#### Lecture 3:

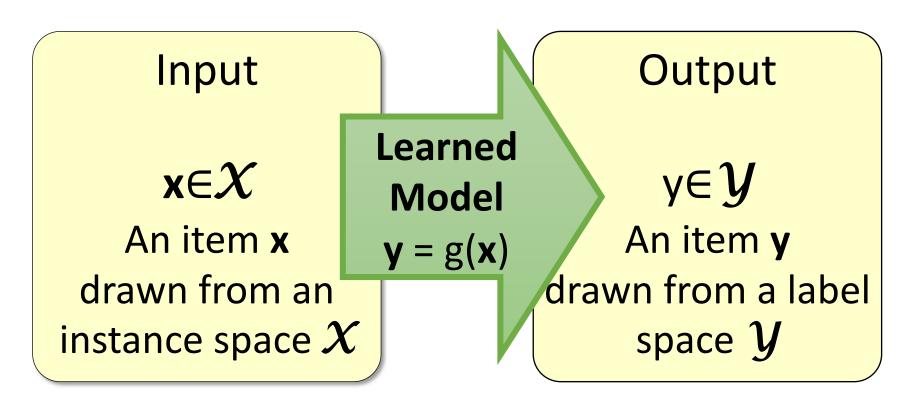
# Hypothesis Space & KNN Fall 2022

Kai-Wei Chang CS @ UCLA

kw+cm146@kwchang.net

The instructor gratefully acknowledges Eric Eaton (UPenn), who assembled the original slides, Jessica Wu (Harvey Mudd), David Kauchak (Pomona), Dan Roth (Upenn), Sriram Sankararaman (UCLA), whose slides are also heavily used, and the many others who made their course materials freely available online.

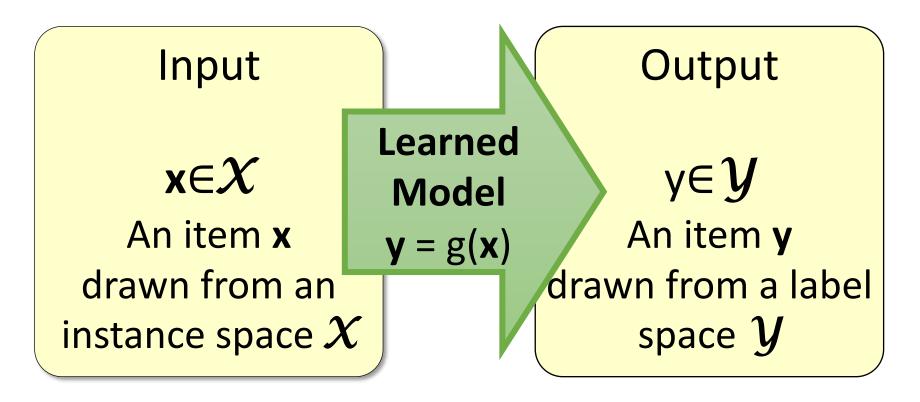
## Supervised Learning



# Using supervised learning

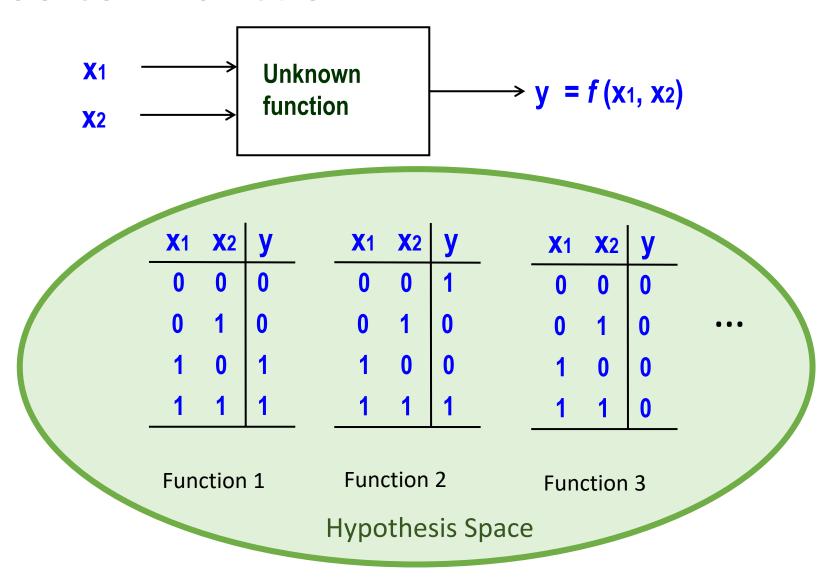
- What is our instance space?
  - Gloss: What kind of features are we using?
- What is our label space?
  - Gloss: What kind of learning task are we dealing with?
- What is our hypothesis space?
  - Gloss: What kind of functions (models) are we learning?
- What learning algorithm do we use?
  - Gloss: How do we learn the model from the labeled data?
- What is our loss function/evaluation metric?
  - Gloss: How do we measure success? What drives learning?

# 3. The model g(x)

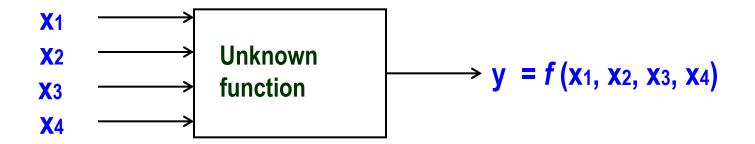


We need to choose what kind of model we want to learn

#### **Boolean Function**



## A Learning Problem



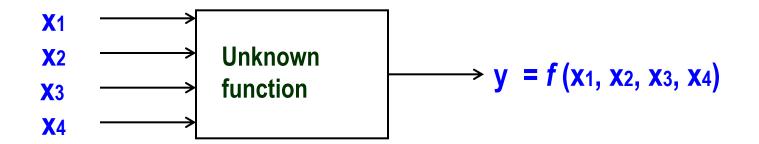
Example	<b>X</b> 1	<b>X</b> 2	<b>X</b> 3	<b>X</b> 4	y
1	0	0	1	0	0
2	0	1	0	0	0
3	0	0	1	1	1
4	1	0	0	1	1
5	0	1	1	0	0
6	1	1	0	0	0
7	0	1	0	1	0

Can you learn this function?

What is it?

A function g is consistent to a dataset  $D = \{(x_i, y_i)\}$  if  $g(x_i) = y_i, \forall i$ 

# Discussion: A Learning Problem



Example	<b>X</b> 1	<b>X</b> 2	<b>X</b> 3	<b>X</b> 4	y
1	0	0	1	0	0
2	0	1	0	0	0
3	0	0	1	1	1
4	1	0	0	1	1
5	0	1	1	0	0
6	1	1	0	0	0
7	0	1	0	1	0

Can you learn this function?

What is it?

A function g is consistent to a dataset

$$D = \{(x_i, y_i)\} \text{ if } g(x_i) = y_i, \forall i$$

How many possible functions over four features? How many function is consistent to D on the left

# Hypothesis Space

How many possible functions over four features?

#### **Complete Ignorance:**

There are  $2^{16} = 65536$  possible function over four input features.

<u>Example</u>	<b>X</b> 1	<b>X</b> 2	<b>X</b> 3	<b>X</b> 4	<u> </u>
ons	0	0	0	0	?
	0	0	0	1	? ? ? ? ? ? ? ? ? ? ? ? ? ?
	0 0 0 0	0	1	0	?
	0	0	1	1	?
	0	1	0	0	?
	0	1	0	1	?
	0	1	1	0	?
	0 0 1 1	1	1	1	?
	1	0	0	0	?
		0 0 0	0	0	?
	1	0	1	0	?
	1		1	1	?
	1	1	0	0	?
	1	1	0	1	?
	1	1	1	0	?
	<u>1</u>	1	1	1	?

# Hypothesis Space

#### **Complete Ignorance:**

There are  $2^{16} = 65536$  possible functions over four input features.

We can't figure out which one is correct until we've seen every possible input-output pair.

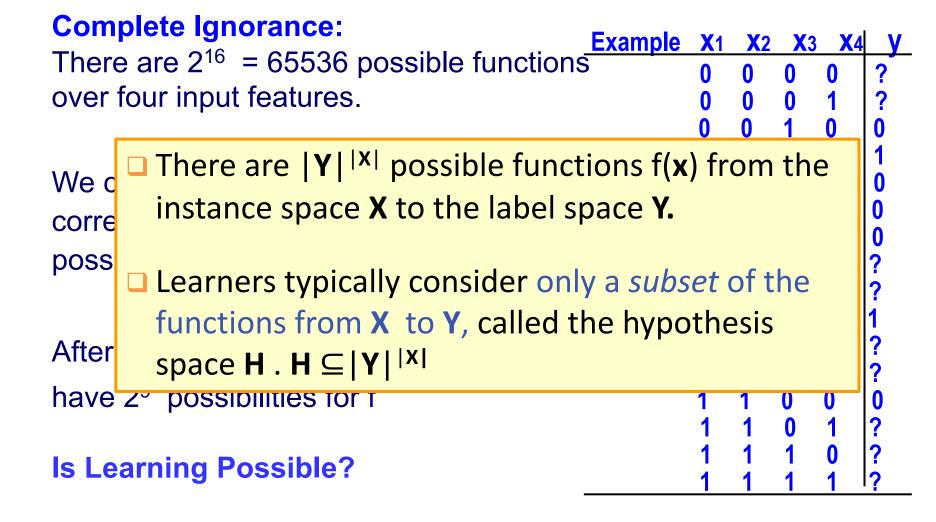
After observing seven examples we still have 2<sup>9</sup> possibilities for f

#### Is Learning Possible?

which one is the most likely one?

Exam	ole	<b>X</b> 1	<b>X</b> 2	X3	3 <b>X</b> 4	l y
		0	0	0	0	?
		0	0	0	1	?
		0	0	1	0	0
		0	0	1	1	1
		0	1	0	0	0
		0	1	0	1	0
		0	1	1_	0	0
		0	1	1	1	?
		1_	0	0	0	?
		1	0	0	1	1
		1	0	1	0	?
		1_	0	1_	_1	?
		1	1	0	0	0
		1	1	0	1	?
		1	1	1	0	?
		1	1	1	1	?

# Hypothesis Space



# Hypothesis Space (2)

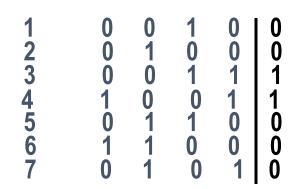
Simple Rules: conjunctive rules

of the form 
$$y=x_i \Lambda x_j \Lambda ... \Lambda x_k$$

e.g., 
$$y = x_2 \wedge x_3$$
  
 $y = x_1 \wedge x_2 \wedge X_4$ 

How large is the hypothesis space?

# Hypothesis Space (2)



Simple Rules: There are only 16 conjunctive rules

of the form  $y=x_i \Lambda x_j \Lambda x_k$ 

Rule	Counterexample	Rule	Counterexample
<b>y</b> = 1		<b>X</b> 2 A <b>X</b> 3	
<b>X</b> 1		<b>X</b> 2 $\Lambda$ <b>X</b> 4	
<b>X</b> 2		<b>X</b> 3 A <b>X</b> 4	
<b>X</b> 3		<b>X</b> 1 $\Lambda$ <b>X</b> 2 $\Lambda$ <b>X</b> 3	
<b>X</b> 4		<b>X</b> 1 Λ <b>X</b> 2 Λ <b>X</b> 4	
<b>X</b> 1 $\Lambda$ <b>X</b> 2		<b>X</b> 1 $\Lambda$ <b>X</b> 3 $\Lambda$ <b>X</b> 4	
<b>X</b> 1 $\Lambda$ <b>X</b> 3		<b>X</b> 2 $\Lambda$ <b>X</b> 3 $\Lambda$ <b>X</b> 4	
<b>X</b> 1 $\Lambda$ <b>X</b> 4		<b>X</b> 1 A <b>X</b> 2 A <b>X</b> 3 A	. <b>X</b> 4

# Hypothesis Space (2)

1	0	0	1	0	1 0
2 3	0	1	0	0 0 1 1 0	0
	0	0		1	1
4 5 6 7	1	0	0	1	1
5	0	1	1	0	0
6	1	1	0	0	0
7	0	1	0	1	0011000

Simple Rules: There are only 16 conjunctive rules

of the form  $y=x_i \Lambda x_j \Lambda x_k$ 

Rule	Counterexample	Rule	<b>Counterexample</b>
<b>y</b> =c		<b>X</b> 2 $\Lambda$ <b>X</b> 3	0011 1
<b>X</b> 1	1100 0	<b>X</b> 2 $\Lambda$ <b>X</b> 4	0011 1
<b>X2</b>	0100 0	<b>X</b> 3 $\Lambda$ <b>X</b> 4	1001 1
<b>X</b> 3	0110 0	<b>X</b> 1 $\Lambda$ <b>X</b> 2 $\Lambda$ <b>X</b> 3	0011 1
<b>X</b> 4	0101 1	<b>X</b> 1 Λ <b>X</b> 2 Λ <b>X</b> 4	0011 1
X1 A X2	1100 0	<b>X</b> 1 $\Lambda$ <b>X</b> 3 $\Lambda$ <b>X</b> 4	0011 1
<b>X</b> 1 $\Lambda$ <b>X</b> 3	0011 1	<b>X</b> 2 $\Lambda$ <b>X</b> 3 $\Lambda$ <b>X</b> 4	0011 1
<b>X</b> 1 $\Lambda$ <b>X</b> 4	0011 1	X1 A X2 A X3 A X	K4 0011 1

No simple rule explains the data. The same is true for **simple clauses**.

# Hypothesis Space (3)

m-of-n rules: There are 32 possible rules of the form "y = 1 if and only if at least m of the following n variables are 1"

**Notation:** 2 variables from the set on the left. **Value**: Index of the counterexample.

variables	1-of 2-of 3-of 4-of	variables	1-of 2-of 3-of 4-of
{ <b>X</b> 1}		{ <b>X2</b> , <b>X</b> 4}	
{ <b>X2</b> }		{ <b>X3</b> , <b>X4</b> }	
<b>{X3</b> }		{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 3}	
<b>{X4</b> }		{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 4}	
{ <b>X1,X2</b> }		{ <b>X</b> 1, <b>X</b> 3, <b>X</b> 4}	
{ <b>X</b> 1, <b>X</b> 3}		$\{X2, X3, X4\}$	
{ <b>X</b> 1, <b>X</b> 4}		{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 3, <b>X</b> 4}	
{ <b>X2,X3</b> }			

# Hypothesis Space (3)

m-of-n rules: There are 32 possible rules of the form "y = 1 if and only if at least m of the following n variables are 1"

**Notation:** 2 variables from the set on the left. **Value**: Index of the counterexample.

variables	1-	1-of 2-of 3-of 4-of			variables	1-of 2-of 3-of 4-of			
{ <b>X</b> 1}	3	•	•		{ <b>X2</b> , <b>X</b> 4}	2	3	•	•
{ <b>X2</b> }	2	•	•	•	{ <b>X</b> 3, <b>X</b> 4}	4	4	•	-
{ <b>X3</b> }	1	•	•	•	{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 3}	1	3	3	-
<b>{X4</b> }	7	•	-		{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 4}	2	3	3	-
{ <b>X</b> 1, <b>X</b> 2}	2	3	•		{ <b>X</b> 1, <b>X</b> 3, <b>X</b> 4}	1 (	* * *	3	-
{ <b>X</b> 1, <b>X</b> 3}	1	3	•		{ <b>X</b> 2, <b>X</b> 3, <b>X</b> 4}	1	5	3	-
{ <b>X</b> 1, <b>X</b> 4}	6	3	•	•	{ <b>X</b> 1, <b>X</b> 2, <b>X</b> 3, <b>X</b> 4}	1	5	3	3
{ <b>X2,X</b> 3}	2	3	-	•					

Found a consistent hypothesistel & KNN

#### Views of Learning

- Learning is the removal of our <u>remaining</u> uncertainty:
- Learning requires guessing a good hypothesis class
  - Start with a small class and enlarge it until it contains an hypothesis that fits the data.
- We could be wrong!
  - Our guess of the hypothesis space could be wrong
    - $\Rightarrow$  y=x4  $\land$  one-of (x1, x3) is also consistent

#### General strategies for Machine Learning

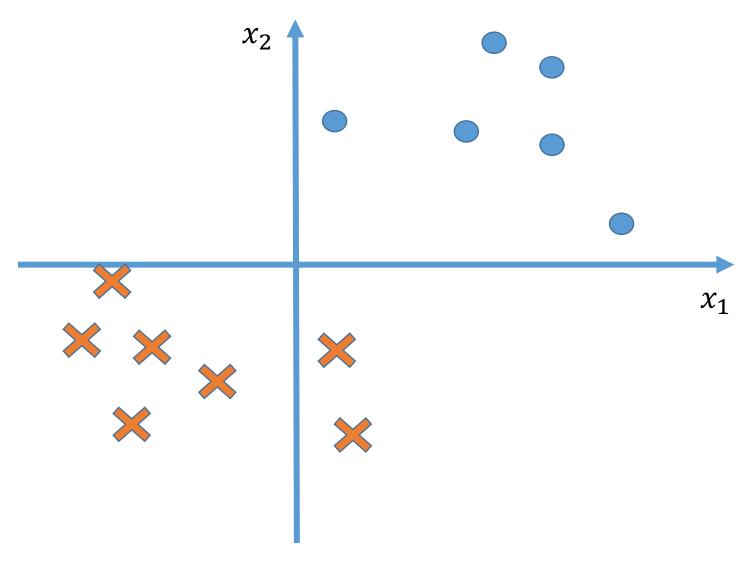
- Develop flexible hypothesis spaces:
  - Decision trees, neural networks, nested collections.
- Develop algorithms for finding the "best" hypothesis in the hypothesis space, that fits the data
- And, <u>hope</u> that it will generalize well

# Hypothesis Space -- Real-Value Features

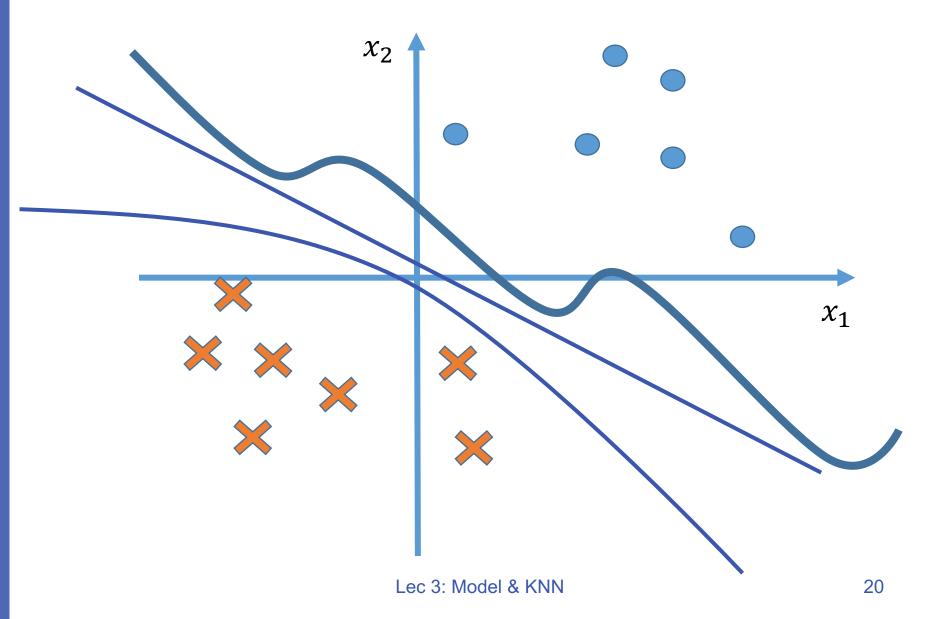




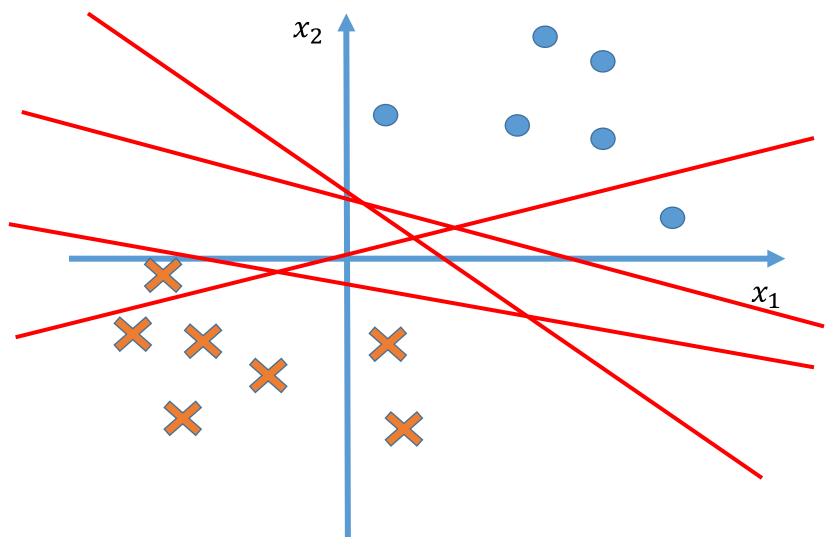
# Example problem



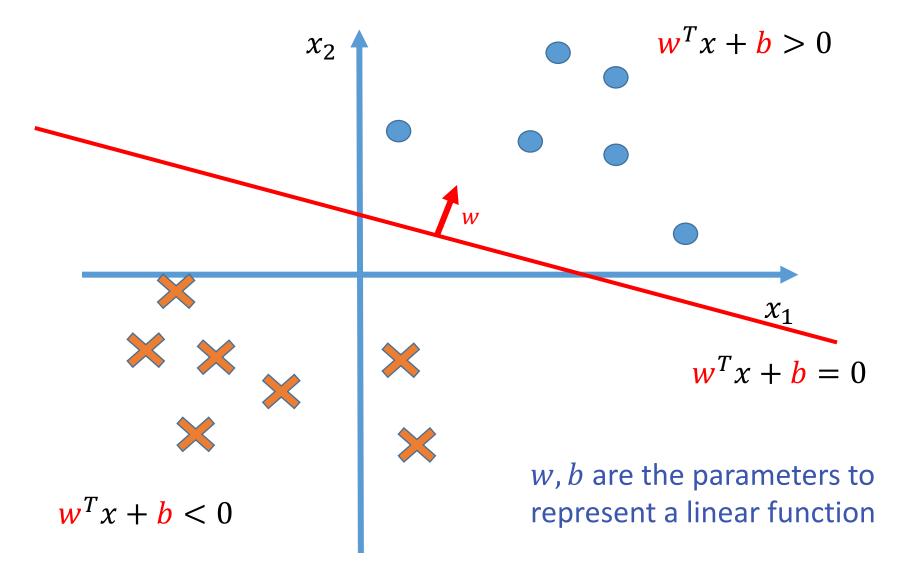
# Hypothesis space:



# Hypothesis space: linear model

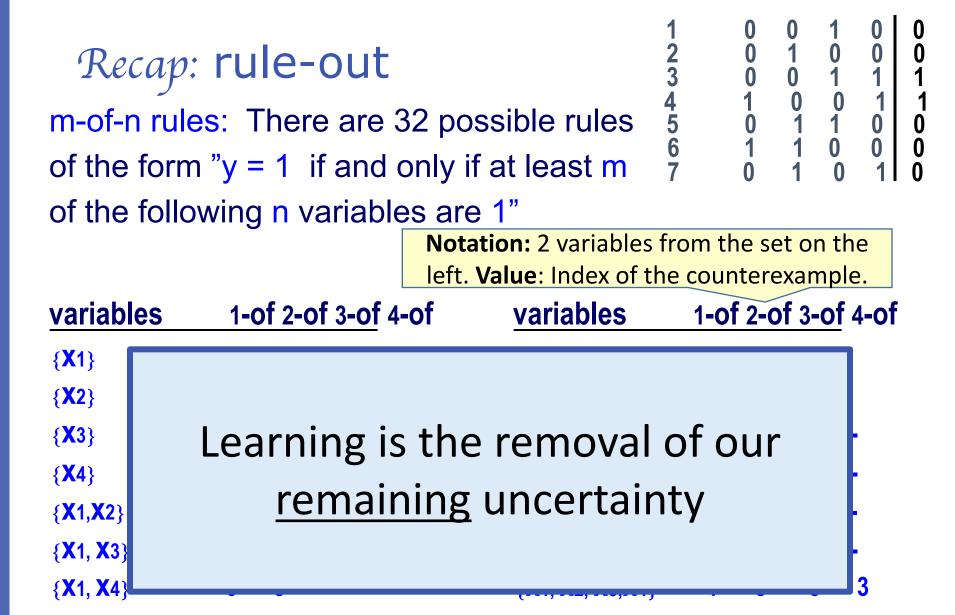


## Hypothesis space: linear model



# How to learn?

How can we find a good model from the hypothesis space?

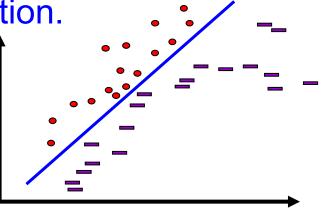


Found a consistent hypothesisted & KNN

**{X2,X3**}

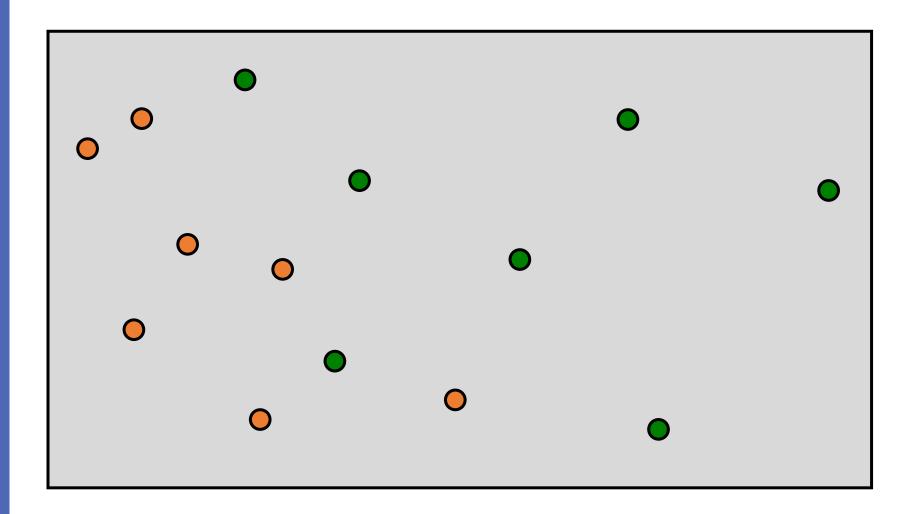
#### How about linear function?

- Challenges
  - The hypothesis space contains infinite # functions
  - Several functions are consistent with the data
- A possibility: Local search
  - Start with a linear threshold function.
  - See how well you are doing.
  - Correct
  - Repeat until you converge.
- Optimize a function with calculus

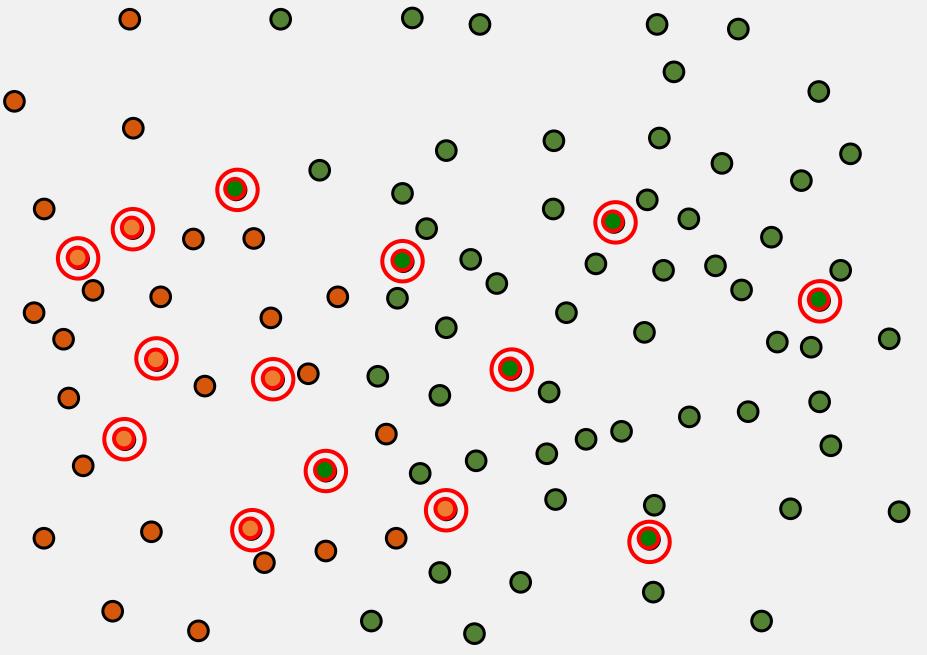


# Choose Hypothesis Space

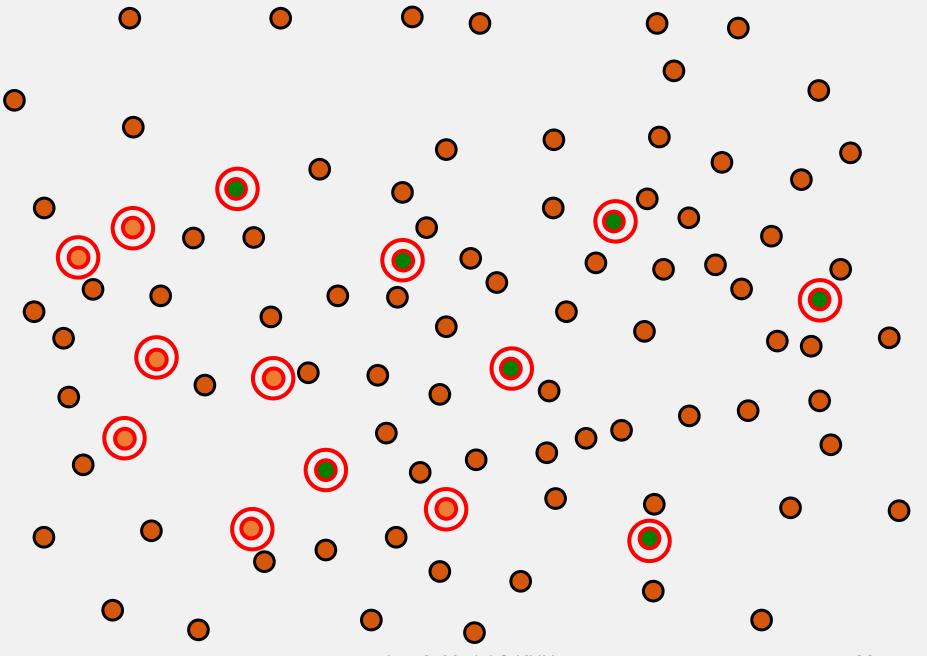
# Our training data



# The instance space Lec 3: Model & KNN



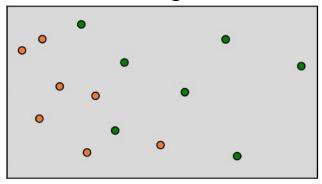
Lec 3: Model & KNN



Lec 3: Model & KNN

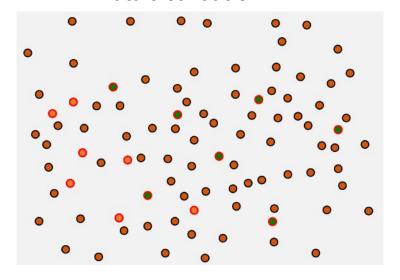
# Which one is more likely?

Training set

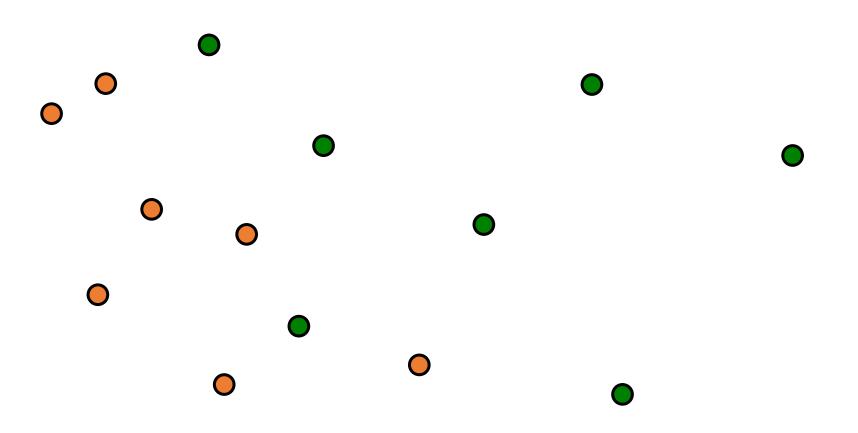


Data distribution A

Data distribution B

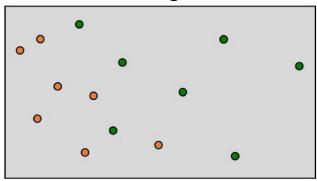


# Our training data



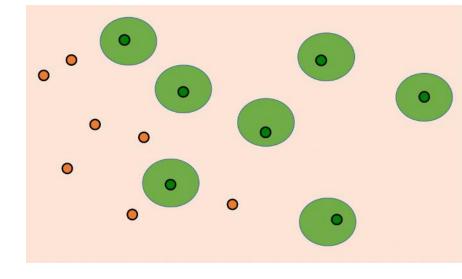
# Which one is more likely to be a good hypothesis?

Training set



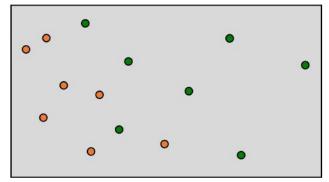
Hypothesis A

Hypothesis B

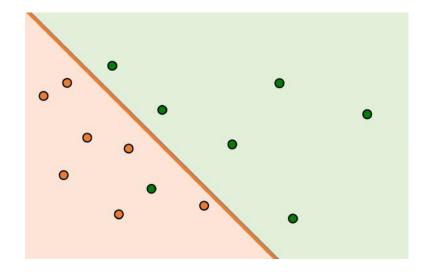


# Which one is more likely to be a good hypothesis?

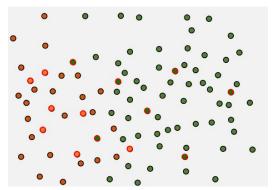
Training set



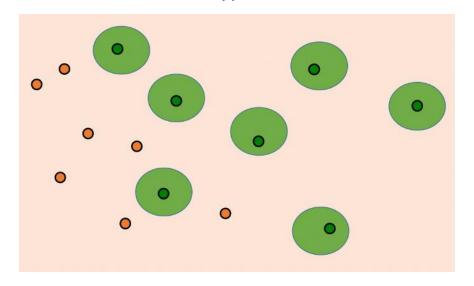
Hypothesis A



(Likely) Data Distribution

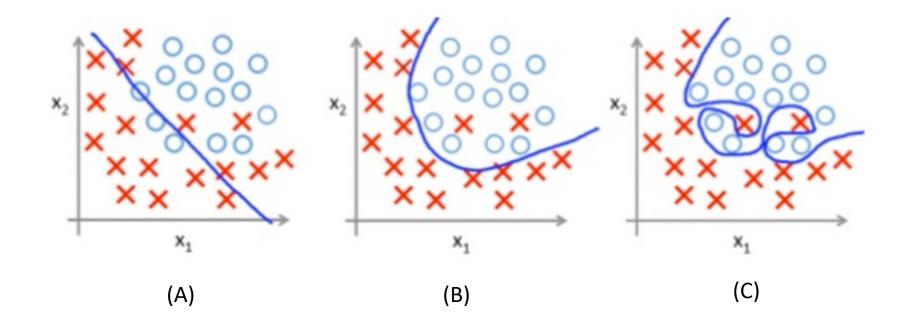


Hypothesis B



# Under-fitting and over-fitting

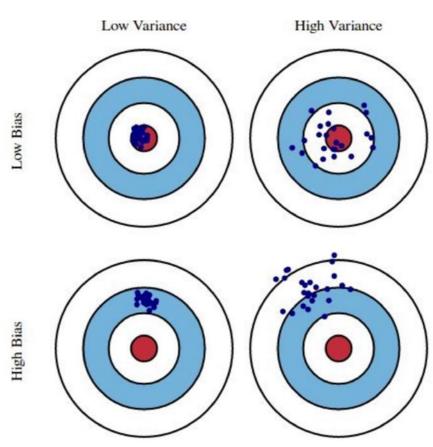
Which classifier (blue line) is the best one?



#### Bias V.S. Variance

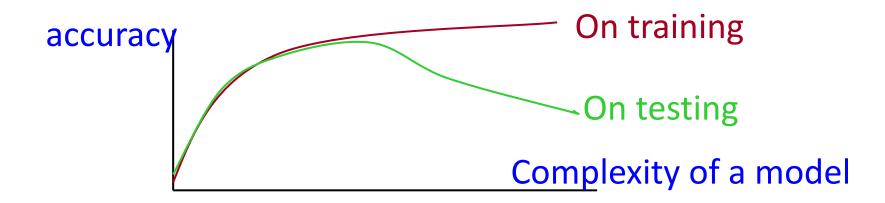
Remember, training data are subsamples drawn from the true distribution

- Exam strategy:
  - Study every chapter well
    - A+: Low var & bias
  - Study only a few chapters
    - ❖ A+? B? C? Low bias; High var
  - Study every chapter roughly
    - ❖ B+: Low var; high bias
  - Go to sleep
    - ❖ B ~D: High var, high bias



## Overfitting the Data

- A classifier perform perfectly on the training data may not lead to the best generalization performance.
  - There may be noise in the training data
  - The algorithm might be making decisions based on very little data



## Prevent overfitting

- Using a less-expressive model
  - E.g., linear model
- Adding regularization
  - Promote simper models
- Data perturbation (add noise in training)
  - Can be done algorithmically (e.g., dropout)
- Stop the optimization process earlier
  - Sounds bad in theory; but works in practice

More discussion in later lectures

## K-Nearest Neighbor

Kai-Wei Chang CS @ UCLA

kw+cm146@kwchang.net

The instructor gratefully acknowledges Dan Roth, Vivek Srikuar, Sriram Sankararaman, Fei Sha, Ameet Talwalkar, Eric Eaton, and Jessica Wu whose slides are heavily used, and many others who made their course material freely available online.

## Motivation: spam mail

hi Spam x

① marina <marina0279@static.vnpt.vn>
to kw ▼

① This message has a from address in static.vnpt.vn but has failed static.vnpt.vn's required tests for authentication. Learn more

You seem like my type and I would like to know you more! Write me if you are interested, here is my email denisavafursula@rambler.ru and, if you want, I will send some of my photos. Hugs, marina

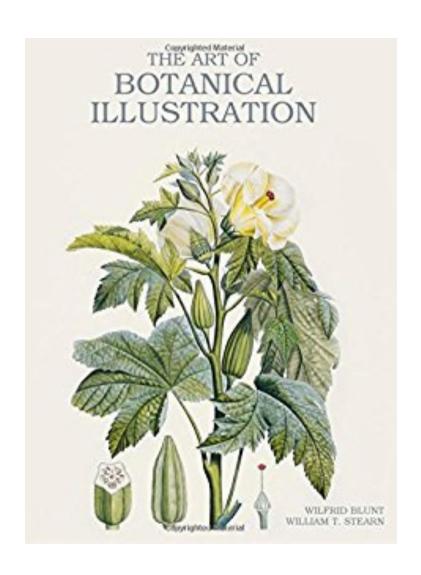


## Motivation: Learning from memorization Recognizing flowers

What is this flower called?



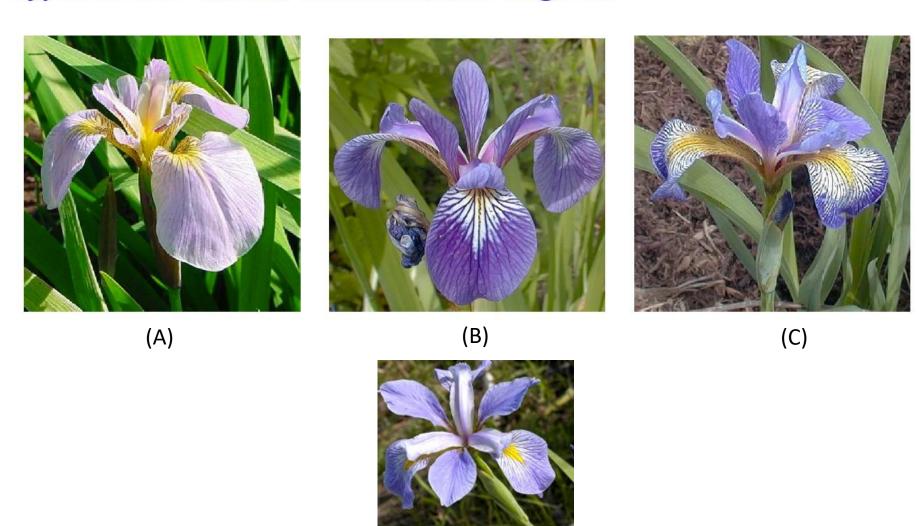
### Look up at Botanical Illustration Books





## Motivation: Learning from memorization Recognizing flowers

Types of Iris: setosa, versicolor, and virginica



## What you will learn in this lecture

- ❖ k-NN algorithm
- Distance between in the vector space
- Parameter tuning
- Decision boundary
- Curse of the Dimensionality (Theoretical Limitation)

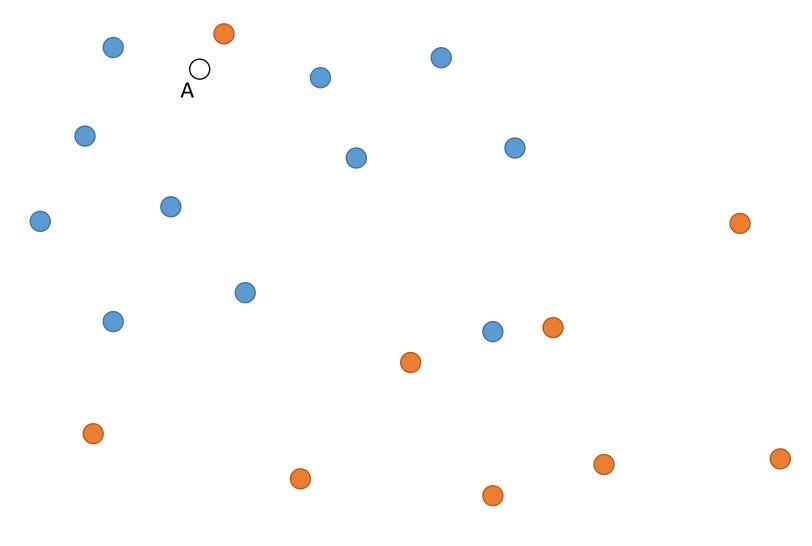
### Nearest Neighbors: The basic version

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

- Prediction: for a new example x
  - ❖ Find the training example x<sub>i</sub> that is *closest* to x
  - Predict the label of x to the label y<sub>i</sub> associated with x<sub>i</sub>

# Example: How would you color the blank circles?



## K-Nearest Neighbors

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.

# Issues in designing KNN algorithm (Modeling)

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

How to define distance?

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.

How do we measure distances between instances in vector space?

In general, a good place to inject knowledge about the domain

Behavior of this approach can depend on this

Numeric features, represented as n dimensional vectors

## Numeric features, represented as n dimensional vectors

Euclidean distance

$$||\mathbf{x}_1 - \mathbf{x}_2||_2 = \sqrt{\sum_{i=1}^n (\mathbf{x}_{1,i} - \mathbf{x}_{2,i})^2}$$

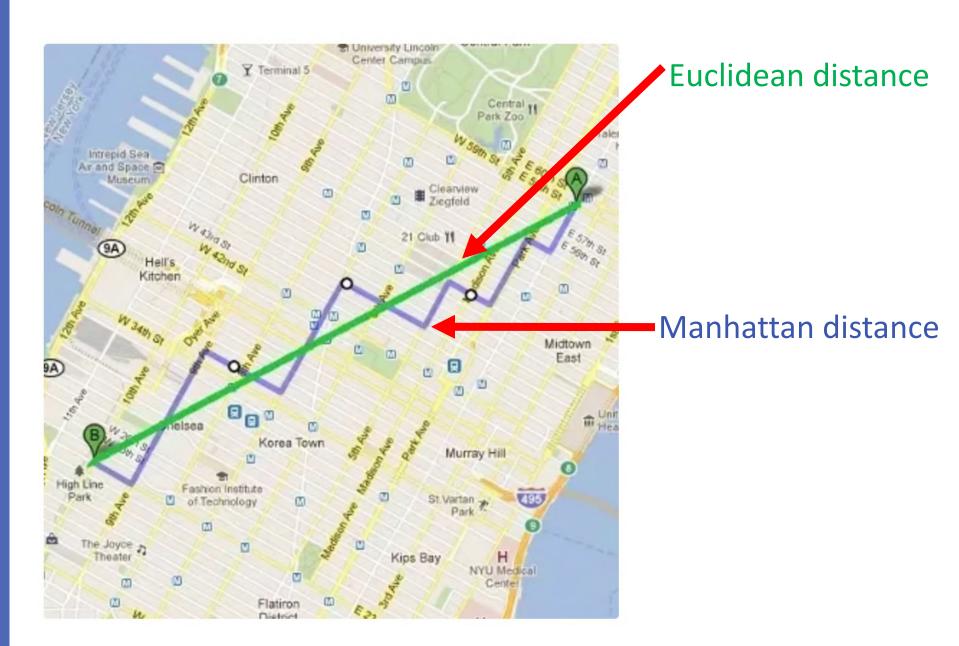
## Numeric features, represented as n dimensional vectors

Euclidean distance

$$||\mathbf{x}_1 - \mathbf{x}_2||_2 = \sqrt{\sum_{i=1}^n (\mathbf{x}_{1,i} - \mathbf{x}_{2,i})^2}$$

Manhattan distance

$$||\mathbf{x}_1 - \mathbf{x}_2||_1 = \sum_{i=1}^{n} |\mathbf{x}_{1,i} - \mathbf{x}_{2,i}|$$



Lec 3: Model & KNN

## Numeric features, represented as n dimensional vectors

Euclidean distance

$$||\mathbf{x}_1 - \mathbf{x}_2||_2 = \sqrt{\sum_{i=1}^n (\mathbf{x}_{1,i} - \mathbf{x}_{2,i})^2}$$

Manhattan distance

$$||\mathbf{x}_1 - \mathbf{x}_2||_1 = \sum_{i=1}^n |\mathbf{x}_{1,i} - \mathbf{x}_{2,i}|$$

- ♣ L<sub>p</sub>-norm
  - ❖ Euclidean = L<sub>2</sub>
  - ❖ Manhattan = L<sub>1</sub>

$$||\mathbf{x}_1 - \mathbf{x}_2||_p = \left(\sum_{i=1}^n |\mathbf{x}_{1,i} - \mathbf{x}_{2,i}|^p\right)^{\frac{1}{p}}$$

P > 0

What about symbolic/categorical features?

#### Symbolic/categorical features

Most common distance is the *Hamming distance* 

- Number of bits that are different
- Or: Number of features that have a different value
- Example:

```
X<sub>1</sub>: {Shape=Triangle, Color=Red, Location=Left, Orientation=Up}
```

X<sub>2</sub>: {Shape=Triangle, Color=Blue, Location=Left, Orientation=Down}

Hamming distance = 2

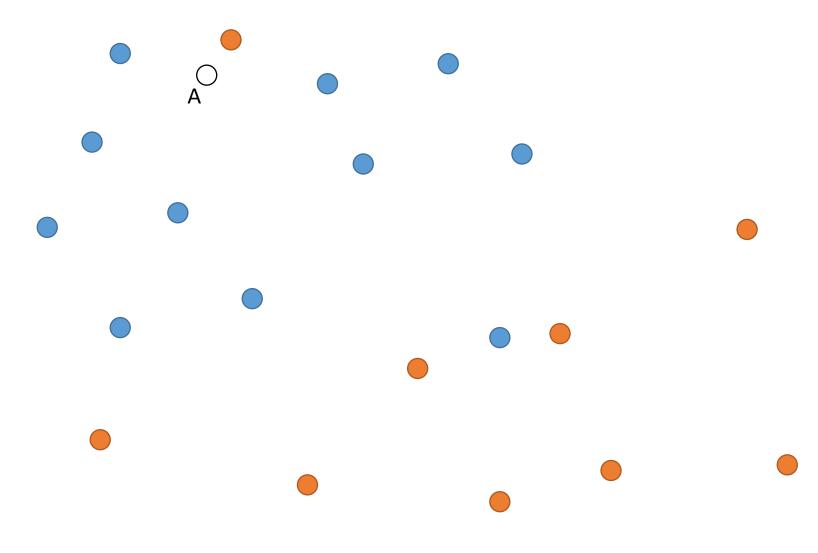
# Issues in designing KNN algorithm (Modeling)

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

- Learning: Just store all the training examples How to choose k and the distance measure?
- Prediction fd wexample x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.

#### Parameter K

What if K is too small? What if K is too large?



### Hyper-parameters in KNN

- (Hyper-)Parameters:
  - Choosing K (# nearest neighbors)
  - ❖ Distance measurement (e.g., p in the L<sub>p</sub>-norm)

$$||\mathbf{x}_1 - \mathbf{x}_2||_p = \left(\sum_{i=1}^n |\mathbf{x}_{1,i} - \mathbf{x}_{2,i}|^p
ight)^{rac{1}{p}}$$

- Those are not specified by the algorithm itself
  - Require empirical studies
  - The best parameter set is task/dataset-specific.

### Train/Dev/Test splits

- You are not allowed to look at Text in parameter turning. Why?
- Split your training data into two sets:
  - Train: Training data (often 80-90%)
  - Dev: Development data (10-20%)
  - Use Dev set (a.k.a. validation set) to find the best parameters



Original Training set

## Recipe of train/dev/test

- For each possible value of the hyper-parameter (e.g., M = 1,2, 3,...,10)
  - $\bullet$  Train a model using  $D^{TRAIN}$
  - $\diamond$  Evaluate the performance on  $D^{DEV}$
- Choose the model parameter with the best performance on D<sup>DEV</sup>
- $\clubsuit$  (optional) Re-train the model on  $D^{TRAIN} \cup D^{DEV}$  with the best parameter set
- $\diamond$  Evaluate the model on  $D^{TEST}$

#### Tradeoff between Train v.s. Dev Size

- Consider having 120 data points; 20 data points are reserved for testing
  - What is the best way to split the remainder?
  - (A) # instances: Train: 95 Dev: 5?
  - ❖ (B) # instances: Train: 60 Dev: 40 ?

## Trade off in Train/Dev splits

Large Train, small Dev (e.g., #train = 95, #dev = 5)

#### **Train**

Dev

Result on dev is not represented

Small Train, Large Dev (e.g., #train = 60, #dev = 40)

#### Train

Dev

No enough data to train a model

#### N-fold cross validation

Instead of a single training-dev split:

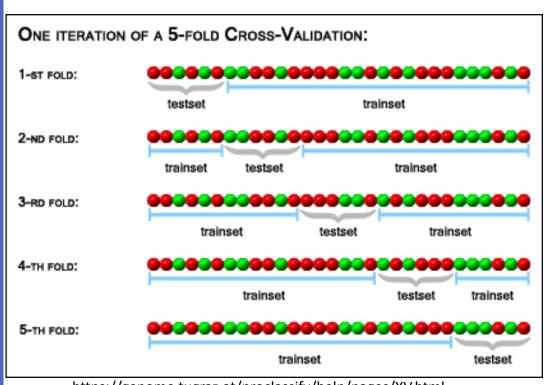
train Dev

Split data into N equal-sized parts



- Train and test N different classifiers
- Report average accuracy and standard deviation of the accuracy

### Example



Parameter 1

Parameter 2

Accuracy: 100% Accuracy: 100%

Accuracy: 50% Accuracy: 100%

Accuracy: 50% Accuracy: 100%

Accuracy: 100% Accuracy: 100%

Accuracy: 100% Accuracy: 50%

https://genome.tugraz.at/proclassify/help/pages/XV.html

Avg Accuracy: 80% Avg Accuracy: 90%

## Finding parameters based on cross validation

- ❖ Given  $D^{TRAIN}$  and  $D^{TEST}$ , for each possible value of the hyper-parameter (e.g., K = 1,2, 3,...,10)
  - ❖ Conduct cross validation on D<sup>TRAIN</sup> with parameter K
- Choose the model parameter with the best cross validation performance
- ❖ (Optional) Re-train the model on D<sup>TRAIN</sup> with the best parameter set
- $\diamond$  Evaluate the model on  $D^{TEST}$

# Issues in designing KNN algorithm (Modeling)

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.

How to aggregate the information and make the prediction?

### K-Nearest Neighbors

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.
    - For classification: Every neighbor votes on the label. Predict the most frequent label among the neighbors.
    - For regression:
      Predict the mean value

Q: other alternatives?

### K-Nearest Neighbors

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the label of x using these k points.
    - For classification: Every neighbor votes on the label. Predict the most frequent label among the neighbors.
    - For regression:
      Prodict the mean

Predict the mean value

Neighbors' labels could be weighted by their distance
Related to Kernel method

# Issues in designing KNN algorithm (computation/algorithm)

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

How to store data?

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the la. of x using these k points.

How to find the closest points?

# Issues in designing KNN algorithm (computation/algorithm)

- Training examples are vectors x<sub>i</sub> associated with a label y<sub>i</sub>
  - ❖ E.g. x<sub>i</sub> = a feature vector for an email, y<sub>i</sub> = SPAM

Learning: Just store all the training examples

How to store data?

- Prediction for a new example x
  - Find the k closest training examples to x
  - Construct the

How to find the closest points?

This is an important research topic, but I will not cover it in this class. Reference: e.g. K-d tree (https://en.wikipedia.org/wiki/K-d\_tree)