CSC 311: Introduction to Machine Learning Lecture 5 - Multiclass Classification & Neural Networks I

Murat A. Erdogdu & Richard Zemel

University of Toronto

- Classification: predicting a discrete-valued target
  - ▶ Binary classification: predicting a binary-valued target
  - ▶ Multiclass classification: predicting a discrete(> 2)-valued target
- Examples of multi-class classification
  - ▶ predict the value of a handwritten digit
  - ▶ classify e-mails as spam, travel, work, personal

• Classification tasks with more than two categories:





- Targets form a discrete set  $\{1, \ldots, K\}$ .
- It's often more convenient to represent them as one-hot vectors, or a one-of-K encoding:

$$\mathbf{t} = \underbrace{(0, \dots, 0, 1, 0, \dots, 0)}_{\text{entry } k \text{ is } 1} \in \mathbb{R}^{K}$$

- Now there are D input dimensions and K output dimensions, so we need  $K \times D$  weights, which we arrange as a weight matrix **W**.
- Also, we have a K-dimensional vector  $\mathbf{b}$  of biases.
- Linear predictions:

$$z_k = \sum_{j=1}^{D} w_{kj} x_j + b_k$$
 for  $k = 1, 2, ..., K$ 

• Vectorized:

$$z = Wx + b$$

# Multiclass Classification

- Predictions are like probabilities: want  $1 \ge y_k \ge 0$  and  $\sum_k y_k = 1$
- A natural activation function to use is the softmax function, a multivariable generalization of the logistic function:

$$y_k = \operatorname{softmax}(z_1, \dots, z_K)_k = \frac{e^{z_k}}{\sum_{k'} e^{z_{k'}}}$$

- The inputs  $z_k$  are called the logits.
- Properties:
  - Outputs are positive and sum to 1 (so they can be interpreted as probabilities)
  - ▶ If one of the  $z_k$  is much larger than the others,  $\operatorname{softmax}(\mathbf{z})_k \approx 1$  (behaves like argmax).
  - **Exercise:** how does the case of K = 2 relate to the logistic function?
- Note: sometimes  $\sigma(\mathbf{z})$  is used to denote the softmax function; in this class, it will denote the logistic function applied elementwise.

• If a model outputs a vector of class probabilities, we can use cross-entropy as the loss function:

$$egin{aligned} \mathcal{L}_{ ext{CE}}(\mathbf{y},\mathbf{t}) &= -\sum_{k=1}^{K} t_k \log y_k \ &= -\mathbf{t}^{ op}(\log \mathbf{y}), \end{aligned}$$

where the log is applied elementwise.

• Just like with logistic regression, we typically combine the softmax and cross-entropy into a softmax-cross-entropy function.

### Multiclass Classification

ć

• Softmax regression:

$$\begin{aligned} \mathbf{z} &= \mathbf{W}\mathbf{x} + \mathbf{b} \\ \mathbf{y} &= \operatorname{softmax}(\mathbf{z}) \\ \mathcal{L}_{\operatorname{CE}} &= -\mathbf{t}^{\top}(\log \mathbf{y}) \end{aligned}$$

• Gradient descent updates can be derived for each row of W:

$$\frac{\partial \mathcal{L}_{\text{CE}}}{\partial \mathbf{w}_k} = \frac{\partial \mathcal{L}_{\text{CE}}}{\partial z_k} \cdot \frac{\partial z_k}{\mathbf{w}_k} = (y_k - t_k) \cdot \mathbf{x}$$
$$\mathbf{w}_k \leftarrow \mathbf{w}_k - \alpha \frac{1}{N} \sum_{i=1}^N (y_k^{(i)} - t_k^{(i)}) \mathbf{x}^{(i)}$$

• Similar to linear/logistic reg (no coincidence) (verify the update)

• Visually, it's obvious that **XOR** is not linearly separable. But how to show this?



# Limits of Linear Classification

# Showing that XOR is not linearly separable (proof by contradiction)

- If two points lie in a half-space, line segment connecting them also lie in the same halfspace.
- Suppose there were some feasible weights (hypothesis). If the positive examples are in the positive half-space, then the green line segment must be as well.
- Similarly, the red line segment must line within the negative half-space.



• But the intersection can't lie in both half-spaces. Contradiction!

## Limits of Linear Classification

• Sometimes we can overcome this limitation using feature maps, just like for linear regression. E.g., for **XOR**:

$$\boldsymbol{\psi}(\mathbf{x}) = \begin{pmatrix} x_1 \\ x_2 \\ x_1 x_2 \end{pmatrix}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

$$\frac{x_1 \quad x_2 \quad \psi_1(\mathbf{x}) \quad \psi_2(\mathbf{x}) \quad \psi_3(\mathbf{x}) \quad t}{0 \quad 0 \quad 0 \quad 0}$$

- This is linearly separable. (Try it!)
- Not a general solution: it can be hard to pick good basis functions. Instead, we'll use neural nets to learn nonlinear hypotheses directly.

Intro ML (UofT)

# Neural Networks

. . .



. . .

# Inspiration: The Brain

• Neurons receive input signals and accumulate voltage. After some threshold they will fire spiking responses.



[Pic credit: www.moleculardevices.com]

# Inspiration: The Brain

• For neural nets, we use a much simpler model neuron, or **unit**:



• Compare with logistic regression:  $y = \sigma(\mathbf{w}^{\top}\mathbf{x} + b)$ 



• By throwing together lots of these incredibly simplistic neuron-like processing units, we can do some powerful computations!

Intro ML (UofT)

- We can connect lots of units together into a **directed acyclic graph**.
- Typically, units are grouped together into **layers**.
- This gives a feed-forward neural network. That's in contrast to recurrent neural networks, which can have cycles.



- Each hidden layer *i* connects  $N_{i-1}$  input units to  $N_i$  output units.
- In the simplest case, all input units are connected to all output units. We call this a **fully connected layer**. We'll consider other layer types later.
- Note: the inputs and outputs for a layer are distinct from the inputs and outputs to the network.
- If we need to compute *M* outputs from *N* inputs, we can do so in parallel using matrix multiplication. This means we'll be using a  $M \times N$  matrix
- The output units are a function of the input units:

 $\mathbf{y} = f(\mathbf{x}) = \phi \left( \mathbf{W} \mathbf{x} + \mathbf{b} \right)$ 

• A multilayer network consisting of fully connected layers is called a **multilayer perceptron**. Despite the name, it has nothing to do with perceptrons!



. . .

### Some activation functions:







Rectified Linear Unit (ReLU)

 $y = \max(0, z)$ 

Soft ReLU  $y = \log 1 + e^z$ 

### Some activation functions:



• Each layer computes a function, so the network computes a composition of functions:

$$\begin{split} \mathbf{h}^{(1)} &= f^{(1)}(\mathbf{x}) = \phi(\mathbf{W}^{(1)}\mathbf{x} + \mathbf{b}^{(1)}) \\ \mathbf{h}^{(2)} &= f^{(2)}(\mathbf{h}^{(1)}) = \phi(\mathbf{W}^{(2)}\mathbf{h}^{(1)} + \mathbf{b}^{(2)}) \\ &\vdots \\ \mathbf{y} &= f^{(L)}(\mathbf{h}^{(L-1)}) \end{split}$$

• Or more simply:

$$\mathbf{y} = f^{(L)} \circ \cdots \circ f^{(1)}(\mathbf{x}).$$

• Neural nets provide modularity: we can implement each layer's computations as a black box.



# Feature Learning

Last layer:

- If task is regression: choose  $\mathbf{y} = f^{(L)}(\mathbf{h}^{(L-1)}) = (\mathbf{w}^{(L)})^T \mathbf{h}^{(L-1)} + b^{(L)}$
- If task is binary classification: choose  $\mathbf{y} = f^{(L)}(\mathbf{h}^{(L-1)}) = \sigma((\mathbf{w}^{(L)})^T \mathbf{h}^{(L-1)} + b^{(L)})$
- Neural nets can be viewed as a way of learning features:



## Feature Learning

- Suppose we're trying to classify images of handwritten digits. Each image is represented as a vector of  $28 \times 28 = 784$  pixel values.
- Each first-layer hidden unit computes  $\phi(\mathbf{w}_i^T \mathbf{x})$ . It acts as a feature detector.
- We can visualize **w** by reshaping it into an image. Here's an example that responds to a diagonal stroke.



### Feature Learning

Here are some of the features learned by the first hidden layer of a handwritten digit classifier:

			1	Ser.		$\langle \hat{X} \rangle$	
<u> </u>					(Call		19
M.	-		約				1
1	$g_{i}$			18	<b>1</b> 3	$3_{\rm sc}$	
					続		
1						1	
	N.	11	$[2]_{ij}^{\mathbf{E}}$		ない		
1			N.	197	191		d'

### Expressive Power

- We've seen that there are some functions that linear classifiers can't represent. Are deep networks any better?
- Suppose a layer's activation function was the identity, so the layer just computes a affine transformation of the input
  - ▶ We call this a linear layer
- Any sequence of *linear* layers can be equivalently represented with a single linear layer.

$$\mathbf{y} = \underbrace{\mathbf{W}^{(3)}\mathbf{W}^{(2)}\mathbf{W}^{(1)}}_{\triangleq \mathbf{W}'}\mathbf{x}$$

• Deep linear networks are no more expressive than linear regression.

### Expressive Power

- Multilayer feed-forward neural nets with *nonlinear* activation functions are **universal function approximators**: they can approximate any function arbitrarily well.
- This has been shown for various activation functions (thresholds, logistic, ReLU, etc.)
  - ▶ Even though ReLU is "almost" linear, it's nonlinear enough.



### Designing a network to classify XOR:

Assume hard threshold activation function





- h<sub>1</sub> computes I[x<sub>1</sub> + x<sub>2</sub> 0.5 > 0]
  i.e. x<sub>1</sub> OR x<sub>2</sub>
  h<sub>2</sub> computes I[x<sub>1</sub> + x<sub>2</sub> 1.5 > 0]
  i.e. x<sub>1</sub> AND x<sub>2</sub>
  y computes I[h<sub>1</sub> h<sub>2</sub> 0.5 > 0] ≡ I[h<sub>1</sub> + (1 h<sub>2</sub>) 1.5 > 0]
  i.e. h AND (NOT h) = x XOP x
  - i.e.  $h_1$  AND (NOT  $h_2$ ) =  $x_1$  XOR  $x_2$

### Expressive Power

### Universality for binary inputs and targets:

- Hard threshold hidden units, linear output
- Strategy:  $2^D$  hidden units, each of which responds to one particular input configuration



• Only requires one hidden layer, though it needs to be extremely wide.

Intro ML (UofT)

### Expressive Power

- What about the logistic activation function?
- You can approximate a hard threshold by scaling up the weights and biases:



• This is good: logistic units are differentiable, so we can train them with gradient descent.

- Limits of universality
  - ▶ You may need to represent an exponentially large network.
  - ▶ How can you find the appropriate weights to represent a given function?
  - ▶ If you can learn any function, you'll just overfit.
  - ▶ Really, we desire a *compact* representation.

### Training neural networks with backpropagation

# Recap: Gradient Descent

• **Recall:** gradient descent moves opposite the gradient (the direction of steepest descent)



- Weight space for a multilayer neural net: one coordinate for each weight or bias of the network, in *all* the layers
- Conceptually, not any different from what we've seen so far just higher dimensional and harder to visualize!
- We want to define a loss  $\mathcal{L}$  and compute the gradient of the cost  $d\mathcal{J}/d\mathbf{w}$ , which is the vector of partial derivatives.
  - ► This is the average of  $d\mathcal{L}/d\mathbf{w}$  over all the training examples, so in this lecture we focus on computing  $d\mathcal{L}/d\mathbf{w}$ .

Intro ML (UofT)

- We've already been using the univariate Chain Rule.
- Recall: if f(x) and x(t) are univariate functions, then

$$\frac{\mathrm{d}}{\mathrm{d}t}f(x(t)) = \frac{\mathrm{d}f}{\mathrm{d}x}\frac{\mathrm{d}x}{\mathrm{d}t}.$$

### Recall: Univariate logistic least squares model

$$z = wx + b$$
  

$$y = \sigma(z)$$
  

$$\mathcal{L} = \frac{1}{2}(y - t)^{2}$$

Let's compute the loss derivatives  $\frac{\partial \mathcal{L}}{\partial w}, \frac{\partial \mathcal{L}}{\partial b}$ 

### Univariate Chain Rule

1

### How you would have done it in calculus class

$$\begin{split} \mathcal{L} &= \frac{1}{2} (\sigma(wx+b)-t)^2 \\ \frac{\partial \mathcal{L}}{\partial w} &= \frac{\partial}{\partial w} \left[ \frac{1}{2} (\sigma(wx+b)-t)^2 \right] \\ &= \frac{1}{2} \frac{\partial}{\partial w} (\sigma(wx+b)-t)^2 \\ &= (\sigma(wx+b)-t) \frac{\partial}{\partial w} (\sigma(wx+b)-t) \\ &= (\sigma(wx+b)-t) \sigma'(wx+b) \frac{\partial}{\partial w} (wx+b) \\ &= (\sigma(wx+b)-t) \sigma'(wx+b) \frac{\partial}{\partial w} (wx+b) \\ &= (\sigma(wx+b)-t) \sigma'(wx+b) x \end{split}$$

What are the disadvantages of this approach?

### A more structured way to do it

#### Computing the derivatives:

Computing the loss:  $\begin{aligned}
z &= wx + b \\
y &= \sigma(z) \\
\mathcal{L} &= \frac{1}{2}(y - t)^2
\end{aligned}$   $\begin{aligned}
\frac{d\mathcal{L}}{dy} &= y - t \\
\frac{d\mathcal{L}}{dz} &= \frac{d\mathcal{L}}{dy}\frac{dy}{dz} = \frac{d\mathcal{L}}{dy}\sigma'(z) \\
\frac{\partial\mathcal{L}}{\partial w} &= \frac{d\mathcal{L}}{dz}\frac{dz}{dw} = \frac{d\mathcal{L}}{dz}x \\
\frac{\partial\mathcal{L}}{\partial b} &= \frac{d\mathcal{L}}{dz}\frac{dz}{db} = \frac{d\mathcal{L}}{dz}
\end{aligned}$ 

Remember, the goal isn't to obtain closed-form solutions, but to be able to write a program that efficiently computes the derivatives.

# Univariate Chain Rule

- We can diagram out the computations using a **computation** graph.
- The nodes represent all the inputs and computed quantities, and the edges represent which nodes are computed directly as a function of which other nodes.



### A slightly more convenient notation:

- Use  $\overline{y}$  to denote the derivative  $d\mathcal{L}/dy$ , sometimes called the **error signal**.
- This emphasizes that the error signals are just values our program is computing (rather than a mathematical operation).

### Computing the loss:

Computing the derivatives:

 $z = wx + b \qquad \qquad \overline{y} = y - t \\ y = \sigma(z) \qquad \qquad \overline{z} = \overline{y} \, \sigma'(z) \\ \mathcal{L} = \frac{1}{2} (y - t)^2 \qquad \qquad \overline{w} = \overline{z} \, x \\ \overline{b} = \overline{z}$ 

### Multivariate Chain Rule

**Problem:** what if the computation graph has fan-out > 1? This requires the **multivariate Chain Rule**!





$$\mathcal{L} = -\sum_k t_k \log y_k$$

### Multivariate Chain Rule

• Suppose we have a function f(x, y) and functions x(t) and y(t). (All the variables here are scalar-valued.) Then

$$\frac{\mathrm{d}}{\mathrm{d}t}f(x(t),y(t)) = \frac{\partial f}{\partial x}\frac{\mathrm{d}x}{\mathrm{d}t} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}t}$$



• Example:

$$f(x, y) = y + e^{xy}$$
$$x(t) = \cos t$$
$$y(t) = t^{2}$$

• Plug in to Chain Rule:

$$\frac{\mathrm{d}f}{\mathrm{d}t} = \frac{\partial f}{\partial x}\frac{\mathrm{d}x}{\mathrm{d}t} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}t}$$
$$= (ye^{xy}) \cdot (-\sin t) + (1 + xe^{xy}) \cdot 2t$$

### Multivariable Chain Rule

• In the context of backpropagation:



• In our notation:

$$\bar{t} = \bar{x} \, \frac{\mathrm{d}x}{\mathrm{d}t} + \bar{y} \, \frac{\mathrm{d}y}{\mathrm{d}t}$$

### Full backpropagation algorithm:

Let  $v_1, \ldots, v_N$  be a **topological ordering** of the computation graph (i.e. parents come before children.)



 $v_N$  denotes the variable we're trying to compute derivatives of (e.g. loss).

forward pass  $\begin{bmatrix} For \ i = 1, \dots, N \\ Compute \ v_i \text{ as a function of } Pa(v_i) \end{bmatrix}$ backward pass  $\begin{bmatrix} \overline{v_N} = 1 \\ For \ i = N - 1, \dots, 1 \\ \overline{v_i} = \sum_{j \in Ch(v_i)} \overline{v_j} \frac{\partial v_j}{\partial v_i} \end{bmatrix}$ Intro ML (UofT) CSC311-Lec5

41 / 46

Example: univariate logistic least squares regression



### Multilayer Perceptron (multiple outputs):



Forward pass:

$$z_{i} = \sum_{j} w_{ij}^{(1)} x_{j} + b_{i}^{(1)}$$
$$h_{i} = \sigma(z_{i})$$
$$y_{k} = \sum_{i} w_{ki}^{(2)} h_{i} + b_{k}^{(2)}$$
$$\mathcal{L} = \frac{1}{2} \sum_{k} (y_{k} - t_{k})^{2}$$

Backward pass:

$$\overline{\mathcal{L}} = 1$$

$$\overline{y_k} = \overline{\mathcal{L}} (y_k - t_k)$$

$$\overline{w_{ki}^{(2)}} = \overline{y_k} h_i$$

$$\overline{b_k^{(2)}} = \overline{y_k}$$

$$\overline{h_i} = \sum_k \overline{y_k} w_{ki}^{(2)}$$

$$\overline{z_i} = \overline{h_i} \sigma'(z_i)$$

$$\overline{w_{ij}^{(1)}} = \overline{z_i} x_j$$

$$\overline{b_i^{(1)}} = \overline{z_i}$$

### In vectorized form:



Forward pass:

$$\begin{aligned} \mathbf{z} &= \mathbf{W}^{(1)}\mathbf{x} + \mathbf{b}^{(1)} \\ \mathbf{h} &= \sigma(\mathbf{z}) \\ \mathbf{y} &= \mathbf{W}^{(2)}\mathbf{h} + \mathbf{b}^{(2)} \\ \mathcal{L} &= \frac{1}{2} \|\mathbf{t} - \mathbf{y}\|^2 \end{aligned}$$

**Backward pass:** 

$$\begin{aligned} \overline{\mathcal{L}} &= 1\\ \overline{\mathbf{y}} &= \overline{\mathcal{L}} \left( \mathbf{y} - \mathbf{t} \right)\\ \overline{\mathbf{W}^{(2)}} &= \overline{\mathbf{y}} \mathbf{h}^\top\\ \overline{\mathbf{b}^{(2)}} &= \overline{\mathbf{y}}\\ \overline{\mathbf{h}} &= \mathbf{W}^{(2)\top} \overline{\mathbf{y}}\\ \overline{\mathbf{z}} &= \overline{\mathbf{h}} \circ \sigma'(\mathbf{z})\\ \overline{\mathbf{W}^{(1)}} &= \overline{\mathbf{z}} \mathbf{x}^\top\\ \overline{\mathbf{b}^{(1)}} &= \overline{\mathbf{z}} \end{aligned}$$

## Computational Cost

• Computational cost of forward pass: one **add-multiply operation** per weight

$$z_i = \sum_j w_{ij}^{(1)} x_j + b_i^{(1)}$$

• Computational cost of backward pass: two add-multiply operations per weight

$$\overline{w_{ki}^{(2)}} = \overline{y_k} h_i$$
$$\overline{h_i} = \sum_k \overline{y_k} w_{ki}^{(2)}$$

- Rule of thumb: the backward pass is about as expensive as two forward passes.
- For a multilayer perceptron, this means the cost is linear in the number of layers, quadratic in the number of units per layer.

Intro ML (UofT)

- Backprop is used to train the overwhelming majority of neural nets today.
  - Even optimization algorithms much fancier than gradient descent (e.g. second-order methods) use backprop to compute the gradients.
- Despite its practical success, backprop is believed to be neurally implausible.