

COSC490LLModels

Homework 4: Neural Language Modeling + Fixed-Window LMs

Name: ____ Kyle Tranfaglia____

Collaborators, if any: ____NA____

Sources used for your homework, if any: __Claude AI for documentation assistance, code debugging, and math assistance__

This assignment focuses on language modeling, while continuing to build up on our prior knowledge of neural networks. We will review several aspects about training neural nets and also extend it to modeling sequences in language.

Homework goals: After completing this homework, you should be comfortable with:

- thinking more deeply about training neural networks; debugging your neural network
- getting more engaged in using PyTorch for training NNs
- training your first neural LM

How to hand in your written work: Via MyClasses as before.

Collaboration: Make certain that you understand the course collaboration policy, described on the course website. You may discuss the homework to understand the problems and the mathematics behind the various learning algorithms, but you are **not allowed to share problem solutions with any other students. You must write the solutions individually.**

1 Concepts, intuitions and big picture

1.1 Multiple-choice questions.

1. Select the sentence that best describes the terms “model”, “architecture”, and “weights”.
 - ☐ Model and weights are the same; they form a succession of mathematical functions to build an architecture.
 - ✓ An architecture is a succession of mathematical functions to build a model and its weights are those functions parameters.

Answer:
2. During forward propagation, in the forward function for a layer l you need to know what is the activation function in a layer (Sigmoid, tanh, ReLU, etc.). During Backpropagation, the corresponding backward function does not need to know the activation function for layer l since the gradient does not depends on it.
 - ☐ True
 - ✓ False

Answer:
3. You have built a network using the tanh activation for all the hidden units. You initialize the weights to relative large values, using `randn(...)*1000`. What will happen?
 - ☐ It doesn't matter. So long as you initialize the weights randomly gradient descent is not affected by whether the weights are large or small.
 - ☐ This will cause the inputs of the tanh to also be very large, thus causing gradients to also become large. You therefore have to set the learning rate to be very small to prevent divergence; this will slow down learning.
 - ☐ This will cause the inputs of the tanh to also be very large, causing the units to be highly activated and thus speed up learning compared to if the weights had to start from small values.
 - ✓ This will cause the inputs of the tanh to also be very large, thus causing gradients to be close to zero. The optimization algorithm will thus become slow.

Answer:
4. What is the “cache” used for in our implementation of forward propagation and backward propagation?
 - ☐ It is used to cache the intermediate values of the cost function during training.
 - ✓ We use it to pass variables computed during forward propagation to the corresponding backward propagation step. It contains useful values for backward propagation to compute derivatives.
 - ☐ It is used to keep track of the hyperparameters that we are searching over, to speed up computation.
 - ☐ We use it to pass variables computed during backward propagation to the corresponding forward propagation step. It contains useful values for forward propagation to compute activations.

Answer:
5. Among the following, which ones are “hyperparameters”? (Check all that apply.)
 - ✓ size of the hidden layers.
 - ✓ learning rate
 - ✓ number of iterations
 - ✓ number of layers in the neural network

Answer:
6. True/False? Vectorization allows you to compute forward propagation in an L -layer neural network without an explicit for-loop (or any other explicit iterative loop) over the layers $l = 1, 2, \dots, L$.
 - ☐ True
 - ✓ False

Answer:
7. True or false? A language model usually does not need labels annotated by humans for its pretraining.
 - ✓ True
 - ☐ False

Answer:
8. What is the order of the language modeling pipeline?
 - ☐ First, the model, which handles text and returns raw predictions. The tokenizer then makes sense of these predictions and converts them back to text when needed.
 - ☐ First, the tokenizer, which handles text and returns IDs. The model handles these IDs and outputs a

prediction, which can be some text.

✓The tokenizer handles text and returns IDs. The model handles these IDs and outputs a prediction. The tokenizer can then be used once again to convert these predictions back to some text.

Answer:

1.2 Short answer questions

1. Look at the definition of [Stochastic] Gradient Descent in PyTorch: <https://pytorch.org/docs/stable/generated/torch.optim.SGD.html>. You will see that this is a bit more complex than what we have seen in the class. Let's understand a few nuances here.

- (a) Notice the `maximize` parameter which controls whether we are running a maximization or minimization. In the algorithm the effect of this parameter is shown as essentially a change in the sign of the gradients: How do you think this change leads to the desired outcome (maximization vs minimization)?

```
if maximize
     $\theta_t \leftarrow \theta_{t-1} + \gamma g_t$ 
else
     $\theta_t \leftarrow \theta_{t-1} - \gamma g_t$ 
```

Answer: The gradient vector indicates the direction of steepest increase for a function. When minimizing, we move opposite to this direction by subtracting the gradient from our parameters, effectively descending toward lower values. When maximizing instead, we simply reverse this process by adding the gradient, which pushes our parameters in the direction of steepest increase. This sign flip transforms gradient descent into gradient ascent, allowing the same algorithm to handle both minimization problems and maximization problems without requiring separate implementations. The `maximize` parameter in PyTorch's SGD optimizer provides this flexibility with a boolean toggle.

- (b) The next set of parameters `momentum`, `dampening`, `weight_decay`. What do you think the impact of these parameters are? Read the documentations and interpret their roles.

Answer: Momentum, dampening, and weight decay in PyTorch's SGD optimizer each serve distinct but complementary roles in improving training. Momentum (typically 0.9) accumulates a velocity vector that helps navigate past local minima and flat regions by considering the history of gradients, similar to a rolling ball that maintains direction despite small obstacles. Dampening reduces the influence of the current gradient on this momentum term, stabilizing training when gradients are noisy. Weight decay implements L2 regularization by adding a penalty proportional to parameter magnitudes, preventing weights from growing too large and thus reducing overfitting. Together, these hyperparameters provide fine-tuned control over optimization dynamics, balancing between convergence speed, training stability, and model generalization.

2. What are few benefits to using Fixed-Window-LM over n -grams language models? (limit your answer to less than 5 sentences). Answer: Fixed-Window Language Models offer several advantages over traditional n -gram models. They maintain a consistent context window size regardless of the sequence length, which provides more stable performance across varying text spans. Their neural network architecture allows them to learn more nuanced semantic relationships and better generalize to unseen word combinations than the strict counting-based approach of n -grams. Fixed-Window models can more effectively handle data sparsity through distributed representations, eliminating the need for smoothing techniques required by n -gram models. Additionally, they typically require less storage space as they encode patterns in neural weights rather than storing explicit probability tables for all possible n -gram combinations.
3. When searching over hyperparameters, a typical recommendation is to do random search rather than a systematic grid search. Why do you think that is the case? (less than 2 sentences). Answer: Random search typically outperforms grid search because most machine learning models have only a few hyperparameters that significantly affect performance, and random search explores the high-importance dimensions more efficiently by testing more distinct values within those dimensions rather than wasting computational resources on exhaustive combinations.
4. Remember the normalization layer that we saw during the class. Here is the corresponding PyTorch page: <https://pytorch.org/docs/stable/generated/torch.nn.LayerNorm.html>. In the normalization formula, why do we use epsilon ϵ in the denominator?

Answer: The epsilon (ϵ) term is added to the denominator in the normalization formula to prevent division by zero. When the variance of the inputs is very small or zero, without epsilon, the normalization calculation would lead to numerical instability or undefined results. This small constant (typically set to values like $1e-5$) ensures that the normalization

operation remains stable even when dealing with inputs that have minimal variance, allowing the training process to continue smoothly without producing NaN values or causing the model to crash.

2 Softmax Smackdown: Squishing the Competition

2.1 Softmax gradient

You might remember in the midterm exam that we saw a neural network with a Softmax and a cross-entropy loss:

$$\hat{\mathbf{y}} = \text{Softmax}(\mathbf{h}), J = \text{CE}(\mathbf{y}, \hat{\mathbf{y}}), \quad \mathbf{h}, \mathbf{y}, \hat{\mathbf{y}} \in \mathbb{R}^d.$$

Basically here $\hat{\mathbf{y}}$ is a d -dimensional probability distribution over d possible options (i.e. $\sum_i \hat{y}_i = 1$ and $\forall i : \hat{y}_i \in [0, 1]$). \mathbf{y} is a d -dimensional one-hot vector, i.e., all of these values are zeros except one that corresponds to the correct label.

$$\nabla_{\mathbf{h}} J = \hat{\mathbf{y}} - \mathbf{y}.$$

Prove the above statement. In your proof, use the statement that you proved in HW3 about gradient of Softmax function: $\frac{d\hat{y}_i}{dh_j} = \hat{y}_i(\delta_{ij} - \hat{y}_j)$, where δ_{ij} is the Kronecker delta function and \hat{y}_i is the value in the i -th index of $\hat{\mathbf{y}}$.

Answer:

$$J = - \sum_{i=1}^d y_i \log(\hat{y}_i)$$

$$\text{Since } \mathbf{y} \text{ is one-hot at index } k: J = -\log(\hat{y}_k)$$

$$\begin{aligned} \frac{\partial J}{\partial h_j} &= -\frac{\partial \log(\hat{y}_k)}{\partial h_j} = -\frac{1}{\hat{y}_k} \frac{\partial \hat{y}_k}{\partial h_j} \\ &= -\frac{1}{\hat{y}_k} \hat{y}_k(\delta_{kj} - \hat{y}_j) = -(\delta_{kj} - \hat{y}_j) \end{aligned}$$

$$\text{For } j = k: \frac{\partial J}{\partial h_k} = -(1 - \hat{y}_k) = \hat{y}_k - 1 = \hat{y}_k - y_k$$

$$\text{For } j \neq k: \frac{\partial J}{\partial h_j} = -(-\hat{y}_j) = \hat{y}_j = \hat{y}_j - 0 = \hat{y}_j - y_j$$

$$\text{Therefore, for all } j: \frac{\partial J}{\partial h_j} = \hat{y}_j - y_j$$

$$\text{In vector form: } \nabla_{\mathbf{h}} J = \hat{\mathbf{y}} - \mathbf{y}$$

2.2 Softmax temperature

Remember the softmax function, $\sigma(\mathbf{z})$? Here we will add a *temperature* parameter $\tau \in \mathbb{R}^+$ to this function:

$$\text{Softmax: } \sigma(\mathbf{z}; \tau)_i = \frac{e^{z_i/\tau}}{\sum_{j=1}^K e^{z_j/\tau}} \quad \text{for } i = 1, \dots, K$$

Show the following:

1. In the limit as temperature goes to zero $\tau \rightarrow 0$, softmax becomes the same as greedy action selection, argmax .

Answer:

Let $z_m = \max z_i$ be the maximum value in z .

For any i where $z_i < z_m$:

$$\frac{e^{z_i/\tau}}{e^{z_m/\tau}} = e^{(z_i - z_m)/\tau} \rightarrow 0 \text{ as } \tau \rightarrow 0$$

Therefore:

$$\sigma(z; \tau)_i \rightarrow 0 \text{ if } z_i < z_m$$

$$\sigma(z; \tau)_i \rightarrow 1 \text{ if } z_i = z_m$$

This is equivalent to the argmax operation.

2. In the limit as temperature goes to infinity $\tau \rightarrow +\infty$, softmax gives equiprobable selection among all actions.

Answer:

$$\text{As } \tau \rightarrow \infty, \frac{z_i}{\tau} \rightarrow 0 \text{ for all } i$$

Therefore:

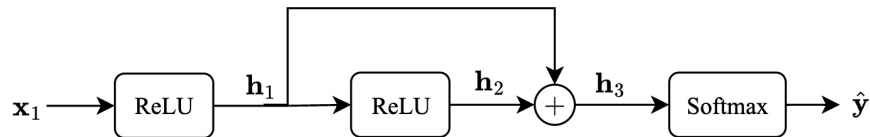
$$\lim_{\tau \rightarrow \infty} e^{z_i/\tau} = e^0 = 1 \text{ for all } i$$

$$\lim_{\tau \rightarrow \infty} \sigma(z; \tau)_i = \frac{1}{\sum_{j=1}^K 1} = \frac{1}{K}$$

This gives equal probability $\frac{1}{K}$ to each action.

3 Backprop Through Residual Connections

As you know, When neural networks become very deep (i.e. have many layers), they become difficult to train due to the vanishing gradient problem, as the gradient is back-propagated through many layers, repeated multiplication can make the gradient extremely small, so that performance plateaus or even degrades. An effective approach is to add skip connections that skip one or more layers. See the provided network.



$$\mathbf{x} \in \mathbb{R}^d, \mathbf{W}_{1,2} \in \mathbb{R}^{d \times d}, \hat{\mathbf{y}} \in \mathbb{R}^d$$

$$\mathbf{z}_1 = \mathbf{W}_1 \mathbf{x}_1, \mathbf{h}_1 = \text{ReLU}(\mathbf{z}_1),$$

$$\mathbf{z}_2 = \mathbf{W}_2 \mathbf{h}_1, \mathbf{h}_2 = \text{ReLU}(\mathbf{z}_2),$$

$$\mathbf{h}_3 = \mathbf{h}_1 + \mathbf{h}_2, \hat{\mathbf{y}} = \text{Softmax}(\mathbf{h}_3), J = \text{CE}(\mathbf{y}, \hat{\mathbf{y}})$$

1. You have seen this in the quiz, but lets try again. Prove that: $\frac{\partial}{\partial z_i} \text{ReLU}(\mathbf{z}) = 1\{z_i > 0\}$ where $1\{x > 0\} =$

$\begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x \leq 0 \end{cases}$. More generally, $\nabla_z \text{ReLU}(\mathbf{z}) = \text{diag}(\mathbf{1}\{\mathbf{z} > 0\})$ where $\mathbf{1}\{\cdot\}$ is applied per each dimension and $\text{diag}(\cdot)$ turns a vector into a diagonal matrix.

Answer: Definition of the ReLU Function:

$$\text{ReLU}(z_i) = \max(0, z_i) = \begin{cases} z_i & \text{if } z_i > 0 \\ 0 & \text{if } z_i \leq 0 \end{cases}$$

Now, let's compute the derivative:

For $z_i > 0$:

$$\frac{\partial}{\partial z_i} \text{ReLU}(z_i) = \frac{\partial}{\partial z_i} z_i = 1$$

For $z_i \leq 0$:

$$\frac{\partial}{\partial z_i} \text{ReLU}(z_i) = \frac{\partial}{\partial z_i} 0 = 0$$

Therefore:

$$\frac{\partial}{\partial z_i} \text{ReLU}(z_i) = \begin{cases} 1 & \text{if } z_i > 0 \\ 0 & \text{if } z_i \leq 0 \end{cases} = \mathbf{1}\{z_i > 0\}$$

For a vector $\mathbf{z} \in \mathbb{R}^n$, we have:

$$\text{ReLU}(\mathbf{z}) = [\max(0, z_1), \max(0, z_2), \dots, \max(0, z_n)]^T$$

The gradient $\nabla_z \text{ReLU}(\mathbf{z})$ is the Jacobian matrix:

$$\nabla_z \text{ReLU}(\mathbf{z}) = \begin{bmatrix} \frac{\partial \text{ReLU}(z_1)}{\partial z_1} & \frac{\partial \text{ReLU}(z_1)}{\partial z_2} & \dots & \frac{\partial \text{ReLU}(z_1)}{\partial z_n} \\ \frac{\partial \text{ReLU}(z_2)}{\partial z_1} & \frac{\partial \text{ReLU}(z_2)}{\partial z_2} & \dots & \frac{\partial \text{ReLU}(z_2)}{\partial z_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \text{ReLU}(z_n)}{\partial z_1} & \frac{\partial \text{ReLU}(z_n)}{\partial z_2} & \dots & \frac{\partial \text{ReLU}(z_n)}{\partial z_n} \end{bmatrix}$$

Since $\text{ReLU}(z_i)$ only depends on z_i and not on any other component of \mathbf{z} , we have:

$$\frac{\partial \text{ReLU}(z_i)}{\partial z_j} = \begin{cases} \frac{\partial \text{ReLU}(z_i)}{\partial z_i} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

From our scalar case proof, we know that $\frac{\partial \text{ReLU}(z_i)}{\partial z_i} = \mathbf{1}\{z_i > 0\}$.

Therefore, the Jacobian becomes:

$$\nabla_z \text{ReLU}(\mathbf{z}) = \begin{bmatrix} \mathbf{1}\{z_1 > 0\} & 0 & \dots & 0 \\ 0 & \mathbf{1}\{z_2 > 0\} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{1}\{z_n > 0\} \end{bmatrix}$$

This is precisely $\text{diag}(\mathbf{1}\{\mathbf{z} > 0\})$, where $\mathbf{1}\{\mathbf{z} > 0\}$ means the indicator function applied element-wise to each component of \mathbf{z} .

- As you see, a single variable (\mathbf{h}_2 in the example) feeds into two different layers of the network. Here we want to show that the two upstream signals stemming from this node are merged as summation during Backprop. Specifically prove that:

$$\frac{\partial \mathbf{h}_3}{\partial \mathbf{h}_1} = \mathbf{I} + \frac{\partial \mathbf{h}_2}{\partial \mathbf{z}_2} \frac{\partial \mathbf{z}_2}{\partial \mathbf{h}_1}$$

Answer: First, we expand h_3 in terms of h_1 and h_2 :

$$h_3 = h_1 + h_2$$

Taking the derivative with respect to h_1 :

$$\frac{\partial h_3}{\partial h_1} = \frac{\partial h_1}{\partial h_1} + \frac{\partial h_2}{\partial h_1}$$

We know that $\frac{\partial h_1}{\partial h_1} = I$ (identity matrix).

For the second term, we need to consider that $h_2 = f(z_2)$ and $z_2 = g(h_1)$ for some functions f and g . By the chain rule:

$$\frac{\partial h_2}{\partial h_1} = \frac{\partial h_2}{\partial z_2} \frac{\partial z_2}{\partial h_1}$$

Therefore:

$$\frac{\partial h_3}{\partial h_1} = I + \frac{\partial h_2}{\partial z_2} \frac{\partial z_2}{\partial h_1}$$

This proves that the gradient from h_3 to h_1 is the sum of:

1. The direct gradient (identity matrix) from the skip connection 2. The gradient through the intermediate layer

This demonstrates why residual connections help with gradient flow - they allow gradients to flow back directly through the identity mapping, avoiding potential vanishing gradient problems.

3. In the given neural network your task is to **compute the gradient** $\frac{\partial J}{\partial x}$. You are allowed (and highly encouraged) to use variables to represent intermediate gradients.

Hint 1: Compute these gradients in order to build up your answer: $\frac{\partial J}{\partial h_3}$, $\frac{\partial J}{\partial h_2}$, $\frac{\partial J}{\partial z_2}$, $\frac{\partial J}{\partial h_1}$, $\frac{\partial J}{\partial z_1}$, $\frac{\partial J}{\partial x}$. Show your work so we are able to give partial credit!

Hint 2: Recall that $\text{downstream} = \text{upstream} * \text{local}$.

Answer:

Step 1: $\frac{\partial J}{\partial h_3}$

This is the gradient of the loss with respect to the final output. Let's denote this as:

$$\frac{\partial J}{\partial h_3} = \delta_{h_3}$$

Step 2: $\frac{\partial J}{\partial h_2}$

Using the chain rule:

$$\begin{aligned} \frac{\partial J}{\partial h_2} &= \frac{\partial J}{\partial h_3} \frac{\partial h_3}{\partial h_2} \\ &= \delta_{h_3} \cdot 1 \quad (\text{since } h_3 = h_1 + h_2) \\ &= \delta_{h_3} \end{aligned}$$

Step 3: $\frac{\partial J}{\partial z_2}$

Applying the chain rule and using the ReLU derivative:

$$\begin{aligned} \frac{\partial J}{\partial z_2} &= \frac{\partial J}{\partial h_2} \frac{\partial h_2}{\partial z_2} \\ &= \delta_{h_3} \cdot \text{diag}(\mathbf{1}\{z_2 > 0\}) \\ &= \delta_{h_3} \odot \mathbf{1}\{z_2 > 0\} \\ &= \delta_{z_2} \end{aligned}$$

where \odot represents element-wise multiplication.

Step 4: $\frac{\partial J}{\partial h_1}$

h_1 affects J through two paths: directly to h_3 and through z_2 to h_2 to h_3 .

$$\begin{aligned}\frac{\partial J}{\partial h_1} &= \frac{\partial J}{\partial h_3} \frac{\partial h_3}{\partial h_1} + \frac{\partial J}{\partial z_2} \frac{\partial z_2}{\partial h_1} \\ &= \delta_{h_3} \cdot 1 + \delta_{z_2} \cdot W_2 \\ &= \delta_{h_3} + \delta_{z_2} W_2 \\ &= \delta_{h_1}\end{aligned}$$

Step 5: $\frac{\partial J}{\partial z_1}$

Similar to Step 3:

$$\begin{aligned}\frac{\partial J}{\partial z_1} &= \frac{\partial J}{\partial h_1} \frac{\partial h_1}{\partial z_1} \\ &= \delta_{h_1} \cdot \text{diag}(\mathbf{1}\{z_1 > 0\}) \\ &= \delta_{h_1} \odot \mathbf{1}\{z_1 > 0\} \\ &= \delta_{z_1}\end{aligned}$$

Step 6: $\frac{\partial J}{\partial x}$

Finally:

$$\begin{aligned}\frac{\partial J}{\partial x} &= \frac{\partial J}{\partial z_1} \frac{\partial z_1}{\partial x} \\ &= \delta_{z_1} \cdot W_1 \\ &= \delta_{z_1} W_1\end{aligned}$$

Expanding this fully:

$$\begin{aligned}\frac{\partial J}{\partial x} &= \delta_{z_1} W_1 \\ &= (\delta_{h_1} \odot \mathbf{1}\{z_1 > 0\}) W_1 \\ &= ((\delta_{h_3} + \delta_{z_2} W_2) \odot \mathbf{1}\{z_1 > 0\}) W_1 \\ &= ((\delta_{h_3} + (\delta_{h_3} \odot \mathbf{1}\{z_2 > 0\}) W_2) \odot \mathbf{1}\{z_1 > 0\}) W_1\end{aligned}$$

This represents the complete gradient of J with respect to x , computed by carefully tracking how the gradient flows backward through the network.

4. Based on your derivations, explain why residual connections help mitigate vanishing gradients. **Answer:** Residual connections mitigate vanishing gradients by providing alternative pathways for gradient flow during back-propagation. As shown in our derivations, when we compute the gradient flowing back to a given layer, we get two components: a direct gradient from the residual connection, and a traditional gradient through the nonlinear transformation. The direct path ensures that at least some gradient flows back unimpeded, even if the traditional path suffers from vanishing gradients due to ReLU activations zeroing out signals or small weights diminishing them. This is evident in the formula $\frac{\partial J}{\partial h_1} = \delta_{h_3} + \delta_{z_2} W_2$, where δ_{h_3} represents the direct gradient that bypasses potential gradient-killing operations. Even if the second term approaches zero due to vanishing gradient issues, the first term still allows for learning. This gradient highway enables the training of much deeper networks than would otherwise be possible, as early layers can still receive meaningful learning signals regardless of network depth.

4 Programming

In this programming homework, we will

- implement your own subword tokenizer.
- implement fixed-window MLP language models

Skeleton Code and Structure: The code base for this homework can be found at MyClasses Files under the hw3 directory. Your task is to fill in the missing parts in the skeleton code, following the requirements, guidance, and tips provided in this pdf and the comments in the corresponding .py files. The code base has the following structure:

- `tokenization.py` implements the Byte-Pair Encoding algorithm for subword tokenization.
- `mlp_lm.py` implements a fixed-window MLP-based language model on a subset of Wikipedia.
- `main.py` provides the entry point to run your implementations in both `tokenization.py` and `mlp_lm.py`.
- `hw4.md` provides instructions on how to setup the environment and run each part of the homework in `main.py`

TODOs — Your tasks include 1) generate plots and/or write short answers based on the results of running the code; 2) fill in the blanks in the skeleton to complete the code. We will explicitly mark these plotting, written answer, and filling-in-the-blank tasks as **TODOs** in the following descriptions, as well as a `# TODO` at the corresponding blank in the code.

Submission: Your submission should contain two parts: 1) plots and short answers under the corresponding questions below; and 2) your completion of the skeleton code base, in a .zip file

4.1 Tokenization Algorithms

All NLP systems have *at least* three main components that help machines understand natural language:

1. Tokenization
2. Embedding
3. Model architectures

Models like BERT, GPT-2 or GPT-3 all share the same components but with different architectures that distinguish one model from another. We are going to focus on the first component of an NLP pipeline which is **tokenization**. An often overlooked concept but it is a field of research in itself. Though we have SOTA algorithms for tokenization it's always a good practice to understand the evolution trail.

Here's what we'll cover:

- What is tokenization?
- Why do we need a tokenizer?
- Types of tokenization - Word, Character and Subword.
- Byte Pair Encoding Algorithm
- Other tokenization algorithms:
 - Unigram Algorithm
 - WordPiece - BERT transformer
 - SentencePiece - End-to-End tokenizer system

4.1.1 What is Tokenization?

Tokenization is the process of representing raw text in smaller units called tokens. These tokens can then be mapped with numbers to further feed to an NLP model.

Read and run the `full_word_tokenization_demo` in `tokenization.py` for an overly simplified example of what a tokenizer does.

This is a very simple example where we just split a text string in to “whole words” on white spaces, and we have not considered grammar, punctuation, or compound words (like “test”, “test-ify”, “test-ing”, etc.).

Problems with word tokenization:

- **Missing words in the training data:** With word tokens, your model won’t recognize the variants of words that were not part of the data on which the model was trained. So, if your model has seen ‘foot’ and ‘ball’ in the training data but the final text has “football”, the model won’t be able to recognize the word and it will be treated with a “<UNK>” token. Similarly, punctuations pose another problem, “let” or “let’s” will need individual tokens and it is an inefficient solution. This will **require a huge vocabulary** to make sure you’ve every variant of the word. Even if you add a **lemmatizer** to solve this problem, you’re adding an extra step in your processing pipeline.
- **Not all languages use space for separating words:** For a language like Chinese, which doesn’t use spaces for word separation, this tokenizer will fail.

4.1.2 Character-based tokenization

To resolve the problems associated with word-based tokenization, an alternative approach of character-by-character tokenization was tried. This solves the problem of missing words as now we are dealing with characters that can be encoded using ASCII or Unicode and it could generate embedding for any word now.

Every character, be it space, apostrophes, or colons, can now be assigned a symbol to generate a sequence of vectors. But this approach had its cons. Character-based models will treat each character and will lead to longer sequences. For a 5-word long sentence, you may need to process 30 tokens instead of 5 word-tokens.

4.1.3 Subword Tokenization

To address the earlier issues, we could think of breaking down the words based on a set of prefixes and suffixes. For example, we can build a system that can identify subwords like “##s”, “##ing”, “##ify”, “un##” etc., where the position of double hash “##” denotes prefix and suffixes. So, a word like “unhappily” is tokenized using subwords like “un##”, “happ”, and “##ily”.

BPE (Byte-Pair Encoding) was originally a data compression algorithm that is used to find the best way to represent data by identifying the common byte pairs. It is now used in NLP to find the best representation of text using the least number of tokens.

Here’s how it works:

1. Add a “</w>” at the end of each word to identify the end of a word and then calculate the word frequency in the text.
2. Split the word into characters and then calculate the character frequency.
3. For a predefined number of iterations (set by you), count the frequency of the consecutive tokens and merge the most frequently occurring pairings.
4. Keep iterating until you have reached the iteration limit or if you have reached the token limit.

We will now go through this algorithm step by step.

Read the `get_word_freq` function in `tokenization.py` that implements the step 1 above to preprocess each word and count its frequency.

TODOs: Read and complete the missing lines in the `get_pairs` function in `tokenization.py` to implement the step 2 above. This function takes the word frequency record returned from `get_word_freq` as input, split the words into tokens (characters at this initial step), and counts token-pairs frequency.

Hint: follow the comments in the code for specific requirements.

Read the `get_most_frequent_pair` and `merge_byte_pairs` functions in `tokenization.py` that implements the step 3 above, merge the top-1 frequent token-pairs in all the words.

In practise, after iterating over the input text for a desired number of times, we extract the resulting tokenization as our subword dictionary. For this purpose, we provide `get_subword_tokens` function in `tokenization.py`

With all these functions, we can now run one step of the BPE algorithm!

Read and run the `test_one_step_bpe.py` in `main.py` to test the BPE algorithm for one step. A correct implementation of `get_pairs` should pass all the tests.

4.1.4 Complete the BPE Algorithm

With the above implementations, we can complete all the steps of the BPE algorithm that iterates over the input corpus.

TODOs: Read and complete the missing lines in the `extract_bpe_subwords` function in `tokenization.py` that implements the full BPE algorithm. Once you finished, run the `test_bpe` function in `main.py`, a correct implementation of `extract_bpe_subwords` should pass all the tests.

Hint: follow the comments in the code and you can reuse the helper functions provided/you implemented above.

So as we iterate with each best pair, we merge (concatenating) the pair and you can see as we recalculate the frequency, the original character token frequency is reduced and the new paired token frequency pops up in the token dictionary.

4.1.5 Running BPE on a subset of Wikipedia

Now, let's run this algorithm on a larger scale. In particular, we will run on many Wikipedia paragraphs. As usual, let's use the Huggingface library to download the data (the `load_bpe_data` function).

TODOs: Read and run the `bpe_on_wikitext` in `main.py` that iterates the BPE algorithm on a subset of Wikipedia, and interprets the final subwords extracted from the Wikipedia documents. In particular, identify examples of subwords that correspond to

1. complete words
2. part of a word
3. non-English words(including other languages or common sequence special characters)

Explain why these subwords have come about. (no more than 10 sentences) *Answer: Looking at the subwords extracted from the WikiText dataset, I can identify several patterns that demonstrate BPE's effectiveness as a tokenization algorithm. Complete words like "Hopkins</w>", "history</w>", and "government</w>" appear as tokens when they occur frequently enough to be merged as whole units. Partial words represent common morphemes that appear across many different words - examples include prefixes like "pro" and "com", suffixes like "tion" and "ment", and the common verb ending "ing". The algorithm also identified non-English characters and sequences, including diacritics, Greek letters, Arabic characters, East Asian characters, and special character sequences. These subwords emerged because BPE identified frequently occurring character sequences in the corpus, creating a vocabulary that balances between character-level tokenization (which would be too granular) and word-level tokenization (which would miss common subword patterns). This approach allows for efficient representation of text with fewer tokens, as the algorithm captures both standalone words and meaningful subword units across languages and special formatting found in the WikiText corpus.*

4.1.6 Additional Readings: Other Tokenization Algorithms

WordPiece

WordPiece is the subword tokenization algorithm used for **BERT**, **DistilBERT**, and **Electra**. The algorithm was outlined in (Schuster and Nakajima, 2012) and is very similar to BPE. WordPiece first initializes the vocabulary to include every character present in the training data and progressively learns a given number of merge rules.

In contrast to BPE, WordPiece does not choose the most frequent symbol pair, but the one that maximizes the likelihood of the training data once added to the vocabulary.

So what does this mean exactly? Referring to the previous example, maximizing the likelihood of the training data is equivalent to finding the symbol pair, whose probability is divided by the probabilities of its first symbol followed by its second symbol is the greatest among all symbol pairs. E.g. “u”, followed by “g” would have only been merged if the probability of “ug” divided by “u”, “g” would have been greater than for any other symbol pair. Intuitively, WordPiece is slightly different from BPE in that it evaluates what it *loses* by merging two symbols to ensure it’s *worth it*.

Unigram

Unigram is a subword tokenization algorithm introduced in (Kudo, 2018). In contrast to BPE or WordPiece, Unigram initializes its base vocabulary to a large number of symbols and progressively trims down each symbol to obtain a smaller vocabulary. The base vocabulary could for instance correspond to all pre-tokenized words and the most common substrings. Unigram is not used directly for any of the models in the transformers, but it’s used in conjunction with SentencePiece (section 4.1.6).

At each training step, the Unigram algorithm defines a loss (often defined as the log-likelihood) over the training data given the current vocabulary and a unigram language model. Then, for each symbol in the vocabulary, the algorithm computes how much the overall loss would increase if the symbol was to be removed from the vocabulary. Unigram then removes p (with p usually being 10% or 20%) percent of the symbols whose loss increase is the lowest, i.e. those symbols that least affect the overall loss over the training data. This process is repeated until the vocabulary has reached the desired size. The Unigram algorithm always keeps the base characters so that any word can be tokenized.

Because Unigram is not based on merge rules (in contrast to BPE and WordPiece), the algorithm has several ways of tokenizing new text after training. As an example, if a trained Unigram tokenizer exhibits the vocabulary: [“b”, “g”, “h”, “n”, “p”, “s”, “u”, “ug”, “un”, “hug”],

“hugs” could be tokenized both as [“hug”, “s”], [“h”, “ug”, “s”] or [“h”, “u”, “g”, “s”]. So which one to choose? Unigram saves the probability of each token in the training corpus on top of saving the vocabulary so that the probability of each possible tokenization can be computed after training. The algorithm simply picks the most likely tokenization in practice but also offers the possibility to sample a possible tokenization according to their probabilities.

Those probabilities are defined by the loss the tokenizer is trained on. Assuming that the training data consists of the words x_1, \dots, x_N and that the set of all possible tokenizations for a word x_i is defined as $S(x_i)$, then the overall loss is defined as

$$\mathcal{L} = - \sum_{i=1}^N \log \left(\sum_{x \in S(x_i)} p(x) \right)$$

SentencePiece

All tokenization algorithms described so far have the same problem: It is assumed that the input text uses spaces to separate words. However, not all languages use spaces to separate words. One possible solution is to use language-specific pre-tokenizers, e.g. XLM uses a specific Chinese, Japanese, and Thai pre-tokenizer). To solve this problem more generally, Kudo and Richardson (2018) treats the input as a raw input stream, thus including the space in the set of characters to use. It then uses the BPE or unigram algorithm to construct the appropriate vocabulary.

The XLNetTokenizer uses SentencePiece for example, which is also why in the example earlier the “_” character was included in the vocabulary. Decoding with SentencePiece is very easy since all tokens can just be concatenated and “_” is replaced by a space.

All transformer models in the library that use SentencePiece use it in combination with unigram. Examples of models using SentencePiece are ALBERT XLNet, Marian, and T5.

4.2 Fixed-Window MLP Language Models

In the second part of the homework, we will build, train, and evaluate fixed-window MLP language models as we learned in class: given the context words in the fixed-size window on the left hand side, predict the next word continuation.

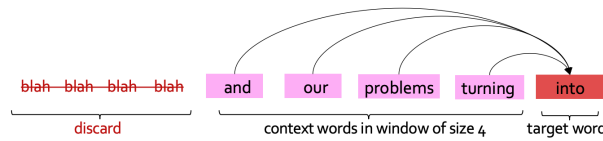


Figure 1: Fixed-window LM

4.2.1 Data Loading and Preprocessing

We will be using the same **WikiText** dataset we used for building n-gram LM in homework 2. We follow similar preprocessing steps to split paragraphs into sentences followed by tokenization (Now we have learned more about subword tokenization in class and the previous question!).

TODOs read the `preprocess_data` function in `ngram_lm.py` and complete the missing lines to prepare input-output pairs for training fixed-window LMs.

Hint: follow the requirements in the code comments.

4.2.2 Build our LM

Let's now turn to building our model. Here, we are following the footsteps of the neural probabilistic language model (NPLM) (Sun and Iyyer, 2021), which is extending earlier studies such as Bengio et al. (2003).

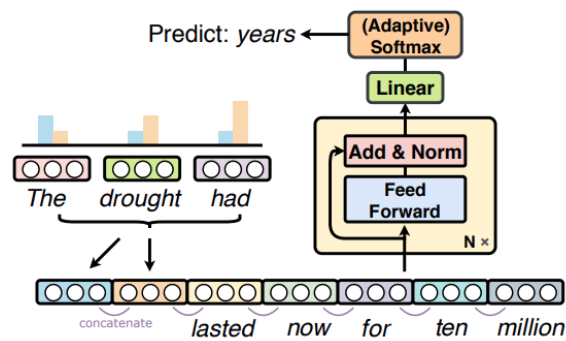


Figure 2: NPLM Architecture

We will follow a modular design for our implementation to make it more interpretable. In particular, will implement 3 layers:

- The **input layer** which loops up word embeddings, concatenates them, and transforms them into a hidden representation.
- The **middle layer** transforms the representation with a non-linearity.
- The **output layer** which transforms a hidden vector to a probability distribution over the words

Let's get to work!

TODOs: read and complete the forward functions for the following classes

- `NPLM_first_block`: input layer that embeds the input token ids into embedding vectors, concatenates the embeddings, applies linear transformation, layer normalization, and dropout
- `NPLM_block`: middle layers with linear transformation, tanh activation, residual connection, layer normalization, and dropout.
- `NPLM_final_block`: output layer that transforms hidden representation to log probability over the vocabulary with log softmax.

Hint: check out `nn.LayerNorm` and `nn.Dropout`, `torch.tanh` and `nn.functional.log_softmax` for more details on these layers and operations. For embedding concatenation, you may find `torch.Tensor.view` useful. Also, follow the step-by-step comments in the code for the requirements of the implementation.

TODOs: read and complete the `__init__` and `forward` functions for the `NPLM` class, which is the final model that stacks all the above layers.

Hint: remember to apply ReLU non-linear activation after each middle layer, details at [nn.functional.relu](#).

4.2.3 Train and Evaluate the LM

Now it's time to train and evaluate it! Like the previous homework, we will use cross-entropy loss between the predictions of our language model and actual words that appeared in our training data. Note that we applied log softmax to the final output of the LM, as described in homework to, we will use **negative log-likelihood loss** as the training criterion to calculate the cross-entropy loss.

As introduced in the class, we will use **Perplexity** to evaluate our LM, as a measure of predictive quality of a language model.

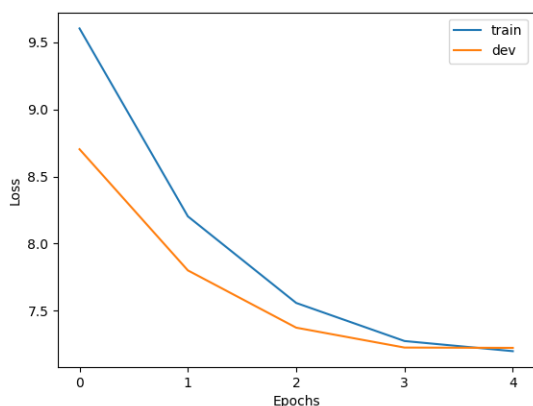
TODOs Read and complete the missing lines in `train` and `evaluate` functions in `mlp_lm.py` to calculate the perplexity.

Hint: remember in the class we discussed the connection between perplexity and cross-entropy loss, and note that in our implementation we took natural logarithm instead of the base of 2.

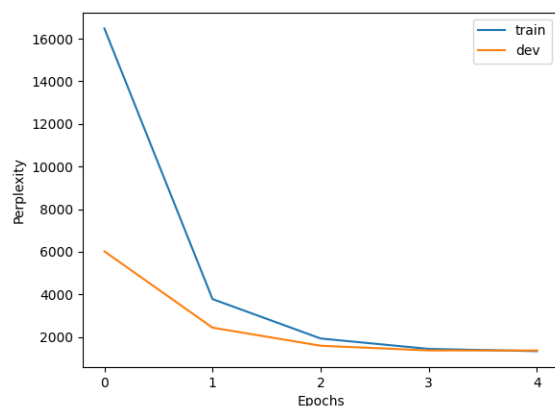
Note we are using Adam (**Adaptive Moment Estimation**) (Kingma and Ba, 2015), which is a popular optimization algorithm used in deep learning and machine learning. It is a stochastic gradient descent (SGD) optimization algorithm that is well suited for training deep neural networks. The algorithm has some internal estimates to dynamically adjust the learning rates for each parameter based on its past gradients, which can result in faster convergence and improved performance compared to traditional SGD.

TODOs Once you finished all the implementations, run `load_data_mlp_lm` and `single_run_mlp_lm` in `main.py` to train and evaluate the model and paste the plots of loss and Perplexity here.

your plots



(a) train and dev loss of the MLP LM



(b) train and dev ppl of the MLP LM

Figure 3: loss and ppl of the MLP LM

4.2.4 Sample From a Pre-trained LM

Note that compared with the original NPLM implementation, we reduce the model size by shrinking both the width and depth of our model, and we only use a small subset of the data. It is expected to take an hour or so to train the model on the CPU of your PC. Training the above LM with full size model and data might take hours to days. To save you time, we have trained a language model for you to play with. All you have to do is to download its weight parameters. Download the **pre-trained weights** and copy it to your local directory under `/hw4/`.

Now that we have the model weight downloaded, we can instantiate a model with these parameters. This will work in two steps.

- First we will need to create a new model (with potentially random weights).

- Then, we will copy the parameter values to the model using `load_state_dict` function.

We then evaluate the loaded model on the dev set. Now that we have loaded a pre-trained LM, how can we sample from it? We will implement two strategies, greedy decoding and top-p sampling (Holtzman et al., 2019) that we briefly discussed in homework 2.

For greedy, we select the most probable words (argmax).

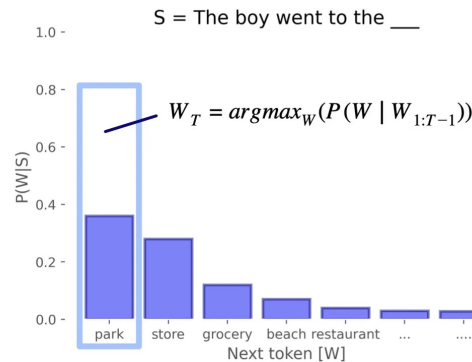


Figure 4: Greedy Decoding

For top-p, we sample from the distribution proportional to word probabilities. Words with higher probabilities will be more likely to be sampled. However, we also have an option of filtering the low-probability tokens, and instead retaining tokens that constitute `texttttop_p` probability.

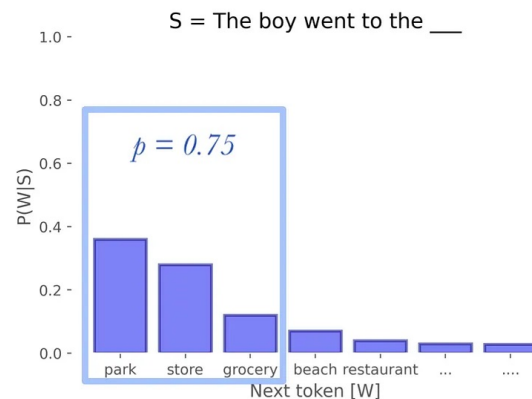


Figure 5: Greedy Decoding

Read `generate_text` and `sample_from_mlp_lm` in `mlp_lm.py` for more details about how to load the pre-trained model, evaluate on dev set and perform greedy/top-p sampling. You can learn more about top-p sampling implementation at [TopPLogitsWarper](#).

TODOs Run the `sample_from_trained_mlp_lm` in `main.py` to sample from the pre-trained LM, paste the completion to the prefix under different sampling strategies here, and describe in 2-3 sentences your findings.

Hint: compare the output of the above generations, which one is your favorite? Explain why this choice of sampling leads to better text generation.

Answer: Note: to generate the following output, some alterations were made to the provided code to prevent errors from inconsistent configurations and tensor shape mismatch. For example, embed dim: 128, hidden dim: 512, and num blocks: 2. The configuration was updated to match the configuration for single run mlp lm. Also, if len(new input.shape) == 1: new input = new input.unsqueeze(0). This was added to prevent tensor shape mismatch.

Here is the following output:

greedy: *The best perks of living on the east the the the, the the the, the the the, the the the, the the the,*

top-p sampling (p=0.0): The best perks of living on the east the the the, the the the, the the the, the the the, the the the, the the the, the the the

top-p sampling (p=0.3): The best perks of living on the east of the of.. the, and of the. the.. of and and the of the of of of the.. of,
top-p sampling (p=1.0): The best perks of living on the east sense that are Valley. death by. her million @ - @ - @ of north, and
to the all and. animated, of several.s

Looking at the generation results, we can observe that different sampling strategies significantly impact text quality. The greedy and $p=0.0$ sampling produces repetitive, unimaginative text that gets stuck in loops, in this case a long string of "the," while $p=0.3$ creates slightly more diverse but still incoherent output. I prefer the $p=1.0$ sampling because it generates the most varied and interesting text with actual content words like "Valley," "death," "million," and "animated." Although it's still not very coherent, it shows more creativity and better approximates natural language by incorporating a wider vocabulary rather than repeating the same patterns.

References

- Bengio, Y., Ducharme, R., Vincent, P., and Jauvin, C. (2003). A neural probabilistic language model. *Journal of machine learning research*, 3(Feb):1137–1155.
- Holtzman, A., Buys, J., Du, L., Forbes, M., and Choi, Y. (2019). The curious case of neural text degeneration. In *International Conference on Learning Representations (ICLR)*.
- Kingma, D. P. and Ba, J. (2015). Adam: A method for stochastic optimization. *CoRR*, abs/1412.6980.
- Kudo, T. (2018). Subword regularization: Improving neural network translation models with multiple subword candidates. In *Annual Meeting of the Association for Computational Linguistics (ACL)*.
- Kudo, T. and Richardson, J. (2018). SentencePiece: A simple and language independent subword tokenizer and detokenizer for neural text processing. In *Conference on Empirical Methods in Natural Language Processing (EMNLP)*.
- Schuster, M. and Nakajima, K. (2012). Japanese and korean voice search. *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5149–5152.
- Sun, S. and Iyyer, M. (2021). Revisiting simple neural probabilistic language models. In *Conference of the North American Chapter of the Association for Computational Linguistics (NAACL)*.