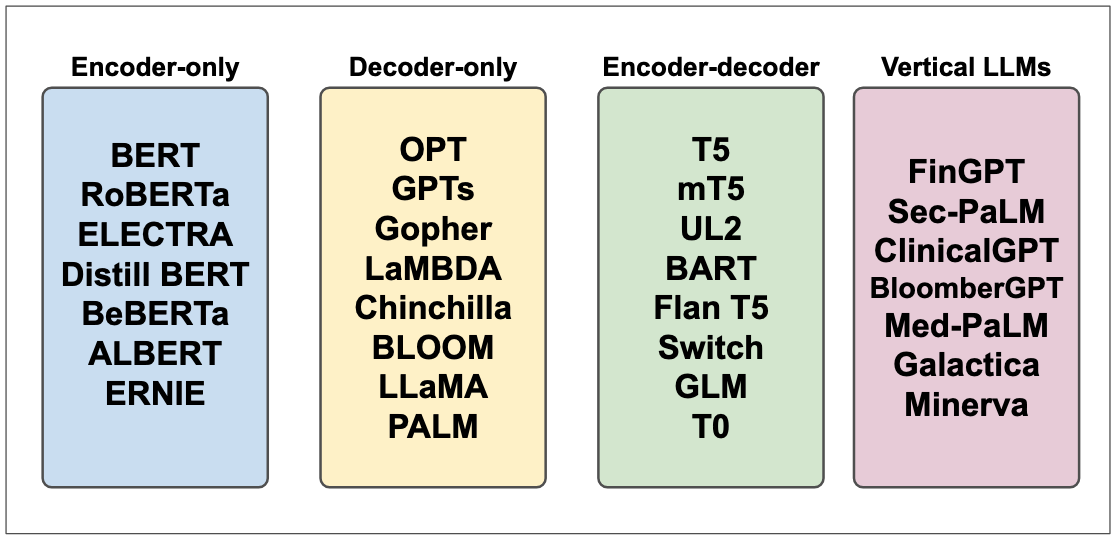


Figure 20: LLMs Topologies. Adapted from ([Yang et al., 2023](https://arxiv.org/abs/2304.13712)).

# Transformers Beyond NLP: Vision and other Modalities

Transformer was introduced for Natural Language Processing(NLP) domain, more precisely, for neural machine translation. In no time, transformers outperformed prior neural networks on most NLP tasks and quickly expanded into other modalities. In this section, we will discuss in brief the emergence of transformers in visual recognition and other modalities.

Visual recognition is one of the earliest modalities that was significantly impacted by transformers. For a long time, ConvNets were state of the arts in visual recognition. It’s thus a critical to ask why researchers care about alternatives to ConvNets. The main downside of ConvNets is their spatial [inductive biases](https://en.wikipedia.org/wiki/Inductive_bias)[[11]](#footnote-177).

One of the earliest applications of transformer to image processing is Image Transformer ([Parmar et al., 2018](https://arxiv.org/abs/1802.05751)) which approached image generation as an autoregressive problem, analogous to text generation. The Image Transformer was a standard transformer applied to a sequence of pixels, trained to generate these pixels autoregressively until it created the complete image. This was a great idea, but as it turns out, images typically have large resolutions, and thus, it was not feasible to apply self-attention to images of 256x256 for instance. There were several works attempting to apply transformer to image domain but one of the first successful works was Vision Transformer([ViT, Dosovitskiy et al., 2020](https://arxiv.org/abs/2010.11929v2)) that applied the transformer encoder to a sequence of images patches. ViT overcame the computational complexities of self-attention by image patchification idea, marking a significant step in extending transfomers to computer vision domain.

As we saw early, a huge contribution of transformers successes in NLP was unsupervised pretraining on massive amount of unlabelled data. The success of Vision Transfomer was also attributed to millions of training images, JFT-300M([Sun et al., 2017](https://arxiv.org/abs/1707.02968)) although later works like MAE([He et al., 2021](https://arxiv.org/abs/2111.06377)) and ([Steiner et al., 2021](https://arxiv.org/abs/2106.10270)) achieved resonably good performance on classical computer vision benchmarks such as ImageNet. MAE is an encoder-decoder self-supervised model that follows BERT pretraining objective of predicting randomly masked patches while the later explores clever augmentations and regularizations to train ViT. ViT has been used as backbone in many influential papers such as CLIP([Radford et al., 2021](https://arxiv.org/abs/2103.00020)), DALLE•2([Ramesh et al., 2022](https://arxiv.org/abs/2204.06125)), Stable Diffusion([Rombach et al., 2021](https://arxiv.org/abs/2112.10752)), among other recent works in visual language models. Aside from ViT enabling joint modelling of vision and language, it has also been augmented with convolutional neural networks to get both worlds in computer vision downstream tasks. Notable works of ConvNets and Vision Transformer topology are DETR([Carion et al., 2020](https://arxiv.org/abs/2005.12872)), PatchConvNet([Touvron et al., 2021](https://arxiv.org/abs/2112.13692)), MobileViT([Mehta et al., 2022](https://arxiv.org/abs/2110.02178v2)), among others.

Vision and language are two of the most important modalities when it comes to human to computer interaction and it’s not surprising that most works incorporating transformers have been in language, vision, or visual language learning. That said, transformers have been used in other modalities such as reinforcement learning([Chen at al., 2021](https://arxiv.org/abs/2106.01345)), robotics([RT1, Brohan et al., 2022](https://robotics-transformer.github.io/), [RoboCat, Bousmalis et al., 2023](https://arxiv.org/abs/2306.11706)), and speech recognition([Radford et al., 2022](https://arxiv.org/abs/2212.04356)). Finally, works such as Gato([Reed et al., 2022](https://arxiv.org/abs/2205.06175)) and ImageBind([Girdhar et al., 2023](https://arxiv.org/abs/2305.05665)) have gone further in modelling pretty much all modalities.

Transformer has established itself as universal architecture and recent works across different modalities prove that, but there are still challenges.

# Transformer: Current Challenges and Future Directions

## Efficient Transformers

Transformer has shown significant performance across various modalities such as language, vision, robotics, and reinforcement learning. Transformer neural network architecture has a set of traits that make it a suitable architecture for those domains: it is expressive, plays well with current optimization techniques, and it can be parallized. From those traits, one can say that transformer is an efficient architecture. That said however, the efficiency of transformer comes with enormous computatation cost due to the quadratic time and memory complexity of self-attention. The compute requirements of transformer has limited its scalability and its applications in low-budget devices such as smartphones and microcontrollers.

Model efficiency is an important thing to take into account when developing and deploying machine learning systems because how a model perform during inference can affects user experience([Dehghani et al., 2022](https://arxiv.org/abs/2110.12894)). There has been zillion transformer models that claim to improve the efficiency(memory footprint and computational cost) of transformer architecture(those models are typically called ***“xformers”***) but those models usually tend to be targeted at one particular benchmark or device. Most of the new ***xformers*** models that claim to reduce the quadratic time and memory complexity of self-attention are much slower than vanilla Transformer and they are rarely used in practice and they don’t have the universality of original Transformer([Tay et al., 2022](https://arxiv.org/abs/2009.06732)).

As ([Tay et al., 2022](https://arxiv.org/abs/2009.06732)) puts it nicely in a survey of “Efficient Transformers”, *the ideal xformer should yes reduce the quadratic time complexity of self-attention, but should stay universal and perform well across all tasks and modalities. It should also not trade-off speed for memory, should not be hard-engineered, should stay elegant and simple.* For more, I recommend you read the survey paper of [efficient transformers](https://arxiv.org/abs/2009.06732).

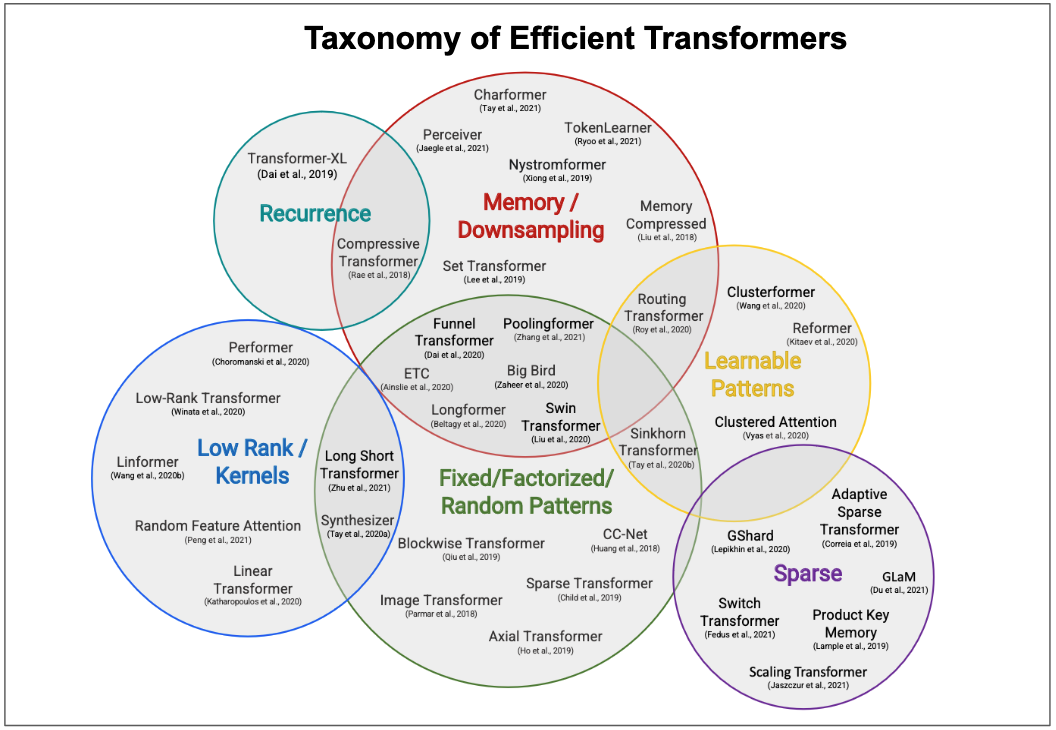


Figure 21: A taxonomy of efficient transformers. Image from ([Tay et al., 2022](https://arxiv.org/abs/2009.06732)).

Virtually all modified transformer models compute the approximation of attention to reduce the cost down. As opposed to those approaches, there is actually one kind of attention that computes exact standard attention values but way faster. That approach is FlashAttention([Dao et al., 2022](https://arxiv.org/abs/2205.14135)) and we will talk about it on a high-level.

Flash Attention is fast and memory-efficient algorithm that computes the exact attention. Flash Attention is 2-4x faster than standard attention. It achieves this enormous increase in compute efficiency by using two main techniques: tiling and recomputation. Tiling happens in forward pass and it involves splitting large matrices in attention(K key and V value) into blocks. Rather than computing attention over entire matrices, flash attention computes it over blocks and concatenate the resulting blocks saving a huge amount of memory. Recomputation happens in backward pass and it basically means recomputing the attention matrix rather than storing it in forward. The idea of flash attention boils down to improving the memory and not decreasing computations because modern GPUs have high theorical FLOPs(Floaping Point Operations, means you want to max that out) but limited memory[[12]](#footnote-201)(means any saving in memory can improve the training speed). HBM is typically large but it is not faster than on-chip SRAM(Static Random Access Memory) and thus, the computations over blocks(of K and V) happens in SRAM(because it is faster) but all full matrices are stored in HBM(because it’s big). This high-level explanation is probably oversimplication provided that Flash Attention is implemented at the GPU level(with CUDA software) and this is in fact the reason why it is IO aware but hopefully that explain what’s going on in this fast algorithm.

Below image shows the memory hierarchy in GPU, Flash Attention algorithm, and amount of time(in ms) taken by each intermediate step in GPT-2 attention versus Flash Attention. Ideally, we would want the bulk of computations to be taken by matrix multiplication(matmul) operations but surprisingly, dropout, softmax, and mask(i.e, GPT-2 is decoder model) end up taking the whole runtime in GPT-2 attention because they are computed over full matrices. Matmuls take less runtime than those other operations because GPUs are exactly designed to be fast at matrix multiplications(they have really high theorical FLOPs and maximizing FLOPs usage doesn’t reduce the runtime). By using tiling and recomputation techniques, the compute time of Flash Attention is significantly low compared to standard attention as you can see below.

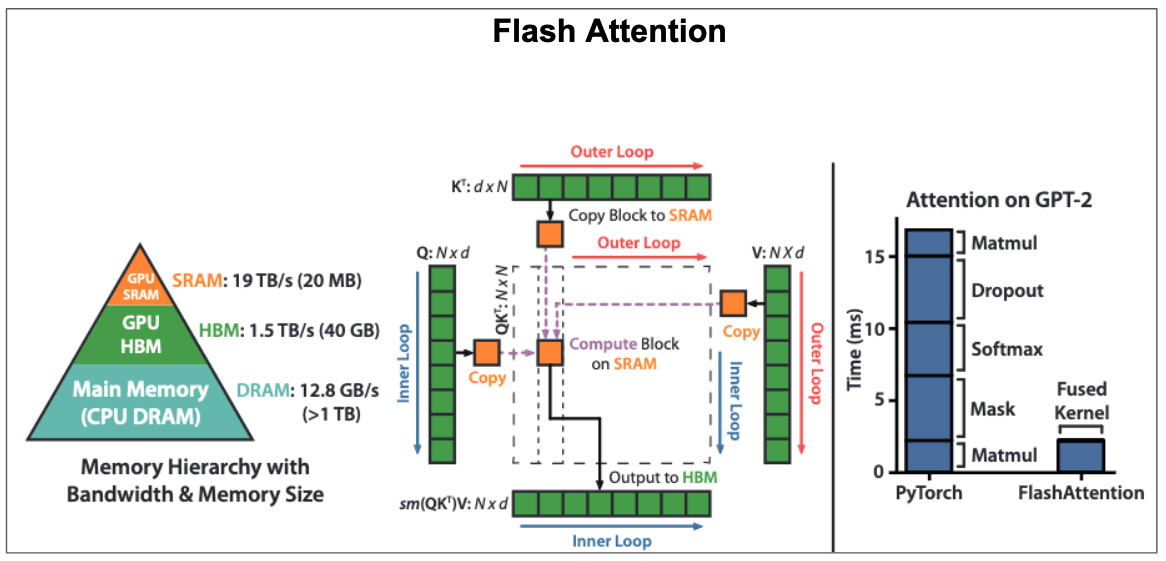


Figure 22: The memory hierachy in GPU, Flash Attention algorithm, and runtime of GPT-2 attention vs Flash Attention.

Flash Attention is intergrated in PyTorch 2.0, Hugging Face transformers, Microsoft’s DeepSpeed, MosaicML composer library and [many other library](https://github.com/Dao-AILab/flash-attention/blob/main/usage.md). You can learn more flash attention in the paper, or watch this video by core author, and the release blogpost. At the time of writing this section, Flash Attention 2([Dao et al., 2023](https://arxiv.org/abs/1911.02150)) was also released and it is even faster than Flash Attention version 1 on several orders of magnitude. Flash Attention-2 improves parallelism by parallelizing over sequence length dimension instead of batch size and number of attention heads and splits Q(query) matrix instead of K and V. This [release blog post](https://crfm.stanford.edu/2023/07/17/flash2.html) explains well what Flash Attention 2 brings to the tensor table.

## Transformers with Effective Long Contexts

Handling long context length is one of the main active area of research in Transformer large models. As direct consequence of the quadratic time and memory complexity of attention, transformer fails to process long context windows. Researching techniques that extend the context window of transformer architecture is an important thing since context window determines the amount of information that you can fit in transformer memory during inference. Tasks like long conversations, summarizing long documents, and executing long-term planning may require models that support long context windows([Chen et al., 2023](https://arxiv.org/abs/2306.15595)).

Alot have been written about context windows and extending them such as ([Sun et al., 2021](https://arxiv.org/abs/2109.09115)), ([Chen et al., 2023](https://arxiv.org/abs/2306.15595)), but I want to highlight a recent paper that presents remarkable findings around long contexts. Recents language models(based on transformer) can takes longer contexts but it’s not clear whether context actually helps. As shown by ([F.Liu et al., 2023](https://arxiv.org/abs/2307.03172)), the performance of language models degrades with increase in input context length. So, even for models that have extended context length, their performance still degrades for longer input contexts. Also, the work also found that language models perform well when the relevant information are placed at the beginning or the end of the input context and significantly degrades when the relevant information are placed in the middle, suggesting that language models are U-shaped reasoners.

The findings highlighted above are appealing and provide broad implications that could be applicable in the design of fine-tuning datasets and during in-context learning, but it’s important to note that none of those is established understandings provided that “how transformer models perform on long context windows” is an active area of research. We hope that future transformer models will be able to operate over long input sequences and at the same time performing well regardless of relevant information are placed. This is in fact the holy grail of large language models.

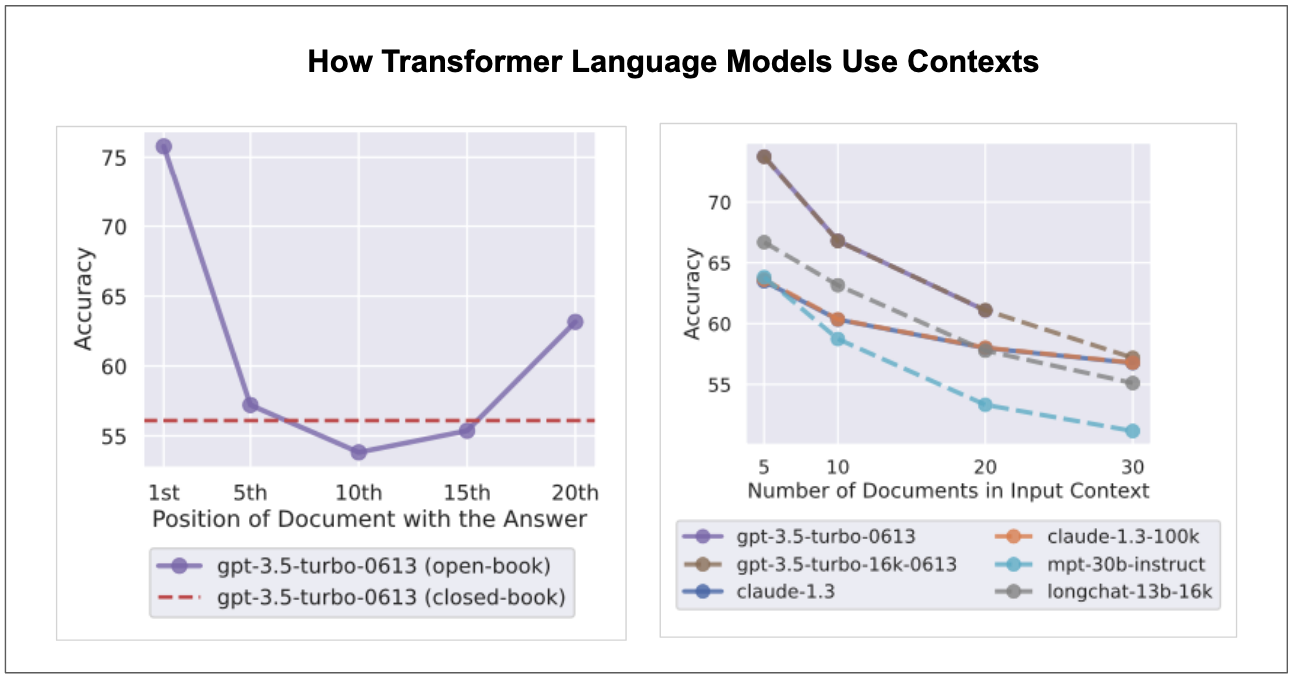


Figure 23: Language models(based on Transformer) tends to perform well when relevant information are at the beginning or at the end of input context(graph on the left) and their performance decreases for longer contexts(graph on the right). The graphs are taken from ([F.Liu et al., 2023](https://arxiv.org/abs/2307.03172)).

## Multimodal Transformer

A primary objective in neural network design is to architect a single, universal model that can efficiently process multiple modalities without necessitating modality-specific encoders or preprocessing. Indeed, transformer models have seen widespread application across various domains, spanning text, images, robotics, and speech. Yet, the goal of creating a truly universal transformer — one that performs equally effectively across all modalities without requiring specific adjustments — remains a challenge. This challenge arises from the inherent differences and complexities in data types and the transformer model itself, which frequently demand modality-specific modifications.

For instance, the process for handling text, images, and speech each have unique considerations due to their individual characteristics. Transformers excel in scenarios where data can be framed as a sequence of tokens, however, the method of transposing a particular modality into such a sequence significantly varies among different modalities. Consequently, the challenge lies in designing a singular architecture that can uniformly extract valuable insights from all data types with comparable efficiency.

The achievement of such an architecture would signify a monumental stride in the field of multimodal learning, paving the way for models that can seamlessly transition between different types of data and potentially unlocking new avenues of exploration in multimodal representation learning.

Nearly all current state-of-the-arts in multimodal learning typically uses separate tokenizer and encoder for each modality and most of them are also designed for visual language learning. This section doesn’t dive deep into the specifics of current multimodal approaches based on transformers but we provide examples for people interested in diving deep: Flamingo(visual language)([Alayrac et al., 2022](https://arxiv.org/abs/2204.14198)), Gato([Reed et al., 2022](https://arxiv.org/abs/2205.06175)), ImageBind([Girdhar et al., 2023](https://arxiv.org/abs/2305.05665)), OFA([Wang et al., 2022](https://arxiv.org/ABS/2202.03052)), Unified-IO([Lu et al., 2022](https://arxiv.org/abs/2206.08916)), Meta-Transformer([Zhang et al., 2023](https://arxiv.org/abs/2307.10802)), among others.

Virtually all transformer challenges stem from its extreme compute requirements. Truly efficient transformers such as FlashAttention will eliminate most of them.

# Open-source Implementations of Transformer

The original transformer model was implemented in Tensor2Tensor library[[13]](#footnote-222) but this was deprecated recently. The successor of of Tensor2Tensor is Trax which is based on JAX[[14]](#footnote-224).

There are many open-source implementations of Transformer model architecture. Let’s briefly talk about three of most popular implementations. HuggingFace [Transformer](https://github.com/huggingface/transformers) library([Wolf et al., 2020](https://arxiv.org/abs/1910.03771)) is arguably one of the most popular implementations of transformers. The library simplifies inference pipelines for NLP(and vision) downstream tasks and can be used to train or finetune transformer-based models. HuggingFace Transformer library is easy to use, it’s clean, and has a large community of developers and contributors. [minGPT](https://github.com/karpathy/minGPT) and [nanoGPT](https://github.com/karpathy/nanoGPT) by Andrej Karpathy are also popular implementations in open-source and research community. Furthermore, [x-transformers](https://github.com/lucidrains/x-transformers) provides concise and experimental implementations of various transformer models usually from new research papers.

Lastly, it’s unlikely you will need to implement transformer model or part of it from scratch because modern deep learning frameworks such as [PyTorch](https://pytorch.org/docs/stable/nn.html#transformer-layers), [Keras](keras.io/api/keras_nlp), and JAX(Via [Flax](https://github.com/google/flax)) provides its implementation as layers that you can import easily just like how you import convolution or linear layers.

# Suggested and Supplementary Resources

This article adds to existing pool of knowledge surrounding the understanding of transformer neural network architecture. Therefore, it would be remiss not to highlight some invaluable resources on Transformer architecture, which we will briefly explore below:

* The Annotated Transformer: This is one of the best and practical resources. It provides line-by-line implementation of transformer architecture with completely usable code. The [original version](https://nlp.seas.harvard.edu/2018/04/03/attention.html) was written by Sasha Rush and [recent version](http://nlp.seas.harvard.edu/annotated-transformer/) was written by Austin Huang and his colleagues.
* Let’s Build GPT from Scratch by Andrej Karpathy: This is arguably the best resource regarding implementations of transformer, most notably, GPT(Generative Pre-training Transformer). Karpathy builds and trains entire GPT from scratch, providing a decent explanation of every step along the way. Here is a [lecture video](https://www.youtube.com/watch?v=kCc8FmEb1nY&list=PLAqhIrjkxbuWI23v9cThsA9GvCAUhRvKZ&index=7&t=1939s) and [accompanying code repository(nanoGPT)](https://github.com/karpathy/nanoGPT/tree/master).
* [Stanford CS25: Transformers United V2](https://web.stanford.edu/class/cs25/) aims at examining how transformers work and how they are applied in different fields from NLP, CV, biology to robotics and more. This course contains excellent talks from researchers. The [introductory class](https://www.youtube.com/watch?v=XfpMkf4rD6E) of recent version of the course delves into transformer architecture and it is given by Karpathy, someone who deeply understands the intricacies of neural networks.
* [Formal Algorithms for Transformers](https://arxiv.org/abs/2207.09238) provides a mathematical overview and formal algorithms of various transformer architectures.
* [Transformer Taxonomy](https://kipp.ly/transformer-taxonomy/) provides an excellent literature review of transformer models, architectural changes since the inception of standard transformer, post pre-training techniques and 3 training techniques.
* The Illustrated Transformer is a remarkable [blog post](https://jalammar.github.io/illustrated-transformer/) that break the transformer model apart and explains each part intuitively.
* Transformer and attention blog series by Lilian Weng also provide excellent understanding of transformer and attention mechanism. A notable example of relevant Lilian Weng blogs are [The Transformer Family Version](https://lilianweng.github.io/posts/2020-04-07-the-transformer-family/)(there is also [version 2](https://lilianweng.github.io/posts/2023-01-27-the-transformer-family-v2/) of this blog) and [Attention? Attention!](https://lilianweng.github.io/posts/2018-06-24-attention/).
* Attention is All You Need [Video](https://www.youtube.com/watch?v=iDulhoQ2pro) by Yannic Kilcher also walkthough the paper, explaining all the relevant concepts and related works well.

The resources provided above are not exhaustive and there are hundreds of other blogs, videos, and papers that explain the transformer well.

# Conclusion

The significance of transformer neural network architecture can not be overstated in the field of deep learning and computer science. The transformer model, initially introduced for neural machine translation has evolved into a versatile and general-purpose architecture, demonstrating impressive performance beyond natural language processing into other various modalities.

Throughout this article, we have delved into the core mechanics of the transformer and its essential components - its encoder and decoder structure, the ingenious attention mechanism, multi-head attention, MLPs, embedding, positional encoding layers, and more. We have explored several benefits of self-attention, along with potential drawbacks. Also, by examining the visualization of attention, we have gained a deeper understanding of how transformers focus on different parts of the input sequence to generate outputs.

Transformers are at the core of large language models(LLMs) which has taken the world by a storm recently. We have seen evolution of LLMs and their different design styles, and the applications of transformers beyond NLP. We have also talked their current challenges, including the need for more efficient models and the effective use of context windows. These challenges present exciting opportunities for future research and improvements.

As deep learning field continues to evolve, transformer architecture remains a foundational building block of modern machine learning systems. There are many variations of transformer architectures, but regardless of what the future of transformers holds, one thing is certain - with attention, you have everything you need. Stay curious, keep learning, and always pay attention!

# Acknowledgment

# References

Vaswani et al., [“Attention is all you need.”](https://arxiv.org/abs/1706.03762) NIPS 2017

Zhang et al., “Text understanding from scratch”, 2016

Lei Bai et al., “Layer Normalization”, 2016

Bahdanau et al.,“Neural Machine Translation by Jointly Learning to Align and Translate”, 2015

Xu et al., “Show, Attend and Tell: Neural Image Caption Generation with Visual Attention”, 2015

Graves et al., “Neural Turing Machines”, 2014

Luong et al., “Effective Approaches to Attention-based Neural Machine Translation”, 2015

Chollet, “Xception: Deep Learning with Depthwise Separable Convolutions”, 2017

He et al., “Deep Residual Learning for Image Recognition”, 2015

Ioffe and Szegedy, “Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift”, 2015

Xiong et al., “On Layer Normalization in the Transformer Architecture”, 2020

Xie et al., “ResiDual: Transformer with Dual Residual Connections”, 2023

Srivastava et al., “Dropout: A Simple Way to Prevent Neural Networks from Overfitting”, 2014

Radford et al., “Language models are unsupervised multitask learners”, 2019

Vig Jesse, “A Multiscale Visualization of Attention in the Transformer Model”, 2019

Devlin et al., “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding”, 2018

Yat et al., “Efficient Transformers: A Survey, 2022”

Yang et al., “Harnessing the Power of LLMs in Practice: A Survey on ChatGPT and Beyond”, 2023

Wei et al., “Chain-of-Thought Prompting Elicits Reasoning in Large Language Models”, 2022

Wei et al., “Larger language models do in-context learning differently”, 2023

Akyurek et al., “What learning algorithm is in-context learning? Investigations with linear models”, 2023

Liu et al., “RoBERTa: A Robustly Optimized BERT Pretraining Approach”, 2019

B. Brown et al., “Language Models are Few-Shot Learners”, 2020

OpenAI, “GPT-4 Technical Report”, 2023

Radford et al., “Improving Language Understanding by Generative Pre-Training”, 2018

Wei et al., “Emergent Abilities of Large Language Models”, 2022

Chowdhery et al., “PaLM: Scaling Language Modeling with Pathways”, 2022

Le Scao et al., “BLOOM: A 176B-Parameter Open-Access Multilingual Language Model”, 2022

Hoffmann et al., “Training Compute-Optimal Large Language Models”, 2022

Touvron et al., “LLaMA: Open and Efficient Foundation Language Models”, 2023

Raffel et al., “Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer”, 2019

Lewis et al., “BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension”, 2019

Tay et al., “UL2: Unifying Language Learning Paradigms”, 2022

Chung et al., “Scaling Instruction-Finetuned Language Models”, 2022

Xue et al., “mT5: A massively multilingual pre-trained text-to-text transformer”, 2020

Wang et al., “SimVLM: Simple Visual Language Model Pretraining with Weak Supervision”, 2021

Chen et al., “PaLI-X: On Scaling up a Multilingual Vision and Language Model”, 2023

Bommasani et al., “On the Opportunities and Risks of Foundation Models”, 2022

Singhal et al., “Large Language Models Encode Clinical Knowledge”, 2022

Wang et al., “ClinicalGPT: Large Language Models Finetuned with Diverse Medical Data and Comprehensive Evaluation”, 2023

Yang et al., “FinGPT: Open-Source Financial Large Language Models”, 2023

Wu et al., “BloombergGPT: A Large Language Model for Finance”, 2023

Parmar et al., “Image Transformer”, 2018

Dosovitskiy et al., “An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale”, 2020

Sun et al., “Revisiting Unreasonable Effectiveness of Data in Deep Learning Era”, 2017

He et al., “Masked Autoencoders Are Scalable Vision Learners”, 2021

Steiner et al., “How to train your ViT? Data, Augmentation, and Regularization in Vision Transformers”, 2021

Radford et al., “Learning Transferable Visual Models From Natural Language Supervision”, 2021

Ramesh et al., “Hierarchical Text-Conditional Image Generation with CLIP Latents”, 2022

Rombach et al., “High-Resolution Image Synthesis with Latent Diffusion Models”, 2021

Carion et al., “End-to-End Object Detection with Transformers”, 2020

Touvron et al., “Augmenting Convolutional networks with attention-based aggregation”, 2021

Mehta et al., “MobileViT: Light-weight, General-purpose, and Mobile-friendly Vision Transformer”, 2022

Chen at al., “Decision Transformer: Reinforcement Learning via Sequence Modeling”, 2021

Brohan et al., “RT-1: Robotics Transformer”, 2022

RoboCat, “RoboCat: A Self-Improving Foundation Agent for Robotic Manipulation”, Bousmalis et al., 2023

Radford et al., “Robust Speech Recognition via Large-Scale Weak Supervision”, 2022

Reed et al., “A Generalist Agent”, 2022

Girdhar et al., “ImageBind: One Embedding Space To Bind Them All”, 2023

Dehghani et al., “The Efficiency Misnomer”, 2022

Tay et al., “Efficient Transformers: A Survey”, 2022

Wolf et al., “HuggingFace’s Transformers: State-of-the-art Natural Language Processing”, 2020

Dao et al., “FlashAttention: Fast and Memory-Efficient Exact Attention with IO-Awareness”, 2022

Dao et al., “FlashAttention-2: Faster Attention with Better Parallelism and Work Partitioning”, 2023

Chen et al., “Extending Context Window of Large Language Models via Positional Interpolation”, 2023

Sun et al., “Do Long-Range Language Models Actually Use Long-Range Context?”, 2021

F.Liu et al., “Lost in the Middle: How Language Models Use Long Contexts”, 2023

Alayrac et al., “Flamingo: a Visual Language Model for Few-Shot Learning” 2022

Wang et al., “OFA: Unifying Architectures, Tasks, and Modalities Through a Simple Sequence-to-Sequence Learning Framework”, 2022

Lu et al., “Unified-IO: A Unified Model for Vision, Language, and Multi-Modal Tasks”, 2022

Zhang et al., “Meta-Transformer: A Unified Framework for Multimodal Learning”, 2023

1. Example adapted from Deep Learning with Python by Francois Chollet [↑](#footnote-ref-61)
2. In the transformer paper, MLPs are what referred to as feed-forward networks(FFNs). I find the terminology of FFNs confusing sometime. MLPs are feed-forward networks but not the other way around. [↑](#footnote-ref-78)
3. If you want to see how embeddings look like and how words with same semantic meaning tend to be closer to each other, you can play with [Embedding Projector](http://projector.tensorflow.org/) [↑](#footnote-ref-83)
4. The core operation in attention is the dot product between query and keys, which, being a summation operation, is permutation invariant [↑](#footnote-ref-85)
5. Hat tip to Sebastian Raschka for sharing this in his [newsletter](https://magazine.sebastianraschka.com/) [↑](#footnote-ref-93)
6. BertViz be accessed at https://github.com/jessevig/bertviz [↑](#footnote-ref-110)
7. Karpathy said that in a Twitter thread. Available here: <https://twitter.com/karpathy/status/1655994367033884672?s=20> [↑](#footnote-ref-136)
8. Next sentence prediction in BERT and next token prediction in standard transformer are different. The idea is roughly similar, but the former is usually for discriminative modelling while the later is for auto-regressive generative modelling [↑](#footnote-ref-139)
9. Next token prediction in decoder LLMs is different to next sentence prediction in BERT. The former operates on token level while the later operates on sentence level [↑](#footnote-ref-145)
10. It’s fair to say that GPT-3 popularized prompt engineering. [↑](#footnote-ref-149)
11. The inductive biases in ConvNets are the results of their translation invariance. Convolution itself is translation equivariance(changing the position of pixels changes the output) but pooling which is often used after convolution is translation invariant(changing the position of pixels doesn’t change the output) and this make the overall ConvNets translation invariant architecture [↑](#footnote-ref-177)
12. GPU main memory is called HBM which stands for High Bandwidth Memory [↑](#footnote-ref-201)
13. Available at <https://github.com/tensorflow/tensor2tensor> [↑](#footnote-ref-222)
14. Available at <https://github.com/google/trax> [↑](#footnote-ref-224)