高级人工智能课程汇报

信息科学与工程学院
Gu Rui
220220942871

June 25 2023

Contents

1 Attention exploration (22 points)

Multi-headed 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* $q \in \mathbb{R}^d$, a set of *value* vectors $\{v_1, ..., v_n\}$, $v_i \in \mathbb{R}^d$, and a set of *key* vectors $\{k_1, ..., k_n\}$, $k_i \in \mathbb{R}^d$, specified as follows:

$$c = \sum_{i=1}^{n} v_i \alpha_i \tag{1}$$

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

with α_i termed the "attention weights". Observe that the output $c \in \mathbb{R}^d$ is an average over the value vectors weighted with respect to α_i.

(a) (4 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 α can be interpreted as a categorical probability distribution.

Answer: Eq.1 has shown that this is a fuzzy query, and we cannot directly match a key vector k with the query vector q, and can only give each key a certain probability distribution weight (i.e. α_{ij}) to get the final output result.

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

Answer: According to the calculation method of Eq.2, if the query vector q has a very high similarity to a key k_i (the dot product is large), and q is basically vertical to other bonds (the point product is zero), then α_i will be maximized.

iii. (1 point) Under the conditions you gave in (ii), **describe** what properties the output c might have.

Answer: Under the conditions described in (ii), the output vector c will be heavily influenced by the value vector v_j associated with the key vector k_j that received the majority of the attention weight. At this point, the c is approximately equal to v_i

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

Answer: When the dot product (similarity) between a specific word key and a query significantly outweighs the dot products of other word keys with the same query, the attention output corresponding to that specific word will closely resemble its associated value. This behavior can be likened to "copying" the value into the output.

(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 va 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 $\{a_1, a_2, \ldots, a_m\}$, while v_b lies in a subspace B formed by the p basis vectors $\{b_1, b_2, \ldots, b_p\}$. (This means that any va can be expressed as a linear combination of its basis vectors, as can v_b. All basis vectors have norm 1 and 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 $\{a_1, a_2, \ldots, a_m\}$, 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, $M_s = v_a$.

Note: both M and v_a, v_b should be expressed as a vector in $\mathbb{R}^d$, not in terms of vectors from A and B.

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

Answer: Assume that A is a matrix of concatenated basis vectors $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}$ and B is a matrix of concatenated basis vector $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_p\}$. Linear combinations of vectors v_a and v_b can then be expressed as:

$$\mathbf{v}_a = c_1\mathbf{a}_1 + c_2\mathbf{a}_2 + \ldots + c_m\mathbf{a}_m = \sum_{i=1}^{m} c_i\mathbf{a}_i = A\mathbf{c}$$

$$\mathbf{v}_b = d_1\mathbf{b}_1 + d_2\mathbf{b}_2 + \ldots + d_p\mathbf{b}_m = \sum_{j=1}^{p} d_j\mathbf{b}_j = B\mathbf{d}$$

We need to construct such M which, when multiplied with $\mathbf{v}_b$, produces $\mathbf{0}$ and, when multiplied with $\mathbf{v}_a$, produces the same vector (in terms of its own space). Let M have the following form:

$$M = \sum_{i=1}^{m} \lambda_i \mathbf{a}_i \mathbf{a}_i^\top$$

Where $\lambda_i, i = 1, \ldots, m$ is the undetermined coefficient, it is derived as follows

$$\begin{aligned}
M\mathbf{s} = \mathbf{v}_a &\Leftrightarrow M\mathbf{v}_a + M\mathbf{v}_b = \mathbf{v}_a \\
&\Leftrightarrow \left(\sum_{i=1}^{m} \lambda_i \mathbf{a}_i \mathbf{a}_i^\top\right)\left(\sum_{i=1}^{m} c_i \mathbf{a}_i + \sum_{j=1}^{p} d_i \mathbf{b}_i\right) = \sum_{i=1}^{m} c_i \mathbf{a}_i \\
&\Leftrightarrow \sum_{i=1}^{m} \lambda_i c_i \mathbf{a}_i \mathbf{a}_i^\top \mathbf{a}_i = \sum_{i=1}^{m} c_i \mathbf{a}_i \quad \text{(orthogonal property)} \\
&\Leftrightarrow \sum_{i=1}^{m} (\lambda_i c_i \mathbf{a}_i^\top \mathbf{a}_i)\mathbf{a}_i = \sum_{i=1}^{m} c_i \mathbf{a}_i \\
&\Rightarrow \lambda_i c_i \mathbf{a}_i^\top \mathbf{a}_i = c_i \\
&\Rightarrow \lambda_i = \frac{1}{\mathbf{a}_i^\top \mathbf{a}_i}, i = 1, \ldots, m.
\end{aligned}$$

It is easy to see that, since $\mathbf{a}_j^\top b_k = 0$ for all j, k, $A^\top B = 0$. And we know that in terms of $\mathbb{R}^d$ (not in terms of A and B), $\mathbf{v}_a$ is just a collection of constants c. Thus the results of M are as follows

$$M = \sum_{i=1}^{m} \frac{\mathbf{a}_i \mathbf{a}_i^\top}{\mathbf{a}_i^\top \mathbf{a}_i} = A^\top$$

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 $k_i^\top k_j$ for all $i \neq j$; and (2) all key vectors have norm 1.[1] **Find an expression** for a query vector q such that $c \approx \frac{1}{2}(v_a + v_b)$.[2]

Thoughts: In essence is to find a q makes $\mathbf{k}_a^\top q = \mathbf{k}_b^\top q$, then we know $q^\top(\mathbf{k}_a - \mathbf{k}_b) = 0$, to find a q perpendicular to $\mathbf{k}_a - \mathbf{k}_b$.

Answer: Assume that c is approximated as follows:

$$c \approx \frac{1}{2}\mathbf{v}_a + \frac{1}{2}\mathbf{v}_b$$

This means we want $\alpha_a \approx 0.5$ and $\alpha_b \approx 0.5$, which can be achieved when (whenever $i \neq a$ and $i \neq b$):

$$\mathbf{k}_a^\top q \approx \mathbf{k}_b^\top q \gg \mathbf{k}_i^\top \mathbf{q}$$

[1] Recall that a vector x has norm 1 if $x^\top x = 1$.

[2] 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.

Like explained in the previous question, if the dot product is big, the probability mass will also be big and we want a balanced mass between α_a and α_b. q will be largest for k_a and k_b when it is a large multiplicative of a vector that contains a component in k_a direction and in k_b direction:

$$\mathbf{q} = \beta(\mathbf{k}_a + \mathbf{k}_b), \quad \text{where} \beta \gg 0$$

Now, since the keys are orthogonal to each other, it is easy to see that:

$$\mathbf{k}_a^\top q = \beta; \mathbf{k}_b^\top q = \beta; \mathbf{k}_i^\top q = 0, \quad \text{whever } i \neq a \text{ and } i \neq b$$

Thus when we exponentiate, only $\exp(\beta)$ will matter, because $\exp(0)$ will be insignificant to the probability mass. We get that:

$$\alpha_a = \alpha_b = \frac{\exp(\beta)}{n - 2 + 2\exp(\beta)} \approx \frac{\exp(\beta)}{2\exp(\beta)} \approx \frac{1}{2}, \text{ for } \beta \gg 0$$

(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 $\{k_1, \ldots, k_n\}$ that are now randomly sampled, $k_i \sim \mathcal{N}(_i, \Sigma_i)$, where the means $_i \in \mathbb{R}^d$ are known to you, but the covariances Σ_i are unknown. Further, assume that the means $_i$ 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 $\Sigma_i = \alpha I \forall i \in 1, 2, \ldots, n$, for vanishingly small α. Design a query q in terms of the μ_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: Because the covariance matrix is small, k_i can be approximately replaced by μ_i:

$$k_i \approx \mu_i$$

Since the key vectors k_a and k_b are orthogonal to each other, the problem can be reduced to the previous case where all keys were orthogonal. Therefore, the expression for the query vector q remains the same as in the previous case:

$$\mathbf{q} = \beta(\mu_a + \mu_b), \quad \text{where } \beta \gg 0$$

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 μ_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 α (as shown in Fig. 1). This causes k_a to point in roughly the same direction as μ_a, but with large variances in magnitude. Further, let $\Sigma_i = \alpha I$ for all $i \neq a$.

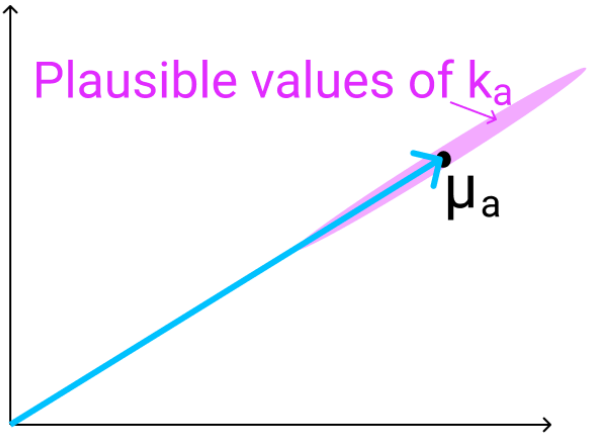

Figure 1: The vector μ_a (shown here in 2D as an example), with the range of possible values of k_a shown in red. As mentioned previously, k_a points in roughly the same direction as μ_a, but may have larger or smaller magnitude.

When you sample $\{k_1, \ldots, k_n\}$ multiple times, and use the q vector that you defined in part i., what qualitatively do you expect the vector c will look like for different samples?

Thoughts: It is easy to think that if there is an obviously large bond vector k_a, then the weight obtained by the single-head attention mechanism is meaningless, because the weighted sum is basically directed in the direction of k_a.

Answer: Since $\mu_i^\top \mu_i = 1$, $\mathbf{k}_a$ varies between $(\alpha + 0.5)\mu_a$ and $(\alpha + 1.5)\mu_a$. All other $\mathbf{k}_i$, whenever $i \neq a$, almost don't vary at all. Noting that α is vanishingly small:

$$\mathbf{k}_a \approx \gamma \mu_a, \quad \text{where } \gamma \sim \mathcal{N}(1, 0.5)$$

$$\mathbf{k}_i \approx \mu_i, \quad \text{whenever } i \neq a$$

Since $\mathbf{q}$ is most similar in directions $\mathbf{k}_a$ and $\mathbf{k}_b$, we can assume that the dot product between $\mathbf{q}$ and any other key vector is 0 (since all key vectors are orthogonal). Thus

there are 2 cases to consider (note that means are normalized and orthogonal to each other):

$$\mathbf{k}_a^\top \mathbf{q} \approx \gamma \mu_a^\top \beta \left(\mu_a + \mu_b\right) \approx \gamma\beta, \quad \text{where } \beta \gg 0$$

$$\mathbf{k}_b^\top \mathbf{q} \approx \mu_b^\top \beta \left(\mu_a + \mu_b\right) \approx \beta, \quad \text{where } \beta \gg 0$$

We can now directly solve for coefficients α_a and α_b, remembering that for large β values $\exp(0)$ are insignificant (note how $\frac{\exp(a)}{\exp(a)+\exp(b)} = \frac{\exp(a)}{\exp(a)+\exp(b)}\frac{\exp(-a)}{\exp(-a)} = \frac{1}{1+\exp(b-a)}$):

$$\alpha_a \approx \frac{\exp(\gamma\beta)}{\exp(\gamma\beta)+\exp(\beta)} \approx \frac{1}{1+\exp(\beta(1-\gamma))}$$

$$\alpha_b \approx \frac{\exp(\beta)}{\exp(\beta)+\exp(\gamma\beta)} \approx \frac{1}{1+\exp(\beta(\gamma-1))}$$

Since γ varies between 0.5 and 1.5, and since $\gamma \gg 0$, we have that:

$$\alpha_a \approx \frac{1}{1+\infty} \approx 0; \quad \alpha_b \approx \frac{1}{1+0} \approx 1; \quad \text{when } \gamma = 0.5$$

$$\alpha_a \approx \frac{1}{1+0} \approx 1; \quad \alpha_b \approx \frac{1}{1+\infty} \approx 0; \quad \text{when } \gamma = 1.5$$

Since $c \approx \alpha_a \mathbf{v}_a + \alpha_b \mathbf{v}_b$ because other terms are insignificant when β is large, we can see that $\mathbf{c}$ oscillates between $\mathbf{v}_a$ and $\mathbf{v}_b$:

$$\mathbf{c} \approx \mathbf{v}_b, \quad \text{when } \gamma \to 0.5; \quad \mathbf{c} \approx \mathbf{v}_b, \text{ when } \gamma \to 1.5$$

(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 $\{k_1, \ldots, k_n\}$ that are randomly sampled, $k_i \sim \mathcal{N}(\mu_i, \Sigma_i)$, where the means μ_i are known to you, but the covariances Σ_i are unknown. Also as before, assume that the means μi 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 α. Design q_1 and q_2 such that c is approximately equal to $\frac{1}{2}(v_a + v_b)$.

Answer: To make c approximately equal to $\frac{1}{2}(\mathbf{v}_a + \mathbf{v}_b)$, we can design the query vectors $\mathbf{q}_1$ and $\mathbf{q}_2$ such that they are approximately equal to the weights of the target vector $\mathbf{v}_a$ and $\mathbf{v}_b$ in the attention mechanism:

$$\mathbf{c}_1 \approx \mathbf{v}_a; \quad \mathbf{c}_2 \approx \mathbf{v}_b$$

Since the covariance matrix Σ_i is very close to zero, this means that the relationship between the key vectors k_i is very simple and can be considered as a point close to the origin. Therefore, we can choose the query vectors $\mathbf{q}_1$ and $\mathbf{q}_2$ and target vectors $\mathbf{v}_a$ and $\mathbf{v}_b$ and μ_b, we can express the $\mathbf{q}_1$ and $\mathbf{q}_2$:

$$\mathbf{q}_1 = \beta\mu_a, \quad \mathbf{q}_2 = \beta\mu_b, \quad \text{for } \beta \gg 0$$

In this case, the output of the attention mechanism, $\mathbf{c}$ would be approximately equal to

$$\mathbf{c} \approx \frac{1}{2}(\mathbf{v}_a + \mathbf{v}_b).$$

ii. (2 points) Assume that the covariance matrices are $\Sigma_a = \alpha I + \frac{1}{2}(\mu_a \mu_a^\top)$ for vanishingly small α, 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? Please briefly explain why. You can ignore cases in which $k_a^\top q_i < 0$.

Thoughts: According to the design of part i, $\mathbf{q}_1 = \mathbf{k}_a$ and $\mathbf{q}_2 = \mathbf{k}_b$, which means that $\mathbf{q}_1$ and $\mathbf{q}_2$ are highly correlated with the corresponding value vectors $\mathbf{v}_a$ and $\mathbf{v}_b$. When we do multi-head attention, each head calculates the weights from its own query vector and gives a weighted average over the value vectors. Because of the presence of $\frac{1}{2}(\mu_a \mu_a^\top)$ in $\Sigma_a = \alpha I + \frac{1}{2}(\mu_a \mu_a^\top)$, it will increase the weight associated with $\mathbf{v}_a$, while the other query vector $\mathbf{q}_i$ will be less associated with $\mathbf{v}_a$. Therefore, the output $\mathbf{c}$ will prefer $\mathbf{v}_a$ over $\mathbf{v}_b$, and the quality of $\mathbf{c}$ will vary for different critical vector samples. This is because long-head attention is able to weighted average the value vectors according to the correlation of the query vectors, while different query vectors lead to different weighted results.

Answer: With regards to question (c) ii., if we choose $\mathbf{q}_1 = \beta\mu_a$ and $\mathbf{q}_2 = \beta\mu_b$, we get that (note that all other key-query dot products will be insignificant):

$$\mathbf{k}_a^\top \mathbf{q}_1 \approx \gamma \mu_a^\top \beta \mu_a \approx \gamma\beta, \quad \text{where } \beta \gg 0$$

$$\mathbf{k}_b^\top \mathbf{q}_2 \approx \mu_b^\top \beta \mu_b \approx \beta, \quad \text{where } \beta \gg 0$$

We can solve for α values (again, note that all other key-query dot products will be insignificant when β is large):

$$\alpha_{a1} \approx \frac{\exp(\gamma\beta)}{\exp(\gamma\beta)} \approx 1; \quad \alpha_{b2} \approx \frac{\exp(\beta)}{\exp(\beta)} \approx 1;$$

Since we can say that $\alpha_{i1} \approx 0$ for any $i \neq a$ and $\alpha_{i2} \approx 0$ for any $i \neq b$ is is easy to see that:

$$\mathbf{c}_1 \approx \mathbf{v}_a, \quad \mathbf{c}_2 \approx \mathbf{v}_b$$

Which means that the final output will always approximately be an average of the values:

$$\mathbf{c} \approx \frac{1}{2}(\mathbf{v}_a + \mathbf{v}_b).$$

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[3]. 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 [1].

As in previous assignments, you will want to develop on your machine locally, then run training on HuaWei Could. Youll need around 5 hours for training, so budget your time accordingly!

Your work with this codebase is as follows:

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

In the `mingpt-demo`/folder is a Jupyter notebook that trains and samples from a

[3]https://github.com/karpathy/minGPT

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`, 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.

Answer:Running the python `src/dataset.py namedata` gives the following output(Fig. 2).

```
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> python src/dataset.py namedata
data has 418352 characters, 256 unique.
x: Where was Khatchig Mouradian born???Lebanon??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□??Lebanon??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: Where was Jacob Henry Studer born???Columbus??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□??Columbus??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: Where was John Stephen born???Glasgow??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: □□□□□□□□□□□□□□□□□□□□□□□□□□□□??Glasgow??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: Where was Georgina Willis born???Australia??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□??Australia??□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

Figure 2: The output obtained from running python `src/dataset.py namedata`

(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.

Changes: Modified line 59 and 127-141 in `run.py`

```
# line 59
model = model.GPT(mconf).to(device)

# line 127-141
if args.reading_params_path is not None: # finetuning with pretrain
  model.load_state_dict(torch.load(args.reading_params_path))
  train_config = trainer.TrainerConfig(max_epochs=10, batch_size=256, \
   learning_rate=6e-4, lr_decay=True, \
   warmup_tokens=512 * 20, \
   final_tokens=200 * len(pretrain_dataset) * block_size, \
   num_workers=0)
else: # finetuning without pretrain
  train_config = trainer.TrainerConfig(max_epochs=75, batch_size=256, \
```

```
    learning_rate=6e-4, lr_decay=True, \
    warmup_tokens=512 * 20, \
    final_tokens=200 * len(pretrain_dataset) * block_size, \
    num_workers=0)
train_dataset = dataset.NameDataset(pretrain_dataset, open(args.finetune_corpus_path, e
trainerGPT = trainer.Trainer(model, train_dataset, None, train_config)
trainerGPT.train()
torch.save(model.state_dict(), args.writing_params_path)
```

(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:

```
# 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 Huawei Cloud). Report your model's accuracy on the dev set (as printed by the second command above). 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: See Fig.3 for the running process.

- Model's accuracy: Correct: 5.0 out of 500.0: 1.0%
- If only "London": Correct: 25.0 out of 500.0: 5.0%

```
epoch 70 iter 7: train loss 0.24959. lr 5.210680e-04: 100%|
epoch 71 iter 7: train loss 0.24794. lr 5.189037e-04: 100%|
epoch 72 iter 7: train loss 0.22551. lr 5.167147e-04: 100%|
epoch 73 iter 7: train loss 0.21910. lr 5.145014e-04: 100%|
epoch 74 iter 7: train loss 0.19675. lr 5.122639e-04: 100%|
epoch 75 iter 7: train loss 0.18360. lr 5.100024e-04: 100%|
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> 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.prediction
data has 418352 characters, 256 unique.
number of parameters: 3323392
500it [00:30, 16.24it/s]
Correct: 5.0 out of 500.0: 1.0%
```

(a) result 1

```
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> 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
data has 418352 characters, 256 unique.
number of parameters: 3323392
437it [00:27, 15.75it/s]
No gold birth places provided; returning (0,0)
Predictions written to vanilla.nopretrain.test.predictions; no targets provided
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> python src\london_baseline.py
Correct: 25.0 out of 500.0: 5.0%
```

(b) result 2

Figure 3: The output obtained from running the script

(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 [2]. 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.

Answer: Running the python `src/dataset.py charcorruption` gives the following output(Fig. 4).

Changes: Completed the `__getitem__()` function in `dataset.py`

```
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> python src/dataset.py charcorruption
data has 418352 characters, 256 unique.
x: Khatchig⁇ournalist, writer and translator bor⁇ Mouradian. Khatchig Mouradian is a j□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: hatchig⁇ournalist, writer and translator bor⁇ Mouradian. Khatchig Mouradian is a j□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: Jac⁇y Studer. Jacob Henry Studer (26 February 1840 Columbus, Ohio - 2 August 1904 New York Cit⁇ob Henr□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: ac⁇y Studer. Jacob Henry Studer (26 February 1840 Columbus, Ohio - 2 August 1904 New York Cit⁇ob Henr□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: ⁇John Stephen. Born in Glasgow, Stephen became a welder's apprentice on leaving school .⁇□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
y: John Stephen. Born in Glasgow, Stephen became a welder's apprentice on leaving school .⁇□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
x: Georgina⁇Georgina Willis is an award winning film director who was born in Australia and now lives in ⁇ Willis. □□□□□□□□□□□□□□□□□
y: eorgina⁇Georgina Willis is an award winning film director who was born in Australia and now lives in ⁇ Willis. □□□□□□□□□□□□□□□□□□□
```

Figure 4: The output obtained from running python `src/dataset.py charcorruption`

```python
def __getitem__(self, idx):
# TODO [part e]: see spec above

# Steps 0 & 1: truncate
document = self.data[idx]
document = document[:random.randint(4, int(self.block_size*7/8))]

# Prepare mask length and cut index
mean_len = round(len(document) / 4)
mask_len = mean_len + random.randint(-mean_len, mean_len)
clip_idx = random.randint(0, mask_len)

# Step 2: prefix, suffix, mc
prefix = document[:clip_idx]
suffix = document[clip_idx+mask_len:]
masked_content = document[clip_idx:clip_idx+mask_len]

# Step 3: generate the masked string by taking out masked content
masked_string = prefix + self.MASK_CHAR + suffix \
  + self.MASK_CHAR + masked_content
masked_string += self.PAD_CHAR * (self.block_size - len(masked_string))

# Step 4: construct in/out
input = masked_string[:-1]
output = masked_string[1:]

# Step 5: encode the input-output pair to a tensor of type long
x = torch.tensor([*map(self.stoi.get, input)], dtype=torch.long)
```

```
    y = torch.tensor([*map(self.stoi.get, output)], dtype=torch.long)

    return x, y
```

(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:Run procedure and results are shown in Fig. 5, 6.

- dev accuracy: Correct: 85.0 out of 500.0: 17.0%

```
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> python src/run.py pretrain vanilla wiki.txt --writing_params_path vanilla.pretrain.params
data has 418352 characters, 256 unique.
number of parameters: 3323392
epoch 1 iter 22: train loss 3.43586. lr 5.999655e-03: 100%|
epoch 2 iter 22: train loss 3.04682. lr 5.998582e-03: 100%|
epoch 3 iter 22: train loss 2.86767. lr 5.996780e-03: 100%|
epoch 4 iter 22: train loss 2.83330. lr 5.994250e-03: 100%|
epoch 5 iter 22: train loss 2.79280. lr 5.990993e-03: 100%|
```

Figure 5: The output obtained from running python `src/run.py pretrain vanilla wiki.txt --writing_params_path vanilla.pretrain.params`

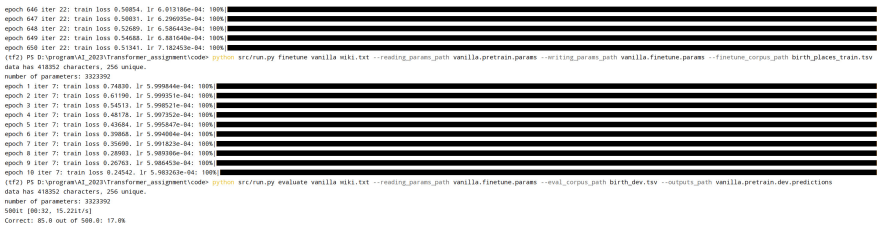

Figure 6: The output obtained from running python `src/run.py evaluate vanilla wiki.txt --reading_params_path vanilla.finetune.params --eval_corpus_path birth_dev.tsv --outputs_path vanilla.pretrain.dev.predictions`

Changes: Modified line 88-94 in `run.py`

```
# line 88-94
train_config = trainer.TrainerConfig(max_epochs=650, batch_size=128, \
  learning_rate=6e-3, lr_decay=True, \
  warmup_tokens=512 * 20, \
  final_tokens=200 * len(pretrain_dataset) * block_size, \
  num_workers=0)
trainerGPT = trainer.Trainer(model, pretrain_dataset, None, train_config)
trainerGPT.train()
torch.save(model.state_dict(), args.writing_params_path)
```

(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. While we've been using 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 ℓ^2 pairs of word vectors is computed in each computation. *Synthesized attention* [3] is a very recent alternative that has potential benefits by removing this dot product (and quadratic computation) entirely. It's a promising idea, and one way for us to ask, "What's important/right about the Transformer architecture, and where can we improve/prune aspects of it?" In `attention.py`, implement the `forward()` method of `SynthesizerAttention`, which implements a variant of the Synthesizer proposed in the cited paper.

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 ℓ is the block size and d is the total dimensionality, d/h is the dimensionality per head.).[4]

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

$$Y_i = \text{softmax}\left(\frac{(XQ_i)(XK_i)^\top}{\sqrt{d/h}}\right)(XV_i) \tag{3}$$

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:

$$Y = [Y_1; \ldots; Y_h]A \tag{4}$$

where $A \in \mathbb{R}^{d \times d}$ and $[Y_1; \ldots; Y_h] \in \mathbb{R}^{\ell \times d}$. 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.

Your job is to implement the following variant of attention. Instead of Eq. 3, implement the following in SynthesizerAttention:

$$Y_i = \text{softmax}\left(\text{ReLU}(XA_i + b_1)B_i + b_2\right)(XV_i), \tag{5}$$

where $A_i \in \mathbf{R}^{d \times d/h}$, $B_i \in \mathbf{R}^{d/h \times \ell}$, and $V_i \in \mathbf{R}^{d \times d/h}$.[5] One way to interpret this is as follows: The term $(XQ_i)(XK_i)^\top$ is an $\ell \times \ell$ matrix of attention scores, computed as all pairs of dot products between word embeddings. The synthesizer variant eschews the all-pairs dot product and directly computes the $\ell \times \ell$ matrix of attention scores

[4]Note that these dimensionalities do not include the minibatch dimension.

[5]Hint: copy over the CausalSelfAttention class, and modify it minimally for this.

by mapping each d-dimensional vector of each head for X to an ℓ-dimesional vector of unnormalized attention weights.

In the rest of the code in the `src/` folder, modify your model to support using either `CausalSelfAttention` or `SynthesizerAttention`. Add the ability to switch between these attention variants depending on whether "vanilla" (for causal self-attention) or "synthesizer" (for the synthesizer variant) is selected in the command line arguments (see the section marked [part g] in `src/run.py`). You are free to implement this functionality in any way you choose, so long as it supports these command line arguments.

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 synthesizer wiki.txt \
  --writing_params_path synthesizer.pretrain.params

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

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

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

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

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: dev accuracy: Correct: 87.0 out of 500.0: 17.4%

```
(tf2) PS D:\program\AI_2023\Transformer_assignment\code> python src/run.py evaluate synthesizer wiki.txt --reading_params_path synthesizer.finetune.params --eval_corpus_path birth_dev.tsv --outputs_path synthesizer.pretrain.dev.predictions
data has 418352 characters, 256 unique.
number of parameters: 3323392
500it [00:33, 14.73it/s]
Correct: 87.0 out of 500.0: 17.4%
```

Figure 7: The output obtained from running python `src/run.py evaluate synthesizer wiki.txt --reading_params_path synthesizer.finetune.params --eval_corpus_path birth_dev.tsv --outputs_path synthesizer.pretrain.dev.predictions`

Changes: Modified line 62-64 in `run.py`

```
mconf.synthesizer = True
model = model.GPT(mconf)
model.to(device)
```

ii. (2 points)Why might the synthesizer self-attention not be able to do, in a single layer, what the key-query-value self-attention can do?

Answer: Synthesizer attention is unable to do what the causal attention can do because it does not extract keys and queries from the input - it estimates that by remapping input to a lower dimensional space for each head. In other words, it is more difficult to represent context because for every word in sequence, that word is unable to choose which parts to pay attention to in the rest of the sequence (because it does not have access to their keys). Thus the synthesizer may not be able to capture the relevance between word pairs.

3 Considerations in pretrained knowledge (5 points)

(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 was able to achieve an accuracy above 10% because it had been pretrained on a large corpus of text data, which helped it learn general language patterns and information. During pretraining, the model learned to

predict the next word in a sentence based on the context it was given. This process allowed the model to develop a basic understanding of grammar, vocabulary, and semantic relationships. As a result, when fine-tuned on the specific task of predicting birthplaces, the pretrained model had some prior knowledge and linguistic abilities that helped it perform better than the non-pretrained model, which started from scratch.

(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:

- One reason why the inability to determine whether the model retrieved the correct birthplace or made up an incorrect one is concerning for user-facing systems is the potential for spreading misinformation. If the model generates incorrect birthplace predictions and presents them as factual information to users, it can lead to the dissemination of false or misleading data. For example, if the model inaccurately predicts a celebrity's birthplace, users relying on the system may unknowingly spread false information through social media or other platforms.
- Another concern is the erosion of trust in the system and its outputs. If users cannot discern whether the predicted birthplaces are reliable or fabricated, it undermines the credibility and usability of the system. Users may become skeptical or hesitant to rely on the system's predictions, especially if they have encountered instances where the predictions were incorrect. This lack of transparency and confidence in the model's outputs can significantly impact the user experience and limit the adoption of such applications.

(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:

- In the absence of pretraining or fine-tuning data for a specific person's name, the model may employ a strategy of generating a birthplace based on statistical patterns observed in the training data. For example, the model might identify common patterns between names and birthplaces, such as geographical associations or cultural trends. It could use this information to make an educated guess about the person's birthplace. However, this strategy should raise concerns in the context of user-facing applications. One reason is the potential for perpetuating stereotypes or biases. If the model relies on statistical patterns that reflect existing societal biases, it may produce birthplace predictions that align with those biases, reinforcing stereotypes or prejudices. This can have negative implications, such as perpetuating discriminatory views or reinforcing unfair generalizations based on demographics.
- Additionally, generating birthplace predictions for individuals without proper data or evidence can lead to the spread of speculative or misleading information. Users may interpret the model's predictions as factual, even if they are based on assumptions or statistical correlations. This can contribute to the proliferation of inaccurate or unverified information, further complicating the task of distinguishing between reliable and unreliable sources of information in user-facing systems.

References

[1] Radford, A., Narasimhan, K., Salimans, T., and Sutskever, I. Improving language understanding with unsupervised learning. Technical report, OpenAI (2018).

[2] 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.

[3] Tay, Y., Bahri, D., Metzler, D., Juan, D.-C., Zhao, Z., and Zheng, C. Synthesizer: Rethinking self-attention in transformer models. arXiv preprint arXiv:2005.00743 (2020).