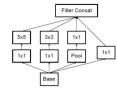
#### Modern CNN

You have been introduced to the original inception module.



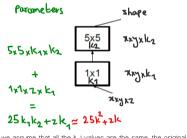
### 1.1 (5 Points)

1

Show that the following module is more parameter efficient than the original one.



The only difference between this model and the original one is in the left branch of architecture. So we should just compare these models by the parameter counts in the left branch. We assume that that the base is in shape x\*y\*z and we use k\_i filters at each convolutional layer. For the simplicity we don't consider bias parameter in the following calculations. Parameters Shape



If we assume that all the k\_i values are the same, the original model has 25k^2 + zk parameters and this model has 18k^2 + zk parameters so this model is more parameter efficient.

- 18 k2+zk

## (5 Points)

Show that you can save more computation by factorizing  $3 \times 3$  convolutions into two  $2 \times 2$  convolutions. (One branch is enough.)

we assume that the shape of the input to the 3+3 convolution layer is x+y+k. For the simplicity we count the number of multiplications for measuring the computational cost. Computational cost Computational cost ادّع 3\*3

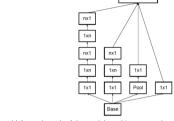
If we assume that all the k\_i values are equal to k, the model with 3\*3 convolution layers computation cost will be about 9xyk^2 whereas the model with of 3\*3 convolutions replaced by two 2\*2 convolutions computation cost will be about 8xyk^2. So we can save more computation by factorizing 3\*3 convolution layers into two 2\*2 convolutions.

#### (10 Points)

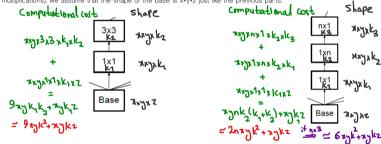
1.3

Show that using asymmetric convolutions as follows saves computation. (One branch is enough.) How do you compare this enhancement with the previous one?

Filter Concat



We take the second leftmost branch of the models architecture and we calculate the computation cost (number of multiplications). We assume that the shape of the base is x\*v\*z just like the previous parts.



As it can be seen same as the previous parts if we assume that all the k\_i values are equal to k we can easily understand that this asymetric convolution inception model saves more computation in comparison with the original model.

There is much more enhancement in the computational cost in this model than there is in the previous one because its computational cost is 6xyk^2 where the previous model's computational cost was 8xyk^2.

#### 1.4 (10 Points)

Consider the following methods for grid size reduction. Which one do you prefer in terms of computational cost? Which one creates a representational bottleneck?



The left method seems to save more computational cost because the inception layers first two dimensions are 17-17 and so when computing the cost we would have the summation of some terms of 17-17. For example in the previous question you can see that there is this xy term in the computational cost of the models. However int the right method first two dimensions of the input layers, is 34-34 and in compare to the left method this could lead to much more computational cost.

Also it can be derived from the figure that the max pooling layer uses a 3.3 filter with stride 2 so the computational cost of the max pooling layer in the left method is 3.3.17.17.20 and in the right method is 3.3.17.17.640. Maxpooling layer seems to have less computational cost in the right method but the since the inception cost would possibly be much higher in the right method we choose the left method as the one with less computational cost.

Also the left method creates a representational bottleneck because it reduces the dimensions in the middle layer and some how loses some data but by using inception in the next layer it increases the dimensions. But in the right method the dimensions are first increased and then decreased, so the left method seems to be a better representation of bottleneck.

## Autoencoders

1000 gene expression profile samples are given to us. These samples contain normal and cancer cases. The objective is to design a model which can distinguish cancer samples from normal ones. To do so, we have split the data into 800 train and 200 test samples. Each gene expression profile is a 20,000 dimension vector of numbers between 0 and 15. We have designed a 7-layer Autoencoder. The first and last layers have 2000 neurons, the second and 6th layers have 200 neurons and the fourth layer has only 20 neurons. Consider that all of the layers are fully-connected layers and the activation function for all of the neurons is sigmoid. The loss function has been chosen to be MSE.

#### (5 Points) 2.1

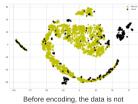
We have trained the network for 100 epochs but the loss function value does not decrease. What is the main reason?

One first simple reason for why the loss function doesn't decrease is that maybe the learning rate is too high and the loss function gets stuck in a loop or even gets too far from local minima. Another reason could be because of bad initialization of the weights which led the loss function to get stuck in a loop or even increase.

### (10 Points)

After solving the problem, we again train the network for 100 epochs. We observe that MSE is less than 0.1 for test samples. Can we thereby conclude that the network is performing well? If not, what should we check?

This ou MSE loss is the loss of the encoder in the ability of encoding the inputs into the latent space so then it could be decoded to its original input. What we wanted to do was to catogrize the samples into cancer or normal using this encoder. The benefit of using such an auto encoder is that we can use the latent space and possibly classify the samples by using a simpler model like logistic regression or support vector classifier on the latent space. So in order to evaluate the models performance we should first encode all the test samples using the autoencoder and then use for example logistic regression and evaluate the accuracy of it's classification. In another word, we should check that if the encoded cancer and normal samples are easily seperable or not. For a better insight, you can see the plots of tsne dimension reduction of the transaction data in the task of finding fraud from transactions before and after using the autoencoder. This example is inspired from ml-classifying-data-using-an-auto-encoder.



easily seperable



After using an autoencoder and encoding the samples into latent space the fraud samples are even linearly seperable.

### 2.3 (10 Points)

After the training process, we notice that with every small change in input values, a lot of neurons from the latent layer will change. What should we do in order to solve this issue? Provide a formula if possible.

By using a varational auto encoder we can solve the problem. In a varational auto encoder the data is encoded to a distribution on latent space and it prevents the model to be sensitive to the changing the input. The loss of a VAE is as follows:

In varational auto encoder, the near points in latent space tend to have alike outputs and the outputs are meaningful.

#### 2.4 (10 Points)

Finally we succeed to train the network in a way that with low test error we can reconstruct input samples from the 20 latent neurons. What property of our input data has helped us in this success?

One important property of gene expression data in predicting a disease is that this data space has a low dimensional support. Meaning that the actual meaningful part of this data can be represented in a few dimensions or in another words in a few genes. In fact cancer samples could be detected by just observing the expression of some important genes and so this autoencoder could perfectly classify the samples using the latent space.

## **3** Generative adversarial networks (Optional)

In this question, we will workout backpropagation with Generative Adversarial Networks (GANs). Recall that a GAN consists of a Generator and a Discriminator playing a game. The Generator takes as input a random sample from some noise distribution (e.g., Gaussian), and its goal is to produce something from a target distribution (which we observe via samples from this distribution). The Discriminator takes as input a batch consisting of a mix of samples from the true dataset and the Generator's output, and its goal is to correctly classify whether its input comes from the true dataset or the Generator.

Definitions:

- X<sup>1</sup>,...,X<sup>n</sup> is a minibatch of n samples from the target data generating distribution For this question, we
  suppose that each X<sup>i</sup> is a k dimensional vector. For example, we, we might be interested in generating a
  synthetic dataset of customer feature vectors in a credit scoring application
- Z<sup>1</sup>,...,Z<sup>n</sup> is a minibatch of n samples from some predetermined noise distribution Note that in general
  these minibatch sizes may be different.
  - The generator  $g(.;\theta_g):Z\to X$  is a neural network
  - The discriminator  $d(.; \theta_d): X \to (0, 1)$  is a neural network

The log likelihood of the output produced by the discriminator is:

$$L(\theta_d, \theta_g) = \sum_{i=1}^{n} \log d(X^i; \theta_d) + \log(1 - D(G(Z^i)))$$
(1)

The training of such a GAN system proceeds as follows; given the generator's parameters, the discriminator is optimized to maximize the above likelihood. Then, given the discriminator's parameters, the generator is optimized to minimize the above likelihood. This process is iteratively repeated. Once training completes, we only require the generator to generate samples from our distribution of interest; we sample a point from our noise distribution and map it to a sample using our generator.

The Discriminator (The generator architecture is defined analogously)

- Consider the discriminator to be a network with layers indexed by  $1, 2, ..., L_d$  for a total of  $L_d$  layers.
  - Let the discriminator's weight matrix for layer l be  $W_d^l$ ; lets assume there are no biases for simplicity
- Let the activations produced by a layer l be given by  $A_d^l$ , and the pre activation values by  $Z_d^l$
- Let q<sup>l</sup><sub>d</sub>(.) be the activation function at layer l

The goal of the discriminator is to maximize the above likelihood function.

### 3.1 (10 Points)

Write down  $\nabla_{\theta_d} L(X; \theta_d, \theta_q)$  in terms of  $\nabla_{\theta_d} D(.)$ 

$$\nabla_{\theta_d} L(X; \theta_d, \theta_d) = \frac{1}{n} \sum_{i=1}^{n} \nabla_{\theta_d} (\log(D(X^i, \theta_d))) + \nabla_{\theta_d} \log(1 - D(G(Z^i)))$$

$$According to = \frac{1}{n} \sum_{i=1}^{n} \frac{\nabla_{\theta_d} D(X^i, \theta_d)}{D(X^i, \theta_d)} - \frac{\nabla_{\theta_d} D(G(Z^i))}{1 - D(G(Z^i))}$$

$$chain rule$$

## 3.2 (15 Points)

Write down

$$\partial L(\theta_d, \theta_g)/\partial z_d^{L_d}$$
 (2)

taking help from your answer in the previous subpart. Remember that the activation function in the last layer of the discriminator is a sigmoid function as the output of the discriminator is a probability.

First note that 
$$\frac{\partial G(x)}{\partial x} = G(x) \times (1 - G(x))$$

Using the previous part's answer we write the  $\frac{\partial L(\theta_d, \theta_g)}{\partial z_d L_d}$ 
 $\frac{\partial L(\theta_d, \theta_g)}{\partial z_d L_d} = \frac{1}{n} \sum_{i=1}^{n} \frac{G(z_d^{-L_d}(X_i)) * (1 - G(z_d^{-L_d}(X_i)))}{D(X_i^{-l_d})}$ 
 $\frac{G(z_d^{-L_d}(G(z_i))) * (1 - G(z_d^{-L_d}(G(z_i))))}{1 - D(G(z_i^{-l_d}))}$ 

### 3.3 (10 Points)

What is mode collapse in GANs? How can it be avoided?

As we know GANs consist of two parts, discriminator and generator. For a GAN to be trained successfully there should be two conditions holding:

The generator should reliably generate data and fool the discriminator.

a. The generator should generate data samples that are diverse as the distribution of the real word data when dealing with multi-modal data.
Model collagse happens when the generator fails to achieve the second goal and for example all of the generated samples are

woder collapse napperts when the generator rais to achieve me second goal and for example all or generated samples are very similar or even identical. In this case the generator may win by creating one realistic data sample that always fools the discriminator, but the second goal doesn't hold any more and this would be a problem especially in a multi modal data. There are three solutions to solve this problem:

- Using Wasserstein loss: Formulates the GAN loss functions to more directly represent minimizing the distance between two
  probability distributions.
- a. Unrolling: Updating the generator's loss function to backpropagate through k steps of gradient updates for the discriminator. This lets the generator see k steps into the future which hopefully encourages the generator to produce more diverse and realistic samples.
- samples.
  3. Packing: Modifying the discriminator to make decisions based on multiple samples all of the same class (either real or artificial).
  When the discriminator looks at a pack of samples at once, it has a better chance of identifying an un-diverse pack as artificial.

## Sequence-to-Sequence Models Comprehension

Answer the following questions

### 4.1 (15 Points)

How can vanishing and exploding gradients be controlled in RNN?

The exploding problem could be solved by gradient clipping because in this approach the gradients are ensured to have their maximum norm bound by a predefined hyperparameter and they are scaled if their norm is too big.

But for vanishing gradients issue in RNN the suggested solution is to change the structure of RNN and use LSTMs instead because in LSTM there is an uniterrupted gradient flow in each cell architecture similar to ResNet.

### 4.2 (5 Points)

What are the advantages of bi-directional LSTM over simple LSTM?

Their advantage is that the information about future is considered when predicting each y. bi-directional LSTM is useful for modeling dependencies between words and phrases in both directions and each cell has information about both past and present.

#### 4.3 (10 Points)

Why is encoder-decoder architecture used in Machine Translation? Explain problems of this architecture.

The reason that we use encoder-decoder is that by using this architecture we can save the input sentence into an encoded vector that preserves the meaning of it using encoder and then we build the output translated sentence using decoder. The problem with normal RNN architecture is that in those kinds of models for the task of translation the translation would be performed word by word without caring about the global meaning of the sentence. Encoder-decoder architecture has some problems too. One of its most important problems is that when the length of the input sequence gets large the model captures the essential information roughly. To solve this problem an approach called teacher forcing is used. Another problem of encoder-decoder architecture is that at the early stages of training the predictions of the model are very bad.

### 4.4 (10 Points)

What is beam search algorithm? Explain this algorithm briefly.

Beam search is a type of search algorithm we use for finding the inference of  $y_{-}t$ .

We would like the argmax of the written probability to find the combination of ys which has the largest probability of happening.

The usual approach to find this probability is to use greedy search and at each step select the word with the highest probability.  $_{\perp}$ 

max 
$$\prod_{i=1}^{t} P(j, |j_{i-1}, \dots, j_i, input) \simeq \prod_{i=1}^{t} \max P(j, |j_{i-1}, \dots, j_i, input)$$

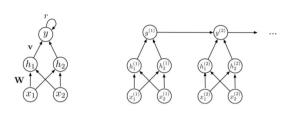
But this search algorithm doesn't find the best combination neccesarily. Another search algorithm is Brute force search that computes the probability for all the available combinations which demands a lot computation. However there is an approach which is something between the brute force and greedy search algorithm and finds the combination better than greedy approach and demands less computation than brute force. In this algorithm we keep a fixed number(k) of candidates having the most probability instead of one in greedy search and we try to expand these k candidates into their y at the next t and again we just select the best k candidates of the resultant candidates. The following figure shows this algorithm steps for kez.



#### 5 RNN Calculation

## (20 points)

We want to process two binary input sequences with 0-1 entries and determine if they are equal. For notation, let  $x_1 = x_1^{(1)}, x_1^{(2)}, \dots, x_1^{(T)}$  be the first input sequence and  $x_2 = x_2^{(1)}, x_2^{(2)}, \dots, x_2^{(T)}$  be the second. We use the RNN architecture shown in the Figure.



We have the following equations in which W is a  $2 \times 2$  matrix, b is a two dimensional bias vector, v is a two dimensional weight vector and  $r, C, C_0$  are scalars.

$$\begin{split} h^{(t)} &= g(Wx^{(t)} + b) \\ y^{(t)} &= \begin{cases} g(v^Th^{(t)} + ry^{(t-1)} + C) & \text{if } \mathbf{t} > 1 \\ g(v^Th^{(t)} + C_0)) & \text{if } \mathbf{t} = 1 \end{cases} \\ g(z) &= \begin{cases} 1 & \text{if } \mathbf{z} > 1 \\ 0 & \text{if } \mathbf{z} < 1 \end{cases} \end{split}$$

Find  $W, b, v, r, C, C_0$  such that at each step  $y^{(t)}$  indicates whether all inputs have matched up to the current

time or not.

We short with 
$$t=1$$
,  $y^{(1)} = g(\sqrt{h}, 0] + (0) = g(\sqrt{g}(W_{x}^{(1)}b) + C_{0})$ 
 $v=\begin{bmatrix} v_{1} \\ v_{2} \end{bmatrix}$ 

Lets gaves  $g$  in each case  $\begin{bmatrix} w_{3} & w_{4} \\ w_{3} & w_{4} \end{bmatrix}$ 
 $v=\begin{bmatrix} v_{1} \\ v_{2} \end{bmatrix}$ 

Lets  $g_{x} = g(w_{x} + v_{y})$ 
 $v=v_{1} + v_{2} + v_{3} + v_{4} + v$ 

9 (4/9 ([41+42]+6)+6)

Vo ([23,44]+6)+(0)1 3([24,42]+6) = [1] = V,+V2+(0)1

 $W = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ ,  $b = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$ ,  $V = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$   $\Rightarrow V_3^{t-1} + C = 0 \Rightarrow V_{-1} = 0 \Rightarrow V_{-1} = 0$ 

b1, b2) 1 b1+w2) 1 b2+w4 (1 b1+w4 (1 b2+w3) W1+w2+b1) 1 W3+w4+b2) again we make some raw guesses for bo W based on the above inequalities.

b=
$$\begin{bmatrix} 2\\2 \end{bmatrix}$$
 W= $\begin{bmatrix} -1\\1\\-1 \end{bmatrix}$  So we have  $C_0=0$ , b= $\begin{bmatrix} 2\\2\\2 \end{bmatrix}$ ,  $V=\begin{bmatrix} 1\\1\\1 \end{bmatrix}$ , W= $\begin{bmatrix} -1\\1\\1\\-1 \end{bmatrix}$ 

now we check the RNN for  $\pm 71$ 

if  $y^{t-1}=0$  we would like  $y^{t}=0$  even:if  $x^{t}=x_0^{t}$ 

So if  $y^{t-1}=0 \Rightarrow y^{t}=y(v^{T}g(wx^{T}b)+C)$ 

#Is could be maximumly 2

yt = 9(v7g(wxt+b)+ ryt-1+C)

$$y = g(\sqrt{g(w_x + b)} + ry + l + C)$$

$$\Rightarrow C = -1$$

$$\Rightarrow |f| y = 1$$
this could be maximized 2
$$\Rightarrow |f| y = 1$$
Then it is similar to tall where  $C_0 = 0$ 

# Word Embedding

## (20 points)

By using the following figure(next page), explain skip-gram. Your explanation must include the probability the model wants to estimate, the concept of the context window, the output of the model, and the loss function

used in the training.

Skip-gram is a nlp task in which given a center word we would like to find its context words or in another words, we would like the most probably surrounding words of this center word. As it can be understood from the figure on next page, this task is done in 6 steps: input: center word x

desired output: a list of words (context words) surrounding this center word with the highest probability (yı, ..., yc)

Here we imagine that the context window's length is m and we are considering 2m surrounding words of the center word.(Context window is the number of words to be predicted which can occur in the range of the given word) W: |V|\*N w1. N\*IVI i- We generate the one hot input vector x 2- We encode this vector using W matrix into a n dimensional vector by computing h=W^T.x

3- Since there is just one embedded input vector we don't need to average different vectors as opposed to CBOW. 4- We then Generate 2m score vectors, u\_{c-m}, ..., u\_{c-i}, u\_{c+i}, ..., u\_{c+m} using u=W'^T . h 5- Now, to find the probability of each vector we'll use the softmax function 6- The word with the highest probability is the result and if the predicted word for a given context position is wrong then we'll use backpropagation to modify our weight vectors W and W'

Probability the model wants to estimate:

(20 points) Suppose that the context window (C) is equal to 1. (For example for each center word, we just consider its left

neighbor) We also denote the loss function as  $L(x, \hat{y}, W, W')$ 

In which  $\hat{y}$  is the one-hot encoded vector of the word in the context window and x is the one-hot encoded

vector of the center word. Using the previous part, calculate  $\frac{\partial L}{\partial w_k}$  in which  $w_k$  is the kth row of matrix W. For simplification purposes, you can assume that  $\frac{\partial Softmax(y)}{\partial y}$  is given as S'(y). However, we highly recommend a complete calculation.

L(1,\hat{\Gamma},\W,\W) =  $-l_0 \int_{0}^{1/2} (P(u_{c_{-m+1}}|W_c)) = -l_0 \int_{0}^{1/2} P(u_{c_{-m+1}}|V_c) = -l_0 \int_{0}^{1/2} \frac{P(u_{c_{-m+1}}|V_c)}{\int_{0}^{1/2} erp(W_c^{1/2})} \int_{0}^{1/2} \frac{P(u_{c_{-m+1}}|W_c)}{\int_{0}^{1/2} erp($ 

 $2m = 1 = 2 - 5^{T} \omega^{T} k + \log \left( \frac{V^{T}}{k_{0}} \exp(\omega_{\kappa}^{T} k) \right) - 2 \left( x, y, w \omega \right) = -y^{T} \omega^{T} \omega^{T} x + \log \left( \frac{V^{T}}{k_{0}} \exp(\omega_{\kappa}^{T} \omega^{T} x) \right)$ 

$$\hat{\mathcal{G}} = \left( \begin{array}{c} \hat{\mathcal{G}}_{1} \\ \hat{\mathcal{G}}_{$$

= 2 Intrite = 2 millarithmen + x min ) + ... + 2 min (x min - + x min ) = 0 - 2 - 2 min = - x (2, min - 9 min) = - x min

