Lecture 2: Image Classification

Administrative: Assignment 1

Due 4/14 11:59pm

- K-Nearest Neighbor
- Linear classifiers: SVM, Softmax
- Two-layer neural network
- Image features

Administrative: Course Project

Project proposal due 4/24 (Monday) 11:59pm

Find your teammates on EdStem

Collaboration: EdStem

"Is X a valid project for 493G1?"

- Anything related to deep learning
- Maximum of 3 students per team
- Make a EdStem private post or come to TA Office Hours

More info on the website

Administrative: Fridays

This Friday 10:30-11:20 am (recording will be made available)

Room: SIG 134

Python / Numpy, Google Cloud Platform, Google Colab

Presenter: Sarah Pratt (TA)

Syllabus

Deep learning Fundamentals	Practical training skills	Applications	
Data-driven approaches	Pytorch 1.4 / Tensorflow 2.0	Image captioning	
Linear classification & kNN	Activation functions	Interpreting machine learning	
Loss functions	Batch normalization	Generative Al	
Optimization	Transfer learning	Fairness & ethics	
Backpropagation	Data augmentation	Data-centric AI	
Multi-layer perceptrons	Momentum / RMSProp / Adam	Deep reinforcement learning	
Neural Networks	Architecture design	Self-supervised learning	
Convolutions	-	Diffusion	
RNNs / LSTMs		LLMs	
Transformers			

Image Classification

A Core Task in Computer Vision

Today:

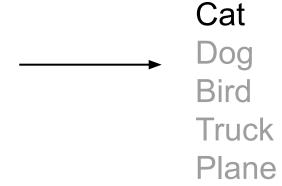
- The image classification task
- Two basic data-driven approaches to image classification
 - K-nearest neighbor and linear classifier

Image Classification: A core task in Computer Vision

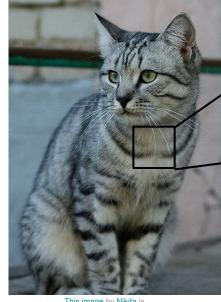


This image by Nikita is licensed under CC-BY 2.0

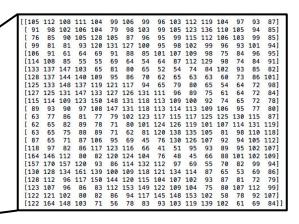
(assume given a set of possible labels)



The Problem: Semantic Gap



This image by Nikita is licensed under CC-BY 2.0



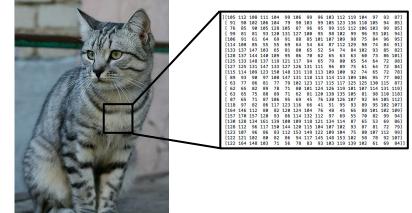
What the computer sees

An image is a tensor of integers between [0, 255]:

e.g. 800 x 600 x 3 (3 channels RGB)

Challenges: Viewpoint variation









All pixels change when the camera moves!

This image by Nikita is licensed under CC-BY 2.0

Challenges: Illumination









This image is CC0 1.0 public domain

RGB values are a function of surface materials, color, light source, etc.

Challenges: Background Clutter





This image is CC0 1.0 public domain

This image is CC0 1.0 public domain

Challenges: Occlusion







This image is CC0 1.0 public domain

This image is CC0 1.0 public domain

This image by jonsson is licensed under CC-BY 2.0

Challenges: Deformation



This image by Umberto Salvagnin is licensed under CC-BY 2.0



This image by Umberto Salvagnin is licensed under CC-BY 2.0



This image by sare bear is licensed under CC-BY 2.0



This image by Tom Thai is licensed under CC-BY 2.0

Challenges: Intraclass variation



This image is CC0 1.0 public domain

Image classification is a building block for other tasks

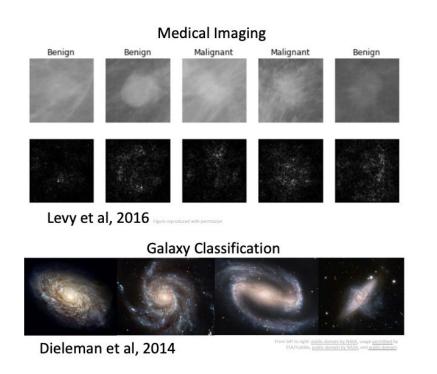




Image classification is a building block for other tasks



Image Captioning Vinyals et al, 2015 Karpathy and Fei-Fei, 2015



A white teddy bear sitting in the grass



A man riding a wave on top of a surfboard



A man in a baseball uniform throwing a ball



A cat sitting on a suitcase on the floor



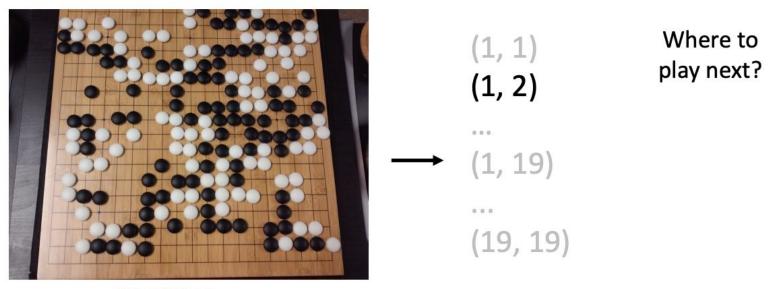
A woman is holding a cat in her hand



A woman standing on a beach holding a surfboard

Image classification is a building block for other tasks

Example: Playing Go



This image is CCO public domain

Modern computer vision algorithms

Classifiers today take 1ms to classify images. And can handle thousands of categories.



This image is CC0 1.0 public domain

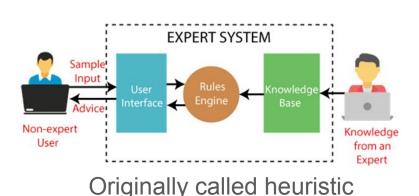
An image classifier: can we implement this as a normal software function?

```
def classify_image(image):
    # Some magic here?
    return class_label
```

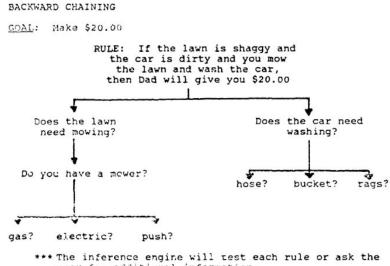
Unlike e.g. sorting a list of numbers,

no obvious way to hard-code the algorithm for recognizing a cat, or other classes.

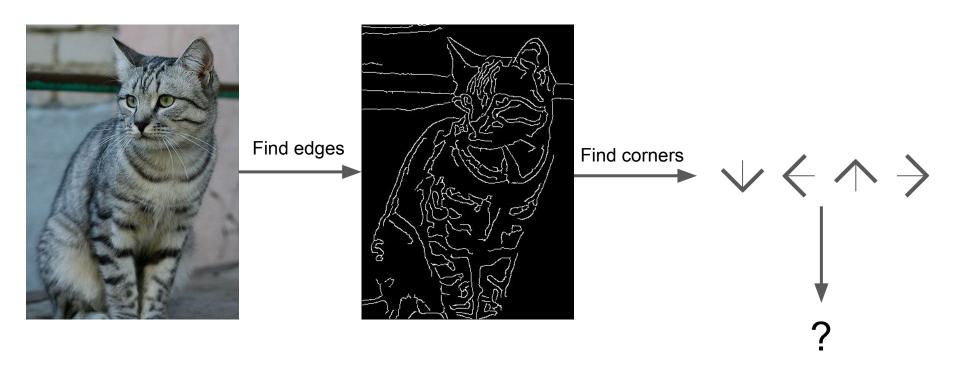
This is why expert systems in the 80s led to the Al winter.



programming project.



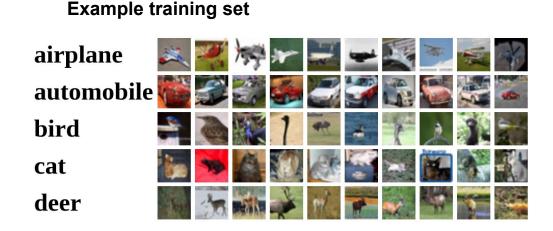
Attempts have been made



John Canny, "A Computational Approach to Edge Detection", IEEE TPAMI 1986

Machine Learning: Data-Driven Approach

1. Collect a dataset of images and labels



Example dataset: MNIST



10 classes: Digits 0 to 928x28 grayscale images50k training images10k test images

Example dataset: CIFAR10



10 classes50k training images (5k per class)10k testing images (1k per class)32x32 RGB images

We will use this dataset for homework assignments

Example dataset: CIFAR100



100 classes50k training images (500 per class)10k testing images (100 per class)32x32 RGB images

20 superclasses with 5 classes each:

Aquatic mammals: beaver, dolphin, otter, seal, whale Trees: Maple, oak, palm, pine, willow

Example dataset: ImageNet (ILSVRC challenge)



1000 classes

~1.3M training images (~1.3K per class)
50K validation images (50 per class)
100K test images (100 per class)

Performance metric: **Top 5 accuracy** Algorithm predicts 5 labels for each image; one of them needs to be right

Example dataset: MIT Places



365 classes of different scene types

~8M training images 18.25K val images (50 per class) 328.5K test images (900 per class)

Images have variable size, often resize to **256x256** for training

Example dataset: Omniglot



1623 categories: characters from 50 different alphabets

20 images per category

Meant to test few shot learning

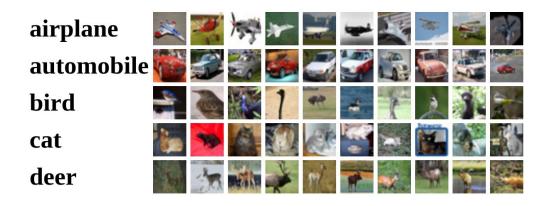
Machine Learning: Data-Driven Approach

- 1. Collect a dataset of images and labels
- 2. Use Machine Learning algorithms to train a classifier
- 3. Evaluate the classifier on new images

```
def train(images, labels):
    # Machine learning!
    return model

def predict(model, test_images):
    # Use model to predict labels
    return test_labels
```

Example training set



Nearest Neighbor Classifier

First classifier: **Nearest Neighbor**

```
def train(images, labels):
                                            Memorize all
  # Machine learning!
                                            data and labels
  return model
                                            Predict the label
def predict(model, test images):
  # Use model to predict labels
                                           of the most similar
  return test_labels
                                            training image
```

First classifier: **Nearest Neighbor**



Training data with labels



query data

Distance Metric





 $ightarrow \mathbb{R}$

What is a good distance metric?

Distance Metric to compare images

L1 distance:
$$d_1(I_1, I_2) = \sum_p |I_1^p - I_2^p|$$

	test image			
56	32	10	1	

56	32	10	18
90	23	128	133
24	26	178	200
2	0	255	220

training image

10	20	24	17
8	10	89	100
12	16	178	170
4	32	233	112

pixel-wise absolute value differences

=	46	12	14	1	
	82	13	39	33	add → 456
	12	10	0	30	→ 456
	2	32	22	108	

```
import numpy as np
class NearestNeighbor:
 def init (self):
    pass
 def train(self, X, y):
    """ X is N x D where each row is an example. Y is 1-dimension of size N """
    # the nearest neighbor classifier simply remembers all the training data
   self.Xtr = X
    self.ytr = y
 def predict(self, X):
    """ X is N x D where each row is an example we wish to predict label for """
    num test = X.shape[0]
    # lets make sure that the output type matches the input type
    Ypred = np.zeros(num test, dtype = self.ytr.dtype)
    # loop over all test rows
    for i in xrange(num test):
     # find the nearest training image to the i'th test image
     # using the L1 distance (sum of absolute value differences)
     distances = np.sum(np.abs(self.Xtr - X[i,:]), axis = 1)
     min index = np.argmin(distances) # get the index with smallest distance
     Ypred[i] = self.ytr[min index] # predict the label of the nearest example
```

Nearest Neighbor classifier

return Ypred

```
import numpy as np
class NearestNeighbor:
 def init (self):
    pass
  def train(self, X, y):
    """ X is N x D where each row is an example. Y is 1-dimension of size N """
    # the nearest neighbor classifier simply remembers all the training data
    self.Xtr = X
    self.ytr = y
  def predict(self, X):
    """ X is N x D where each row is an example we wish to predict label for """
    num test = X.shape[0]
   # lets make sure that the output type matches the input type
    Ypred = np.zeros(num test, dtype = self.ytr.dtype)
    # loop over all test rows
    for i in xrange(num test):
     # find the nearest training image to the i'th test image
     # using the L1 distance (sum of absolute value differences)
     distances = np.sum(np.abs(self.Xtr - X[i,:]), axis = 1)
     min index = np.argmin(distances) # get the index with smallest distance
     Ypred[i] = self.ytr[min index] # predict the label of the nearest example
    return Ypred
```

Nearest Neighbor classifier

Memorize training data

```
import numpy as np
class NearestNeighbor:
 def init (self):
    pass
 def train(self, X, y):
    """ X is N x D where each row is an example. Y is 1-dimension of size N """
    # the nearest neighbor classifier simply remembers all the training data
    self.Xtr = X
    self.ytr = y
 def predict(self, X):
    """ X is N x D where each row is an example we wish to predict label for """
    num test = X.shape[0]
   # lets make sure that the output type matches the input type
    Ypred = np.zeros(num test, dtype = self.ytr.dtype)
    # loop over all test rows
```

```
Nearest Neighbor classifier
```

```
For each test image:
Find closest train image
Predict label of nearest image
```

```
for i in xrange(num_test):
    # find the nearest training image to the i'th test image
    # using the L1 distance (sum of absolute value differences)
    distances = np.sum(np.abs(self.Xtr - X[i,:]), axis = 1)
    min_index = np.argmin(distances) # get the index with smallest distance
    Ypred[i] = self.ytr[min_index] # predict the label of the nearest example

return Ypred
```

```
import numpy as np
class NearestNeighbor:
 def init (self):
    pass
 def train(self, X, y):
    """ X is N x D where each row is an example. Y is 1-dimension of size N """
    # the nearest neighbor classifier simply remembers all the training data
    self.Xtr = X
    self.ytr = y
 def predict(self, X):
    """ X is N x D where each row is an example we wish to predict label for """
    num test = X.shape[0]
    # lets make sure that the output type matches the input type
    Ypred = np.zeros(num test, dtype = self.ytr.dtype)
    # loop over all test rows
    for i in xrange(num test):
     # find the nearest training image to the i'th test image
     # using the L1 distance (sum of absolute value differences)
     distances = np.sum(np.abs(self.Xtr - X[i,:]), axis = 1)
     min index = np.argmin(distances) # get the index with smallest distance
     Ypred[i] = self.ytr[min index] # predict the label of the nearest example
    return Ypred
```

Nearest Neighbor classifier

Q: With N examples, how fast are training and prediction?

Ans: Train O(1), predict O(N)

This is bad: we want classifiers that are **fast** at prediction; **slow** for training is ok

```
import numpy as np
class NearestNeighbor:
 def init (self):
    pass
 def train(self, X, y):
    """ X is N x D where each row is an example. Y is 1-dimension of size N """
    # the nearest neighbor classifier simply remembers all the training data
    self.Xtr = X
    self.ytr = y
 def predict(self, X):
    """ X is N x D where each row is an example we wish to predict label for """
    num test = X.shape[0]
   # lets make sure that the output type matches the input type
    Ypred = np.zeros(num test, dtype = self.ytr.dtype)
    # loop over all test rows
    for i in xrange(num test):
     # find the nearest training image to the i'th test image
     # using the L1 distance (sum of absolute value differences)
     distances = np.sum(np.abs(self.Xtr - X[i,:]), axis = 1)
     min index = np.argmin(distances) # get the index with smallest distance
     Ypred[i] = self.ytr[min index] # predict the label of the nearest example
    return Ypred
```

Nearest Neighbor classifier

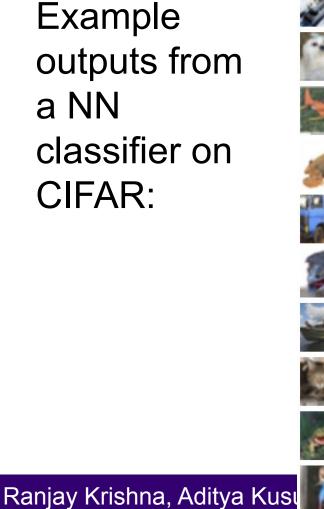
Many methods exist for fast / approximate nearest neighbor (beyond the scope of 231N!)

A good implementation:

https://github.com/facebookresearch/faiss

Johnson et al, "Billion-scale similarity search with GPUs", arXiv 2017

Example a NN classifier on **CIFAR**:









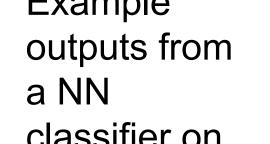




































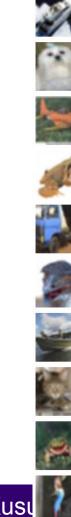








Example outputs from a NN classifier on **CIFAR**:







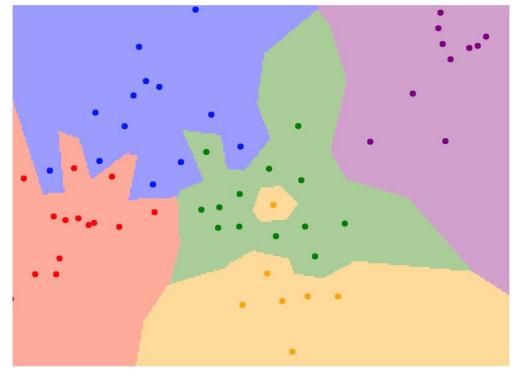




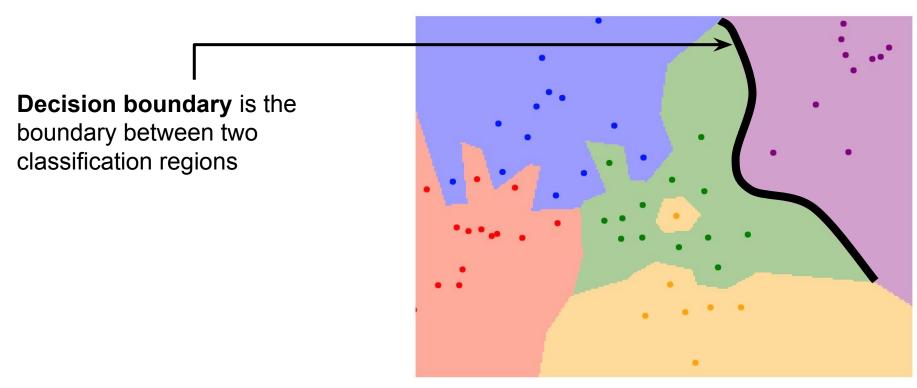
Assume each dot is a training image.

Assume all images are two dimensional.

What does this classifier look like?



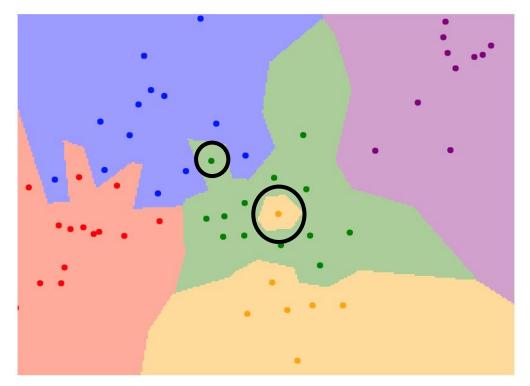
1-nearest neighbor



1-nearest neighbor

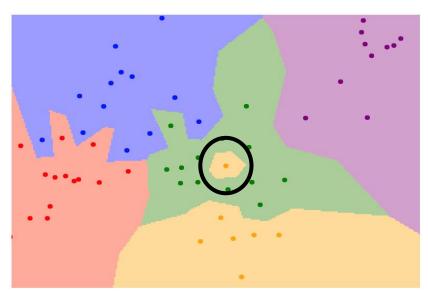
Yellow point in the middle of green might be mislabeled.

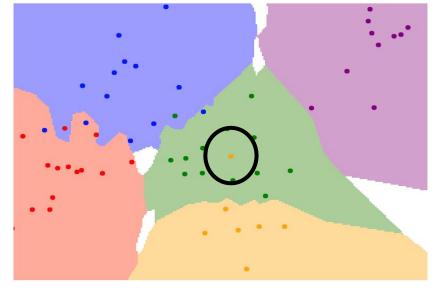
1-NN is not robust to label noise.



1-nearest neighbor

Instead of copying label from nearest neighbor, take **majority vote** from K closest points

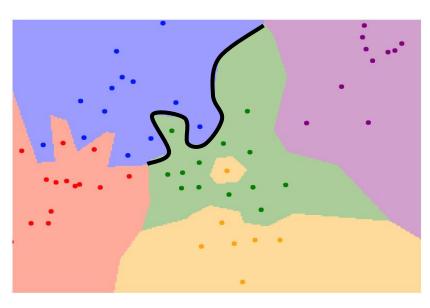


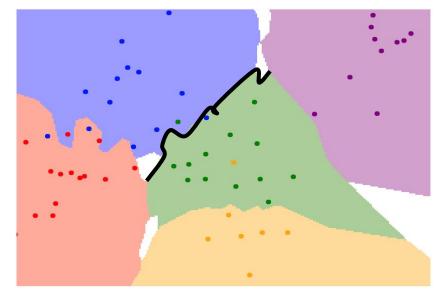


K = 1

K = 3

Using more neighbors helps smooth out rough decision boundaries





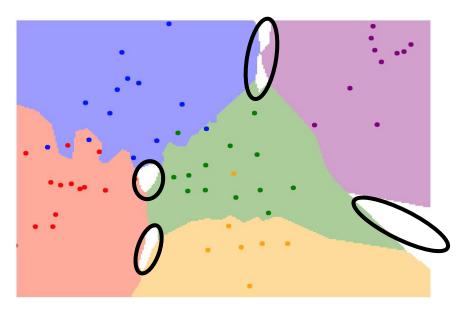
K = 1

K = 3

Find more labels near uncertain white regions

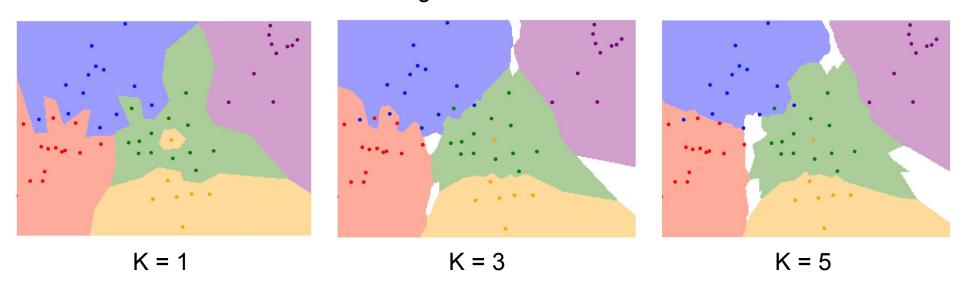






K = 3

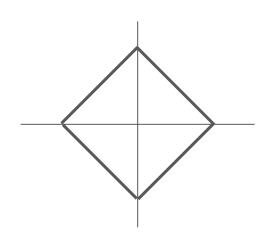
Larger K smooths boundaries more and leads to more uncertain regions



K-Nearest Neighbors: Distance Metric

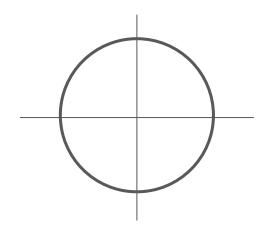
L1 (Manhattan) distance

$$d_1(I_1,I_2) = \sum_p |I_1^p - I_2^p|$$



L2 (Euclidean) distance

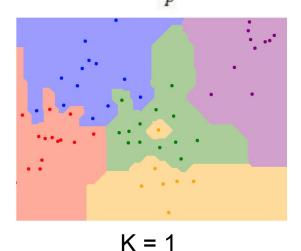
$$d_2(I_1,I_2)=\sqrt{\sum_pig(I_1^p-I_2^pig)^2}$$



K-Nearest Neighbors: Distance Metric

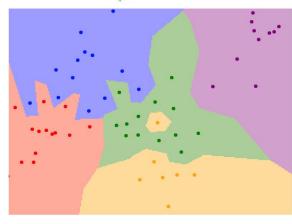
L1 (Manhattan) distance

$$d_1(I_1,I_2) = \sum_p |I_1^p - I_2^p|$$



L2 (Euclidean) distance

$$d_2(I_1,I_2)=\sqrt{\sum_pig(I_1^p-I_2^pig)^2}$$



$$K = 1$$

Hyperparameters

What is the best value of **k** to use? What is the best **distance** to use?

These are **hyperparameters**: choices about the algorithms themselves.

Very problem/dataset-dependent. Must try them all out and see what works best.

Idea #1: Choose hyperparameters that work best on the training data

train

Idea #1: Choose hyperparameters that work best on the training data

BAD: K = 1 always works perfectly on training data

train

Idea #1: Choose hyperparameters that work best on the training data

BAD: K = 1 always works perfectly on training data

train

Idea #2: choose hyperparameters that work best on test data

train

test

Idea #1: Choose hyperparameters **BAD**: K = 1 always works perfectly on training data that work best on the training data train **Idea #2**: choose hyperparameters **BAD**: No idea how algorithm that work best on test data will perform on new data train test

Never do this!

BAD: K = 1 always works **Idea #1**: Choose hyperparameters perfectly on training data that work best on the training data train **Idea #2**: choose hyperparameters **BAD**: No idea how algorithm that work best on test data will perform on new data train test Idea #3: Split data into train, val; choose **Better!** hyperparameters on val and evaluate on test validation train test

train

Idea #4: Cross-Validation: Split data into folds, try each fold as validation and average the results

fold 1	fold 2	fold 3	fold 4	fold 5	test
fold 1	fold 2	fold 3	fold 4	fold 5	test
fold 1	fold 2	fold 3	fold 4	fold 5	test

Useful for small datasets, but not used too frequently in deep learning

Example Dataset: CIFAR10

10 classes50,000 training images10,000 testing images



Alex Krizhevsky, "Learning Multiple Layers of Features from Tiny Images", Technical Report, 2009.

Example Dataset: CIFAR10

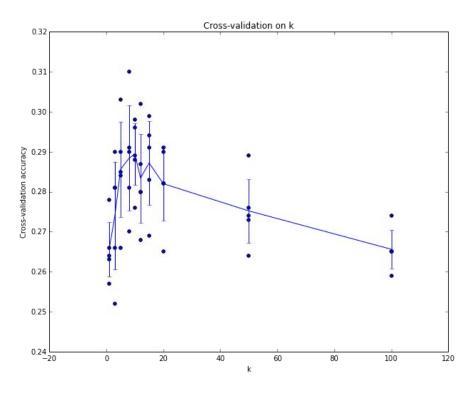
10 classes50,000 training images10,000 testing images



Test images and nearest neighbors



Alex Krizhevsky, "Learning Multiple Layers of Features from Tiny Images", Technical Report, 2009.

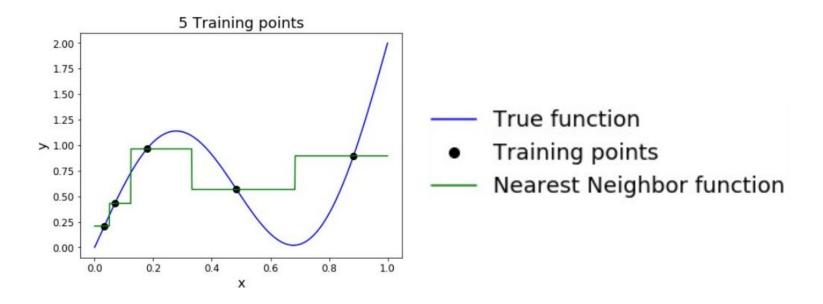


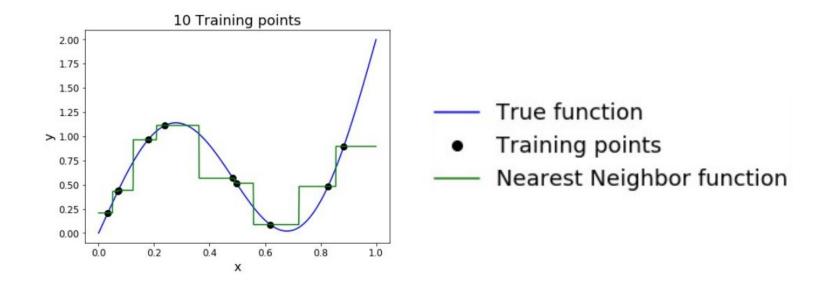
Example of 5-fold cross-validation for the value of **k**.

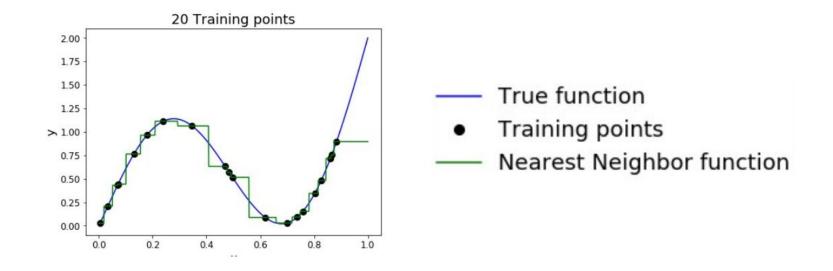
Each point: single outcome.

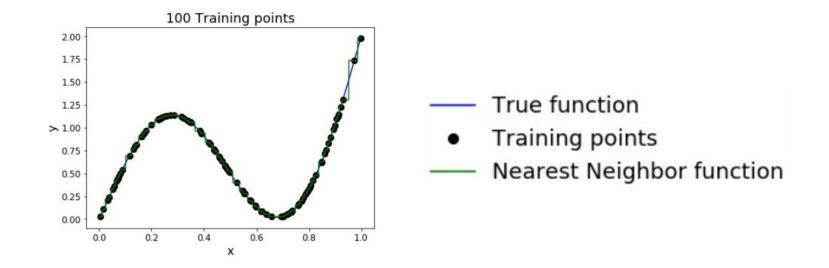
The line goes through the mean, bars indicated standard deviation

(Seems that $k \sim = 7$ works best for this data)



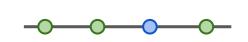






Problem: curse of dimensionality

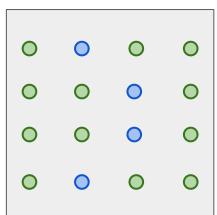
Curse of dimensionality: For uniform coverage of space, number of training points needed grows exponentially with dimension



Points = 4

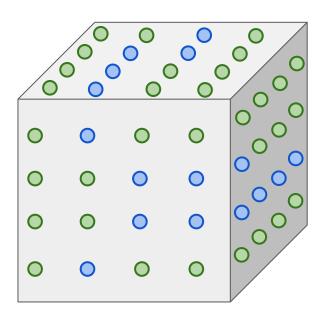
Dimensions =
$$2$$

Points = 4^2



Dimensions =
$$3$$

Points = 4^3



Problem: curse of dimensionality

Curse of dimensionality: For uniform coverage of space, number of training points needed grows exponentially with dimension

Number of possible 32x32 binary images:

$$2^{32\times32} = 10^{308}$$

Number of elementary particles in the visible universe: 10⁹⁷

K-Nearest Neighbors: Summary

In image classification we start with a training set of images and labels, and must predict labels on the **test set**

The **K-Nearest Neighbors** classifier predicts labels based on the K nearest training examples

Distance metric and K are hyperparameters

Choose hyperparameters using the **validation set**;

Only run on the test set once at the very end!

k-Nearest Neighbor with pixel distance never used.

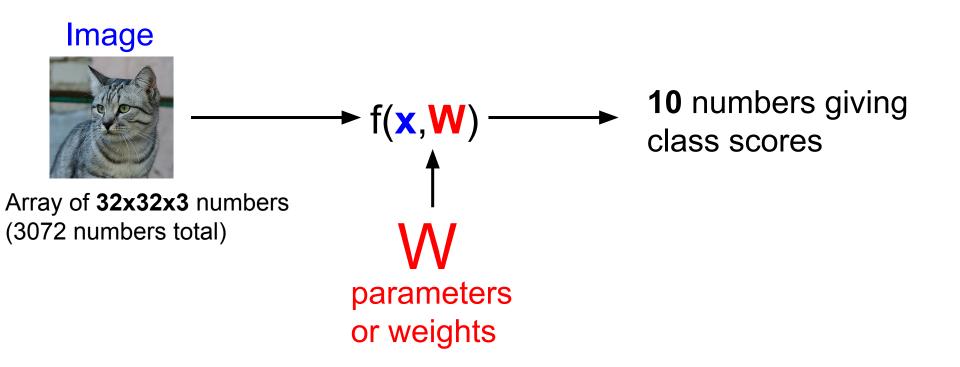
Distance metrics on pixels are not informative



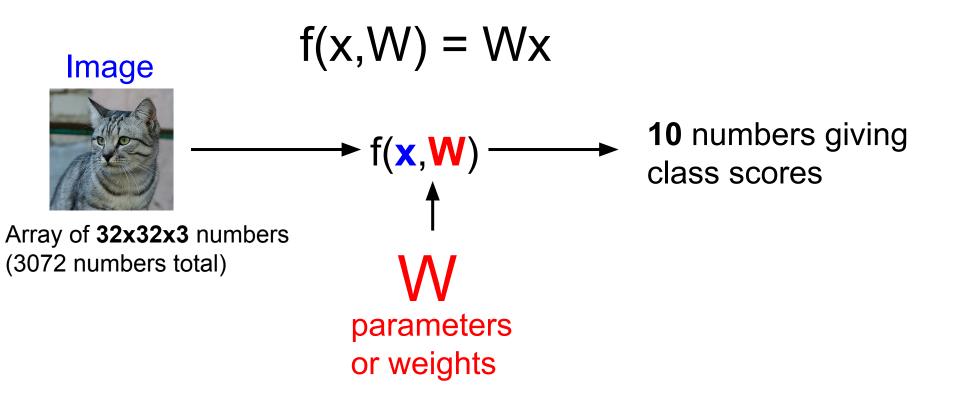
(All three images on the right have the same pixel distances to the one on the left)

Linear Classifier

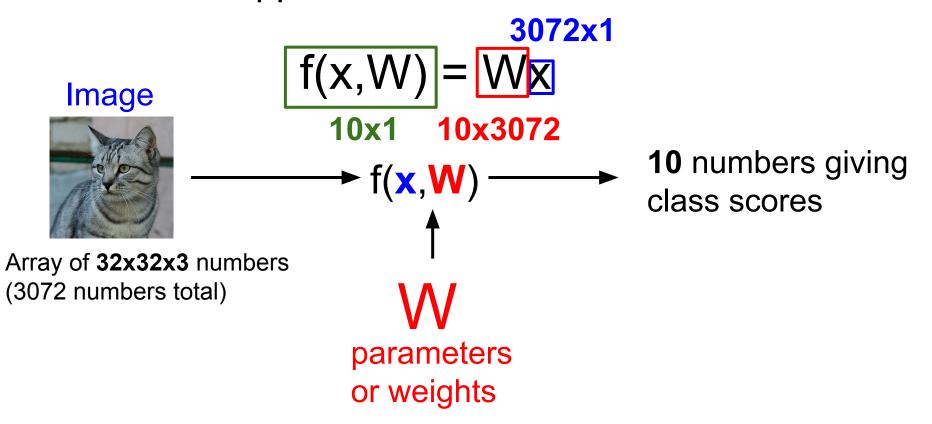
Parametric Approach



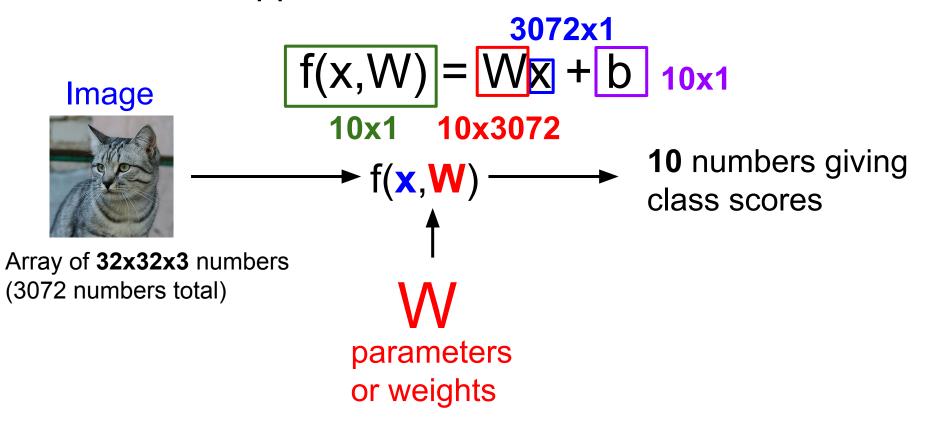
Parametric Approach: Linear Classifier



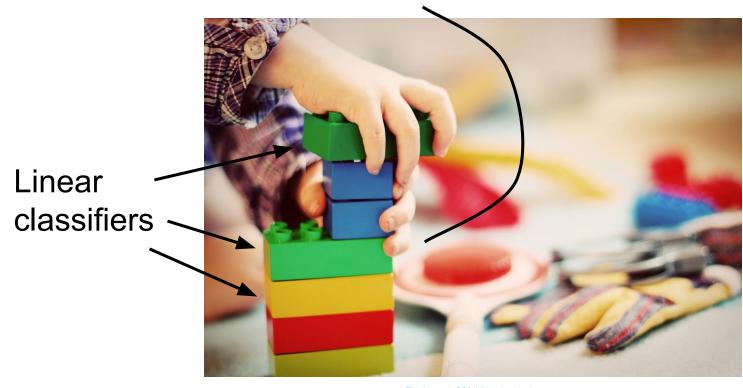
Parametric Approach: Linear Classifier



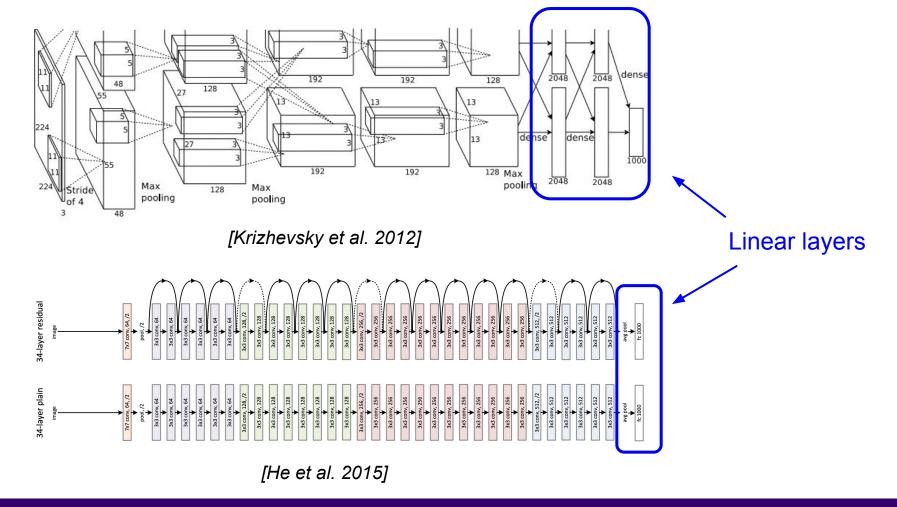
Parametric Approach: Linear Classifier



Neural Network



This image is CC0 1.0 public domain



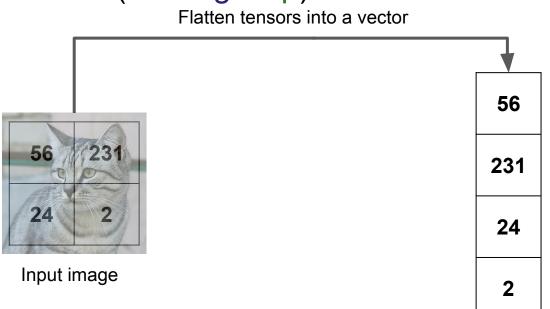
Recall CIFAR10



50,000 training images each image is **32x32x3**

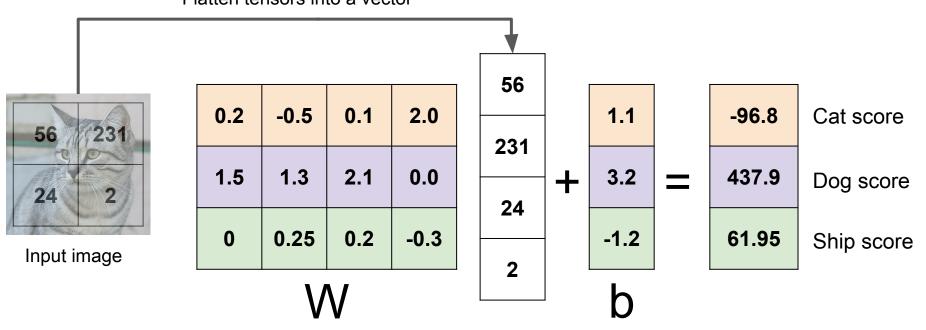
10,000 test images.

Algebraic viewpoint: Example with an image with 4 pixels, and 3 classes (cat/dog/ship)



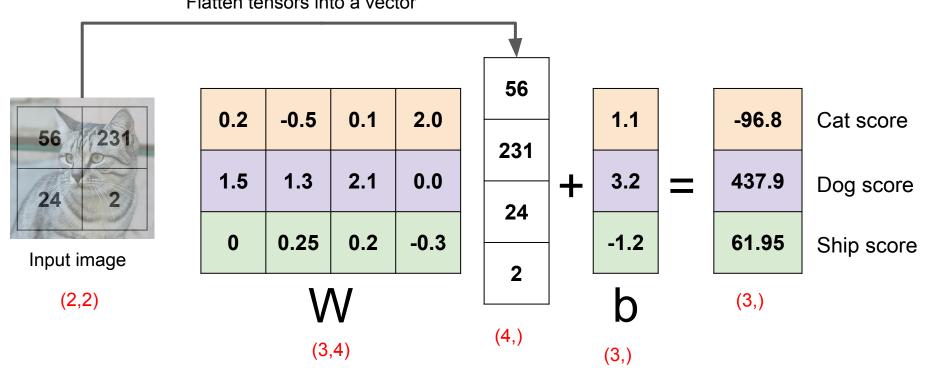
Algebraic viewpoint: Example with an image with 4 pixels, and 3 classes (cat/dog/ship)

Flatten tensors into a vector



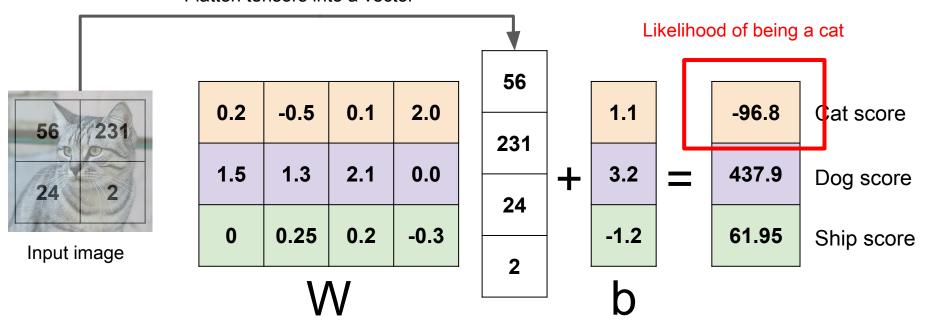
Algebraic viewpoint: Example with an image with 4 pixels, and 3 classes (cat/dog/ship)

Flatten tensors into a vector

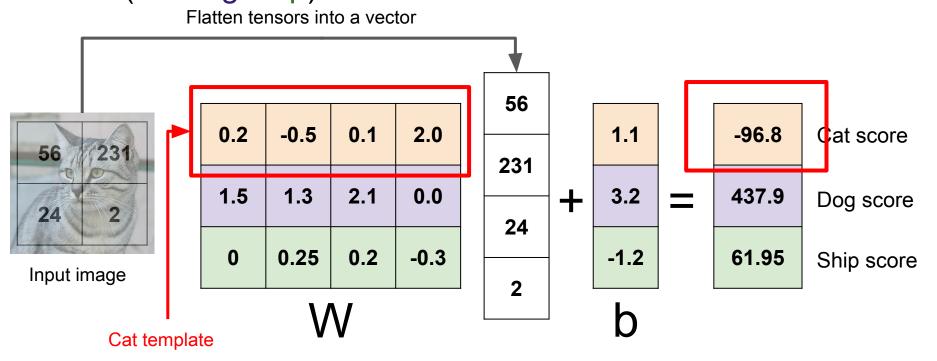


Algebraic viewpoint: Example with an image with 4 pixels, and 3 classes (cat/dog/ship)

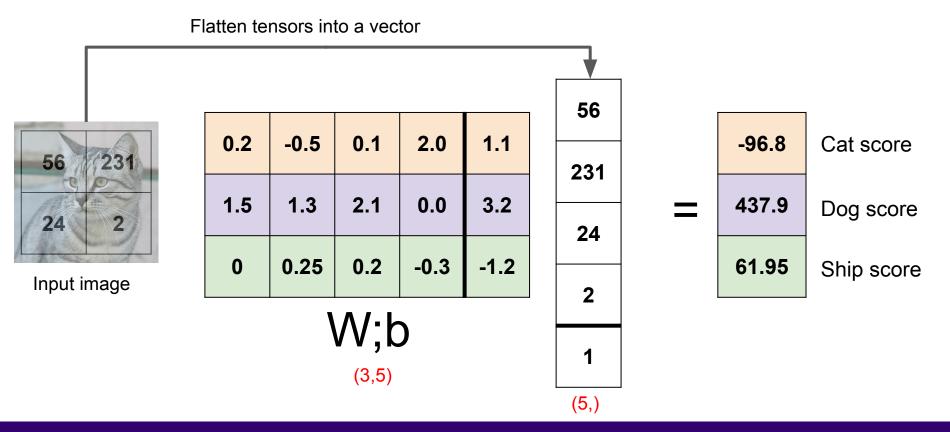
Flatten tensors into a vector



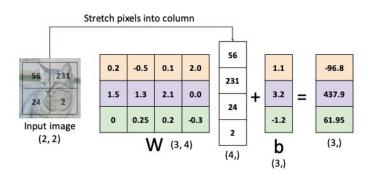
Algebraic viewpoint: Example with an image with 4 pixels, and 3 classes (cat/dog/ship)

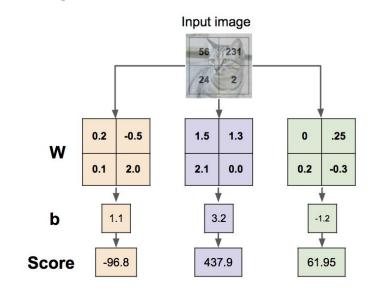


Algebraic viewpoint: Bias trick to simply computation

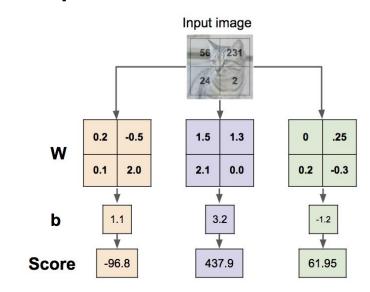


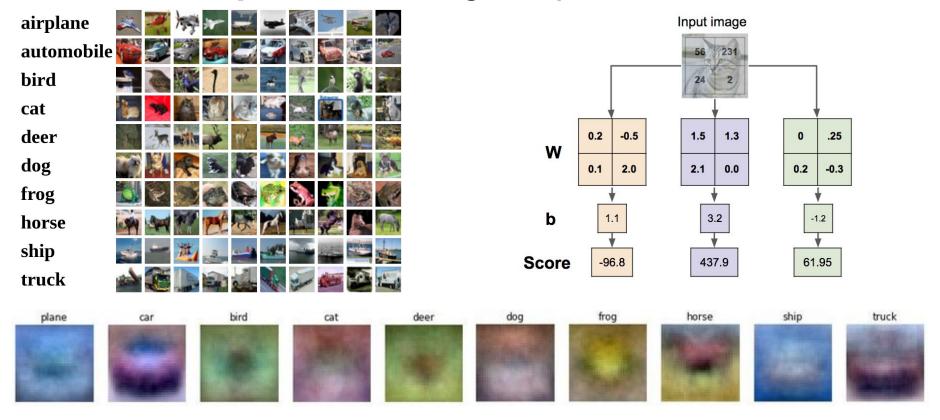
Algebraic viewpoint:

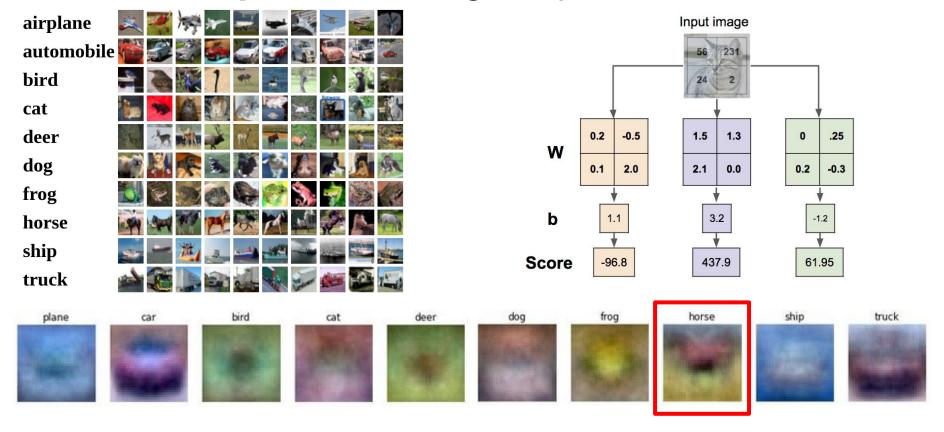


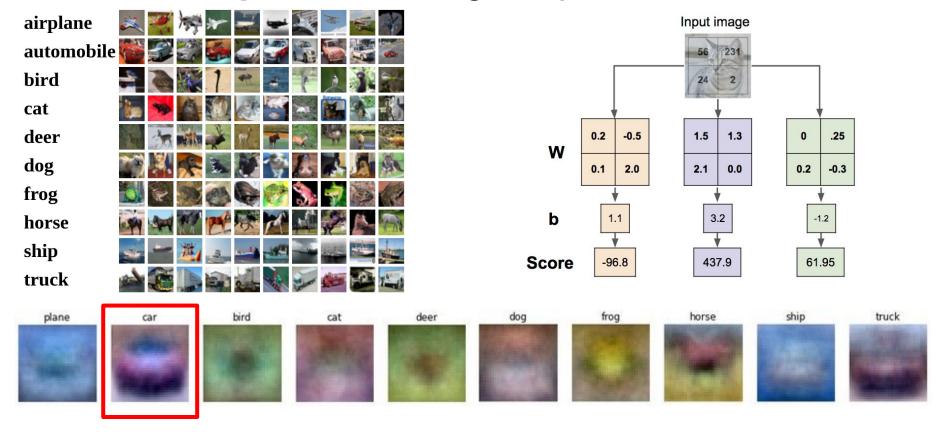




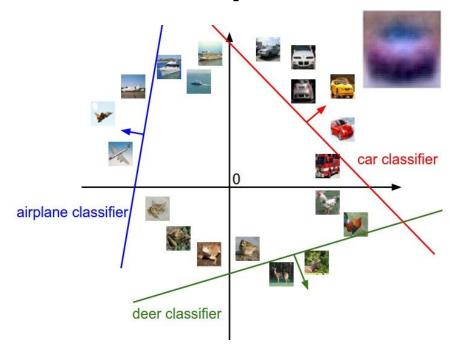








Geometric Viewpoint: linear decision boundaries



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

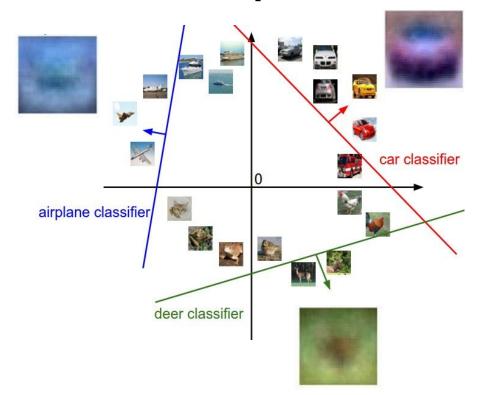


Array of **32x32x3** numbers (3072 numbers total)

Plot created using Wolfram Cloud

Cat image by Nikita is licensed under CC-BY 2.0

Geometric Viewpoint: linear decision boundaries



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

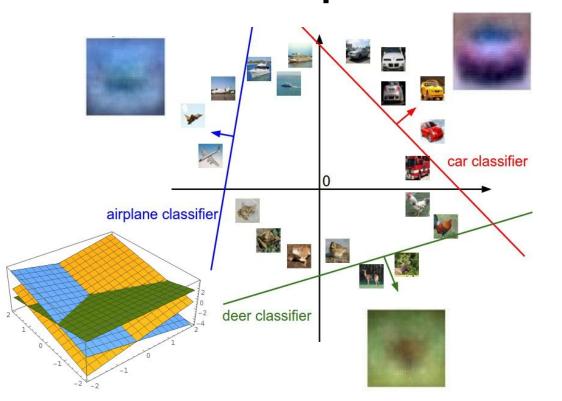


Array of **32x32x3** numbers (3072 numbers total)

Plot created using Wolfram Cloud

Cat image by Nikita is licensed under CC-BY 2.0

Geometric Viewpoint: linear decision boundaries



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



Array of **32x32x3** numbers (3072 numbers total)

Plot created using Wolfram Cloud

Cat image by Nikita is licensed under CC-BY 2.0

Hard cases for a linear classifier

Class 1

First and third quadrants

Class 2

Second and fourth quadrants

Class 1:

1 <= L2 norm <= 2

Class 2

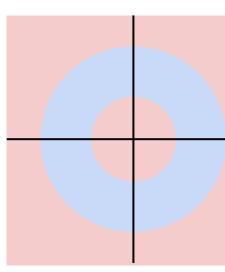
Everything else

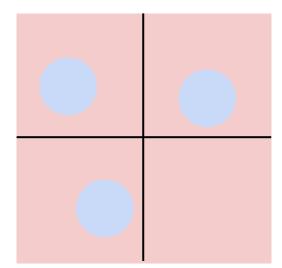
Class 1:

Three modes

Class 2

Everything else

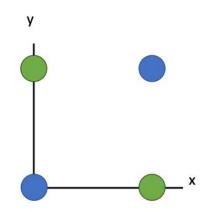


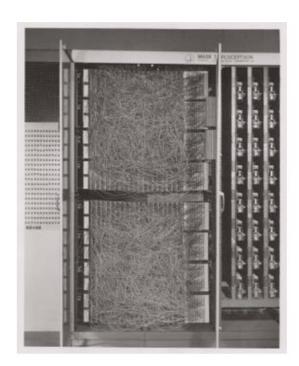


Recall the Minsky report 1969 from last lecture

Unable to learn the XNOR function

Х	Υ	F(x,y)
0	0	0
0	1	1
1	0	1
1	1	0

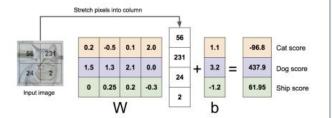




Three viewpoints for interpreting linear classifiers

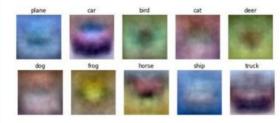
Algebraic Viewpoint

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



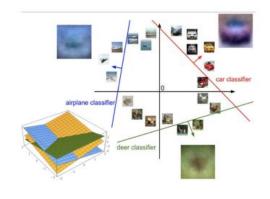
Visual Viewpoint

One template per class



Geometric Viewpoint

Hyperplanes cutting up space



Coming up:

- Loss function
- Optimization
- ConvNets!

f(x,W) = Wx + b

(quantifying what it means to have a "good" W)

(start with random W and find a W that minimizes the loss)

(tweak the functional form of f)