# sheet05

November 25, 2024

#### 1 Sheet 5

Oliver Sange, Sam Rouppe van der Voort, Elias Huber

```
[43]: import os
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
```

### 1.1 2 Logistic regression: an LLM lie detector

Download the data from https://heibox.uni-heidelberg.de/f/38bd3f2a9b7944248cc2/ Unzip it and place the lie\_detection folder in the folder named data to get the following structure: "data/lie\_detection/datasets" and "data/lie\_detection/acts".

This is how you can load a dataset of LLM activations. Use a new Datamanager if you want to have a new dataset. Use the same data manager if you want to combine datasets.

```
dm.add_dataset(dataset_name, "Llama3", "8B", "chat", layer=12, split=0.8, __
       ⇔center=False,
                      device='cpu', path_to_datasets=path_to_datasets,_
       →path_to_acts=path_to_acts)
      acts_train, labels_train = dm.get('train') # train set
      acts_test, labels_test = dm.get('val')
      print(acts_train.shape, labels_train.shape)
     torch.Size([1196, 4096]) torch.Size([1196])
[45]: # have a look at the statements that were fed to the LLM to produce the
       →activations:
      df = pd.read_csv(f"{path_to_datasets}/{dataset_name}.csv")
      print(df.head(10))
                                              statement label
                                                                     city \
     0
                   The city of Krasnodar is in Russia.
                                                             1 Krasnodar
     1
             The city of Krasnodar is in South Africa.
                                                             0 Krasnodar
     2
                        The city of Lodz is in Poland.
                                                             1
                                                                     Lodz
     3
        The city of Lodz is in the Dominican Republic.
                                                                     Lodz
                                                             0
                  The city of Maracay is in Venezuela.
     4
                                                             1
                                                                  Maracay
     5
                      The city of Maracay is in China.
                                                             0
                                                                  Maracay
                    The city of Baku is in Azerbaijan.
     6
                                                             1
                                                                     Baku
     7
                       The city of Baku is in Ukraine.
                                                             0
                                                                     Baku
                        The city of Baoji is in China.
     8
                                                             1
                                                                    Baoji
     9
                    The city of Baoji is in Guatemala.
                                                                    Baoji
                        country correct_country
     0
                        Russia
                                         Russia
     1
                  South Africa
                                         Russia
     2
                        Poland
                                         Poland
                                         Poland
     3
        the Dominican Republic
     4
                     Venezuela
                                      Venezuela
     5
                                      Venezuela
                         China
     6
                    Azerbaijan
                                     Azerbaijan
     7
                       Ukraine
                                     Azerbaijan
     8
                         China
                                          China
     9
                     Guatemala
                                          China
     1.1.1 a)
[46]: from sklearn.linear_model import LogisticRegression
      def train_log_reg(X,y,penalty=None,tol=1e-4): # training- data, labels
          clf = LogisticRegression(penalty=penalty,tol=tol)
          clf.fit(X, y)
```

```
return clf

def test_log_reg(clf, X, y): # test- data, labels
    #clf.predict(X)
    return clf.score(X,y)
```

```
for i in range(len(dataset_names)):
    dataset_name = dataset_names[i] # choose some dataset from the above_u

datasets, index "O" loads the "cities" dataset for example

print(f"{dataset_name} performance:")

# the dataloader automatically loads the training data for us

dm = DataManager()

dm.add_dataset(dataset_name, "Llama3", "8B", "chat", layer=12, split=0.8,u

center=False,

device='cpu', path_to_datasets=path_to_datasets,u

path_to_acts=path_to_acts)

acts_train, labels_train = dm.get('train') # train set

acts_test, labels_test = dm.get('val')

clf = train_log_reg(acts_train, labels_train)

score_clf = test_log_reg(clf,acts_test, labels_test)

print(f"score: {score_clf}")
```

```
cities performance :
score: 1.0
neg_cities performance :
score: 1.0
sp_en_trans performance :
score: 1.0
neg_sp_en_trans performance :
score: 1.0
```

The true and flase statements are linearly seperable since we get, perfect or near perfect score without regularization.

#### 1.1.2 b)

```
cities_clf_regularization = train_log_reg(acts_train, labels_train,penalty='12')
```

```
[49]: print("Cities classifier performance on out of distribution test sets:")
     for i in range(1,len(dataset names)):
         dataset_name = dataset_names[i] # choose some dataset from the above_u
       ⇔datasets, index "O" loads the "cities" dataset for example
         print(f"{dataset_name} :")
          # the dataloader automatically loads the training data for us
         dm = DataManager()
         dm.add_dataset(dataset_name, "Llama3", "8B", "chat", layer=12, split=0.8, __
       ⇔center=False,
                          device='cpu', path_to_datasets=path_to_datasets,_
       path_to_acts=path_to_acts)
         acts_test, labels_test = dm.get('val')
         score_cities_clf = test_log_reg(cities_clf,acts_test, labels_test)
         print(f"score unregularized: {score_cities_clf}")
         score_cities_clf_reg = test_log_reg(cities_clf_regularization,acts_test,__
       →labels test)
          print(f"score regularized: {score_cities_clf_reg}")
```

We see that the model does generalize to different true or flase statements, but not to negating true or flase questions.

#### 1.1.3 c)

```
dm = DataManager()
      dm.add_dataset("neg_cities", "Llama3", "8B", "chat", layer=12, split=0.8, __
       ⇔center=False,
                      device='cpu', path_to_datasets=path_to_datasets,_
       ⇒path to acts=path to acts)
      acts_train_neg, labels_train_neg = dm.get('train') # train set
      acts_test_neg, labels_test_neg = dm.get('val')
      # adding the data sets together:
      train_data = t.cat((acts_train, acts_train_neg), dim=0)
      train labels = t.cat((labels train, labels train neg), dim=0)
      test_data = t.cat((acts_test, acts_test_neg), dim=0)
      test_labels = t.cat((labels_test, labels_test_neg), dim=0)
      # shuffeling data and train data
      indices_tr = t.randperm(len(train_labels))
      indices_te = t.randperm(len(test_labels))
      train_data = train_data[indices_tr]
      train_labels = train_labels[indices_tr]
      test_data = train_data[indices_te]
      test_labels = train_labels[indices_te]
[51]: cities cities neg clf = train log reg(train data, train labels)
      cities_cities_neg_clf_regularization = train_log_reg(train_data,__
       ⇔train labels,penalty='12')
[52]: print("Cities and negation citites classifier performance on out of [1]

→distribution test sets:")
      for i in range(2,len(dataset names)):
          dataset_name = dataset_names[i] # choose some dataset from the above_
       ⇔datasets, index "0" loads the "cities" dataset for example
          print(f"{dataset_name} :")
          # the dataloader automatically loads the training data for us
          dm = DataManager()
          dm.add dataset(dataset name, "Llama3", "8B", "chat", layer=12, split=0.8, |
       ⇔center=False,
                          device='cpu', path_to_datasets=path_to_datasets,__
       path_to_acts=path_to_acts)
          acts_test, labels_test = dm.get('val')
          score_cities_cities_neg_clf = test_log_reg(cities_cities_neg_clf,acts_test,_
       →labels test)
          print(f"score unregularized: {score_cities_cities_neg_clf}")
```

```
score_cities_cities_neg_reg =
test_log_reg(cities_clf_regularization,acts_test, labels_test)
print(f"score regularized: {score_cities_cities_neg_reg}")
```

```
Cities and negation citites classifier performance on out of distribution test sets:

sp_en_trans:
score unregularized: 1.0
score regularized: 0.9859154929577465
neg_sp_en_trans:
score unregularized: 0.971830985915493
score regularized: 0.5352112676056338
```

It seems like we can train a logistic regression model for predicting both negating and non negating true false questions, and that it also seems like it generalizes well. Here the unregularized model performed better.

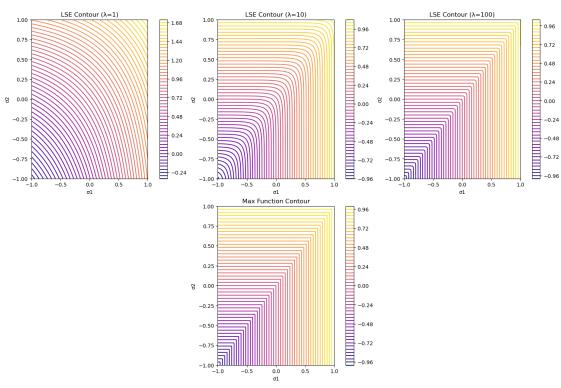
### 1.2 3 Log-sum-exp and soft(arg)max

### 1.2.1 (b)

```
[53]: import numpy as np
      import matplotlib.pyplot as plt
      # Define the LSE function
      def lse(sigma1, sigma2, lambd):
          return (1 / lambd) * np.log(np.exp(lambd * sigma1) + np.exp(lambd * sigma2))
      # Define the max function
      def max_func(sigma1, sigma2):
          return np.maximum(sigma1, sigma2)
      # Generate a grid of sigma1 and sigma2 values
      sigma1 = np.linspace(-1, 1, 500)
      sigma2 = np.linspace(-1, 1, 500)
      sigma1_grid, sigma2_grid = np.meshgrid(sigma1, sigma2)
      # Compute the max function values
      max_values = max_func(sigma1_grid, sigma2_grid)
      # Compute LSE for different values of lambda
      lambdas = [1, 10, 100]
      lse_values = {1: lse(sigma1_grid, sigma2_grid, 1) for 1 in lambdas}
      # Plot the contours
      fig, axes = plt.subplots(2, len(lambdas), figsize=(15, 10),
       ⇔constrained_layout=True)
```

```
# Plot LSE contours
for i, l in enumerate(lambdas):
    cs = axes[0, i].contour(sigma1_grid, sigma2_grid, lse_values[1], levels=50,__
 axes[0, i].set_title(f"LSE Contour (={1})")
   axes[0, i].set xlabel("1")
   axes[0, i].set_ylabel("2")
   fig.colorbar(cs, ax=axes[0, i])
# Plot max function contours
cs = axes[1, 1].contour(sigma1_grid, sigma2_grid, max_values, levels=50,__

cmap='plasma')
axes[1, 1].set_title("Max Function Contour")
axes[1, 1].set_xlabel("1")
axes[1, 1].set_ylabel("2")
fig.colorbar(cs, ax=axes[1, 1])
# Clear unnecessary axes in second row
axes[1, 0].axis('off')
axes[1, 2].axis('off')
plt.show()
```



We observe that for high lambda the sofargmax converges to the argmax contour.

#### 1.2.2 (c)

```
[54]: # Define the softmax components
      def softargmax components(sigma1, sigma2, lambd):
          exp1 = np.exp(lambd * sigma1)
          exp2 = np.exp(lambd * sigma2)
          total = exp1 + exp2
          return exp1 / total, exp2 / total
      # Define the one-hot components for argmax
      def onehot_argmax_components(sigma1, sigma2):
          mask1 = sigma1 > sigma2 # First component of the one-hot vector
          mask2 = ~mask1
                                 # Second component of the one-hot vector (opposite
       ⇔of mask1)
          return mask1.astype(float), mask2.astype(float)
      # Generate a grid of sigma1 and sigma2 values
      sigma1 = np.linspace(-1, 1, 500)
      sigma2 = np.linspace(-1, 1, 500)
      sigma1_grid, sigma2_grid = np.meshgrid(sigma1, sigma2)
      # Compute softargmax and one-hot components
      lambdas = [1, 10, 100]
      softargmax_results = {1: softargmax_components(sigma1_grid, sigma2_grid, 1) for_
      →l in lambdas}
      onehot_results = onehot_argmax_components(sigma1_grid, sigma2_grid)
      # Plot the results
      fig, axes = plt.subplots(len(lambdas), 4, figsize=(20, 15),
       ⇔constrained_layout=True)
      for i, l in enumerate(lambdas):
          # Softarqmax components
          comp1, comp2 = softargmax results[1]
          im1 = axes[i, 0].imshow(comp1, extent=[-1, 1, -1, 1], origin='lower',_L

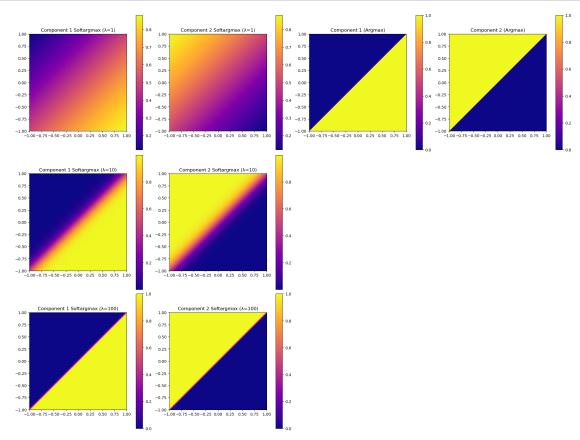
cmap='plasma')

          im2 = axes[i, 1].imshow(comp2, extent=[-1, 1, -1, 1], origin='lower', 

cmap='plasma')
          axes[i, 0].set_title(f"Component 1 Softargmax (={1})")
          axes[i, 1].set_title(f"Component 2 Softargmax (={1})")
          fig.colorbar(im1, ax=axes[i, 0])
          fig.colorbar(im2, ax=axes[i, 1])
      # One-hot components
      comp1_onehot, comp2_onehot = onehot_results
```

```
im3 = axes[0, 2].imshow(comp1_onehot, extent=[-1, 1, -1, 1], origin='lower', u
cmap='plasma')
im4 = axes[0, 3].imshow(comp2_onehot, extent=[-1, 1, -1, 1], origin='lower', u
cmap='plasma')
axes[0, 2].set_title("Component 1 (Argmax)")
axes[0, 3].set_title("Component 2 (Argmax)")
fig.colorbar(im3, ax=axes[0, 2])
fig.colorbar(im4, ax=axes[0, 3])

# Clear unused axes in rows for one-hot ( only affects softargmax)
for row in range(1, len(lambdas)):
    axes[row, 2].axis('off')
    axes[row, 3].axis('off')
```



## 1.3 4 Linear regions of MLPs

### 1.3.1 a)

```
[55]: from torch import nn
      import torch
      import numpy as np
      class MLP(nn.Module):
          Multilayer Perceptron.
        def __init__(self):
          super().__init__()
          self.layers = nn.Sequential(
            nn.Linear(2,20),
           nn.ReLU(),
            nn.Linear(20,1)
          )
        def forward(self, x):
          '''Forward pass'''
          return self.layers(x)
      mlp = MLP()
      params = sum(p.numel() for p in mlp.parameters())
      print(f"Number of parameters: {params}")
```

Number of parameters: 81

## 1.3.2 b)

```
class nn_output_analyzer():
    def __init__(self,model,n_points,xrange):
        self.model = model
        self.num_points = n_points
        self.xrange = xrange

def grid(self):
    # Create grid of points
    x = np.linspace(-self.xrange, self.xrange, self.num_points)
    y = np.linspace(-self.xrange, self.xrange, self.num_points)
    X, Y = np.meshgrid(x, y)

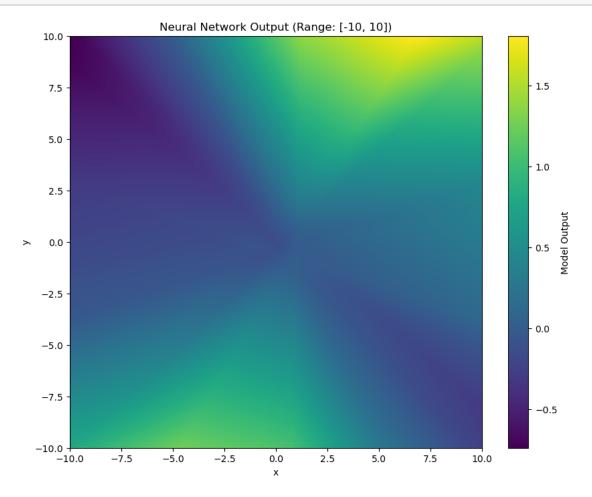
# Prepare input for the model
```

```
grid_points = np.column_stack((X.ravel(), Y.ravel()))
      grid_points_tensor = torch.FloatTensor(grid_points)
       # Evaluate model
      self.model.eval()
      with torch.no_grad():
           Z = self.model(grid_points_tensor).numpy().reshape(self.num_points,_
⇔self.num_points)
      self.Z = Z
       # Create visualization
      plt.figure(figsize=(10, 8))
      plt.imshow(Z, extent=[-self.xrange, self.xrange, -self.xrange, self.
⇔xrange] ,
                  origin='lower', cmap='viridis')
      plt.colorbar(label='Model Output')
      plt.title(f'Neural Network Output (Range: [{-self.xrange}, {self.

¬xrange}])')
      plt.xlabel('x')
      plt.ylabel('y')
      plt.show()
  def grad(self):
             # Compute spatial gradients
      dy, dx = np.gradient(self.Z)
       # Create subplots for visualization
      fig, (ax2, ax3) = plt.subplots(1, 2, figsize=(20, 6))
       # Plot x-component of gradient
      im2 = ax2.imshow(dx, extent=[-self.xrange, self.xrange, -self.xrange,_u
⇔self.xrange],
                        origin='lower', cmap='prism')
      ax2.set_title('Gradient (x-component)')
      ax2.set_xlabel('x')
      ax2.set ylabel('v')
      plt.colorbar(im2, ax=ax2, label='f/x')
       # Plot y-component of gradient
      im3 = ax3.imshow(dy, extent=[-self.xrange, self.xrange, -self.xrange,_u
⇔self.xrange],
                        origin='lower', cmap='prism')
      ax3.set_title('Gradient (y-component)')
      ax3.set_xlabel('x')
      ax3.set_ylabel('y')
      plt.colorbar(im3, ax=ax3, label=' f/ y')
      plt.tight_layout()
```

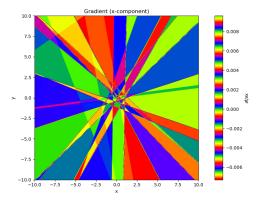
plt.show()

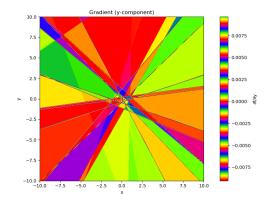
[57]: analyze = nn\_output\_analyzer(mlp,n\_points=500,xrange=10)
analyze.grid()



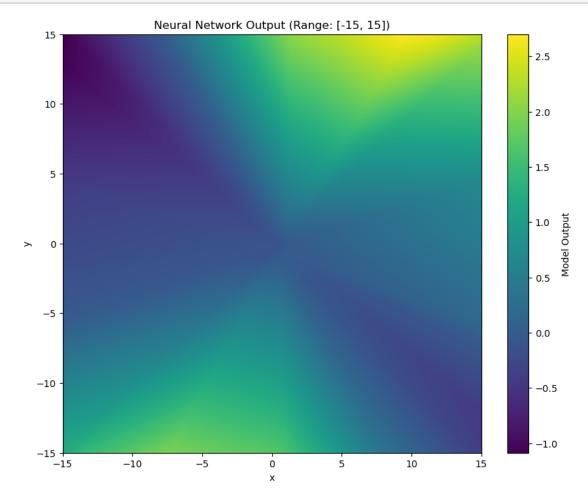
1.3.3 c)

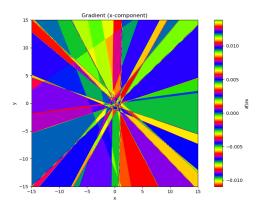
[58]: analyze.grad()

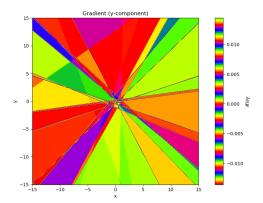




[59]: analyze = nn\_output\_analyzer(mlp,n\_points=500,xrange=15)
analyze.grid()
analyze.grad()







We observe that we can capture the whole structure for a range of 15.

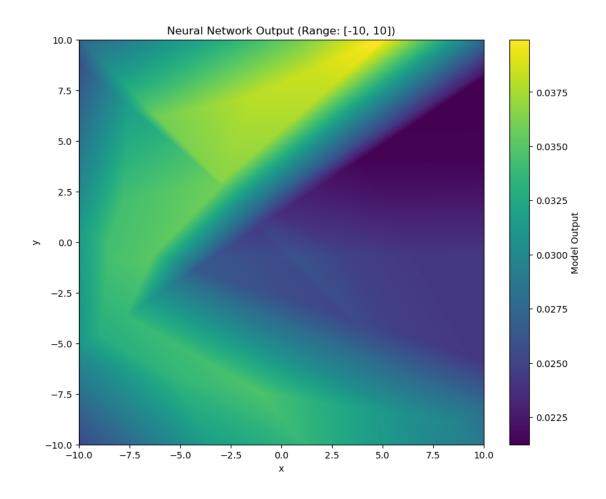
## 1.3.4 d)

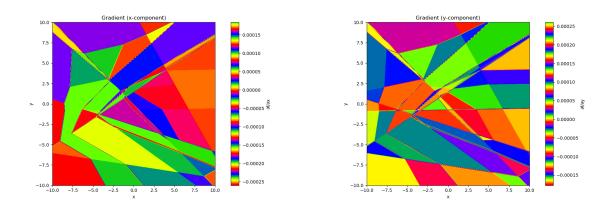
```
[60]: class MLP2(nn.Module):
          Multilayer Perceptron.
        def __init__(self):
          super().__init__()
          self.layers = nn.Sequential(
            nn.Linear(2,5),
            nn.ReLU(),
            nn.Linear(5,5),
            nn.ReLU(),
            nn.Linear(5,5),
            nn.ReLU(),
            nn.Linear(5,5),
            nn.ReLU(),
            nn.Linear(5,1)
        def forward(self, x):
          '''Forward pass'''
          return self.layers(x)
      mlp2 = MLP2()
      params = sum(p.numel() for p in mlp.parameters())
      print(f"Number of parameters: {params}")
```

Number of parameters: 81

```
[61]: class MLP2(nn.Module):
         Multilayer Perceptron.
        def __init__(self):
          super().__init__()
          self.layers = nn.Sequential(
            nn.Linear(2,5),
            nn.ReLU(),
            nn.Linear(5,5),
            nn.ReLU(),
            nn.Linear(5,5),
            nn.ReLU(),
            nn.Linear(5,5),
           nn.ReLU(),
           nn.Linear(5,1)
          )
        def forward(self, x):
          '''Forward pass'''
          return self.layers(x)
      mlp2 = MLP2()
      params = sum(p.numel() for p in mlp.parameters())
      print(f"Number of parameters: {params}")
      analyze = nn_output_analyzer(mlp2,n_points=500,xrange = 10)
      analyze.grid()
      analyze.grad()
```

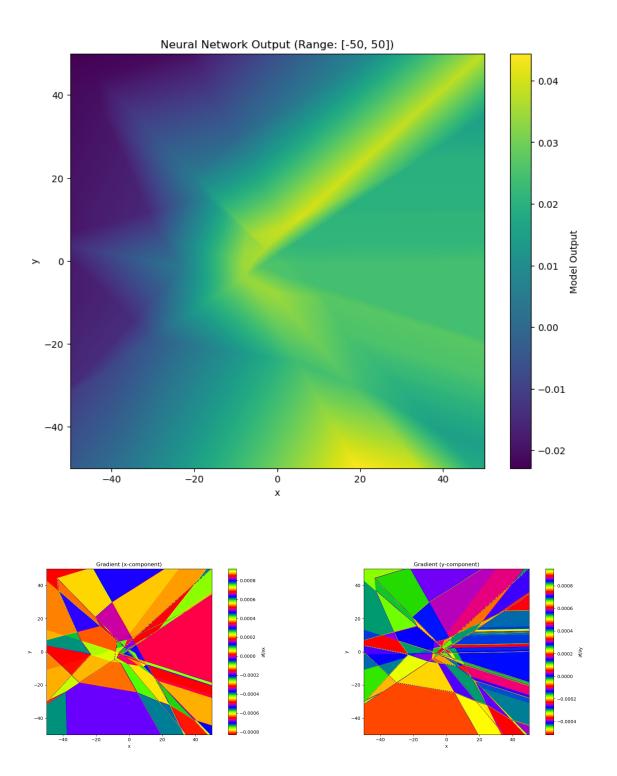
Number of parameters: 81





We observe that we can roughly observe the whole strucure for a range of 50.

```
[62]: analyze = nn_output_analyzer(mlp2,n_points=500,xrange = 50)
analyze.grid()
analyze.grad()
```



We observe that we have to zoom further out for the deep network when comparing to the shalow one to capture the whole structure. We also estimate there to be more affine regions for the deeper network even though both networks have the same parameter count. This is due to the efficiency of depth.

Machine Learning and Physics Sheet 05

a) 
$$\int (x) = \frac{1}{1+e^x}$$

$$= \frac{e^x}{(1+e^x)^2} = \frac{e^x}{(1+e^x)^2} = \frac{1}{e^x \cdot 2+e^x} = \frac{1}{e^x \cdot 2+e^x}$$

$$= \frac{1}{4 \cosh(x)^2}$$

$$= \frac{1}{4 \cosh(x)^2}$$

$$= \frac{1}{4 \cosh(x)^2}$$

$$= \frac{e^x}{e^x}$$
we show that  $2 \sqrt[3]{2x} - 1 = \tanh(x)$ 

$$= \frac{1}{4 e^{2x}}$$

$$=$$

This is the case for w=(1), b=-1/2, so

5 (-1,1)(1) - 1/2 < 1/2 | since 5(-1/2) < 1/2

5(4,1/3)-1/2, since 5(1-1/2)=5(1/2)=5

×=(2,1)

K= (2,3)

$$\frac{e^2}{e^2x} \frac{e^2x}{e^2x} = \frac{e^2x}{(1+e^2x)^2} = \frac{e^2x}{(1+e^2x)^2} = \frac{e^2x}{(1+e^2x)^2}$$

$$= \frac{e^2x}{(1+e^2x)^2} = \frac{e^2x}{(1+e^2x)^2}$$

So wtx, +5 < 0, etc.

J((1,1)(2)-1) 21/2

V(C1/1/2) 1/2 71/2

a) constant offset: softmax(5+C:1) = exp(Nor+Cu) Sk exp (Alt;+6)) G=Ck = exch explosi) = softnax (JA) for C= [ E | E | Dk rescally input: softhax (c.o. 1) = exp(100) Sin expl NO:-E) = exp(low)c Sinep(to) & softnex (T, A) In several the softmax shows identical results only for a constant affect, not for researchy. We this follow that 5, and 52 yield identical reals. d) Deriutile after Lith component: Je Ise (Vi) = 0 1 los (5 exp(Avi)) = A exp(10) e) he prove the statement by showns the inequality in Lath dischers. lim Ise(0,1) = how Alos( Sep(105)) > how A by (entirex) = there are (o) In seltin) = in flal sexp(15) = in flag (Ketings) = in hook) + That the max to max to