Deep Learning CS583 fall 2022
Quiz 2

November 28, 2022

Instructor: Jia Xu

Student name: Dhruv Vaghela

Student ID: 20015603

Student email address: dvaghela@stevens.edu

- **Read these instructions carefully**
- Fill-in your personal info, as indicated above.
- There are eight questions. Each question worths the same (2.5 points).
- Both computer-typed and hand-writing in the very clear form are accepted.
- This is an closed-book test.
- You should work on the exam only by yourself.
- Submit your PDF/Doc/Pages **by 17:30 November 28th** on Canvas under quiz 2.

good luck!

1 Question

- Consider a Generative Adversarial Network (GAN) which successfully produces images of apples. Which of the following propositions is false?

  (i) The generator aims to learn the distribution of apple images.

  (ii) The discriminator can be used to classify images as apple versus non-apple.

  (iii) After training the GAN, the discriminator loss eventually reaches a constant value.

  (iv) The generator can produce unseen images of apples.

Answer: (ii) The discriminator can be used to classify images as apple versus non-apple.

2 Question

Consider the following linear auto-encoder with 1 input and 1 output: $\tilde{x} = w_2 w_1 x$, trained with the squared reconstruction error:

$L(W) = \frac{1}{P} \sum_{i=1}^{P} \frac{1}{2}(x^i - w_2 w_1 x^i)^2$

The scalar training samples have variance 1.

(a) What is the set of solutions (with 0 loss)?

(b) Does the loss have a saddle point? Where?

Answer 2(a): w2w1 = 1

Answer 2(b): Yes, the loss have a saddle point at w1 = 0 and w2 = 0.

3 Question

- Tell the difference among supervised and unsupervised learning and reinforcement learning.

Supervised Learning: This particular learning paradigm deals with the labelled data and the output data patterns are known to the system.

Unsupervised Learning: Unsupervised learning deals with unlabeled data where the output is based on the pool of perceptions.

Reinforcement Learning: An agent learns through delayed feedback by interacting with the environment and making decisions based on prior knowledge (retains as a penalty or reward).

- Give the formula for the loss function used in multiclass classification problems (categorical cross-entropy).

- Is it possible to construct a single layer neural network with threshold activation function implementing XOR of two bits? Construct a neural network implementing XOR.

- Is it possible to construct a single layer neural network with threshold activation function implementing addition of two bits?

- Construct a single layer neural network (define architecture, activation function and give a vector of weights) with a single output implementing conjunction of n bits.

4 Question

Auto-Encoders: auto-encoders are machines of the form

$\tilde{Y} = Decoder(W_d, Z)$

$Z = Encoder(W_e, Y)$

where We are the parameters of the encoder, and W_d is the parameters of the decoder.

(a) Given a training set $\{Y_i, i \in [1, P]\}$, write a possible loss function with which to train a sparse auto-encoder.

(b) Assuming the decoder is linear Decoder $(W_d, Z) = W_d Z$, what constraint should we add to prevent the system from converging to a trivial and useless solution?

5 Question

Consider the following linear auto-encoder with 1 input and 1 output: $\tilde{x} = w_2 w_1 x$, trained with the squared reconstruction error:

$L(W) = \frac{1}{P} \sum_{i=1}^{P} \frac{1}{2}(x^i - w_2 w_1 x^i)^2$

The scalar training samples have variance 1.

(a) What is the set of solutions (with 0 loss)?

(b) Does the loss have a saddle point? Where?

Answer 5(a): w2w1 = 1

Answer 5(b): Yes, the loss have a saddle point at w1 = 0 and w2 = 0.

6 Question

A neural network has been encrypted on a device. You can access neither its architecture nor the values of its parameters. Is it possible to create an adversarial example to attack this network? Explain why.

Yes. A number of black box attacks involve model extraction to create a local model, sometimes known as a substitute or surrogate model. This can be achieved by getting the model architecture and replicating the model with exact input and hidden layer parameters. Existing attacks are then executed against the local model to generate adversarial samples with the hope that these samples also evade the target model.

7 Question

- What is the advantage and disadvantage of attentional models compared to RNNs.

- Draw the computational graph of a one-hidden layer feed-forward neural network and write the derivatives of each variable in the backpropagation.

8 Question

Choose one correct answer from four candidates:

- In practice, what is the most accurate description for activation functions (such as Sigmoid, Sum, Tanh, ReLU) used in neural networks?

    1. They must be differentiable.
    2. They can be non-differentiable, but only for a small number of points.
    3. They can be any continuous functions.
    4. They must be non-linear to be learnable.

    Answer: Option 2

- Given a neural network with N input nodes, no hidden layers, one output node, with entropy loss and sigmoid activation functions, which of the following algorithms (with the proper hyper-parameters and initialization) can be used to find the global optimum?

    1. Stochastic Gradient Descent
    2. Batch Gradient Descent
    3. Mini-Batch Gradient Descent
    4. All of the above

    Answer: Option 4

- You want to train a neural network to predict the next 30 daily prices using the previous 30 daily prices as inputs. Which model selection and explanation make the most sense?

    1. A fully connected deep feed-forward network because it considers all input prices in the hidden layers to make the best decision.
    2. A single one-directional RNN because it considers the order of the prices, and the output length is the same as the input length.
    3. A bidirectional RNN because the prediction benefits from future labels.
    4. A one-directional encoder-decoder architecture can generate a sequence of future prices based on all historical input prices.

    Answer: Option 4