

# CS 224N: Assignment 5: Self-Attention, Transformers, and Pretraining

**Note.** Here are some things to keep in mind as you plan your time for this assignment.

- There are math questions again!
- The total amount of PyTorch code to write, and code complexity, of this assignment is lower than Assignment 4. However, you're also given less guidance or scaffolding in how to write the code.
- This assignment involves a pretraining step that takes approximately 2 hours to perform on Azure, and you'll have to do it twice. Colab set-up notebook has been provided similar to Assignment 4. The 2 hour timeline is an upper bound on the training time assuming older/slower GPU. On faster GPUs, the pretraining can finish in around 30-40 minutes.

This assignment is an investigation into Transformer self-attention building blocks, and the effects of pre-training. It covers mathematical properties of Transformers and self-attention through written questions. Further, you'll get experience with practical system-building through repurposing an existing codebase. The assignment is split into a written (mathematical) part and a coding part, with its own written questions. Here's a quick summary:

1. **Mathematical exploration:** What kinds of operations can self-attention easily implement? Why should we use fancier things like multi-headed self-attention? This section will use some mathematical investigations to illuminate a few of the motivations of self-attention and Transformer networks. **Note:** for all questions, you should justify your answer with mathematical reasoning when required.
2. **Extending a research codebase:** In this portion of the assignment, you'll get some experience and intuition for a cutting-edge research topic in NLP: teaching NLP models facts about the world through pretraining, and accessing that knowledge through finetuning. You'll train a Transformer model to attempt to answer simple questions of the form "Where was person [x] born?" – without providing any input text from which to draw the answer. You'll find that models are able to learn some facts about where people were born through pretraining, and access that information during fine-tuning to answer the questions.

Then, you'll take a harder look at the system you built, and reason about the implications and concerns about relying on such implicit pretrained knowledge.

This assignment was originally created by John Hewitt, CS 224N Head TA in Winter 2021.

## 1. Attention exploration (20 points)

Multi-head self-attention is the core modeling component of Transformers. In this question, we'll get some practice working with the self-attention equations, and motivate why multi-headed self-attention can be preferable to single-headed self-attention.

Recall that attention can be viewed as an operation on a *query* vector  $q \in \mathbb{R}^d$ , a set of *value* vectors  $\{v_1, \dots, v_n\}, v_i \in \mathbb{R}^d$ , and a set of *key* vectors  $\{k_1, \dots, k_n\}, k_i \in \mathbb{R}^d$ , specified as follows:

$$c = \sum_{i=1}^n v_i \alpha_i \quad (1)$$

$$\alpha_i = \frac{\exp(k_i^\top q)}{\sum_{j=1}^n \exp(k_j^\top q)} \quad (2)$$

with  $\alpha = \{\alpha_1, \dots, \alpha_n\}$  termed the “attention weights”. Observe that the output  $c \in \mathbb{R}^d$  is an average over the value vectors weighted with respect to  $\alpha$ .

- (a) (5 points) **Copying in attention.** One advantage of attention is that it's particularly easy to “copy” a value vector to the output  $c$ . In this problem, we'll motivate why this is the case.

- i. (1 point) **Explain** why  $\alpha$  can be interpreted as a categorical probability distribution.

**Answer:**  $\alpha$  can be interpreted as a categorical probability distribution because it is equivalent to a classification problem in machine learning. Both have a softmax output which is a probability distribution. Unlike a classification problem, where the probability distribution is over the number of classes to predict, the attention weights are a probability distribution over the tokens in the embedding inputs.

- ii. (2 points) The distribution  $\alpha$  is typically relatively “diffuse”; the probability mass is spread out between many different  $\alpha_i$ . However, this is not always the case. **Describe** (in one sentence) under what conditions the categorical distribution  $\alpha$  puts almost all of its weight on some  $\alpha_j$ , where  $j \in \{1, \dots, n\}$  (i.e.  $\alpha_j \gg \sum_{i \neq j} \alpha_i$ ). What must be true about the query  $q$  and/or the keys  $\{k_1, \dots, k_n\}$ ?

**Answer:** Mathematically, it must be true that the dot product of  $k_j$  and  $q$  is very large and therefore the most directionally similar vs. the dot products of the other keys and the query vector.

$$k_j^T q \gg k_i^T q \text{ where } i = 1..n, i \neq j \quad (3)$$

- iii. (1 point) Under the conditions you gave in (ii), **describe** the output  $c$ .

**Answer:** The output of  $c$  is a weighted average of the key vectors and their respective attention weights, which given the conditions specified in (ii), thus we can expect

$$c \approx v_j \alpha_j \quad (4)$$

- iv. (1 point) **Explain** (in two sentences or fewer) what your answer to (ii) and (iii) means intuitively.

**Answer:** Intuitively, the answer in (ii) means that one specific word in the sentence is getting a significant amount of attention, like in Question/Answering, where the word in the sentence is the date or in Named Entity Recognition where the word is a location. Intuitively, the answer in (iii) means that there will be a strong association between query and  $v_j$ .

- (b) (7 points) **An average of two.** Instead of focusing on just one vector  $v_j$ , a Transformer model might want to incorporate information from *multiple* source vectors. Consider the case where we instead want to incorporate information from **two** vectors  $v_a$  and  $v_b$ , with corresponding key vectors  $k_a$  and  $k_b$ .

- i. (3 points) How should we combine two  $d$ -dimensional vectors  $v_a, v_b$  into one output vector  $c$  in a way that preserves information from both vectors? In machine learning, one common way to do so is to take the average:  $c = \frac{1}{2}(v_a + v_b)$ . It might seem hard to extract information about the original vectors  $v_a$  and  $v_b$  from the resulting  $c$ , but under certain conditions one can do so. In this problem, we'll see why this is the case.

Suppose that although we don't know  $v_a$  or  $v_b$ , we do know that  $v_a$  lies in a subspace  $A$  formed by the  $m$  basis vectors  $\{a_1, a_2, \dots, a_m\}$ , while  $v_b$  lies in a subspace  $B$  formed by the  $p$  basis vectors  $\{b_1, b_2, \dots, b_p\}$ . (This means that any  $v_a$  can be expressed as a linear combination of its basis vectors, as can  $v_b$ . All basis vectors have norm 1 and are orthogonal to each other.) Additionally, suppose that the two subspaces are orthogonal; i.e.  $a_j^\top b_k = 0$  for all  $j, k$ .

Using the basis vectors  $\{a_1, a_2, \dots, a_m\}$ , construct a matrix  $M$  such that for arbitrary vectors  $v_a \in A$  and  $v_b \in B$ , we can use  $M$  to extract  $v_a$  from the sum vector  $s = v_a + v_b$ . In other words, we want to construct  $M$  such that for any  $v_a, v_b$ ,  $Ms = v_a$ . Show that  $Ms = v_a$  holds for your  $M$ .

**Hint:** Given that the vectors  $\{a_1, a_2, \dots, a_m\}$  are both *orthogonal* and *form a basis* for  $v_a$ , we know that there exist some  $c_1, c_2, \dots, c_m$  such that  $v_a = c_1 a_1 + c_2 a_2 + \dots + c_m a_m$ . Can you create a vector of these weights  $c$ ?

**Answer:** Suppose  $M = [a_1, a_2, \dots, a_m]^2$ .

$$Ms = [a_1, a_2, \dots, a_m]^2 s \quad (5)$$

$$= [a_1, a_2, \dots, a_m]([a_1, a_2, \dots, a_m]v_a + [a_1, a_2, \dots, a_m]v_b) \quad (6)$$

$$= [a_1, a_2, \dots, a_m]([a_1, a_2, \dots, a_m][c_1 a_1 + c_2 a_2 + \dots + c_m a_m] + [a_1, a_2, \dots, a_m][d_1 b_1 + d_2 b_2 + \dots + d_m b_m]) \quad (7)$$

$$= [a_1, a_2, \dots, a_m][c_1, c_2, \dots, c_m]^T + 0 \quad (8)$$

$$= v_a \quad (9)$$

- ii. (4 points) As before, let  $v_a$  and  $v_b$  be two value vectors corresponding to key vectors  $k_a$  and  $k_b$ , respectively. Assume that (1) all key vectors are orthogonal, so  $k_i^\top k_j = 0$  for all  $i \neq j$ ; and (2) all key vectors have norm 1.<sup>1</sup> **Find an expression** for a query vector  $q$  such that  $c \approx \frac{1}{2}(v_a + v_b)$ , and justify your answer.<sup>2</sup>

**Answer:**  $c \approx \frac{1}{2}(v_a + v_b)$  implies  $\alpha_a \approx \frac{1}{2}$  and  $\alpha_b \approx \frac{1}{2}$  and  $\alpha_{i \notin \{a, b\}} \approx 0$

$$\alpha_a = \frac{\exp(k_a^\top q)}{\sum_{j=1}^n \exp(k_j^\top q)} = \frac{\exp(k_a^\top q)}{\exp(k_a^\top q) + \exp(k_b^\top q)} \approx \frac{1}{2} \quad (10)$$

$$2 \exp(k_a^\top q) = \exp(k_a^\top q) + \exp(k_b^\top q) \quad (11)$$

$$\log \exp(k_a^\top q)^2 = \log \exp(k_a^\top q) + \log \exp(k_b^\top q) \quad (12)$$

<sup>1</sup>Recall that a vector  $x$  has norm 1 iff  $x^\top x = 1$ .

<sup>2</sup>Hint: while the softmax function will never *exactly* average the two vectors, you can get close by using a large scalar multiple in the expression.

$$(k_a^T q)^2 = k_a^T q + k_b^T q \quad (13)$$

$$(k_a^T k_a) q = k_a + k_b \quad (14)$$

$$q = \frac{1}{(k_a^T k_a)} (k_a + k_b) = \frac{1}{\|k_a\|_2^2} (k_a + k_b) \quad (15)$$

$$q = k_a + k_b \quad (16)$$

- (c) (5 points) **Drawbacks of single-headed attention:** In the previous part, we saw how it was *possible* for a single-headed attention to focus equally on two values. The same concept could easily be extended to any subset of values. In this question we'll see why it's not a *practical* solution. Consider a set of key vectors  $\{k_1, \dots, k_n\}$  that are now randomly sampled,  $k_i \sim \mathcal{N}(\mu_i, \Sigma_i)$ , where the means  $\mu_i \in \mathbb{R}^d$  are known to you, but the covariances  $\Sigma_i$  are unknown. Further, assume that the means  $\mu_i$  are all perpendicular;  $\mu_i^\top \mu_j = 0$  if  $i \neq j$ , and unit norm,  $\|\mu_i\| = 1$ .

- i. (2 points) Assume that the covariance matrices are  $\Sigma_i = \alpha I, \forall i \in \{1, 2, \dots, n\}$ , for vanishingly small  $\alpha$ . Design a query  $q$  in terms of the  $\mu_i$  such that as before,  $c \approx \frac{1}{2}(v_a + v_b)$ , and provide a brief argument as to why it works.

**Answer:** It works because we're effectively introducing random noise as Gaussian distributions, where the covariance is vanishingly small.

$$q = \mathcal{N}(\mu_a + \mu_b, \alpha I) \quad (17)$$

- ii. (3 points) Though single-headed attention is resistant to small perturbations in the keys, some types of larger perturbations may pose a bigger issue. Specifically, in some cases, one key vector  $k_a$  may be larger or smaller in norm than the others, while still pointing in the same direction as  $\mu_a$ . As an example, let us consider a covariance for item  $a$  as  $\Sigma_a = \alpha I + \frac{1}{2}(\mu_a \mu_a^\top)$  for vanishingly small  $\alpha$  (as shown in figure 1). This causes  $k_a$  to point in roughly the same direction as  $\mu_a$ , but with large variances in magnitude. Further, let  $\Sigma_i = \alpha I$  for all  $i \neq a$ .

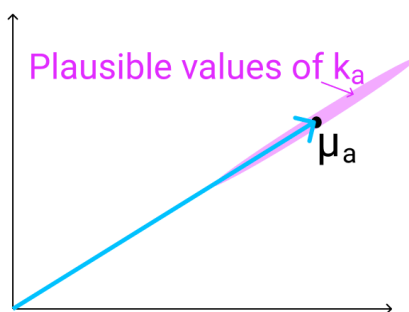


Figure 1: The vector  $\mu_a$  (shown here in 2D as an example), with the range of possible values of  $k_a$  shown in red. As mentioned previously,  $k_a$  points in roughly the same direction as  $\mu_a$ , but may have larger or smaller magnitude.

When you sample  $\{k_1, \dots, k_n\}$  multiple times, and use the  $q$  vector that you defined in part i., what do you expect the vector  $c$  will look like qualitatively for different samples? Think about how it differs from part (i) and how  $c$ 's variance would be affected.

**Answer:** Qualitatively,  $c$  will be more approximate to the key vectors with larger norms.

$$c \approx \frac{\exp(\mu_a q)}{\exp(\mu_a q) + \exp(\mu_b q)} v_a + \frac{\exp(\mu_b q)}{\exp(\mu_a q) + \exp(\mu_b q)} v_b \quad (18)$$

$$\approx \frac{1}{1 + \exp(\mu_b q - \mu_a q)} v_a + \frac{1}{\exp(\mu_a q - \mu_b q) + 1} v_b \quad (19)$$

$$\approx \frac{1}{1 + \exp(\mu_b^T \mu_b - \mu_a^T \mu_a)} v_a + \frac{1}{\exp(\mu_a^T \mu_a - \mu_b^T \mu_b) + 1} v_b \quad (20)$$

- (d) (3 points) **Benefits of multi-headed attention:** Now we'll see some of the power of multi-headed attention. We'll consider a simple version of multi-headed attention which is identical to single-headed self-attention as we've presented it in this homework, except two query vectors ( $q_1$  and  $q_2$ ) are defined, which leads to a pair of vectors ( $c_1$  and  $c_2$ ), each the output of single-headed attention given its respective query vector. The final output of the multi-headed attention is their average,  $\frac{1}{2}(c_1 + c_2)$ . As in question 1(c), consider a set of key vectors  $\{k_1, \dots, k_n\}$  that are randomly sampled,  $k_i \sim \mathcal{N}(\mu_i, \Sigma_i)$ , where the means  $\mu_i$  are known to you, but the covariances  $\Sigma_i$  are unknown. Also as before, assume that the means  $\mu_i$  are mutually orthogonal;  $\mu_i^\top \mu_j = 0$  if  $i \neq j$ , and unit norm,  $\|\mu_i\| = 1$ .

- i. (1 point) Assume that the covariance matrices are  $\Sigma_i = \alpha I$ , for vanishingly small  $\alpha$ . Design  $q_1$  and  $q_2$  such that  $c$  is approximately equal to  $\frac{1}{2}(v_a + v_b)$ . Note that  $q_1$  and  $q_2$  should have different expressions.

**Answer:**

$$q_a = \mu_a \quad (21)$$

$$q_b = \mu_b \quad (22)$$

- ii. (2 points) Assume that the covariance matrices are  $\Sigma_a = \alpha I + \frac{1}{2}(\mu_a \mu_a^\top)$  for vanishingly small  $\alpha$ , and  $\Sigma_i = \alpha I$  for all  $i \neq a$ . Take the query vectors  $q_1$  and  $q_2$  that you designed in part i. What, qualitatively, do you expect the output  $c$  to look like across different samples of the key vectors? Explain briefly in terms of variance in  $c_1$  and  $c_2$ . You can ignore cases in which  $k_a^\top q_i < 0$ .

**Answer:**  $c_1 \approx v_a, c_2 \approx v_b$  so

$$c = \frac{1}{2}(c_1 + c_2) \approx \frac{1}{2}(v_a + v_b) \quad (23)$$

## 2. Pretrained Transformer models and knowledge access (35 points)

You'll train a Transformer to perform a task that involves accessing knowledge about the world — knowledge which isn't provided via the task's training data (at least if you want to generalize outside the training set). You'll find that it more or less fails entirely at the task. You'll then learn how to pretrain that Transformer on Wikipedia text that contains world knowledge, and find that finetuning that Transformer on the same knowledge-intensive task enables the model to access some of the knowledge learned at pretraining time. You'll find that this enables models to perform considerably above chance on a held out development set.

The code you're provided with is a fork of Andrej Karpathy's [minGPT](#). It's nicer than most research code in that it's relatively simple and transparent. The "GPT" in minGPT refers to the Transformer language model of OpenAI, originally described in [this paper](#) [2].

As in previous assignments, you will want to develop on your machine locally, then run training on Azure/Colab. You can use the same conda environment from previous assignments for local development,

and the same process for training on a GPU.<sup>3</sup> You'll need around 5 hours for training, so budget your time accordingly! We have provided a sample Colab with the the commands that require GPU training. **Note that dataset multi-processing can fail on local machines without GPU, so to debug locally, you might have to change `num_workers` to 0.**

Your work with this codebase is as follows:

- (a) (0 points) **Check out the demo.**

In the `mingpt-demo/` folder is a Jupyter notebook `play_char.ipynb` that trains and samples from a Transformer language model. Take a look at it (locally on your computer) to get somewhat familiar with how it defines and trains models. Some of the code you're writing below will be inspired by what you see in this notebook.

Note that you do not have to write any code or submit written answers for this part.

- (b) (0 points) **Read through `NameDataset` in `src/dataset.py`, our dataset for reading name-birthplace pairs.**

The task we'll be working on with our pretrained models is attempting to access the birth place of a notable person, as written in their Wikipedia page. We'll think of this as a particularly simple form of question answering:

*Q: Where was [person] born?*

*A: [place]*

From now on, you'll be working with the `src/` folder. **The code in `mingpt-demo/` won't be changed or evaluated for this assignment.** In `dataset.py`, you'll find the the class `NameDataset`, which reads a TSV (tab-separated values) file of name/place pairs and produces examples of the above form that we can feed to our Transformer model.

To get a sense of the examples we'll be working with, if you run the following code, it'll load your `NameDataset` on the training set `birth_places_train.tsv` and print out a few examples.

```
python src/dataset.py namedata
```

Note that you do not have to write any code or submit written answers for this part.

- (c) (0 points) **Implement finetuning (without pretraining).**

Take a look at `run.py`. It has some skeleton code specifying flags you'll eventually need to handle as command line arguments. In particular, you might want to *pretrain*, *finetune*, or *evaluate* a model with this code. For now, we'll focus on the finetuning function, in the case without pretraining.

Taking inspiration from the training code in the `play_char.ipynb` file, write code to finetune a Transformer model on the name/birthplace dataset, via examples from the `NameDataset` class. For now, implement the case without pretraining (i.e. create a model from scratch and train it on the birthplace prediction task from part (b)). You'll have to modify two sections, marked [part c] in the code: one to initialize the model, and one to finetune it. Note that you only need to initialize the model in the case labeled "vanilla" for now (later in section (g), we will explore a model variant). Use the hyperparameters for the `Trainer` specified in the `run.py` code.

Also take a look at the *evaluation* code which has been implemented for you. It samples predictions from the trained model and calls `evaluate_places()` to get the total percentage of correct place predictions. You will run this code in part (d) to evaluate your trained models.

This is an intermediate step for later portions, including Part d, which contains commands you can run to check your implementation. No written answer is required for this part.

- (d) (5 points) **Make predictions (without pretraining).**

Train your model on `birth_places_train.tsv`, and evaluate on `birth_dev.tsv`. Specifically, you should now be able to run the following three commands:

---

<sup>3</sup>See [CS224n Azure Guide](#) for a refresher on Azure.

```
# Train on the names dataset
python src/run.py finetune vanilla wiki.txt \
    --writing_params_path vanilla.model.params \
    --finetune_corpus_path birth_places_train.tsv

# Evaluate on the dev set, writing out predictions
python src/run.py evaluate vanilla wiki.txt \
    --reading_params_path vanilla.model.params \
    --eval_corpus_path birth_dev.tsv \
    --outputs_path vanilla.nopretrain.dev.predictions

# Evaluate on the test set, writing out predictions
python src/run.py evaluate vanilla wiki.txt \
    --reading_params_path vanilla.model.params \
    --eval_corpus_path birth_test_inputs.tsv \
    --outputs_path vanilla.nopretrain.test.predictions
```

Training will take less than 10 minutes (on Azure). Report your model's accuracy on the dev set (as printed by the second command above). Similar to assignment 4, we also have Tensorboard logging in assignment 5 for debugging. It can be launched using `tensorboard --logdir expt/`. Don't be surprised if it is well below 10%; we will be digging into why in Part 3. As a reference point, we want to also calculate the accuracy the model would have achieved if it had just predicted "London" as the birth place for everyone in the dev set. Fill in `london.baseline.py` to calculate the accuracy of that approach and report your result in your write-up. You should be able to leverage existing code such that the file is only a few lines long.

**Answer:** Model accuracy on the dev set is 0.008 (0.8%). If we just predicted London as the birth place for everyone in the dev set then accuracy would be 0.05 (5%).

- (e) (10 points) **Define a *span corruption* function for pretraining.**

In the file `src/dataset.py`, implement the `__getitem__()` function for the dataset class `CharCorruptionDataset`. Follow the instructions provided in the comments in `dataset.py`. Span corruption is explored in the [T5 paper \[3\]](#). It randomly selects spans of text in a document and replaces them with unique tokens (noising). Models take this noised text, and are required to output a pattern of each unique sentinel followed by the tokens that were replaced by that sentinel in the input. In this question, you'll implement a simplification that only masks out a single sequence of characters.

This question will be graded via autograder based on whether your span corruption function implements some basic properties of our spec. We'll instantiate the `CharCorruptionDataset` with our own data, and draw examples from it.

To help you debug, if you run the following code, it'll sample a few examples from your `CharCorruptionDataset` on the pretraining dataset `wiki.txt` and print them out for you.

```
python src/dataset.py charcorruption
```

No written answer is required for this part.

- (f) (10 points) **Pretrain, finetune, and make predictions. Budget 2 hours for training.**

Now fill in the *pretrain* portion of `run.py`, which will pretrain a model on the span corruption task. Additionally, modify your *finetune* portion to handle finetuning in the case *with* pretraining. In particular, if a path to a pretrained model is provided in the bash command, load this model before finetuning it on the birthplace prediction task. Pretrain your model on `wiki.txt` (which should take approximately two hours), finetune it on `NameDataset` and evaluate it. Specifically, you should

be able to run the following four commands: (Don't be concerned if the loss appears to plateau in the middle of pretraining; it will eventually go back down.)

```
# Pretrain the model
python src/run.py pretrain vanilla wiki.txt \
    --writing_params_path vanilla.pretrain.params

# Finetune the model
python src/run.py finetune vanilla wiki.txt \
    --reading_params_path vanilla.pretrain.params \
    --writing_params_path vanilla.finetune.params \
    --finetune_corpus_path birth_places_train.tsv

# Evaluate on the dev set; write to disk
python src/run.py evaluate vanilla wiki.txt \
    --reading_params_path vanilla.finetune.params \
    --eval_corpus_path birth_dev.tsv \
    --outputs_path vanilla.pretrain.dev.predictions

# Evaluate on the test set; write to disk
python src/run.py evaluate vanilla wiki.txt \
    --reading_params_path vanilla.finetune.params \
    --eval_corpus_path birth_test_inputs.tsv \
    --outputs_path vanilla.pretrain.test.predictions
```

Report the accuracy on the dev set (printed by the third command above). We expect the dev accuracy will be at least 10%, and will expect a similar accuracy on the held out test set.

**Answer:** After pre-training and fine-tuning, evaluating on the dev set yielded 34.4% accuracy.

- (g) (10 points) **Research! Write and try out a more efficient variant of Attention (Budget 2 hours for pretraining!)**

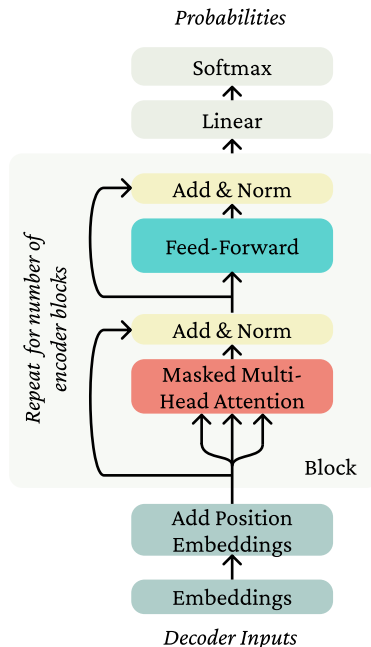
We'll now go to changing the Transformer architecture itself – specifically the first and last transformer blocks. The transformer model uses a self-attention scoring function based on dot products, this involves a rather intensive computation that's quadratic in the sequence length. This is because the dot product between  $\ell^2$  pairs of word vectors is computed in each computation, where  $\ell$  is the sequence length. If we can reduce the length of the sequence passed on the self-attention module, we should observe significant reduction in compute. For example, if we develop a technique that can reduce the sequence length to half, we can save around 75% of the compute time!

PerceiverAR [1] proposes a solution to make the model more efficient by reducing the sequence length of the input to self-attention for the intermediate layers. In the first layer, the input sequence is projected onto a lower-dimensional basis. Subsequently, all self-attention layers operate in this smaller subspace. The last layer projects the output back to the original input sequence length. In this assignment, we propose a simpler version of the PerceiverAR transformer model.

The provided CausalSelfAttention layer implements the following attention for each head of the multi-headed attention: Let  $X \in \mathbb{R}^{\ell \times d}$  (where  $\ell$  is the block size and  $d$  is the total dimensionality,  $d/h$  is the dimensionality per head).<sup>4</sup>

<sup>4</sup>Note that these dimensionalities do not include the minibatch dimension.





### Transformer Decoder

Figure 2: Illustration of the transformer block.

Let  $Q_i, K_i, V_i \in \mathbb{R}^{d \times d/h}$ . Then the output of the self-attention head is

$$Y_i = \text{softmax}\left(\frac{(XQ_i)(XK_i)^\top}{\sqrt{d/h}}\right)(XV_i) \quad (24)$$

where  $Y_i \in \mathbb{R}^{\ell \times d/h}$ . Then the output of the self-attention is a linear transformation of the concatenation of the heads:

$$Y = [Y_1; \dots; Y_h]A \quad (25)$$

where  $A \in \mathbb{R}^{d \times d}$  and  $[Y_1; \dots; Y_h] \in \mathbb{R}^{\ell \times d}$ . The code also includes dropout layers which we haven't written here. We suggest looking at the provided code and noting how this equation is implemented in PyTorch.

Our model uses this self-attention layer in the transformer block as shown in Figure 2. As discussed in the lecture, the transformer block contains residual connections and layer normalization layers. If we compare this diagram with the `Block` code provided in `model.py`, we notice that the implementation does not perform layer normalization on the output of the MLP (Feed-Forward), but on the input of the `Block`. This can be considered equivalent since we have a series of transformer blocks on top of each other.

In the Perceiver model architecture, we replace the first transformer `Block` in the model with the `DownProjectBlock`. This block reduces the length of the sequence from  $\ell$  to  $m$ . This is followed by a series of regular transformer blocks, which would now perform self-attention on the reduced sequence length of  $m$ . We replace the last block of the model with the `UpProjectBlock`, which takes in the  $m$  length output of the previous block, and projects it back to the original sequence length of  $\ell$ .

You need to implement the `DownProjectBlock` in `model.py` that reduces the dimensionality of the sequence in the first block. To do this, perform cross-attention on the input sequence with a

learnable basis  $C \in \mathbb{R}^{m \times d}$  as the query, where  $m < \ell$ . Consequently, Equation 24 becomes:

$$Y_i^{(1)} = \text{softmax}\left(\frac{(CQ_i)(XK_i)^\top}{\sqrt{d/h}}\right)(XV_i) \quad (26)$$

resulting in  $Y_i^{(1)} \in \mathbb{R}^{m \times d}$ , with  $^{(1)}$  denoting that the output corresponds to the first layer. With this dimensionality reduction, the subsequent `CausalSelfAttention` layers operate on inputs  $\in \mathbb{R}^{m \times d}$  instead of  $\mathbb{R}^{\ell \times d}$ . We refer to  $m$  as the `bottleneck_dim` in code. Note that for implementing Equation 26, we need to perform cross attention between the learnable basis  $C$  and the input sequence. This has been provided to you as the `CausalCrossAttention` layer. We recommend reading through `attention.py` to understand how to use the cross-attention layer, and map which arguments correspond to the key, value and query inputs. Initialize the basis vector matrix  $C$  using Xavier Uniform initialization.

To get back to the original dimensions, the last block in the model is replaced with the `UpProjectBlock`. This block will bring back the output sequence length to be the same as input sequence length by performing cross-attention on the previous layer's output  $Y^{L-1}$  with the original input vector  $X$  as the query:

$$Y_i^{(L)} = \text{softmax}\left(\frac{(XQ_i)(Y^{(L-1)}K_i)^\top}{\sqrt{d/h}}\right)(Y^{(L-1)}V_i) \quad (27)$$

where  $L$  is the total number of layers. This results in the final output vector having the same dimension as expected in the original `CausalSelfAttention` mechanism. Implement this functionality in the `UpProjectBlock` in `model.py`.

We provide the code to assemble the model using your implemented `DownProjectBlock` and `UpProjectBlock`. The model uses these blocks when the `variant` parameter is specified as `perceiver`.

Below are bash commands that your code should support in order to pretrain the model, finetune it, and make predictions on the dev and test sets. Note that the pretraining process will take approximately 2 hours.

```

# Pretrain the model
python src/run.py pretrain perceiver wiki.txt --bottleneck_dim 64 \
    --pretrain_lr 6e-4 --writing_params_path perceiver.pretrain.params

# Finetune the model
python src/run.py finetune perceiver wiki.txt --bottleneck_dim 64 \
    --reading_params_path perceiver.pretrain.params \
    --writing_params_path perceiver.finetune.params \
    --finetune_corpus_path birth_places_train.tsv

# Evaluate on the dev set; write to disk
python src/run.py evaluate perceiver wiki.txt --bottleneck_dim 64 \
    --reading_params_path perceiver.finetune.params \
    --eval_corpus_path birth_dev.tsv \
    --outputs_path perceiver.pretrain.dev.predictions

# Evaluate on the test set; write to disk
python src/run.py evaluate perceiver wiki.txt --bottleneck_dim 64 \
    --reading_params_path perceiver.finetune.params \
    --eval_corpus_path birth_test_inputs.tsv \
    --outputs_path perceiver.pretrain.test.predictions

```

Report the accuracy of your perceiver attention model on birthplace prediction on `birth_dev.tsv` after pretraining and fine-tuning.

Save the predictions of the model on `birth_test_inputs.tsv` to `perceiver.pretrain.test.predictions`.

For this section, you'll submit: `perceiver.finetune.params`, `perceiver.pretrain.dev.predictions`, and `perceiver.pretrain.test.predictions`. Your model should get at least 6% accuracy on the dev set.

- i. (8 points) We'll score your model as to whether it gets at least 5% accuracy on the test set, which has answers held out.

**Answer:** After pre-training the perceiver and fine-tuning it, the accuracy on the dev set was 20.8%.

- ii. (2 points) Provide an expression for the time complexity of the Perceiver model and the vanilla model, in terms of number of layers ( $L$ ), input sequence length ( $\ell$ ) and basis bottleneck dimension ( $m$ ).

**Answer:** The time complexity of a vanilla transformer's self-attention layer, where number of layers is  $L$ , input sequence length  $\ell$  is the below.

$$O(L\ell^2) \tag{28}$$

The time complexity of the Perceiver's self-attention layer is the below.

$$O(Lm^2) \tag{29}$$

### 3. Considerations in pretrained knowledge (5 points)

Please type the answers to these written questions (to make TA lives easier).

- (a) (1 point) Succinctly explain why the pretrained (vanilla) model was able to achieve an accuracy of above 10%, whereas the non-pretrained model was not.

**Answer:** The pretrained vanilla model is trained on a larger training data set, while the non-pretrained model is trained on a task-specific subset. Pretraining encodes more information, which could be potentially retrieved by downstream NLP task. Therefore the pretrained vanilla model achieves a higher accuracy than the non-pretrained model.

- (b) (2 points) Take a look at some of the correct predictions of the pretrain+finetuned vanilla model, as well as some of the errors. We think you'll find that it's impossible to tell, just looking at the output, whether the model *retrieved* the correct birth place, or *made up* an incorrect birth place. Consider the implications of this for user-facing systems that involve pretrained NLP components. Come up with two **distinct** reasons why this model behavior (i.e. unable to tell whether it's retrieved or made up) may cause concern for such applications, and an example for each reason.

**Answer:** The impossibility of discerning fact from hallucinated NLP outputs is a concern for users for these two reasons:

1. Even unintentionally, pre-trained NLP components have the potential to spread misinformation unless there is a concerted effort to fact-check NLP systems and enhance users' critical thinking. This can result in further blurring of the line between fact and fiction, especially in highly divisive topic areas such as politics, climate change, and abortion, and may exacerbate disagreements in other domains. Therefore, it is crucial to ensure that NLP systems are carefully monitored and regulated to prevent unintended negative consequences.
  2. Pre-trained NLP models must be used with great caution in domains that demand high levels of assurance and integrity, such as policing, counter-terrorism, and warfare. Since it is challenging to distinguish between real and fake NLP outputs, any misuse or error can have immediate and severe consequences on people's livelihoods. For instance, in policing, it could result in unjust detainment, while in warfare, it could mean the difference between life and death.
- (c) (2 points) If your model didn't see a person's name at pretraining time, and that person was not seen at fine-tuning time either, it is not possible for it to have "learned" where they lived. Yet, your model will produce *something* as a predicted birth place for that person's name if asked. Concisely describe a strategy your model might take for predicting a birth place for that person's name, and one reason why this should cause concern for the use of such applications. (You do not need to submit the same answer for 3c as for 3b.)

**Answer:** To improve the robustness of the model's outputs, we can take a three pronged strategy. First, we can implement input validation by checking whether person's name provided during inference time is in the pre-training and fine-tuning vocab. If the name is found, we proceed with generating a response, otherwise we stop and inform the user. Second, we could incorporate user feedback by creating a mechanism for the user to flag if they believe the answer is wrong. Finally, we can update model to handle new or unseen data collected from inference requests. To achieve this, we can extend the pretrained vocab using a method akin to "augmenting each layer in the original pretrained model with an extension module for out-of-vocab words"<sup>5</sup>. This approach can help the model handle new or unseen words leading to more robust outputs.

## Submission Instructions

You will submit this assignment on GradeScope as two submissions – one for **Assignment 5 [coding]** and another for **Assignment 5 [written]**:

1. Verify that the following files exist at these specified paths within your assignment directory:

---

<sup>5</sup>Tai et al. (2020) exBERT: Extending Pre-trained Models with Domain -specific Vocabulary Under Constrained Training Resources, EMNLP 2020 pp 1433-1439, Accessed via <https://aclanthology.org/2020.findings-emnlp.129.pdf>

- The no-pretraining model and predictions: `vanilla.model.params`, `vanilla.nopretrain.dev.predictions`, `vanilla.nopretrain.test.predictions`
  - The pretrain-finetune model and predictions: `vanilla.finetune.params`, `vanilla.pretrain.dev.predictions`, `vanilla.pretrain.test.predictions`
  - The Perceiver model and predictions: `perceiver.finetune.params`, `perceiver.pretrain.dev.predictions`, `perceiver.pretrain.test.predictions`
2. Run the `collect_submission.sh` script to produce your `assignment5.zip` file.
  3. Upload your `assignment5.zip` file to GradeScope to **Assignment 5 [coding]**.
  4. Check that the public autograder tests passed correctly.
  5. Upload your written solutions, for questions 1, parts of 2, and 3, to GradeScope to **Assignment 5 [written]**. Tag it properly!

## References

- [1] HAWTHORNE, C., JAEGLE, A., CANGA, C., BORGEAUD, S., NASH, C., MALINOWSKI, M., DIELEMAN, S., VINYALS, O., BOTVINICK, M. M., SIMON, I., SHEAHAN, H., ZEGHIDOUR, N., ALAYRAC, J., CARREIRA, J., AND ENGEL, J. H. General-purpose, long-context autoregressive modeling with perceiver AR. In *International Conference on Machine Learning, ICML 2022, 17-23 July 2022, Baltimore, Maryland, USA* (2022), vol. 162 of *Proceedings of Machine Learning Research*, pp. 8535–8558.
- [2] RADFORD, A., NARASIMHAN, K., SALIMANS, T., AND SUTSKEVER, I. Improving language understanding with unsupervised learning. *Technical report, OpenAI* (2018).
- [3] RAFFEL, C., SHAZEER, N., ROBERTS, A., LEE, K., NARANG, S., MATENA, M., ZHOU, Y., LI, W., AND LIU, P. J. Exploring the limits of transfer learning with a unified text-to-text transformer. *Journal of Machine Learning Research* 21, 140 (2020), 1–67.