# CS236299 Lab 2-3: Language modeling with neural networks

## October 16, 2024

[]: # Please do not change this cell because some hidden tests might depend on it.

```
import os
     # Otter grader does not handle ! commands well, so we define and use our
     # own function to execute shell commands.
     def shell(commands, warn=True):
         """Executes the string `commands` as a sequence of shell commands.
            Prints the result to stdout and returns the exit status.
            Provides a printed warning on non-zero exit status unless `warn`
           flag is unset.
         file = os.popen(commands)
         print (file.read().rstrip('\n'))
         exit_status = file.close()
         if warn and exit_status != None:
             print(f"Completed with errors. Exit status: {exit_status}\n")
         return exit_status
     shell("""
     ls requirements.txt >/dev/null 2>&1
     if [ ! $? = 0 ]; then
     rm -rf .tmp
     git clone https://github.com/cs187-2024/lab2-6.git .tmp
     mv .tmp/tests ./
     mv .tmp/requirements.txt ./
     rm -rf .tmp
     fi
     pip install -q -r requirements.txt
[]: # Initialize Otter
     import otter
     grader = otter.Notebook()
[]: # Please do not change this cell because some hidden tests might depend on it.
     import os
```

```
# Otter grader does not handle ! commands well, so we define and use our
# own function to execute shell commands.
def shell(commands, warn=True):
    """Executes the string `commands` as a sequence of shell commands.
       Prints the result to stdout and returns the exit status.
       Provides a printed warning on non-zero exit status unless `warn`
       flag is unset.
    file = os.popen(commands)
    print (file.read().rstrip('\n'))
    exit_status = file.close()
    if warn and exit_status != None:
        print(f"Completed with errors. Exit status: {exit_status}\n")
    return exit_status
shell("""
ls requirements.txt >/dev/null 2>&1
if [ ! $? = 0 ]; then
rm -rf .tmp
git clone git@github.com:cs236299-2023-spring/lab2-3.git .tmp
mv .tmp/tests ./
mv .tmp/requirements.txt ./
rm -rf .tmp
pip install -q -r requirements.txt
""")
```

In previous labs, you have explored two different language model architectures: the n-gram model and Recurrent Neural Network (RNN) model. Both of these models utilize context to predict the most likely next word in a sequence, but they do so in distinct ways.

The n-gram model bases its predictions solely on the previous n words. This method, though simple, is limited by its fixed context window. On the other hand, the RNN language model uses a hidden state that carries representations from previous time steps, theoretically enabling the model to capture long-range dependencies in text. However, in practice, RNNs often struggle with very long sequences due to issues like vanishing gradients, making them less effective for modeling extended texts.

In the upcoming lab, you will implement and explore the *attention mechanism*, a powerful technique for encoding and utilizing context from previous time steps. This will be your first step toward understanding the Transformer model, one of the most important language model innovations in recent years.

New bits of PyTorch used in the solution set for this lab, and which you may therefore find useful:

- torch.bmm
- torch.cumsum

- torch.masked\_fill
- torch.softmax
- torch.transpose
- torch.triu

## 1 Preparation – Loading packages and data

```
[]: import json
  import math
  import random
  import wget
  import matplotlib.pyplot as plt

import torch
  import torch.nn as nn

from tokenizers import Tokenizer
  from transformers import PreTrainedTokenizerFast

from tqdm.auto import tqdm
```

```
[]: # Set random seeds
SEED = 1234
torch.manual_seed(SEED)
random.seed(SEED)

# GPU check, sets runtime type to "GPU" where available
device = torch.device("cuda" if torch.cuda.is_available() else "cpu")
print(device)
```

We use the same data as in lab 2-3 – the Federalist papers.

Once again we will split the dataset into training, validation, and test sets. Since we have provided pretrained models, you won't be using the training set in this lab. For the validation set, we have separate ones for papers authored by Hamilton (validation\_hamilton) and papers authored by Madison (validation\_madison).

```
[]: # Split training, validation, and test sets
     TRAIN_RATIO = 0.9
     # Extract the papers of unknown authorship
     testing = list(filter(lambda ex: ex['authors'] == 'Hamilton or Madison',
                           dataset))
     # Change gold labels in-place
     for ex in testing:
       ex['authors'] = 'Madison'
     # Extract the papers by Madison
     dataset_madison = list(filter(lambda ex: ex['authors'] == 'Madison', dataset))
     random.seed(SEED)
     random.shuffle(dataset_madison)
     training size madison = int(math.floor(TRAIN_RATIO * len(dataset_madison)))
     validation_madison = dataset_madison[training_size_madison:]
     # Extract the papers by Hamilton
     dataset hamilton = list(filter(lambda ex: ex['authors']=='Hamilton', dataset))
     random.seed(SEED)
     random.shuffle(dataset_hamilton)
     training_size_hamilton = int(math.floor(TRAIN_RATIO * len(dataset_hamilton)))
     validation_hamilton = dataset_hamilton[training_size_hamilton:]
     # We only consider the first 200 tokens of each document for speed
     def truncate(s, k=200):
       for document in s:
         document['tokens'] = document['tokens'][:k]
```

Before diving into the *attention mechanism*, we'd like to offer some intuitions about its underlying idea. You'll begin by exploring simple models that will help you understand the basic concepts behind it.

## 2 A uniform attention model

Recall the forward step in RNN models:

$$h_t = \sigma(Uh_{t-1} + Wy_i)$$

Notice how  $h_t$  has access to representations from previous time steps only through  $h_{t-1}$ . In addition, calculating  $h_t$  requires waiting for the computation of  $h_{t-1}$ ; for this reason, RNNs are inherently serial in their computations. You will now test a new approach where the context at time step t directly incorporates word embeddings from all previous time steps.

You will first explore a simple and naive model called *The Uniform Attention Model*, so-called because at each time step the model assigns equal attention to all previous words when calculating the distribution for the next word.

At each time step t,  $h_t$  is calculated based on the sum of all the previous word embeddings  $y_1, y_2....y_t$  as follows:

$$h_t = \sum_{i=1}^t y_i$$

Complete the forward function.

Hint: You might find torch.cumsum helpful.

```
[]: class UATTNLM(torch.nn.Module):
    def __init__(self, hf_tokenizer, embedding_size, hidden_size):
        super().__init__()
        self.hf_tokenizer = hf_tokenizer
        self.pad_index = hf_tokenizer.pad_token_id
        self.hidden_size = hidden_size
        vocab_size = len(hf_tokenizer)

# Create modules
        self.embed = torch.nn.Embedding(vocab_size, embedding_size)
        self.hidden2output = torch.nn.Linear(hidden_size, vocab_size)

def forward(self, context_words):
```

```
"""Computes the distribution over the next word given context\sqcup
→ `history_words`.
  Arguments:
     context_words: a list of word strings, could be an empty list when_
\hookrightarrow generating
                     the first word.
  Returns:
     logits, should be a tensor of size (bsz, vocab_size)
     11 11 11
  self.eval()
   context = self.hf_tokenizer(context_words, is_split_into_words=True,_
→return_tensors='pt')['input_ids']\
             .long()\
             .to(device) # bsz, context_len
   context_len = context.size(1)
   # For generating the first word, we feed in a special beginning-of-sentence
⇔symbol <pad>,
   # which is also what we use for padding. In future labs we'll be using \Box
⇔ <bos>, but as long
   # as training and evaluation use the same beginning-of-sentence symbol, it_{\sqcup}
\rightarrow doesn't matter
   # which particular symbol we use.
  if context len == 0:
     context = context.new(1, 1).fill_(self.pad_index)
     context len = context.size(1)
  hidden = None
  # TODO: calculate output and set logits
   # Logits should be a tensor of size (1, vocab_size)
   # The structure of the network is
       embeddings -> output -> hidden2output -> logits
  return logits
```

Now, let's load the models for Hamilton and Madison. The model u\_attn\_lm\_madison was trained on documents authored by Madison, while u\_attn\_lm\_hamilton was trained on documents authored by Hamilton.

Let's try to sample from the model. Don't expect a fluent text yet—more improvements are needed in the model.

```
[]: def sample(model, context):
         """Returns a token sampled from the `model` assuming the `context`"""
         logits = model(context)[:,-1] # calls internally to model.forward(context)
          # Normalize to get probabilities
         probs = torch.softmax(logits, -1).view(-1) # vocab_size
         # Match probabilities with actual word types
         distribution = {}
         for i, prob in enumerate(probs):
           word = model.hf_tokenizer.decode(i, clean_up_tokenization_spaces=True)
           distribution[word] = prob.item()
         prob_remaining = random.random()
         for token, prob in sorted(distribution.items()):
             if prob_remaining < prob:</pre>
                 return token
                 prob_remaining -= prob
         raise ValueError
     def sample sequence(model, start context, count=100):
         """Returns a sequence of tokens of length `count` sampled successively
            from the `model` starting with the `start_context`
         11 11 11
         random.seed(SEED) # for reproducibility
         context = list(start_context)
         result = list(start_context)
         for i in range(0, count):
             next = sample(model, tuple(context))
             result.append(next)
             context = context + [next]
         return result
```

Question: In fact, this model should be familiar to you. Do you remember what it's called?

Type your answer here, replacing this text.

In the previous model, we made a simple assumption – that all previous words are equally important. Of course, this simple assumption is wrong in general, as different time steps can have varying levels of importance and dependencies.

Next, you will build a model that differentiates between time steps.

Are you ready? You're about to learn about one of the most important and influential mechanisms invented in recent years.

### 3 The attention mechanism

The previous model was quite basic and suffered from an obvious problem:

At each time step, we assumed the dependencies on the previous time steps, the context, were static. Ideally, we want the model to determine dynamically at each stage which parts of the context are more relevant and which are less, that is, which parts of the context to *attend to*.

You'll now be introduced to the *attention mechanism* (proposed in this seminal paper), a powerful architecture that allows models to selectively focus on different parts of the input sequence. This mechanism has become a cornerstone in modern natural-language processing, significantly enhancing a model's ability to model language distributions.

Attention works by *querying* a (dynamically sized) sequence of *keys* associated with *values*. These key-value pairs are associated with the context elements of a particular token.

As usual, the query, keys, and values are represented as vectors. The query process provides a score that specifies how much each key should be attended to. The attention can then be summarized by taking an average of the *values* weighted by the attention score of the corresponding *keys*. This *context vector* can then be used as another input to other processes you will learn about in the next lab.

More formally, let's suppose we have a query vector  $\mathbf{q} \in \mathbb{R}^D$ , a set of S key-value pairs  $\{(\mathbf{k}_i, \mathbf{v}_i) \in \mathbb{R}^D \times \mathbb{R}^D : i \in \{1, 2, \cdots, S\}\}$ , where D is the hidden size. What we want to do through the attention mechanism is to use the query to attend to the keys, and summarize those values associated with the "relevant" keys into a fixed-size context vector  $\mathbf{c} \in \mathbb{R}^D$ . Note that this is different from directly compressing the key-value pairs into a fixed-size vector, since depending on the query, we might end up with different context vectors.

To determine the score for a given query and key, it is standard to use a measure of similarity between the query and key. You've seen such similarity measures before, in labs 1-1 and 1-2. A good choice is simply the normalized dot product between query and key. We'll thus take the

attention score for query  $\mathbf{q}$  and key  $\mathbf{k}_i$  to be

$$a_i = \frac{\exp(\mathbf{q} \cdot \mathbf{k}_i)}{Z},$$

where  $\cdot$  denotes the dot product (inner product) and exp is exponentiation which ensures that all scores are nonnegative, and

$$Z = \sum_{i=1}^{S} \exp(\mathbf{q} \cdot \mathbf{k}_i)$$

is the normalizer to guarantee the scores all sum to one. (There are multiple ways of parameterizing the attention function, but the form we present here is the most popular one.) You might have noticed that the operation above is essentially a softmax over  $\mathbf{q} \cdot \mathbf{k}$ .

The attention scores **a** lie on a *simplex* (meaning  $a_i \ge 0$  and  $\sum_i a_i = 1$ ), which lends it some interpretability: the closer  $a_i$  is to 1, the more "relevant" a key  $k_i$  (and hence its value  $v_i$ ) is to the given query.

To compute the context vector  $\mathbf{c}$ , we take the weighted sum of values using the corresponding attention scores as weights:

$$\mathbf{c} = \sum_{i=1}^{S} a_i \mathbf{v}_i$$

The closer  $a_i$  is to 1, the higher the weight  $\mathbf{v}_i$  receives, and the more the context vector "attends to" the value  $v_i$  at position i.

**Question:** In the extreme, if there exists i for which  $a_i$  is 1, then what will the value of  $\mathbf{c}$  be?

Type your answer here, replacing this text.

In practice, instead of computing the context vector once for each query, we want to combine together computations for different queries (for different positions) to allow for parallel processing on GPUs. This will become especially useful for the transformer implementation in the next lab. We use a matrix  $Q \in \mathbb{R}^{T \times D}$  to store T queries, a matrix  $K \in \mathbb{R}^{S \times D}$  to store S keys, and a matrix  $V \in \mathbb{R}^{S \times D}$  to store the corresponding values. Then we can write down how we compute the attention scores  $A \in \mathbb{R}^{T \times S}$  in a matrix form:

$$A = \operatorname{softmax}(QK^\top, \dim = -1)$$

and to get the context matrix  $C \in \mathbb{R}^{T \times D}$ , we have

$$C = AV$$

**Question:** What is the shape of A? What does  $A_{ij}$  represent?

Type your answer here, replacing this text.

Your first job is to implement this calculation by finishing the attention function below, which takes the Q, K, and V matrices and returns the A and C matrices. Note that for these matrices, there is one additional dimension for the batching, so instead of  $Q \in \mathbb{R}^{T \times D}$ ,  $K, V \in \mathbb{R}^{S \times D}$ ,  $A \in \mathbb{R}^{T \times S}$ ,  $C \in \mathbb{R}^{T \times D}$ , we have  $Q \in \mathbb{R}^{B \times T \times D}$ ,  $K, V \in \mathbb{R}^{B \times S \times D}$ ,  $A \in \mathbb{R}^{B \times T \times S}$ ,  $C \in \mathbb{R}^{B \times T \times D}$ , where B is the batch size. In addition, the function below also takes an argument mask of size  $\mathbb{R}^{B \times T \times S}$  to

mark where attentions are disallowed. This is useful not only in disallowing attending to padding symbols, but also to efficiently train the model.

**Hint:** You might find torch.bmm helpful for batched matrix multiplications. You might need to transpose and reshape tensors to be able to use this function.

**Hint:** As mentioned in the beginning of the lab, you might also find torch.transpose, torch.reshape, torch.masked\_fill, and torch.softmax useful.

**Hint:** A simple trick for masking an attention score is to set it to negative infinity before normalization.

```
[]: #TODO - finish implementing this function.
     def attention(batched_Q, batched_K, batched_V, mask=None):
       Performs the attention operation and returns the attention matrix
       `batched_A` and the context matrix `batched_C` using queries
       `batched_Q`, keys `batched_K`, and values `batched_V`.
       Arguments:
           batched_Q: (bsz, q_len, D)
           batched_K: (bsz, k_len, D)
           batched_V: (bsz, k_len, D)
           mask: (bsz, q_len, k_len). An optional boolean mask *disallowing*
                 attentions where the mask value is *`False`*.
       Returns:
           batched_A: the normalized attention scores (bsz, q_len, k_len)
           batched_C: a tensor of size (bsz, q_len, D).
       11 11 11
      # Check sizes
       D = batched Q.size(-1)
      bsz = batched_Q.size(0)
       q_len = batched_Q.size(1)
       k_len = batched_K.size(1)
       assert batched_K.size(-1) == D and batched_V.size(-1) == D
       assert batched_K.size(0) == bsz and batched_V.size(0) == bsz
       assert batched_V.size(1) == k_len
       if mask is not None:
         assert mask.size() == torch.Size([bsz, q_len, k_len])
       batched A = \dots
       batched C = \dots
       # Verify that things sum up to one properly.
       assert torch.all(torch.isclose(batched_A.sum(-1),
                                      torch.ones(bsz, q_len).to(device)))
       return batched_A, batched_C
```

#### 3.1 Causal attention mask

To efficiently train the model, we want to batch the attention operations together such that they can be fully parallelized along the sequence length dimension. (The non-attention operations are position-wise so they are trivally parallelizable.) Each word  $y_t$  attends to t-1 previous words  $y_1, \ldots, y_{t-1}$ , which means each word  $y_t$  has a different set of key-value pairs. Is it possible to batch them together?

The solution is to use attention masks. For every word  $y_t$ , we give it all key-value pairs at  $y_1, \ldots, y_T$ , and we disallow attending to future words  $y_t, y_{t+1}, \ldots, y_T$  through an attention mask. (Recall that the attention function takes a mask argument.) We usually call this attention mask a causal attention mask, as it prevents the leakage of information from the future into the past. Since every  $y_t$  has the same set of (key, value) pairs, we can batch them and compute the context vectors using a single call to the function attention.

What should such a mask be? Implement the causal\_mask function below to generate this mask.

Hint: you might find torch.triu useful.

```
[]: #TODO - implement this function, which returns a causal attention mask

def causal_mask(T):
    """
    Generate a causal mask.
    Arguments:
        T: the length of target sequence
    Returns:
        mask: a T x T tensor, where `mask[i, j]` should be `True`
        if y_i can attend to y_j, and `False` if y_i cannot
        attend to y_j
    """
    mask = ...
    return mask.to(device)
```

We can visualize the attention mask and manually check if it's what we expected.

```
[]: fig, ax = plt.subplots(figsize=(8, 6))

T = 7
mask = causal_mask(T)
ax.imshow(mask.cpu())

# Uncomment the line below if the plot does not show up
# Make sure to comment that before submitting to gradescope
# since there would be some autograder issues with `plt.show()`
#plt.show()
```

by using causal masks, all positions (at the same layer) can be computed all at once (if the lower layer has been computed). The parallelizability of the attention mechanism is the key to its success since it allows for training it on vast amounts of data.

Now we are ready to complete the attention model. > Hint: The causal mask is a 2-D matrix, but

we want to add a batch dimension, and expand it to be of the desired size. For this purpose, you can use torch.repeat.

Complete the forward function

```
[]: class ATTNLM(torch.nn.Module):
       def __init__(self, hf_tokenizer, embedding_size, hidden_size):
         super().__init__()
         self.hf_tokenizer = hf_tokenizer
         self.pad_index = hf_tokenizer.pad_token_id
         self.hidden_size = hidden_size
         vocab_size = len(hf_tokenizer)
         # Create modules
         self.embed = torch.nn.Embedding(vocab_size, embedding_size)
         self.q proj = nn.Linear(hidden size, hidden size)
         self.k_proj = nn.Linear(hidden_size, hidden_size)
         self.v_proj = nn.Linear(hidden_size, hidden_size)
         self.hidden2output = torch.nn.Linear(hidden_size, vocab_size)
       def forward(self, context_words):
         """Computes the distribution over the next word given context_{\sqcup}
      → `history_words`.
         Arguments:
           context_words: batch a list of word strings, could be an empty list when ⊔
      \hookrightarrow generating
                           the first word.
         Returns:
           logits, should be a tensor of size (batch, seq_length, vocab_size)
         self.eval()
         context = self.hf_tokenizer(context_words, is_split_into_words=True,__
      →return_tensors='pt')['input_ids']\
                    .long()\
                    .to(device) # bsz, context_len
         context_len = context.size(1)
         context_bsz = context.size(0)
         # For generating the first word, we feed in a special beginning-of-sentence
      ⇔symbol <pad>,
         # which is also what we use for padding. In future labs we'll be using \Box
      ⇔ <bos>, but as long
         # as training and evaluation use the same beginning-of-sentence symbol, it_{\sqcup}
      \hookrightarrow doesn't matter
         # which particular symbol we use.
         if context len == 0:
           context = context.new(1, 1).fill_(self.pad_index)
```

```
context_len = context.size(1)

hidden = None
# TODO: finish feedforward and set logits
# Logits should be a tensor of size (bsz, seq_length, vocab_size)
# The structure of the network is
# embeddings -> output -> hidden2output -> logits
output = attention(q, k, v, mask)[1]
logits = self.hidden2output(output)

return logits
```

Now, let's load the pretrained models for Hamilton and Madison. The model attn\_lm\_madison was trained on documents authored by Madison, whereas attn\_lm\_hamilton was trained on documents authored by Hamilton.

### 3.2 Sampling from the attention model

Let's try to sample from the models.

```
[]: print(' '.join(sample_sequence(attn_lm_madison, ('constitution', 'proposed', \( \to 'by', 'the'))), "\n")
    print(' '.join(sample_sequence(attn_lm_hamilton, ('constitution', 'proposed', \( \to 'by', 'the'))))
```

## 3.3 Evaluating text according to the attention model

```
[]: document_madison = validation_madison[0]['tokens']
document_hamilton = validation_hamilton[0]['tokens']
```

Just like in Lab 2-3, we want to evaluate the models using perplexity.

```
[]: def neglogprob(tokens, model):
         """Returns the negative log probability of a sequence of `tokens`
            according to a `model`
         score = 0.0
         for i in range(len(tokens)):
           context = tokens[:i]
           token = tokens[i]
           distribution = model(context)
           logits = model(context)[:,-1]
           probs = torch.softmax(logits, -1).view(-1) # vocab size
           distribution = {}
           for i, prob in enumerate(probs):
             word = hf_tokenizer.decode(i, clean_up_tokenization_spaces=True)
             distribution[word] = prob.item()
           prob = distribution[token] if token in distribution else

distribution['[UNK]']

           score += -math.log2(prob)
         return score
```

```
[]: def perplexity(tokens, model):
    """Returns the perplexity of a sequence of `tokens` according to a `model`
    """
    return 2 ** (neglogprob(tokens, model) / (len(tokens)))
```

Calculate the perplexity of each model on each document.

```
[]: # TODO
attn_ppl_madison_model_madison_document = ...
attn_ppl_hamilton_model_madison_document = ...
attn_ppl_madison_model_hamilton_document = ...
attn_ppl_hamilton_model_hamilton_document = ...
```

Now, let's compare those perplexity values. Do the results make sense to you?

```
[]: print (f"Author Madison Model Hamilton Model\n"

f"Madison {attn_ppl_madison_model_madison_document:5.1f} 
{attn_ppl_hamilton_model_madison_document:5.1f}\n"

f"Hamilton {attn_ppl_madison_model_hamilton_document:5.1f} 
{attn_ppl_hamilton_model_hamilton_document:5.1f}")
```

Although attention is a powerful concept, it alone isn't enough to build a strong model. In the next lab, you will learn about the *Transformer language model*, which is built on the attention mechanism along with several other important components.

## 4 Lab debrief

Question: We're interested in any thoughts your group has about this lab so that we can improve this lab for later years, and to inform later labs for this year. Please list any issues that arose or comments you have to improve the lab. Useful things to comment on include the following:

- Was the lab too long or too short?
- Were the readings appropriate for the lab?
- Was it clear (at least after you completed the lab) what the points of the exercises were?
- Are there additions or changes you think would make the lab better?

Type your answer here, replacing this text.

## End of Lab 2-3

To double-check your work, the cell below will rerun all of the autograder tests.

[]: grader.check\_all()