1 Recurrent Neural Network

The world is full of sequential information, from video to language modelling to time series data. In particular, we would like to model these sequences using neural networks, and solve some major types of tasks that we would like to solve with sequence models.

1.1 Types of Problems

- **One-to-one** problems take a single input $x$ and produce a single output $y$. Problems like classification (takes an image as input, and produces a class label as output) and semantic segmentation (image as input, segmentation mask as output) fall under this category.

- **One-to-many** problems take a single input, and produce a sequence of output. Problems like image captioning (takes a single image as input, and produces a caption (a sequence of words) as output) fall under this category.

- **Many-to-many** problems take sequences of inputs and produce sequences of outputs. Problems like language translation (sequence of words in one language to sequence of words in another) fall under this category.

![Figure 1: Types of problems we would like to solve using sequential models](image)

1.2 Why the Recurrence?

As you read through this discussion worksheet, you don’t process each word entirely on its own, but instead use your understanding from the previous words as well. Traditional neural networks do not have the capability to use its reasoning about previous events to infer later ones. For example, if we would like to classify what is happening at every frame in a movie, this can be framed as an image classification task where the network is provided the current image. However, it is unclear how a traditional neural network should incorporate knowledge from the previous frames in the film to inform later ones.
Recurrent neural networks (RNNs) address this issue, by using the idea of “recurrent connections.” RNNs are networks with loops in them that allow information from previous inputs to persist as the network processes the future inputs. These recurrent connections allow information to propagate from “the past” (earlier in the sequence) to the future (later in the sequence).

In Figure 2, we illustrate the RNN computation as it is unrolled through time. Each $i \in \{0, \ldots, t\}$ represents a new timestep in the network. By feeding in a state computed from earlier timesteps as an input together with the current input, information can persist throughout the time as the network “remembers” the past inputs it processed.

1.3 Vanilla RNN

In the following section, we will use the following notation. Denote the input sequence as $x_t \in \mathbb{R}^k$ for $t \in \{1, \ldots, T\}$, and output of the network be $y_t \in \mathbb{R}^m$ for $t \in \{1, \ldots, T\}$. In the following example, we construct a "vanilla" many-to-many RNN, consisting of a node that updates the hidden state $h_t$ and produces an output $y_t$ at each timestep with the following equations:

$$h_t = \tanh(W_{h,h}h_{t-1} + W_{x,h}x_t + B_h)$$
$$y_t = W_{h,y}h_t + B_y$$

where $h_t$ is the time step of a hidden state (one can think of $h_{t-1}$ as the previous hidden state), $W_{..}$ be the set of weights (for example, $W_{x,h}$ represents weight matrix that accepts an input vector and produce a new hidden state), $y_t$ be the output at timestep $t$ and $B_h$ and $B_y$ be the bias terms. We can also represent it as the diagram below,
In this vanilla RNN, we update to a hidden state “$h_t$” based on the previous hidden state $h_{t-1}$ and input at the current time $x_t$, and produce an output which that is a simple affine function of the hidden state. To compute the forward (and backward) passes of the network, we have to "unroll" the network, as shown in Figure 2. This "unrolling" process creates something that resembles a very deep feed forward network (with depth corresponding to the length of the input sequence), with shared affine parameters at each layer. Our gradient is computed by summing the losses from each time-step of the output.

**Problem: Gradients in Vanilla RNN**

Why are vanishing or exploding gradients an issue for RNNs?

**Solution: Gradients in Vanilla RNN**

A major issue with the vanilla RNN is that they suffers from vanishing/exploding gradients similarly to issues with deep feedforward networks. At each timestep, the hidden state $h_t$ is multiplied by $W$, at the last timestep, the value of $h_t$ is effectively multiplied by $W^\top$. This means that depending on the singular values of the matrix $W$, the gradients of the loss with respect to $W$ may become very large or very small as they pass back down the unrolled network. Additionally, the tanh activation at each step can also contribute to the vanishing gradient problem.
Problem: Coding RNNs Up!

Complete the class definition, started for you below,

```python
import numpy as np
class VanillaRNN:
    def __init__(self):
        self.hidden_state = np.zeros((3, 3))
        self.W_hh = np.random.randn(3, 3)
        self.W_xh = np.random.randn(3, 3)
        self.W_hy = np.random.randn(3, 3)
        self.Bh = np.random.randn(3)
        self.By = np.random.randn(3)

    def forward(self, x):
        # Processes the input at a single timestep and updates the hidden state
        self.hidden_state = np.tanh(np.dot(self.hidden_state, self.W_hh) + np.dot(x, self.W_xh) + self.Bh)
        self.output = np.dot(self.W_hy, self.hidden_state) + self.By
        return self.output
```

Solution: Coding RNNs Up!

```python
import numpy as np
class VanillaRNN:
    def __init__(self):
        self.hidden_state = np.zeros((3, 3))
        self.W_hh = np.random.randn(3, 3)
        self.W_xh = np.random.randn(3, 3)
        self.W_hy = np.random.randn(3, 3)
        self.Bh = np.random.randn(3)
        self.By = np.random.randn(3)

    def forward(self, x):
        self.hidden_state = np.tanh(np.dot(self.hidden_state, self.W_hh) + np.dot(x, self.W_xh) + self.Bh)
        self.output = np.dot(self.W_hy, self.hidden_state) + self.By
        return self.output
```
To address the problem of vanishing and exploding gradients, we can use a different kind of recurrent cell - the LSTM cell (standing for "long short term memory"). The layout of the cell is shown in Figure 4. The LSTM has two states which are passed between timesteps: a "cell memory" $C_t$ and the hidden state $h_t$. The LSTM update is given as follows:

$$f_t = \sigma(x_t U_f + h_{t-1} W_f)$$
$$i_t = \sigma(x_t U_i + h_{t-1} W_i)$$
$$o_t = \sigma(x_t U_o + h_{t-1} W_o)$$
$$\tilde{C}_t = \tanh(x_t U_g + h_{t-1} W_g)$$
$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t$$
$$h_t = \tanh(C_t) \odot o_t$$

where $\odot$ represents the Hadamard Product (elementwise multiplication).

The update function is rather complex, but it makes a lot of sense when looking at it in the context of the cell state $C_t$ as a "memory". First, we compute the value $f_t$, which we call the "forget" gate, as it controls how we retain information through time. Because of the sigmoid activation function, $f_t$ is bounded between 0 and 1, and the first thing we do is multiply the previous memory by $f_t$. Intuitively, if $f_t$ is close to 1, we "remember" the previous state, and if $f_t$ is close to 0, we forget it. Next, we compute $i_t$, which we consider as the "input/update" gate, which controls how much we update the cell memory at the current timestep. The update gate gets added to the memory cell, so it takes information from the current input $x_t$ and adds it to the memory. Finally, the output gate $o_t$ controls the output of the network, the value that gets passed on to the next cell.

We can compare the LSTM to a vanilla RNN. Since a vanilla RNN had to use the hidden state $h_t$ both to produce outputs as well as store memories, $h_t$ gets updated with an affine map and a tanh activation at every timestep, which can easily lead to vanishing or exploding gradients. On the other hand, the LSTM can use the cell state $C_t$ as its "long-term memory," and backpropagation through the long term memory is much easier since the cell states change fairly slowly in a simple way (simply being a moving average of the compute $\tilde{C}_t$’s.). On the other hand, the hidden state in the LSTM can serve as a "short-term memory" and change quickly through time.

![Figure 4: An overview of the LSTM cell](image-url)
Problem: Backpropagation Through LSTM

Denote the final cost function as $J$. Compute the gradient $\frac{\partial J}{\partial W}$ using a combination of the following gradients,

$$
\frac{\partial h_t}{\partial h_{t-1}} \cdot \frac{\partial h_{t-1}}{\partial W^g} \cdot \frac{\partial J}{\partial h_t} \cdot \frac{\partial C_t}{\partial h_t} \cdot \frac{\partial C_{t-1}}{\partial C_t} \cdot \frac{\partial C_t}{\partial o_t} \cdot \frac{\partial h_t}{\partial o_t}
$$

Solution: Backpropagation Through LSTM

$$
\frac{\partial J}{\partial W} = \sum_{t=1}^{T} \frac{\partial J}{\partial h_t} \frac{\partial h_t}{\partial h_t}
= \sum_{t=1}^{T} \frac{\partial J}{\partial h_t} \left( \frac{\partial h_t}{\partial C_t} \left( \frac{\partial C_t}{\partial W^g} + \frac{\partial C_t}{\partial C_{t-1}} \frac{\partial C_{t-1}}{\partial W^g} \right) + \frac{\partial h_t}{\partial h_{t-1}} \frac{\partial h_{t-1}}{\partial W^g} \right)
$$

Problem: Vanishing Gradient in LSTMs

Using the previously derived gradient, which part of $\frac{\partial J}{\partial W}$ allows LSTMs to mitigate the vanishing gradient problem?

Solution: Backpropagation Through LSTM

We know $\frac{\partial C_t}{\partial C_{t-1}} = f_t$, so the forget gate can act as the identity function when $f_t = 1$. This allows the gradients entering the current cell to pass to the previous cell (partially analogous to skip connections in ResNet).