Deep Learning

## First classifier: Nearest Neighbor

```
def train(images, labels):
    # Machine learning!
    return model
def predict(model, test_images):
    # Use model to predict labels
    return test_labels
```

Memorize all data and labels

Predict the label
$\longrightarrow$ of the most similar training image

## Example



## Linear classifiers: Motivation

- kNN produce decision boundaries by calculating them during prediction.
- Can we define a (simple) function during training to define decision boundaries directly?



## Parametric Approach: Linear Classifier

Image

$$
f(x, W)=W x
$$



10 numbers defining class scores

parameters or weights

## Parametric Approach: Linear Classifier

$$
\mathbf{w}_{1} \cdot \mathbf{x}=\mathbf{w}_{1,1}{ }^{*} \mathrm{x}_{1}+\ldots+\mathbf{W}_{1,3072}{ }^{*} \mathrm{X}_{3072} \quad \text { Shape: }(10,3072)
$$

## $f(x, W)=W x+b$



## Loss Function



L: Metric to assess what loss of data classification our model incurs

## Hinge loss



## Cross-Entropy Loss <br> $L_{i}=-\log \left(\frac{e^{s y_{i}}}{\sum_{j} e^{s_{j}}}\right)$



## Linear Classifier

optimization


## Gradient Descent

Iteratively step in the direction of the negative gradient (direction of local steepest descent)

```
# Vanilla gradient descent
w = initialize_weights()
for t in range(num_steps):
    dw = compute_gradient(loss_fn, data, w)
    w -= learning_rate * dw
```


## Hyperparameters:

- Weight initialization method
- Number of steps
- Learning rate



## Problems with SGD

## Gradients are calculated from

 minibatches $\rightarrow$ they can be noisy$$
\begin{aligned}
L(W) & =\frac{1}{N} \sum_{i=1}^{N} L_{i}\left(x_{i}, y_{i}, W\right) \\
\nabla_{W} L(W) & =\frac{1}{N} \sum_{i=1}^{N} \nabla_{W} L_{i}\left(x_{i}, y_{i}, W\right)
\end{aligned}
$$



## SGD + Momentum

Local Minima



Saddle points


Gradient Noise


## Adam



SGD

SGD+Momentum

RMSProp

Adam

## Summary

1. Use Linear Models for image classification problems
2. Use Loss Functions to express preferences over different selection of weights

$$
\begin{aligned}
L_{i} & =-\log \left(\frac{e^{s_{y}}}{\sum_{j} e^{s_{j}}}\right) \text { Softmax } \\
L_{i} & =\sum_{j \neq y_{i}} \max \left(0, s_{j}-s_{y_{i}}+1\right) \\
L & =\frac{1}{N} \sum_{i=1}^{N} L_{i}+R(W)
\end{aligned}
$$

3. Use Stochastic Gradient Descent to minimize our loss functions and train the model
```
v = 0
for t in range(num_steps):
    dw = compute_gradient(w)
    v = rho * v + dw
    w -= learning_rate * v
```



## Cifar10 Linear Classifier


optimization


## Geometric Interpretation: Linear Classifier


$f(x, W)=W x+b$


Array of $32 \times 32 \times 3$ numbers (3072 numbers total)

## Geometric Interpretation: Linear Classifier



## Geometric Interpretation: Linear Classifier



## Geometric Interpretation: Linear Classifier



## Geometric Interpretation: Linear Classifier



## Visual Interpretation: Linear Classifier

Flatten tensors into a vector

Linear classifier has one "template" per category

## Visual Interpretation: Linear Classifier

Flatten tensors into a vector

A single template cannot capture multiple modes of the data


## Linear Classifiers



Geometric Interpretation

Hyperplanes separating space


## Linear Classifiers shortcomings

## Geometric Viewpoint



Some training data can't be separated with a hyperplane

Visual Viewpoint


One template per class: Can't recognize different modes of a class

## Apply Transformations



## Transformation

Extract features using transformations

## Apply Transformations



Extract features using transformations

## Apply Transformations



## Apply Transformations



## Example: Color Histogram



## Example: Histogram of Oriented Gradients (HoG)

Input image


Histogram of Oriented Gradients


## Image Feature Aggregation



## Image Features

## Feature Extraction



## Image Features

## Feature Extraction



10 numbers giving
training scores for classes

Neural Networks
(Before) Linear score function:

$$
\begin{gathered}
f=W x \\
x \in \mathbb{R}^{D}, W \in \mathbb{R}^{C \times D}
\end{gathered}
$$

Neural Networks
(Before) Linear score function:

$$
f=W x
$$

(Now) 2-layer Neural Network

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

$$
W_{2} \in \mathbb{R}^{C \times H} \quad W_{1} \in \mathbb{R}^{H \times D} \quad x \in \mathbb{R}^{D}
$$

## Neural Networks

(Before) Linear score function:

$$
f=W x
$$

(Now) 2-layer Neural Network $f=W_{2} \max \left(0, W_{1} x\right)$ or 3-layer Neural Network

$$
f=W_{3} \max \left(0, W_{2} \max \left(0, W_{1} x\right)\right)
$$

$$
W_{3} \in \mathbb{R}^{C \times H_{2}} \quad W_{2} \in \mathbb{R}^{H_{2} \times H_{1}} \quad W_{1} \in \mathbb{R}^{H_{1} \times D} \quad x \in \mathbb{R}^{D}
$$

Neural Networks

$$
f=W x
$$

(Before) Linear score function: $f=W_{2} \max \left(0, W_{1} x\right)$
(Now) 2-layer Neural Network


## Neural Networks

(Before) Linear score function:

$$
f=W x
$$

(Now) 2-layer Neural Network $\quad f=W_{2} \max \left(0, W_{1} x\right)$

Element (i, j) of $W_{1}$ gives the effect on $h_{i}$ from $x_{j}$


100

$$
x \in \mathbb{R}^{D}, W_{1} \in \mathbb{R}^{H \times D}, W_{2} \in \mathbb{R}^{C \times H}
$$

## Neural Networks

(Before) Linear score function:

$$
f=W x
$$

(Now) 2-layer Neural Network

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

Element ( $\mathrm{i}, \mathrm{j}$ ) of $\mathrm{W}_{1}$ gives the effect on $h_{i}$ from $x_{j}$

All elements of $x$ affect all elements of $h$


100

Fully-connected neural network Also "Multi-Layer Perceptron" (MLP)

Element ( $\mathrm{i}, \mathrm{j}$ ) of $\mathrm{W}_{2}$ gives the effect on $\mathrm{s}_{\mathrm{i}}$ from $\mathrm{h}_{\mathrm{j}}$

All elements of $h$ affect all elements of $s$

## Neural Networks

(Before) Linear score function:

Linear classifier: One template per class

(Now) 2-layer Neural Network
100
$x \in \mathbb{R}^{D}, W_{1} \in \mathbb{R}^{H \times D}, W_{2} \in \mathbb{R}^{C \times H}$

## Neural Networks

(Before) Linear score function:

(Now) 2-layer Neural Network


## Neural Networks

Can use different templates to cover multiple modes of a class

(Before) Linear score function:
(Now) 2-layer Neural Network
 100

$$
x \in \mathbb{R}^{D}, W_{1} \in \mathbb{R}^{H \times D}, W_{2} \in \mathbb{R}^{C \times H}
$$

## Neural Networks

Most templates not interpretable

(Before) Linear score function:
(Now) 2-layer Neural Network


$$
100
$$

$$
x \in \mathbb{R}^{D}, W_{1} \in \mathbb{R}^{H \times D}, W_{2} \in \mathbb{R}^{C \times H}
$$

## Deep Neural Networks



## Activation Functions

2-layer Neural Network

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

The function $\operatorname{ReLU}(z)=\max (0, z)$ is called "Rectified Linear Unit"


This is called the activation function of the neural network

## Activation Functions

2-layer Neural Network

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

The function $\operatorname{ReLU}(z)=\max (0, z)$ is called "Rectified Linear Unit"


This is called the activation function of the neural network

Without activation function:

$$
s=W_{2} W_{1} x
$$

## Activation Functions

2-layer Neural Network $\quad f=W_{2} \max \left(0, W_{1} x\right)$

The function $\operatorname{Re} L U(z)=\max (0, z)$ is called "Rectified Linear Unit"


This is called the activation function of the neural network

Without activation function:

$$
\begin{aligned}
& s=W_{2} W_{1} x \\
& W_{3}= W_{2} W_{1} \in \mathbb{R}^{C \times H} \\
& \rightarrow \text { Linear classifier }
\end{aligned}
$$

## Activation Functions

## Sigmoid

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

tanh
$\tanh (x)$

ReLU
$\max (0, x)$

## Leaky ReLU $\max (0.1 x, x)$



## Maxout

$\max \left(w_{1}^{T} x+b_{1}, w_{2}^{T} x+b_{2}\right)$

## ELU

$$
\begin{cases}x & x \geq 0 \\ \alpha\left(e^{x}-1\right) & x<0\end{cases}
$$



## Activation Functions

## Sigmoid

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

tanh
$\tanh (x)$

ReLU
$\max (0, x)$



## Leaky ReLU

 $\max (0.1 x, x)$

## Maxout

$$
\max \left(w_{1}^{T} x+b_{1}, w_{2}^{T} x+b_{2}\right)
$$

## ELU

$$
\begin{cases}x & x \geq 0 \\ \alpha\left(e^{x}-1\right) & x<0\end{cases}
$$



# Feature Transform 

Consider a linear transform: $h=W x$ Where x , h are both 2-dimensional


## Feature Transform

Consider a linear transform: $h=W x$ Where x , h are both 2-dimensional


Feature Transform
Consider a linear transform: $h=W x$ Where x , h are both 2-dimensional


## Feature Transform

Points not linearly
separable in original space


Consider a linear transform: $h=W x$ Where x , h are both 2-dimensional

## Feature Transform

Points not linearly
separable in original space


Consider a linear transform: $h=W x$ Where x , h are both 2-dimensional

Not linearly separable


Feature Transform
Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional


Feature Transform
Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional


Feature Transform
Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional


Feature Transform
Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional


Feature Transform
Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional


## Feature Transform

Points not linearly
separable in original space


## Feature Transform

Points not linearly
separable in original space


## Feature Transform

Points not linearly
separable in original space


## Feature Transform

Points not linearly
separable in original space


Linear classifier in feature space gives nonlinear classifier in original space

Consider a neural net hidden layer:
$h=\operatorname{ReLU}(W x)=\max (0, W x)$
Where x , h are both 2-dimensional

Feature transform: $\xrightarrow{\mathrm{h}=\operatorname{ReLU}(\mathrm{Wx})}$

h1

Points are linearly
separable in features space!

## Setting the number of layers and their sizes



More hidden units = more capacity

## Regularization

$$
L(W)=\underbrace{\frac{1}{N} \sum_{i=1}^{N} L_{i}\left(f\left(x_{i}, W\right), y_{i}\right)}+\underbrace{\lambda R(W)}
$$

Data loss: Model predictions should match training data

Regularization: Prevent the model from doing too well on training data

## Regularization with constant number of layers



## Neural Net sample code


hidden layer
import numpy as np
from numpy. random import randn

N, Din, H, Dout = 64, 1000, 100, 10 $x, y=r a n d n(N, D i n), ~ r a n d n(N, ~ D o u t) ~$ w1, w2 = randn(Din, H), randn(H, Dout) for $t$ in range(10000):
h = $1.0 /(1.0+n p . \exp (-x \cdot \operatorname{dot}(w 1)))$
y_pred $=$ h.dot(w2)
loss = np.square(y_pred -y$).$ sum()
dy_pred $=2.0 *\left(y \_p r e d-y\right)$
dw2 = h.T.dot(dy_pred)
dh = dy_pred.dot(w2.T)
$\mathrm{dw} 1=\mathrm{x} \cdot \mathrm{T} . \operatorname{dot}(\mathrm{dh} * \mathrm{~h} *(1-\mathrm{h}))$
$\mathrm{w} 1-=1 \mathrm{e}-4 * \mathrm{dw} 1$
w2 -= 1e-4 * dw2

## Neural Net sample code



import numpy as np
from numpy. random import randn

N, Din, H, Dout $=64,1000,100,10$ $x, y=r a n d n(N, D i n), ~ r a n d n(N, ~ D o u t)$ w1, w2 = randn(Din, H), randn(H, Dout) for $t$ in range(10000):
$h=1.0 /(1.0+n p \cdot \exp (-x \cdot \operatorname{dot}(w 1)))$
y_pred $=$ h.dot(w2)
loss $=$ np.square $\left(y \_p r e d-y\right) . s u m()$
dy_pred $=2.0 *\left(y \_p r e d-y\right)$
dw2 = h.T.dot(dy_pred)
dh = dy_pred.dot(w2.T)
$\mathrm{dw} 1=\mathrm{x} \cdot \mathrm{T} \cdot \operatorname{dot}(\mathrm{dh} * \mathrm{~h} *(1-\mathrm{h}))$
$\mathrm{w} 1-=1 \mathrm{e}-4 * \mathrm{dw} 1$
w2 -= 1e-4 * dw2

## Neural Net sample code



import numpy as np
from numpy. random import randn

N, Din, H, Dout $=64,1000,100,10$ $\mathrm{x}, \mathrm{y}=$ randn(N, Din), randn(N, Dout) w1, w2 = randn(Din, H), randn(H, Dout) for $t$ in range(10000):
$h=1.0 /(1.0+n p \cdot \exp (-x \cdot \operatorname{dot}(w 1)))$

$$
\text { y_pred }=\text { h.dot(w2) }
$$

$$
\text { loss }=\text { np.square }\left(y \_p r e d-y\right) . s u m()
$$

$$
\text { dy_pred }=2.0 *\left(y \_p r e d-y\right)
$$

dw2 = h.T.dot(dy_pred)
dh = dy_pred.dot(w2.T)

$$
\mathrm{dw} 1=\mathrm{x} \cdot \mathrm{~T} \cdot \operatorname{dot}(\mathrm{dh} * \mathrm{~h} *(1-\mathrm{h}))
$$

$$
\mathrm{w} 1-=1 \mathrm{e}-4 * \mathrm{dw} 1
$$

$$
\mathrm{w} 2-=1 \mathrm{e}-4 * \mathrm{dw} 2
$$

## Neural Net sample code



Initialize weights and data


Compute loss (sigmoid activation, L2 loss)


Compute gradients
import numpy as np
from numpy. random import randn

N, Din, H, Dout = 64, 1000, 100, 10 $x, y=r a n d n(N, D i n), ~ r a n d n(N, ~ D o u t)$ w1, w2 = randn(Din, H), randn(H, Dout) for $t$ in range(10000):

$$
\text { h = } 1.0 /(1.0+n p . \exp (-x . \operatorname{dot}(w 1)))
$$

y_pred = h.dot(w2)
loss = np.square(y_pred - y).sum()

$$
\text { dy_pred }=2.0 *\left(y \_p r e d-y\right)
$$

dw2 = h.T.dot(dy_pred)
dh = dy_pred.dot(w2.T)

$$
\mathrm{dw} 1=\mathrm{x} \cdot \mathrm{~T} \cdot \operatorname{dot}(\mathrm{dh} * \mathrm{~h} *(1-\mathrm{h}))
$$

$$
\mathrm{w} 1-=1 \mathrm{e}-4 * \mathrm{dw} 1
$$

$$
\mathrm{w} 2-=1 \mathrm{e}-4 * \mathrm{dw} 2
$$

## Neural Net sample code



import numpy as np
from numpy. random import randn

N, Din, H, Dout = 64, 1000, 100, 10 $x, y=r a n d n(N, D i n), ~ r a n d n(N, ~ D o u t)$ w1, w2 = randn(Din, H), randn(H, Dout) for $t$ in range(10000):

$$
\text { h = } 1.0 /(1.0+n p . \exp (-x . \operatorname{dot}(w 1)))
$$

y_pred = h.dot(w2)
loss = np.square(y_pred - y).sum()

$$
\text { dy_pred }=2.0 *\left(y \_p r e d-y\right)
$$

dw2 = h.T.dot(dy_pred)
dh = dy_pred.dot(w2.T)

$$
\mathrm{dw} 1=\mathrm{x} \cdot \mathrm{~T} \cdot \operatorname{dot}(\mathrm{dh} * \mathrm{~h} *(1-\mathrm{h}))
$$

$$
\mathrm{w} 1-=1 \mathrm{e}-4 * \mathrm{dw} 1
$$

$$
\mathrm{w} 2-=1 \mathrm{e}-4 * \mathrm{dw} 2
$$

## Spatial Information

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

Flatten lattice into vector
Input image
$(2,2)$

| 56 |
| :---: |
| 231 |
| 24 |
| 2 |

Histogram of Oriented Gradients

(4,)

## Spatial Information

$$
f=W_{2} \max \left(0, W_{1} x\right)
$$

Flatten lattice into vector


## Spatial Information

$f=W_{2} \max \left(0, W_{1} x\right)$
Flatten lattice into vector


## Components of a Fully-Connected Network

Fully-Connected Layers


Activation Function


## Components of a Convolutional Network

Fully-Connected Layers


Convolution Layers


## Activation Function



Normalization

$$
\hat{x}_{i, j}=\frac{x_{i, j}-\mu_{j}}{\sqrt{\sigma_{j}^{2}+\varepsilon}}
$$

## Components of a Convolutional Network

Fully-Connected Layers


Convolution Layers
Pooling Layers


Activation Function



Normalization


Fully-Connected Layer
$32 \times 32 \times 3$ image -> flatten to $3072 \times 1$


## Fully-Connected Layer

$32 \times 32 \times 3$ image -> flatten to $3072 \times 1$
$1 \xrightarrow{\square}$

## Convolution Layer

$3 \times 32 \times 32$ image: preserve structure


## Convolution Layer

$3 \times 32 \times 32$ image


## $3 \times 5 \times 5$ filter



Convolve the filter with the image i.e. "slide over the image spatially, computing dot products"

## Convolution Layer

$3 \times 32 \times 32$ image


Filters always extend the full depth of the input volume

## $3 \times 5 \times 5$ filter



Convolve the filter with the image i.e. "slide over the image spatially, computing dot products"

## Convolution Layer

$3 \times 32 \times 32$ image


## 1 number:

the result of taking a dot product between the filter and a small $3 \times 5 \times 5$ chunk of the image
(i.e. $3 * 5 * 5=75$-dimensional dot product + bias)
$w^{T} x+b$

## Convolution Layer

$3 \times 32 \times 32$ image

convolve (slide) over all spatial locations


Convolution Layer
$3 \times 32 \times 32$ image

two $1 \times 28 \times 28$
activation map
convolve (slide) over all spatial locations


Convolution Layer
$28 \times 28$ grid, at each point a 6 -dim vector

3×32×32 image


Consider 6 filters, each $3 x 5 x 5$


Stack activations to get a $6 \times 28 \times 28$ output image

Convolution Layer

3×32×32 image


Also 6-dim bias vector:

$28 \times 28$ grid, at each point a 6-dim vector


Stack activations to get a $6 \times 28 \times 28$ output image

Convolution Layer
3×32×32 image


Also 6-dim bias vector:


6 activation maps, each $1 \times 28 \times 28$

Stack activations to get a $6 \times 28 \times 28$ output image

Batch of images



Convolution Layer $\mathrm{N} \times \mathrm{C}_{\text {in }} \times \mathrm{H} \times \mathrm{W}$ Batch of images



Also $\mathrm{C}_{\text {out }}$-dim bias vector:

Convolution
Layer
$\mathrm{N} \times \mathrm{C}_{\text {out }} \times \mathrm{H}^{\prime} \times \mathrm{W}^{\prime}$ Batch of outputs


## Stacking Convolutions



## Stacking Convolutions: Add Non-linearity



## What do convolutional filters learn?



## What do convolutional filters learn?



Linear classifier: One template per class


Input:
$\mathrm{N} \times 3 \times 32 \times 32$

First hidden layer:

$$
N \times 6 \times 28 \times 28
$$

## What do convolutional filters learn?



Input:
$\mathrm{N} \times 3 \times 32 \times 32$

First hidden layer:
$N \times 6 \times 28 \times 28$

MLP: Bank of whole-image templates


## What do convolutional filters learn?



First-layer conv filters: local image templates (Often learns oriented edges, opposing colors)


AlexNet: 64 filters, each $3 \times 11 \times 11$

