Lecture 12: Computational Learning Theory & Kernel Winter 2018

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 the many others who made their course material freely available online.

Recap: Computational Learning Theory

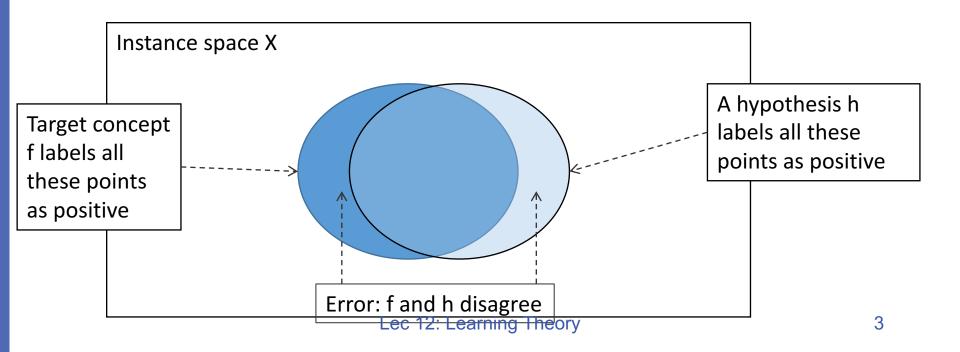
- The Theory of Generalization
 - Using training instance to rule out incorrect hypotheses
- Probably Approximately Correct (PAC) learning
 - \clubsuit How many examples you need to see to obtain a learned function with error $\leq \epsilon$ with high probability
- Shattering and the VC dimension

Recap: Error of a hypothesis

Definition

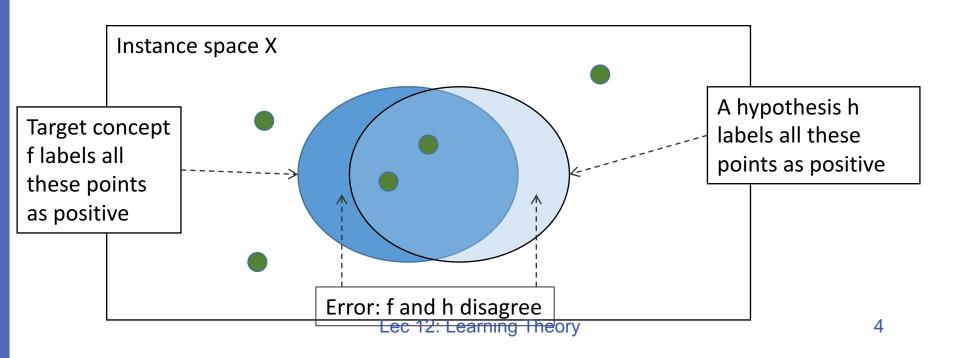
Given a distribution D over examples, the *error* of a hypothesis h with respect to a target concept f is

$$err_D(h) = Pr_{x \sim D}[h(x) \neq f(x)]$$



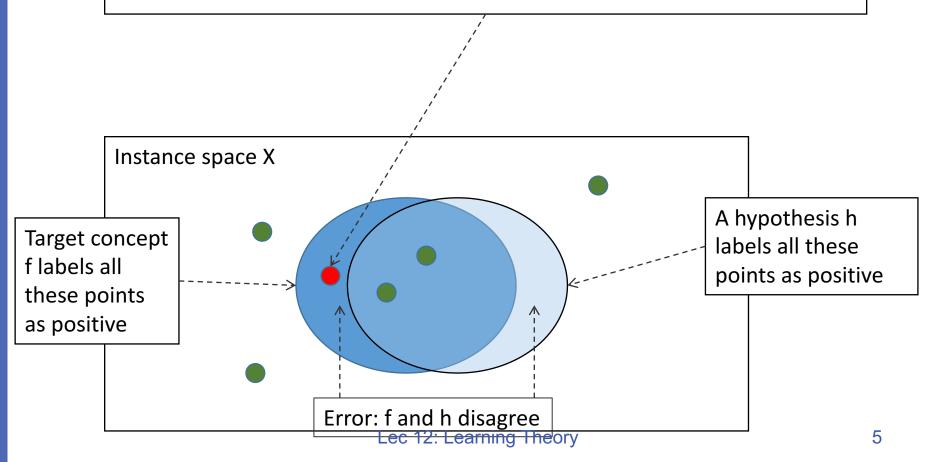
Recap: Error of a hypothesis

Overfitting: You may have a learned model that is consistent with the training data but still makes mistakes.



Recap: Error of a hypothesis

With the IID sampling assumption, we either have seen this example in the training phase, or it is unlikely to see it in the test time.



Requirements of Learning

- Cannot expect a learner to learn a concept exactly
 - Instead, we "agree" to misclassify uncommon examples that do not show up in the training set

PAC Learnability

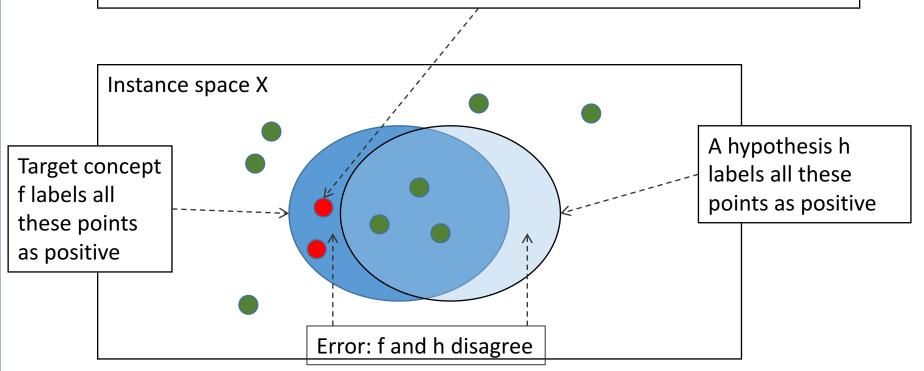
Turing Award: Leslie Valiant.

Consider a concept class C defined over an instance space X (containing instances of length n), and a learner L using a hypothesis space H

The concept class C is PAC learnable by L using H if for all $f \in \mathcal{C}$, for all distribution D over X, and fixed $\epsilon > 0$, $\delta < 1$, given m examples sampled i.i.d. according to D, the algorithm L produces, with probability at least (1- δ), a hypothesis h \in H that has error at most ϵ , where m is *polynomial* in 1/ ϵ , 1/ δ , n and size(H)

Intuition of PAC Learnability

With the IID sampling assumption, if a concept is reasonable. After, we saw enough samples, it is unlikely to have many these red points



Recap: Learning Conjunctions

Protocol 1:

Teacher provides a set of example (x, f(x))

What would f look like?

Whenever the output is 1, x_1 is present

With the given data, we only learned an *approximation* to the true concept. Is it good enough?

Recap: Learning Conjunctions: Analysis

Theorem: Suppose we are learning a conjunctive concept with n dimensional Boolean features using m training examples. If

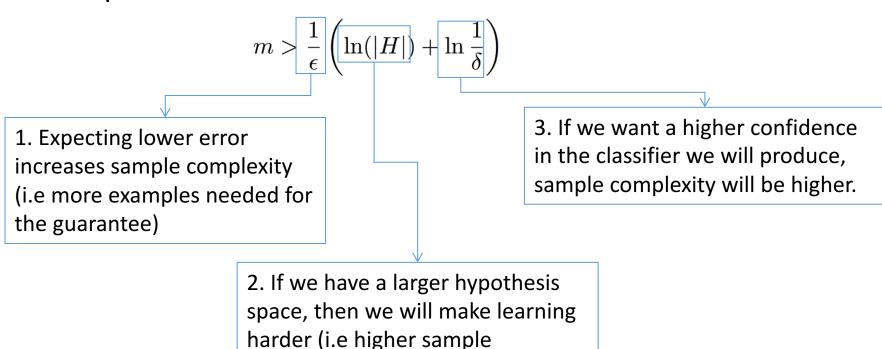
$$m > \frac{n}{\epsilon} \left(\log(n) + \log\left(\frac{1}{\delta}\right) \right)$$

then, with probability > 1 - δ , the error of the learned hypothesis err_D(h) will be less than ϵ .

A general result

Let H be any hypothesis space.

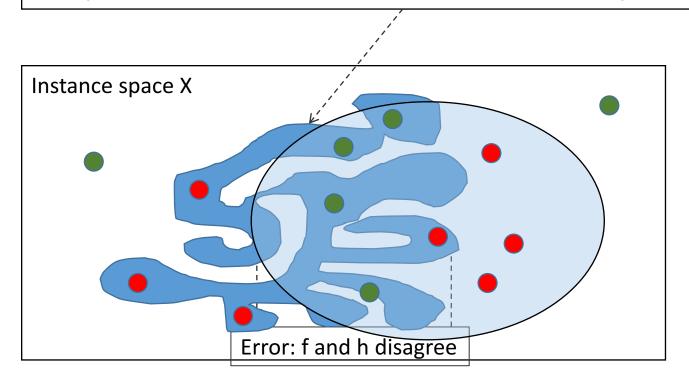
With probability 1 - δ a hypothesis h \rightarrow H that is consistent with a training set of size m will have an error $\leq \epsilon$ on future examples if



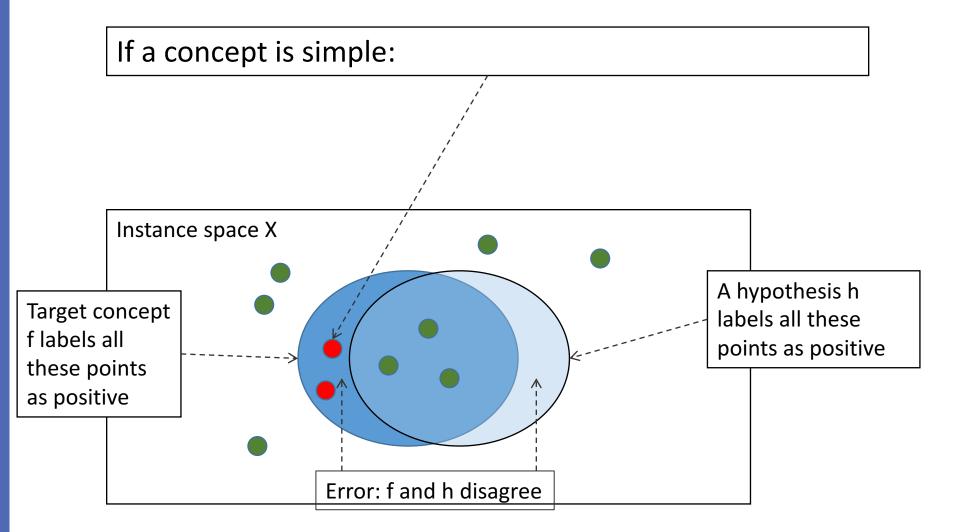
complexity)

Intuition of PAC Learnability

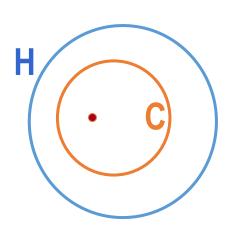
With the IID sampling assumption, if a concept is too complicated. We need to see exponential number of samples, such that we can rule out those red points



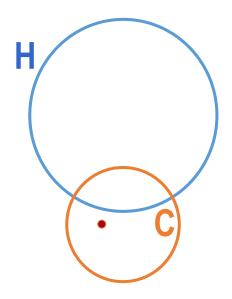
Intuition of PAC Learnability



What if the concept space is different from the hypothesis space? [not in exam]



It is fine, we can still find the right function



The training error will not be zero

Generalization bound [not in exam]

A bound on how much the true error will deviate from the training error. If we have more than m examples, then with high probability $1-\delta$

$$err_D(h) - err_S(h) \leq \sqrt{\frac{\ln|H| + \ln(1/\delta)}{2m}}$$
 Generalization error Training error

Generalization bound

A bound on how much the true error will deviate from the

Now, we know if size(H) is finite, we can define what is learnable. This works for Boolean functions.

Next question: What if size(H) is infinity?

This lecture: Computational Learning Theory

The Theory of Generalization

Probably Approximately Correct (PAC) learning

Shattering and the VC dimension

Infinite Hypothesis Space

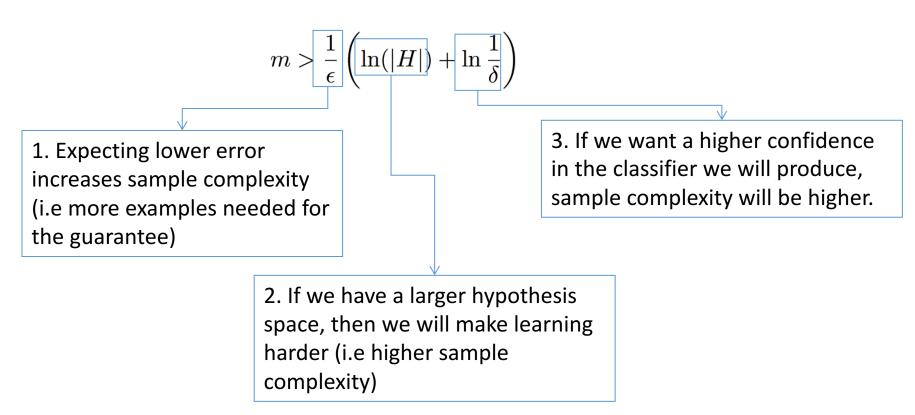
The previous analysis was restricted to finite hypothesis spaces

- Some infinite hypothesis spaces are more expressive than others
 - Linear threshold function vs. a combination of LTUs

Need a measure of the expressiveness of an infinite hypothesis space other than its size

A general result

If |H| is infinite, m is always infinite as well.



Vapnik-Chervonenkis dimension

- The Vapnik-Chervonenkis dimension (VC dimension) provides such a measure
 - * "What is the expressive capacity of a set of functions?"
- Analogous to |H|, there are bounds for sample complexity using VC(H)

VC dimension and consistent learners [not in exam]

- Using VC(H) as a measure of expressiveness we have a sample complexity bound for infinite hypothesis spaces
- ❖ Given a sample D with m examples, find some h → H is consistent with all m examples. If

$$m > \frac{1}{\epsilon} \left(8VC(H) \log \frac{13}{\epsilon} + 4 \log \frac{2}{\delta} \right)$$

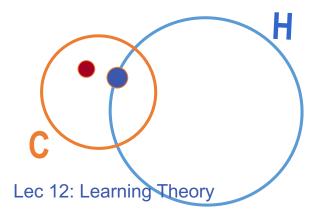
Then with probability at least $(1-\delta)$, h has error less than ε .

You don't need to remember this equation but just need to understand the meaning

Generation bound for agnostic learner [not in exam]

If we have m examples, then with probability $1 - \delta$, a the true error of a hypothesis h with training error err_s(h) is bounded by

$$err_D(h) \le err_S(h) + \sqrt{\frac{VC(H)\left(\ln\frac{2m}{VC(H)} + 1\right) + \ln\frac{4}{\delta}}{m}}$$



Intuition of VC dimension

Although there are infinitely many hypotheses, many of them are similar

- The idea of learning is by eliminating incorrect hypotheses
 - We can eliminate infinite # hypotheses for each training sample

Recap: Learning Conjunctions

Protocol 1:

Teacher provides a set of example (x, f(x))

♦ <(0,1,0,1,0,0,...0,1,1), 0>

$$x_1 \land x_2 \land x_3 \dots x_{99} \land x_{100}$$

 $x_1 \land x_2 \land x_3 \dots x_{99}$
 $x_1 \land x_3 \dots x_{99} \land x_{100}$
 $x_2 \land x_3 \dots x_{99} \land x_{100}$
 $x_2 \land x_3 \dots x_{99}$
 $x_3 \dots x_{99} \land x_{100}$

Recap: Learning Conjunctions

Protocol 1:

Teacher provides a set of example (x, f(x))

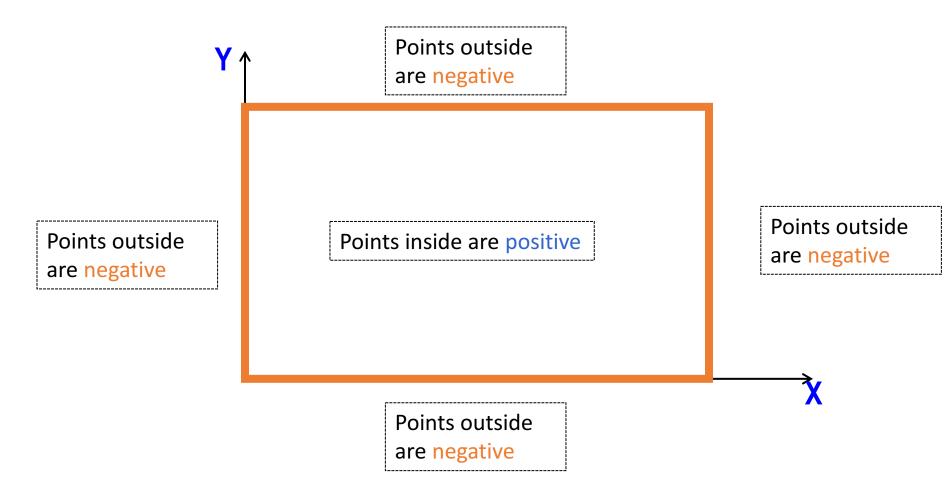
One instance can eliminate many hypothesis

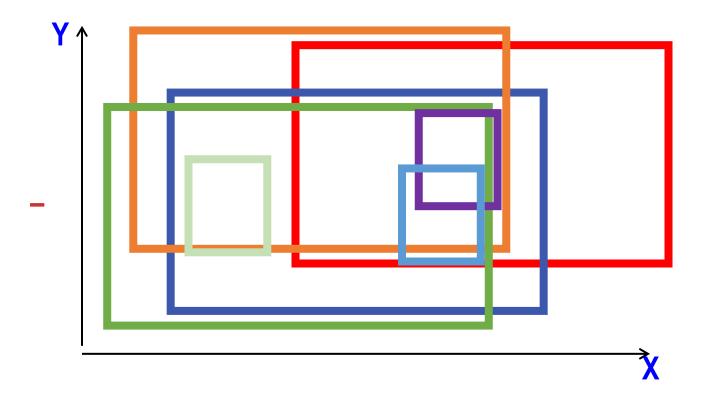
Intuition of VC dimention: Learning Rectangles



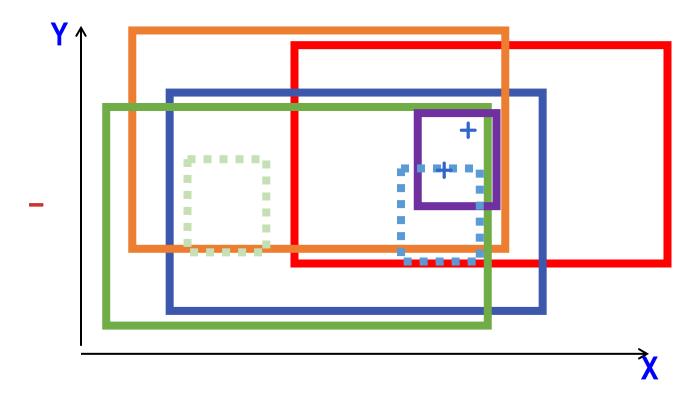
Assume the target concept is an axis parallel rectangle

Learning Rectangles

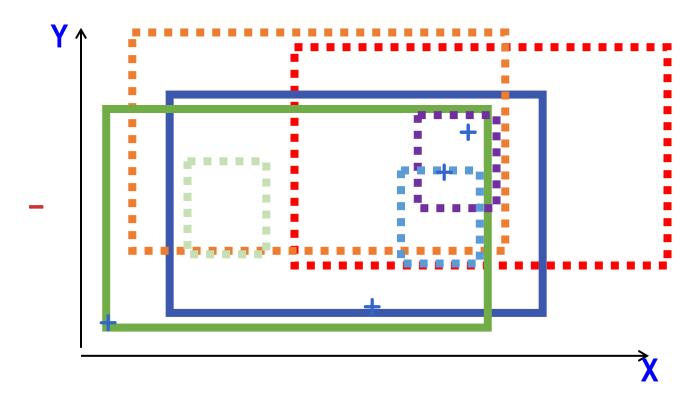


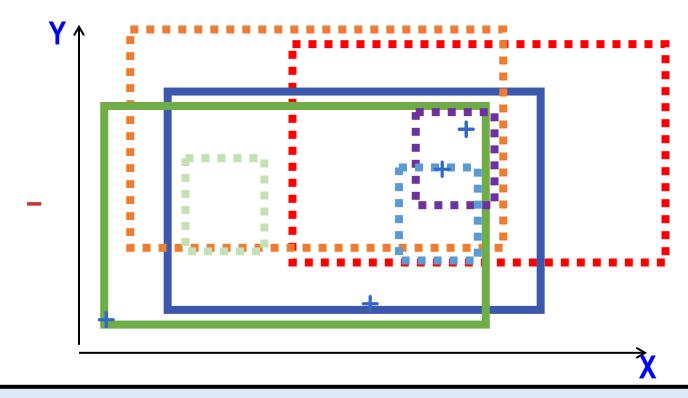












Key observation: Despite there are infinite # hypothesis The blue & red rectangles have the same predictions

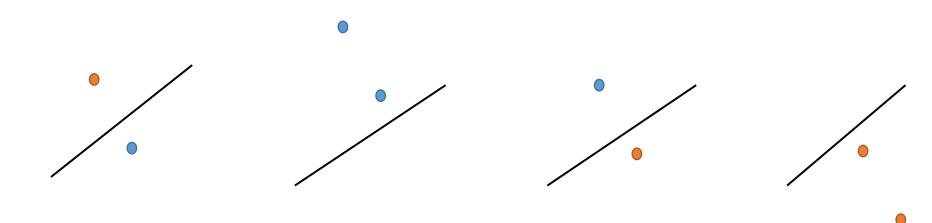
Let's think about expressivity of functions

 \bigcirc

Suppose we have two points.
Can linear classifiers correctly classify any labeling of these points?

Linear functions are expressive enough to *shatter* 2 points

Let's think about expressivity of functions

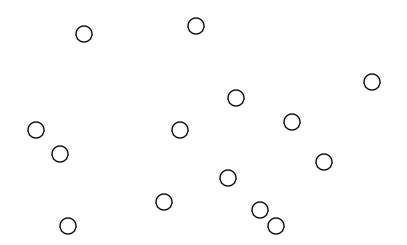


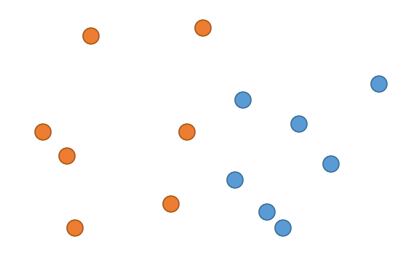
Suppose we have two points.

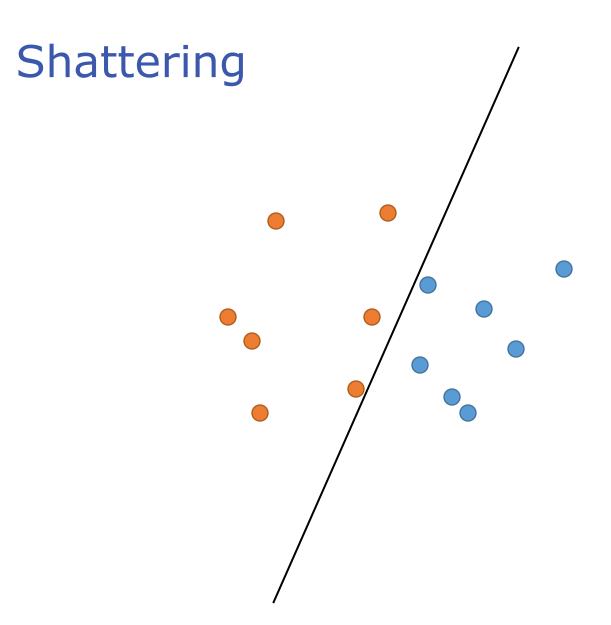
Can linear classifiers correctly classify any labeling of these points?

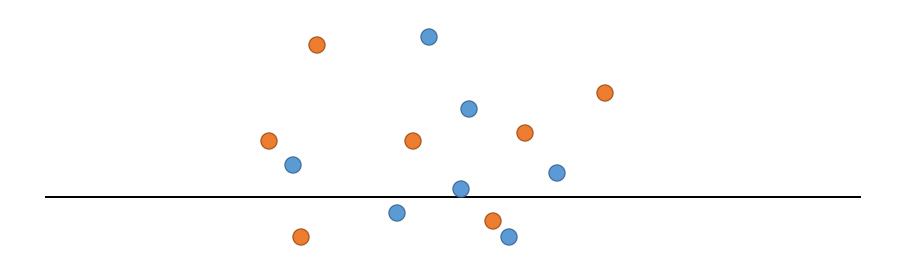
Linear functions are expressive enough to *shatter* 2 points

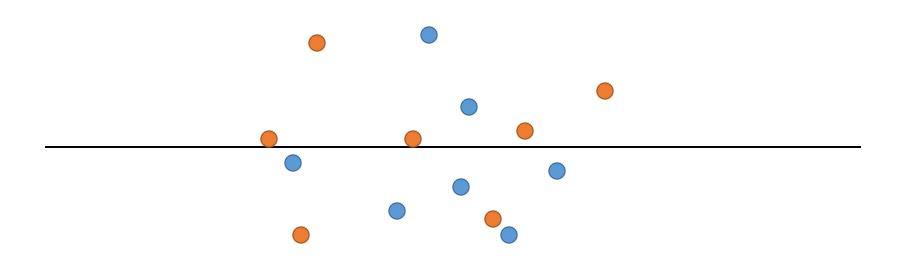
Shattering

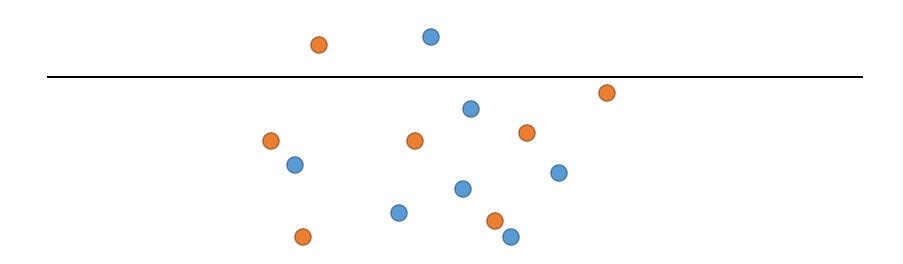


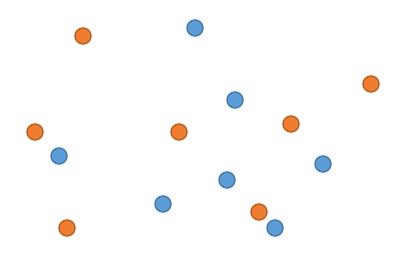


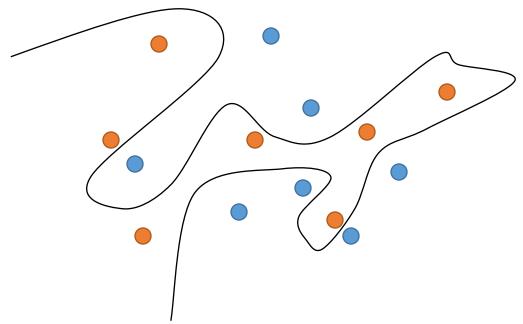












Linear functions are not expressive to shatter fourteen points Because there is a labeling that can not be separated by them

Of course, a more complex function could separate them

Definition: A set S of examples is shattered by a set of functions H if for every partition of the examples in S into positive and negative examples there is a function in H that gives exactly these labels to the examples

Intuition: A rich set of functions shatters large sets of points

Left bounded intervals

Example 1: Hypothesis class of left bounded intervals on the real axis: [0,a) for some real number a>0

Sets of two points cannot be shattered

That is: given two points, you can label them in such a way that no concept in this class will be consistent with their labeling

Real intervals

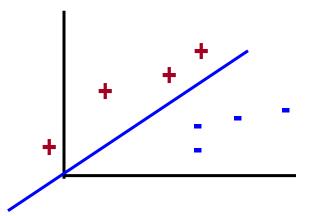
Example 2: Hypothesis class is the set of intervals on the real axis: [a,b],for some real numbers b>a



All sets of one or two points can be shattered But some sets of three points cannot be shattered

Definition: A set S of examples is shattered by a set of functions H if for every partition of the examples in S into positive and negative examples there is a function in H that gives exactly these labels to the examples

Example 3: 2-D Half spaces in a plane



Can one point be shattered?

Is there any two points can be shattered?

Is there any three points?
Can any three points be shattered?

Vapnik-Chervonenkis Dimension

Definition: The VC dimension of hypothesis space H over instance space X is the size of the largest *finite* subset of X that is shattered by H

- If there exists any subset of size d that can be shattered, VC(H) >= d
 - Even one subset will do
- ❖ If no subset of size d can be shattered, then VC(H) < d</p>

Shattering: The adversarial game

You



You: Hypothesis class H can shatter these d points I provide

You: Aha! There is a function h ∈ H that correctly predicts your evil labeling

An adversary

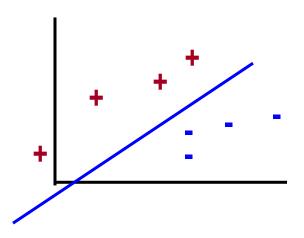


Adversary: That's what you think! Here is a labeling that will defeat you.

Adversary: Argh! You win this round. But I'll be back.....

Example Half spaces in a plane

- ❖ Prove VC >=1
 - Show any point can be shattered

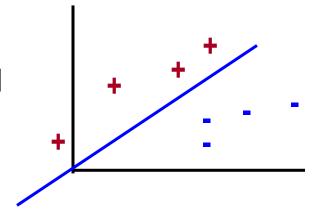


- ❖ Prove VC >=2
 - Show there exists 2 points can be shattered

- ❖ Prove VC >=3
 - Show there exists 3 points can be shattered

Example Half spaces in a plane

- Prove VC <4</p>
 - Show no 4 points can be shattered
- ❖ Therefore, VC = 3



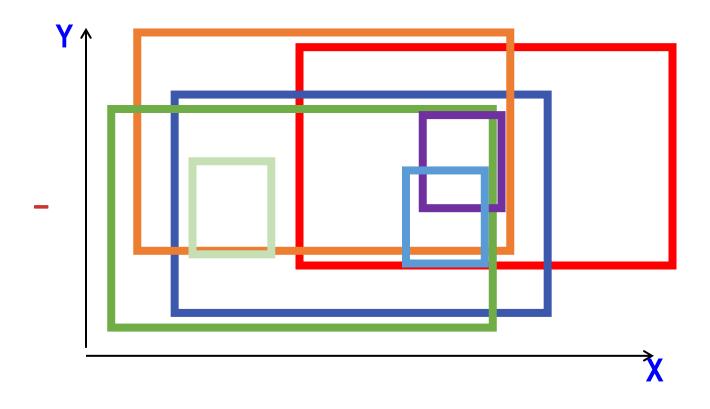
- Suppose three of them lie on the same line, label the outside points + and the inner one –
- Other wise, make a convex hull. Label points outside + and the inner one –
- Four points cannot be shattered!

VC dimension of Half spaces

- ❖ In general, the VC dimension of an n-dimensional linear function is n+1
- \bullet Give the same δ and m

This term will decrease
$$err_D(h) \leq err_S(h) + \sqrt{\frac{VC(H)\left(\ln\frac{2m}{VC(H)} + 1\right) + \ln\frac{4}{\delta}}{m}}$$

Exercise



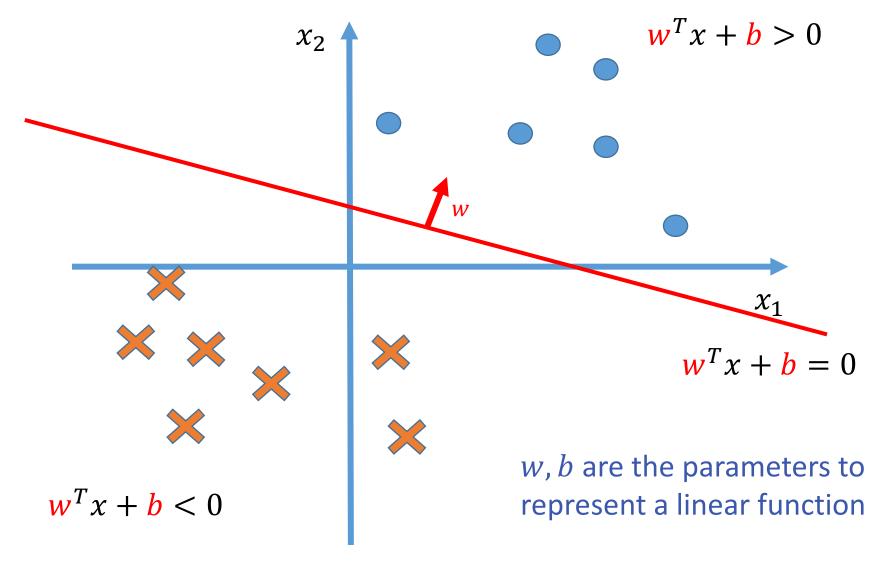
What is the VC dimension for the rectangle concept space?

Computational Learning Theory

- The Theory of Generalization
 - Using training instance to rule out incorrect hypotheses
- Probably Approximately Correct (PAC) learning
 - \clubsuit How many examples you need to see to obtain a learned function with error $\leq \epsilon$
- Shattering and the VC dimension

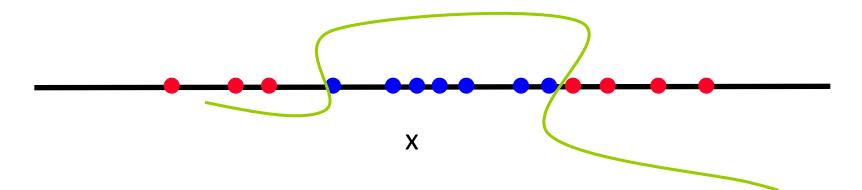
Kernel and Kernel methods

Hypothesis space: linear model



Functions Can be Made Linear

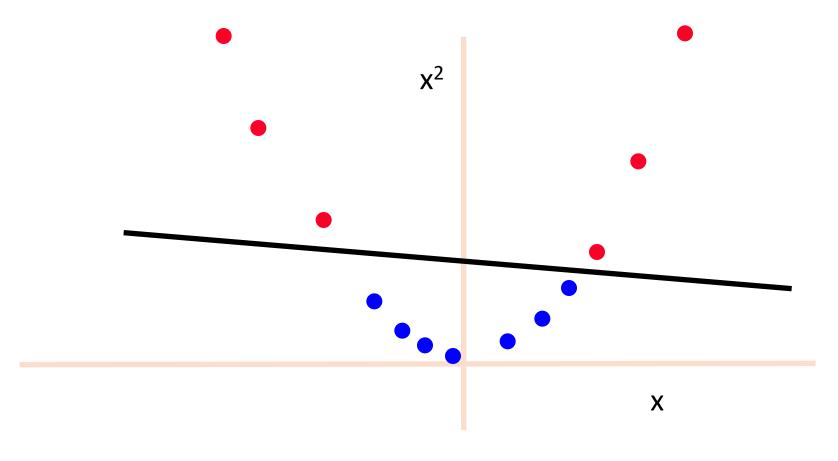
- Data are not linearly separable in one dimension
- Not separable if you insist on using a specific class of functions



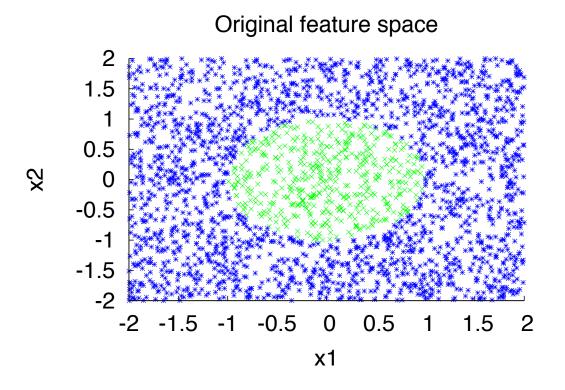
Can we do some mapping to make it linear spreadable?

Blown Up Feature Space

❖ Data are separable in <x, x²> space

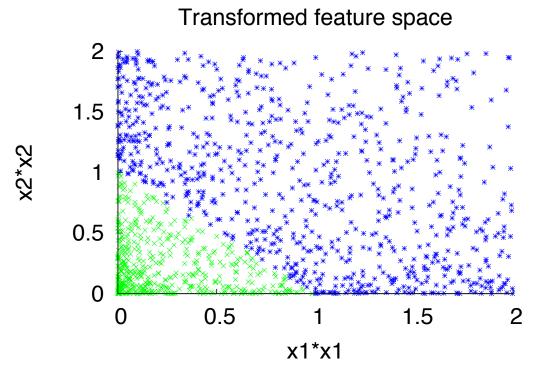


Making data linearly separable



$$f(x) = 1 \text{ iff } x_1^2 + x_2^2 \le 1$$

Making data linearly separable



Transform data:
$$\mathbf{x} = (x_1, x_2) => \mathbf{x'} = (x_1^2, x_2^2)$$

 $f(\mathbf{x'}) = 1$ iff $x'_1 + x'_2 \le 1$

The Perceptron Algorithm [Rosenblatt 1958]

Given a training set
$$\mathcal{D} = \{(x, y)\}$$

- 1. Initialize $w \leftarrow \mathbf{0} \in \mathbb{R}^n$
- 2. For (x,y) in \mathcal{D} :
- 3. if $y(\mathbf{w}^{\mathsf{T}}\mathbf{x}) \leq \mathbf{0}$
- 4. $w \leftarrow w + yx$
- 5.
- 6. Return w

Prediction: $y^{\text{test}} \leftarrow \text{sg}n(\mathbf{w}^{\mathsf{T}}\mathbf{x}^{\text{test}})$

Assume $y \in \{1, -1\}$

The Perceptron Algorithm [Rosenblatt 1958]

Given a training set
$$\mathcal{D} = \{(x, y)\}$$

- 1. Initialize $w \leftarrow 0 \in \mathbb{R}^{2n}$
- 2. For (x,y) in \mathcal{D} :

$$\text{if } y \ \mathbf{w}^T \begin{bmatrix} \mathbf{x} \\ \mathbf{x}^2 \end{bmatrix} \leq \mathbf{0}$$

$$\begin{array}{c} 4. \\ 5. \end{array} \qquad w \leftarrow w + y \begin{bmatrix} x \\ x^2 \end{bmatrix}$$

6.

Assume $y \in \{1, -1\}$

What if our mapping function is more complex?

Prediction:
$$y^{\text{test}} \leftarrow \text{sgn}(\mathbf{w}^{\top} \begin{bmatrix} \mathbf{x} \\ \mathbf{x}^2 \end{bmatrix})$$

The Perceptron Algorithm [Rosenblatt 1958]

Given a training set
$$\mathcal{D} = \{(x, y)\}$$

- 1. Initialize $\mathbf{w} \leftarrow \mathbf{0} \in \mathbb{R}^n$
- 2. For (x,y) in \mathcal{D} :
- 3. if $y(\mathbf{w}^{\mathsf{T}}\mathbf{x}) \leq \mathbf{0}$
- 4. $w \leftarrow w + yx$
- 5.
- 6. Return w

Observation: w is a combination of the input instances!!

Prediction:
$$y^{\text{test}} \leftarrow \text{sg}n(\mathbf{w}^{\mathsf{T}}\mathbf{x}^{\text{test}})$$

Assume $y \in \{1, -1\}$

Dual Representation

if
$$y(\mathbf{w}^{\mathsf{T}}\mathbf{x}) \leq \mathbf{0}$$

 $\mathbf{w} \leftarrow \mathbf{w} + y\mathbf{x}$

- Let w be an initial weight vector for perceptron. Let $(x_1,+)$, $(x_2,+)$, $(x_3,-)$, $(x_4,-)$ be examples and assume mistakes are made on x_1 , x_2 and x_4 .
- What is the resulting weight vector?

$$W = W + x_1 + x_2 - x_4$$

In general, the weight vector w can be written as a linear combination of examples:

$$w = \sum_{1...m} \alpha_i y_i x_i$$

 \diamond Where α_i is the number of mistakes made on x_i .

Predicting with linear classifiers

- Prediction = $sgn(\mathbf{w}^T\mathbf{x})$ and $\mathbf{w} = \sum_{i=1}^m \alpha_i y_i \mathbf{x}_i$
- That is, we just showed that

$$\mathbf{w}^T \mathbf{x} = \sum_i \alpha_i y_i \mathbf{x}_i^T \mathbf{x}$$

- We only need to compute dot products between training examples and the new example x
- This is true even if we map examples to a high dimensional space

$$\mathbf{w}^T \phi(\mathbf{x}) = \sum \alpha_i y_i \phi(\mathbf{x}_i)^T \phi(\mathbf{x})$$

Many learning algorithm require to compute inner products

Perceptron:

$$y(\mathbf{w}^{\mathsf{T}}\mathbf{x}) \leq \mathbf{0}$$

K-NN:

$$similarity(x, x^{neighbor}) = x^T x^{neighbor}$$

 $dist(x, x^{neighbor}) = ||x - x^{neighbor}||^2$

$$dist(x, x^{neighbor}) = ||x||^2 + ||x^{neighbor}||^2 - 2x^T x^{neighbor}$$

Is there a smarter way to compute the inner product?

Dot products in high dimensional spaces

Let us define a dot product in the high dimensional space

$$K(\mathbf{x}, \mathbf{z}) = \phi(\mathbf{x})^T \phi(\mathbf{z})$$

Dot products in high dimensional spaces

Let us define a dot product in the high dimensional space

$$K(\mathbf{x}, \mathbf{z}) = \phi(\mathbf{x})^T \phi(\mathbf{z})$$

So prediction with this high dimensional lifting map is

$$sgn(\mathbf{w}^T \phi(\mathbf{x})) = sgn\left(\sum_i \alpha_i y_i K(\mathbf{x}_i, \mathbf{x})\right)$$

because
$$\mathbf{w}^T \phi(\mathbf{x}) = \sum_i \alpha_i y_i \phi(\mathbf{x}_i)^T \phi(\mathbf{x})$$

Lec 12: Learning Theory

Dot products in high dimensional spaces

Let us define a dot product in the high dimensional space

$$K(\mathbf{x}, \mathbf{z}) = \phi(\mathbf{x})^T \phi(\mathbf{z})$$

So prediction with this high dimensional lifting map is

because
$$\mathbf{w}^T \phi(\mathbf{x}) = \sum_i \alpha_i y_i \phi(\mathbf{x}_i)^T \phi(\mathbf{x})$$

Lec 12: Learning Theory

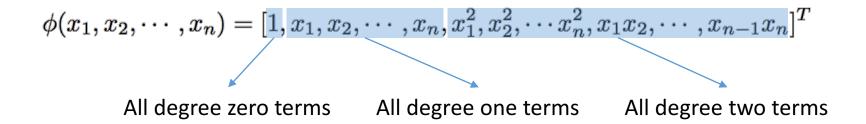
$$\phi(x_1, x_2, \dots, x_n) = [1, x_1, x_2, \dots, x_n, x_1^2, x_2^2, \dots, x_n^2, x_1x_2, \dots, x_{n-1}x_n]^T$$

Given two examples x and z we want to map them to a high dimensional space

$$\phi(x_1, x_2, \dots, x_n) = [1, x_1, x_2, \dots, x_n, x_1^2, x_2^2, \dots, x_n^2, x_1x_2, \dots, x_{n-1}x_n]^T$$

All degree zero terms

$$\phi(x_1,x_2,\cdots,x_n)=[1,x_1,x_2,\cdots,x_n,x_1^2,x_2^2,\cdots x_n^2,x_1x_2,\cdots,x_{n-1}x_n]^T$$
 All degree zero terms All degree one terms



$$\phi(x_1,x_2,\cdots,x_n)=[1,x_1,x_2,\cdots,x_n,x_1^2,x_2^2,\cdots x_n^2,x_1x_2,\cdots,x_{n-1}x_n]^T$$
 All degree zero terms All degree one terms All degree two terms

and compute the dot product
$$A = \phi(\mathbf{x})^T \phi(\mathbf{z})$$
 [takes time]

Given two examples x and z we want to map them to a high dimensional space

$$\phi(x_1, x_2, \dots, x_n) = [1, x_1, x_2, \dots, x_n, x_1^2, x_2^2, \dots x_n^2, x_1 x_2, \dots, x_{n-1} x_n]^T$$
 and compute the dot product $A = \phi(\mathbf{x})^T \phi(\mathbf{z})$ [takes time]

Instead, in the original space, compute

$$B = K(\mathbf{x}, \mathbf{z}) = (1 + \mathbf{x}^T \mathbf{z})^2$$

Theorem: A = B (Coefficients do not really matter)

Given two examples x and z we want to map them to a high dimensional space [for example, quadratic]

$$\phi(x_1, x_2, \cdots, x_n) = [1, x_1, x_2, \cdots, x_n, x_1^2, x_2^2, \cdots x_n^2, x_1 x_2, \cdots, x_{n-1} x_n]^T$$
 and compute the dot product $A = \phi(\mathbf{x})^T \phi(\mathbf{z})$ [takes time]

Instead, in the original space, compute

$$B = K(\mathbf{x}, \mathbf{z}) = (1 + \mathbf{x}^T \mathbf{z})^2$$

Given two examples x and z we want to map them to a high dimensional space [for example, quadratic]

$$\phi(x_1, x_2, \cdots, x_n) = [1, x_1, x_2, \cdots, x_n, x_1^2, x_2^2, \cdots x_n^2, x_1 x_2, \cdots, x_{n-1} x_n]^T$$
 and compute the dot product $A = \phi(\mathbf{x})^T \phi(\mathbf{z})$ [takes time]

Instead, in the original space, compute

$$B = K(\mathbf{x}, \mathbf{z}) = (1 + \mathbf{x}^T \mathbf{z})^2$$

Claim: Compute B instead of A (Coefficients do not really matter)

The Kernel Trick

Suppose we wish to compute

$$K(\mathbf{x}, \mathbf{z}) = \phi(\mathbf{x})^{\mathsf{T}} \phi(\mathbf{z})$$

Here ϕ maps **x** and **z** to a high dimensional space

The Kernel Trick: Save time/space by computing the value of K(x, z) by performing operations in the original space (without a feature transformation!)