

CSE 417T

Introduction to Machine Learning

Lecture 17

Instructor: Chien-Ju (CJ) Ho

Logistics

- Homework 4 is due April 19 (Monday)
 - Please start it early
 - The deadline is intentionally delayed to accommodate wellness day
 - Keep track of your own late days
 - Gradescope doesn't allow separate deadlines
 - Your submissions won't be graded if you exceed the late-day limit
- Homework 5 will overlap with Homework 4
 - Plan to announce it in the week of Apr 13

Recap

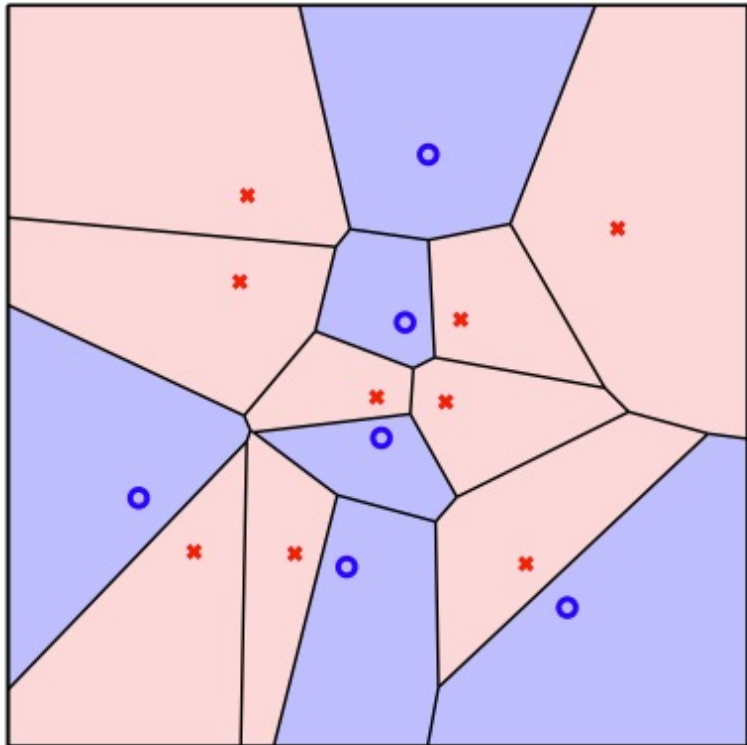
Nearest Neighbor

- Predict \vec{x} according to its nearest neighbor
 - Given $D = \{(\vec{x}_1, y_1), (\vec{x}_2, y_2), \dots, (\vec{x}_N, y_N)\}$
 - Let $\vec{x}_{[1]}$ be \vec{x} 's nearest neighbor, i.e., the closest point to \vec{x} in D
 - Let $y_{[i]}(\vec{x})$ or $y_{[i]}$ be the label of $\vec{x}_{[i]}$
- Nearest neighbor hypothesis

$$g(\vec{x}) = y_{[1]}(\vec{x})$$

Nearest Neighbor

$g(\vec{x})$ looks like a Voronoi diagram



- Properties of Nearest Neighbor (NN)
 - No training is needed
 - Good interpretability
 - In-sample error $E_{in} = 0$
 - VC dimension is ∞
- This seems to imply bad learning models from what we talk about so far? Why we care?
- What we really care about is E_{out}
 - VC analysis: $E_{out} \leq E_{in} + \text{Generalization error}$
 - We can infer E_{out} through E_{in} and model complexity
 - NN has nice guarantees outside of VC analysis

Nearest Neighbor is 2-Optimal

- Given mild conditions, for nearest neighbor, when $N \rightarrow \infty$, with high probability,

$$E_{out} \leq 2E_{out}^*$$

- That is, we can not infer E_{out} from E_{in} , but we know it cannot be much worse than the **best anyone can do**.

Informal intuitions:

Assumption for nearest neighbor:

- Target function is continuous
- That is, nearby points have similar label distributions

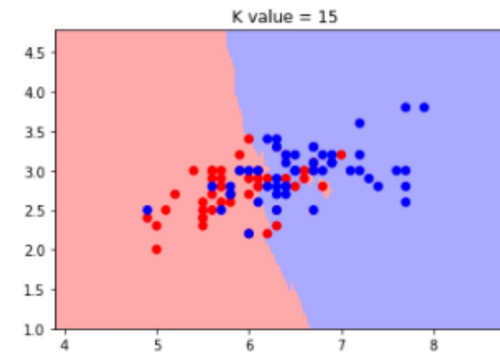
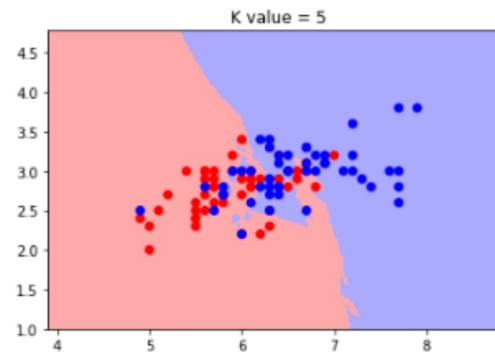
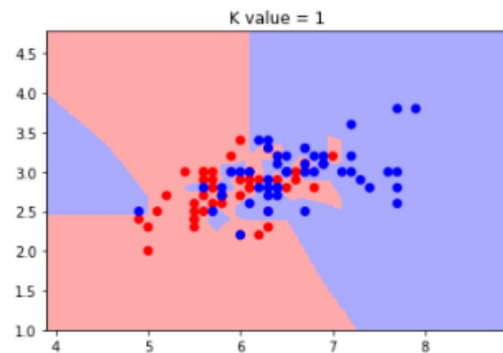
As N goes large, there are “close enough” points for prediction

Today's Lecture

The notes are not intended to be comprehensive. They should be accompanied by lectures and/or textbook.
Let me know if you spot errors.

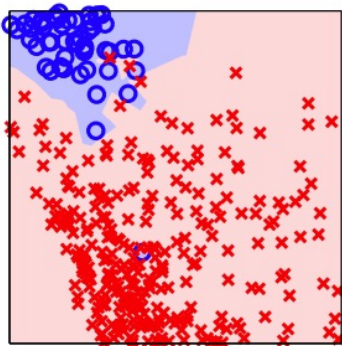
k -Nearest Neighbor (K-NN)

- Nearest neighbor
 - Influenced heavily by noisy data
- k -nearest neighbor (K-NN)
 - $g(\vec{x}) = \text{sign}\left(\sum_{i=1}^k y_{[i]}(\vec{x})\right)$
 - (k is often odd for binary classification)

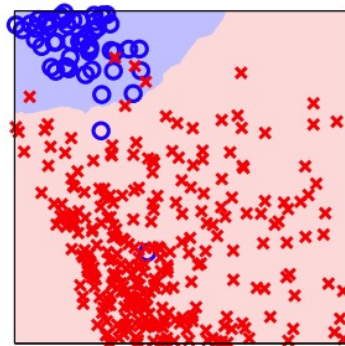


Impacts of k in k -Nearest Neighbor

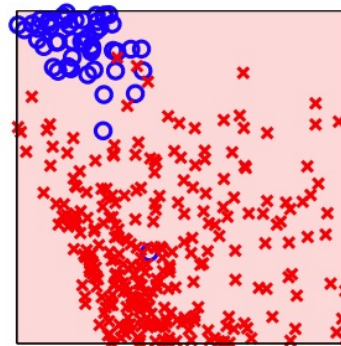
- $k = 1$: the nearest neighbor hypothesis
 - many, complicated decision boundaries; may overfit
- $k = N$, g predicts the most common label in the training dataset
 - no decision boundaries; may underfit
- k controls the complexity of the hypothesis set
 - k affects how well the learned hypothesis will generalize



1-NN rule



21-NN rule



127-NN rule

How to Choose k

- Making the choice of k a function of N , denoted by $k(N)$
- Theorem:
 - For $N \rightarrow \infty$, if $k(N) \rightarrow \infty$ and $\frac{k(N)}{N} \rightarrow 0$
 - Then $E_{in}(g) \rightarrow E_{out}(g)$ and $E_{out}(g) \rightarrow E_{out}(g^*)$
- Example: $k(N) = \sqrt{N}$ satisfies the condition

Informal intuitions:

$k(N) \rightarrow \infty$: select infinitely many neighbors

$\frac{k(N)}{N} \rightarrow 0$: all the nearest neighbors are next to \vec{x}

=> We can almost reconstruct the target function

How to Choose k

- Making the choice of k a function of N , denoted by $k(N)$
- Theorem:
 - For $N \rightarrow \infty$, if $k(N) \rightarrow \infty$ and $\frac{k(N)}{N} \rightarrow 0$
 - Then $E_{in}(g) \rightarrow E_{out}(g)$ and $E_{out}(g) \rightarrow E_{out}(g^*)$
- Example: $k(N) = \sqrt{N}$ satisfies the condition
- Other practical rules of thumb:
 - $k = 3$ is often a good enough choice
 - Using validation to choose k

Summary of k -NN So Far

- Pros
 - Simple algorithm
 - Good interpretations
 - Nice theoretical guarantee
 - Easy to adapt to regression (average of nearest neighbors) and multi-class classification (majority voting)
- Cons
 - Curse of dimensionality
 - Computational issue
 - each prediction requires $O(N)$ computation

Curse of Dimensionality

- Generally, higher dimensions implies harder learning (think VC)
- Things are worse with similarity-based methods
 - Rely on assumptions that nearby points have similar labels
 - As the dimension grows, most of the points will not be nearby to each other...

Illustration of Curse of Dimensionality

- Think about Euclidean distance: $d(\vec{x}, \vec{x}') = \|\vec{x} - \vec{x}'\|$
- Illustration
 - Consider the space $[0,1]^d$ (a hypercube with length of each side = 1)
 - What's the side length ℓ of a hypercube that takes up 1% of the space?
 - $d = 1$: $\ell = 0.01$
 - $d = 2$: $\ell = 0.1$
 - ...
 - $d = 100$: $\ell^d = 0.01 \Rightarrow \ell \approx 0.95$

Illustration of Curse of Dimensionality

- Consider the distance to the origin when $d = 100$
 - Consider the case that the value of each dimension is uniformly drawn
 - Only 1% of the points will be in the hypercube $[0,0.95]^{100}$
 - Most of the points will be far away from the origin
 - Most of the points will be far away from each other
- No simple solutions....
 - Getting more data
 - Reduce dimensions (see LFD 9.2)

Computational Issues

- k -Nearest Neighbor is computationally demanding
 - Need to store all data points: space complexity $O(Nd)$
 - For each prediction for \vec{x}
 - Calculate the distance to every point in D
 - Find the k closest points
 - Time complexity $O(Nd + N \log k)$
- There are still ongoing works to address this issue
- Two general approaches:
 - Reduce the number of data points
 - Store the data in some data structure to speed up searching
 - See LFD 6.2.3 for more discussion

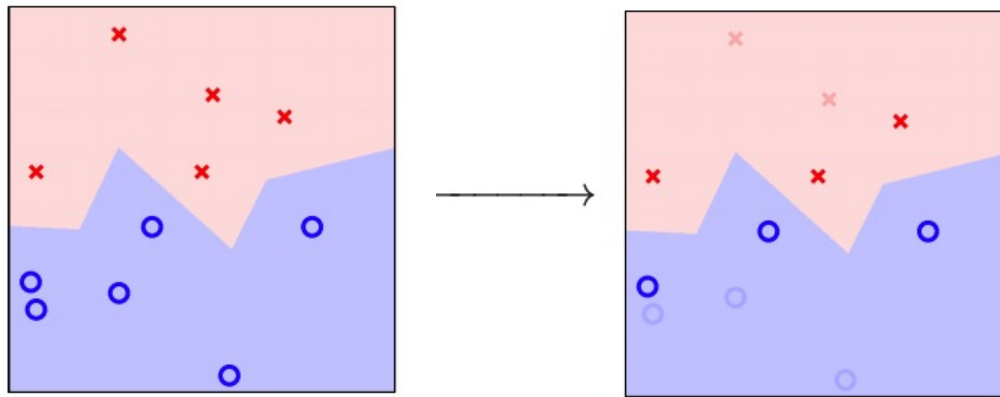
Computational Issues for k-NN

Two directions of approaches

- Reduce the number of data points
- Store the data in some data structure to speed up searching

Reduce the Amount of Data

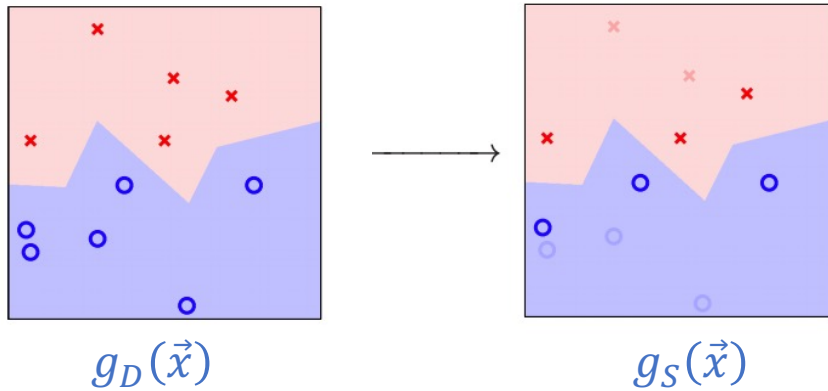
- Consider the following example



- Goal: Can we drop data that doesn't impact the decision boundary?
 - Find $S \in D$, such that $g_S(\vec{x}) = g_D(\vec{x}) \forall \vec{x}$
 - Generally a hard goal to achieve

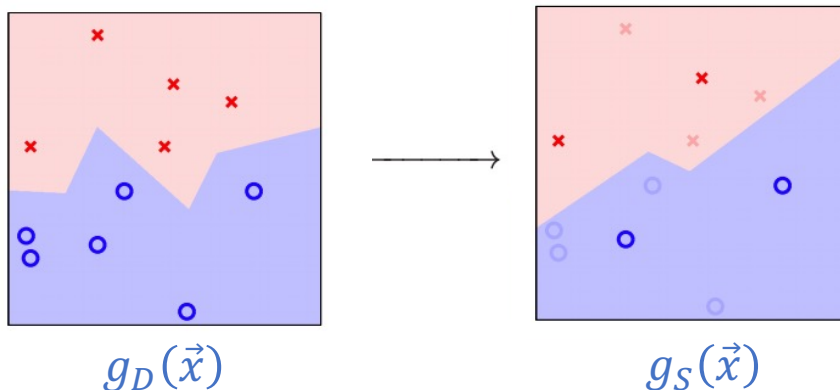
A Probably Easier Goal

- Instead of making the **decision boundary** consistent



Find $S \in D$, such that $g_S(\vec{x}) = g_D(\vec{x}) \forall \vec{x}$

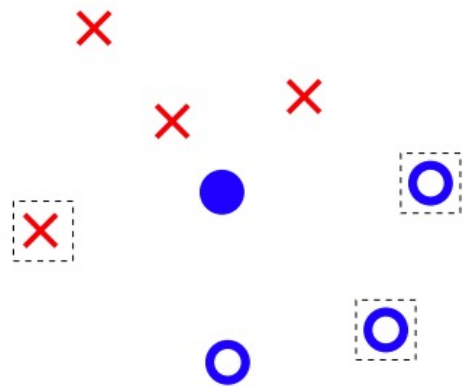
- Aim for making the prediction on the **training data** consistent



Find $S \in D$, such that $g_S(\vec{x}) = g_D(\vec{x}) \forall \vec{x} \in D$

Condensed Nearest Neighbor (CNN)

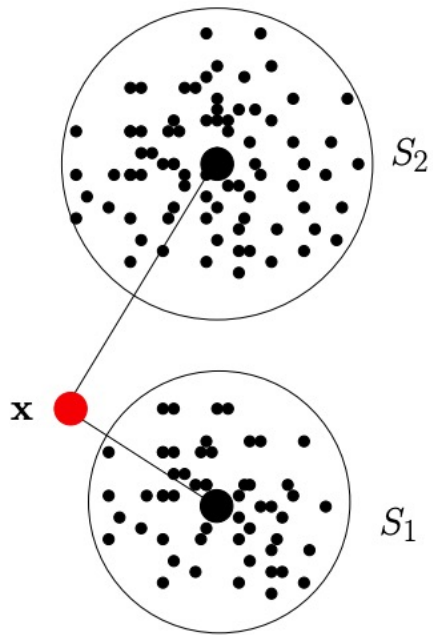
- Goal: Find $S \in D$, such that $g_S(\vec{x}) = g_D(\vec{x}) \forall \vec{x} \in D$



- CNN: An iterative algorithm
 - Random initialize a subset of data points S
 - While (there exists point $\vec{x}_* \in D$ such that $g_S(\vec{x}_*) \neq g_D(\vec{x}_*)$)
 - Let y_* be $g_D(\vec{x}_*)$
 - Find the nearest point $\vec{x}' \in D \setminus S$ with the label y_*
 - Insert \vec{x}' to S
- No theoretical guarantees
- Reasonable empirical performance

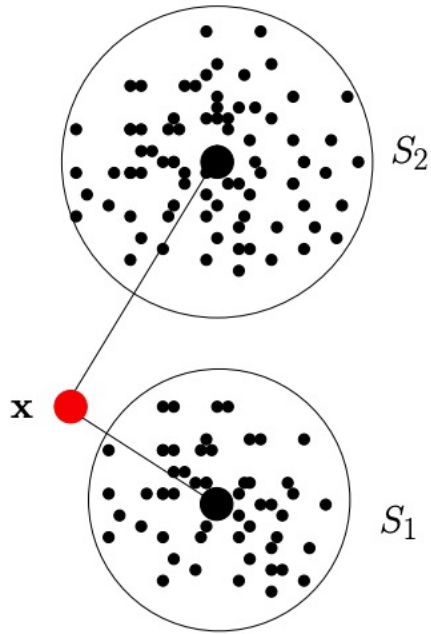
Speed Up the Search for Nearest Neighbor

- For each prediction for \vec{x} , we need to find the nearest point in D
- Can we speed up this process?



- S_1 and S_2 are two clusters
 - Centers $\vec{\mu}_1, \vec{\mu}_2$ and radii r_1, r_2
- Let S_1 be the nearest cluster for \vec{x}
- Let $\vec{x}'_{[1]}$ be the nearest point in S_1
- Distance from \vec{x} to any point in S_2 is at least $\|\vec{x} - \vec{\mu}_2\| - r_2$
- If $\|\vec{x} - \vec{x}'_{[1]}\| \leq \|\vec{x} - \vec{\mu}_2\| - r_2$
 - we don't need to search points in S_2

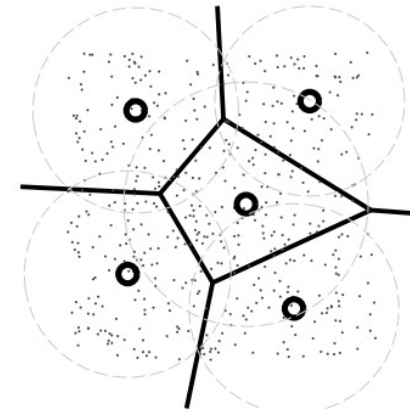
Speed Up the Search for Nearest Neighbor



- Condition to ignore S_2 : $\|\vec{x} - \vec{x}'_{[1]}\| \leq \|\vec{x} - \vec{\mu}_2\| - r_2$
- We also know that: $\|\vec{x} - \vec{x}'_{[1]}\| \leq \|\vec{x} - \vec{\mu}_1\| + r_1$
- If we have clusters that
 - $\|\vec{x} - \vec{\mu}_1\| + r_1 \leq \|\vec{x} - \vec{\mu}_2\| - r_2$
 - i.e., $r_1 + r_2 \leq \|\vec{x} - \vec{\mu}_2\| - \|\vec{x} - \vec{\mu}_1\| \approx \|\vec{\mu}_1 - \vec{\mu}_2\|$
 - (the approximation assumes \vec{x} is close to $\vec{\mu}_1$)
- Then the condition to ignore S_2 can hold
- Goal: Cluster data such that $r_1 + r_2 \leq \|\vec{\mu}_1 - \vec{\mu}_2\|$
 - Different clusters to be far away
 - Points in the same are dense

Lloyd's Algorithm: Construct Clusters

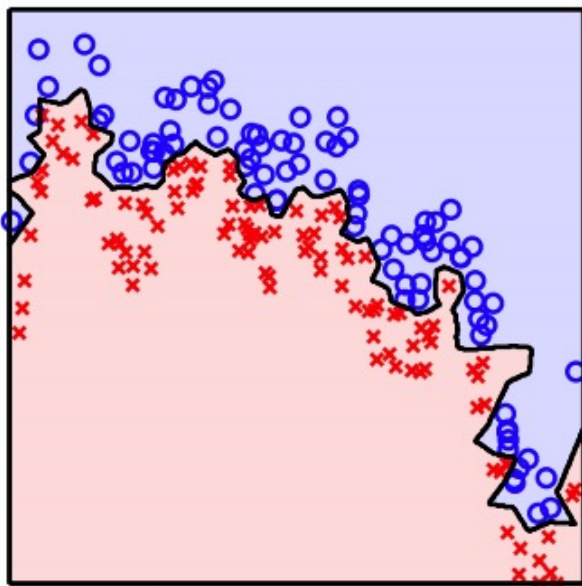
- Goal: Cluster data into K clusters
 - Again, hard in general, but we can use greedy-based approaches
- Lloyd's Algorithm
 1. Randomly pick K points as centers
 2. Create the Voronoi regions as clusters
 3. Update the centers (calculating the mean)
 4. Update the region
 5. Repeat 3 and 4
- This is the first (and probably the only) unsupervised learning algorithm we talked about in this course.



Final Remark:

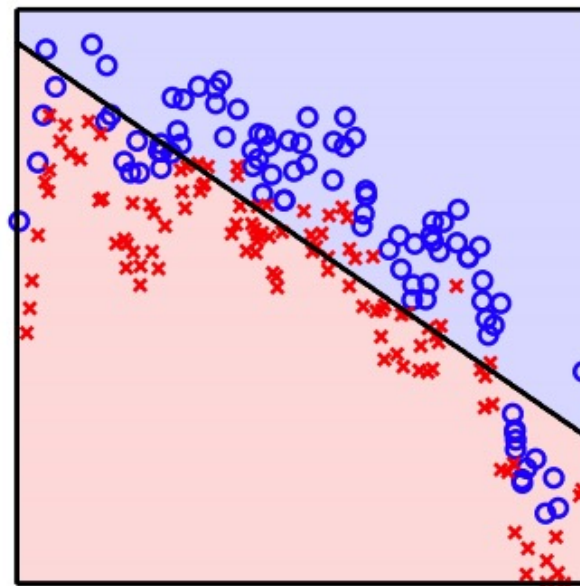
Nearest Neighbor is Nonparametric

Nearest Neighbor



no parameters
expressive/flexible
 $g(\mathbf{x})$ needs data
generic, can model anything

Linear models

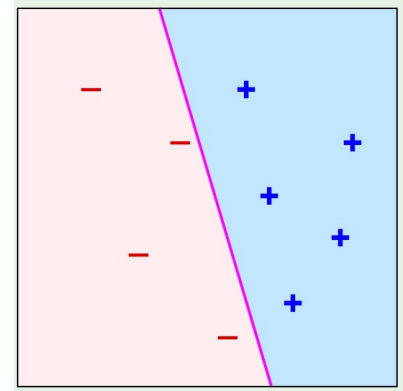


$(d + 1)$ parameters
rigid, always linear
 $g(\mathbf{x})$ needs only weights
specialized

Support Vector Machines (SVM)

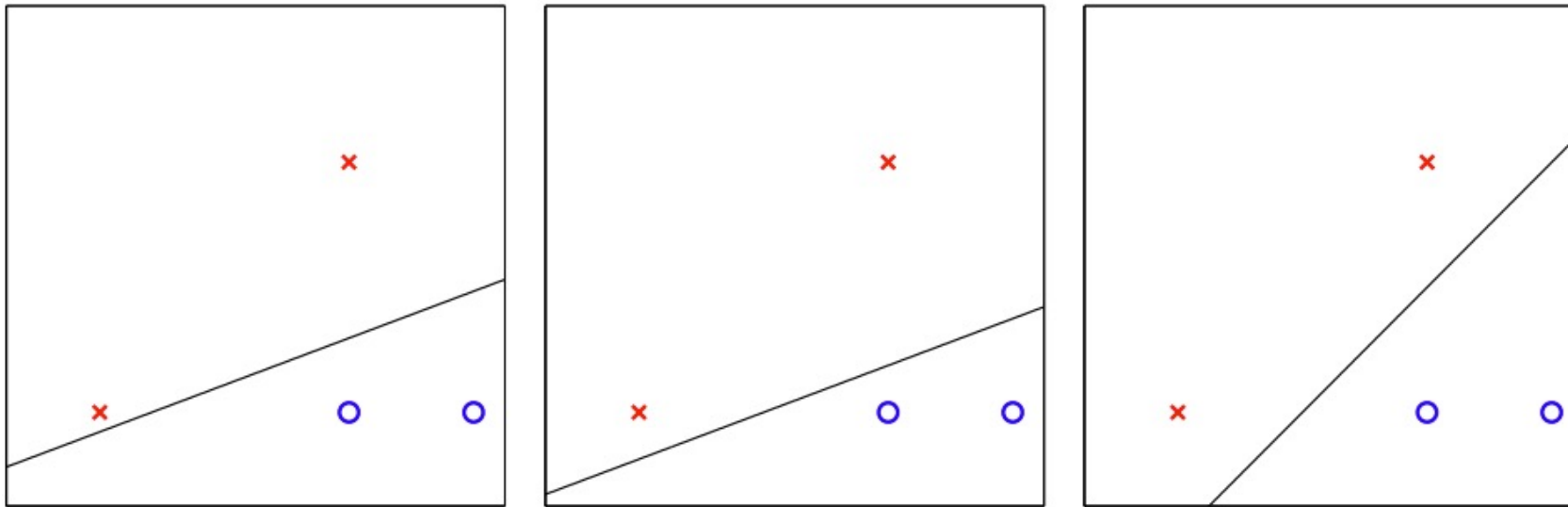
What Do We Know about Linear Classification?

- What we discussed so far:
 - PLA: Find a linear separator that separates the data within finite steps, if data is linear separable.
 - Pocket algorithm: empirically keep the best separator during PLA.
 - Surrogate loss: Using logistic regression for linear classification.
- Challenges
 - Binary classification error is hard to optimize
 - We cannot use “gradient descent” type of algorithm minimize E_{in} .
- Support vector machines (SVM) tries to look at things a bit differently.



Linear Classification

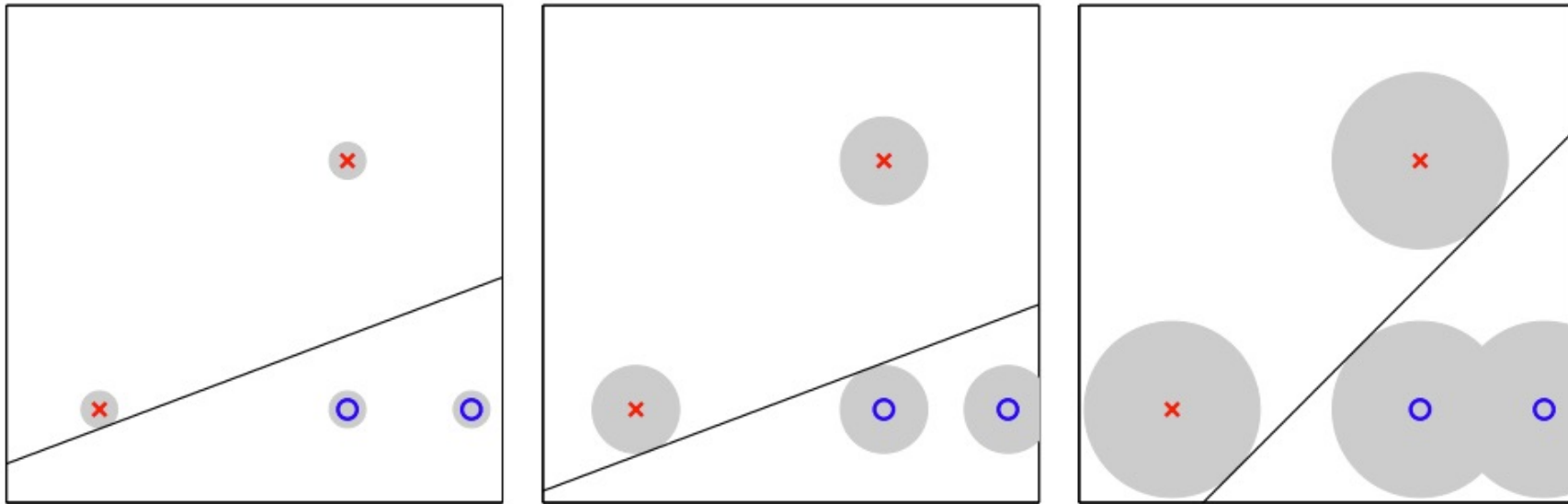
- Which separator would you choose?



Probably the right one.
Why?

Linear Classification

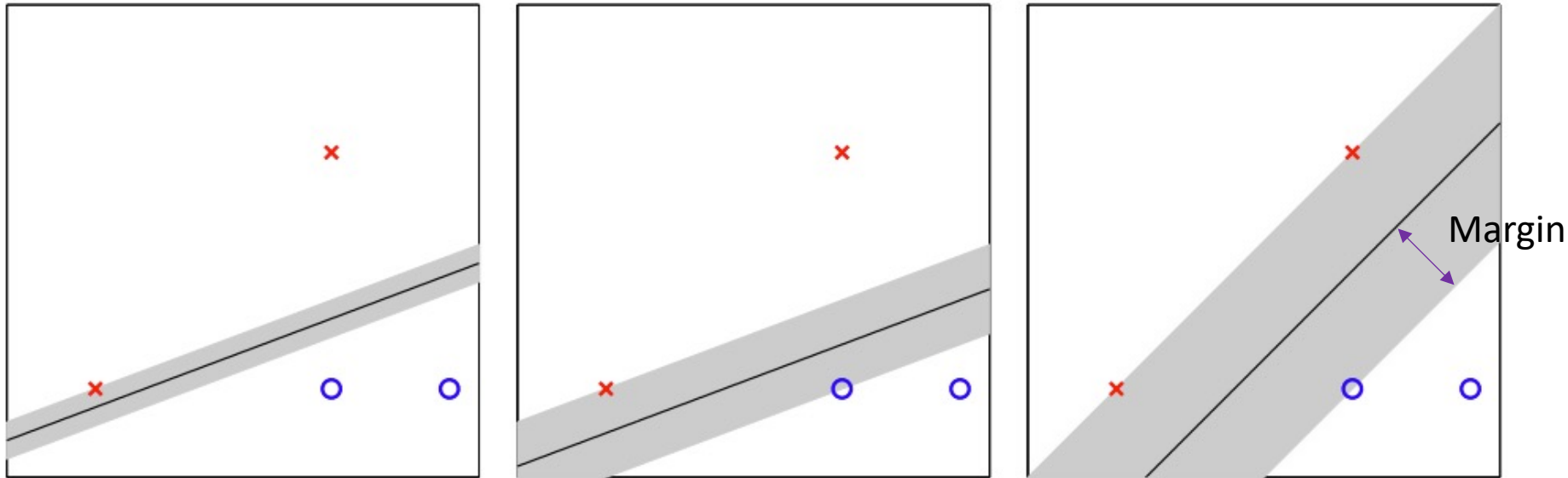
- Which separator would you choose?



More robust to noise (e.g., measurement error of \vec{x})

Linear Classification

- Which separator would you choose?



Margin: shortest distance from the separator to the points in D
(Informal argument)

Higher margin \Rightarrow more “constrained” hypothesis \Rightarrow lower VC dimension

Support Vector Machine

- Goal:
 - Find the **max-margin** linear separator that separates the data
 - Recall the goal of PLA: Find the linear separator that separates the data

- Notations:

Notations we used so far:

- $\vec{x} = (x_0, x_1, \dots, x_d)$
- $\vec{w} = (w_0, w_1, \dots, w_d)$
- Linear separator
$$h(\vec{x}) = \text{sign}(\vec{w}^T \vec{x})$$

Notations we will use in SVM

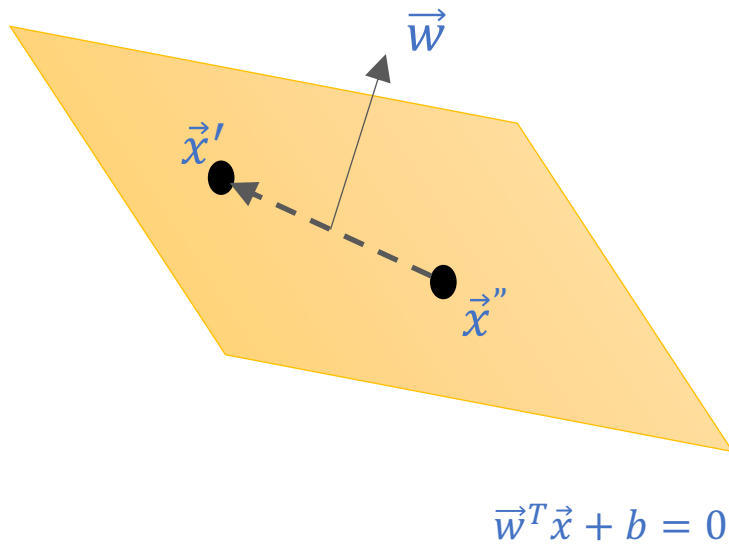
- $\vec{x} = (x_1, \dots, x_d)$
- $\vec{w} = (w_1, \dots, w_d)$
- Linear separator
$$h(\vec{x}) = \text{sign}(\vec{w}^T \vec{x} + b)$$

Separating the bias/intercept b is important for us to characterize the margin.

We will use (\vec{w}, b) to characterize the hypothesis

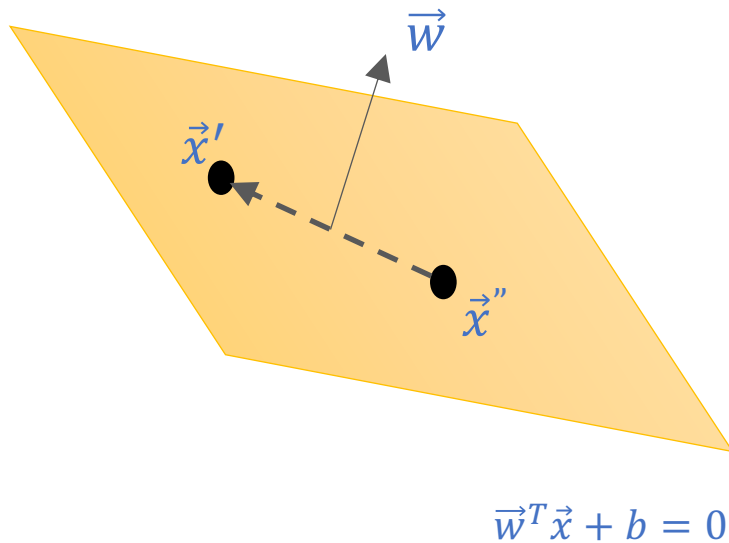
Relevant Review of Linear Algebra

- Claim: \vec{w} is the norm vector of the hyperplane $\vec{w}^T \vec{x} + b = 0$



Relevant Review of Linear Algebra

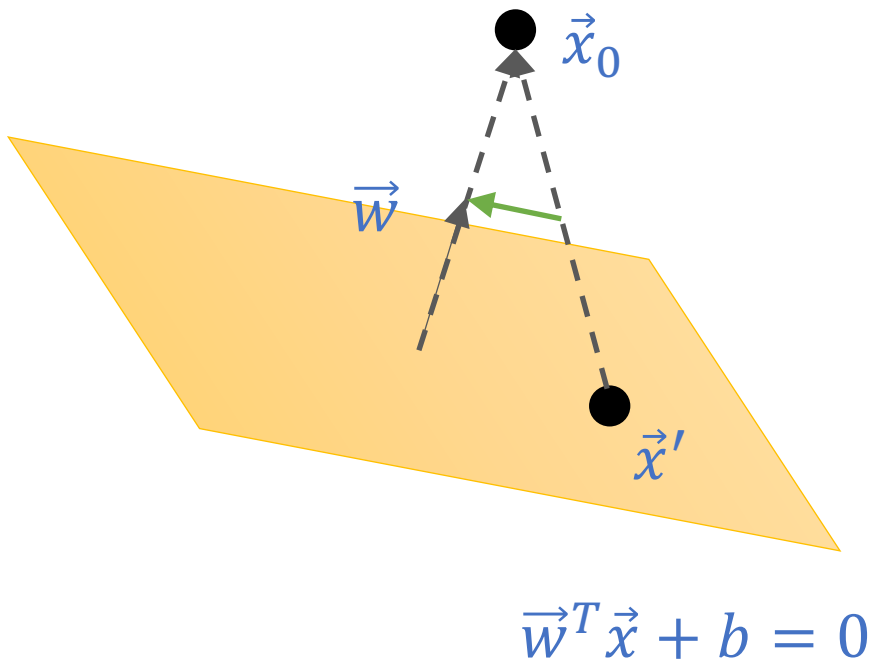
- Claim: \vec{w} is the norm vector of the hyperplane $\vec{w}^T \vec{x} + b = 0$



- Consider any two points \vec{x}' and \vec{x}'' on the hyperplane
 - $\vec{w}^T \vec{x}' + b = 0$
 - $\vec{w}^T \vec{x}'' + b = 0$
- Combining the above
 - $\vec{w}^T (\vec{x}' - \vec{x}'') = 0$
- \vec{w} is orthogonal to the hyperplane
- \vec{w} is the norm vector of the hyperplane

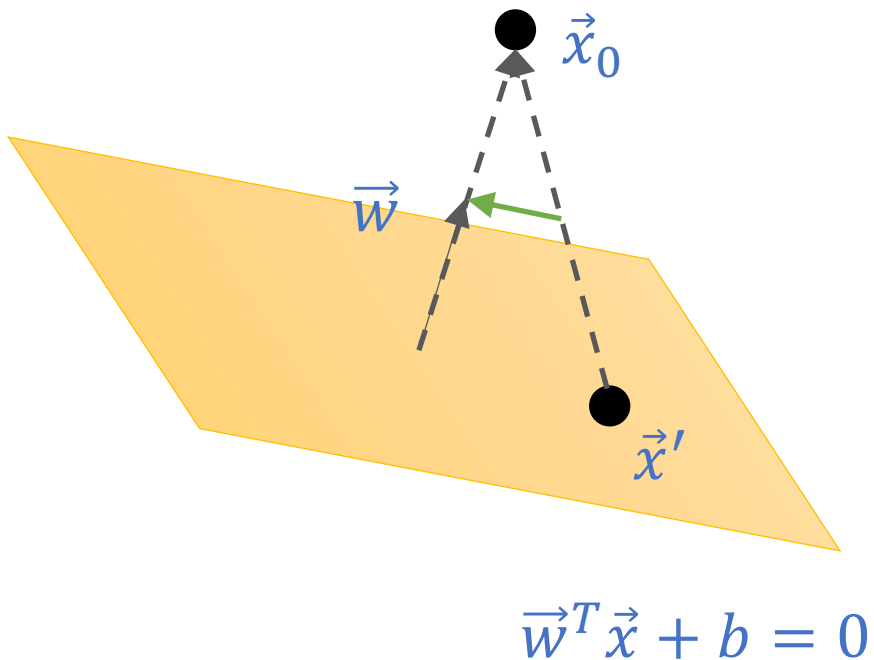
Relevant Review of Linear Algebra

- What is the distance between a point \vec{x}_0 and a hyperplane $\vec{w}^T \vec{x} + b = 0$



Relevant Review of Linear Algebra

- What is the distance between a point \vec{x}_0 and a hyperplane $\vec{w}^T \vec{x} + b = 0$



- Consider an arbitrary point \vec{x}' on the hyperplane
- Distance between the point \vec{x}_0 and the hyperplane

$$\begin{aligned} dist(\vec{x}_0, \vec{w}, b) &= \left| \frac{\vec{w}^T}{\|\vec{w}\|} (\vec{x}_0 - \vec{x}') \right| \\ &= \left| \frac{1}{\|\vec{w}\|} (\vec{w}^T \vec{x}_0 - \vec{w}^T \vec{x}') \right| \\ &= \left| \frac{1}{\|\vec{w}\|} (\vec{w}^T \vec{x}_0 + b) \right| \end{aligned}$$