Linear Classifiers

CS771: Introduction to Machine Learning

Purushottam Kar

Announcements

Please declare your assignment groups using the form below https://forms.gle/Zqe3yZyGv7rvzjm56

5 registered students per group (no auditors)

Deadline for filling this form August 09 (Friday), 11:59PM IST

Assignment 1 will be released soon thereafter and we will simply assign remaining students to arbitrary groups after above deadline

Groups that are not of proper size (5) may be reorganized by us

Please fill the form only once per project group

Auditor groups should not fill this form

Project groups will be listed on the website



Recap of Last Lecture

- Looked at a weighted variant of the NN algorithm
- Studied decision trees which have several benefits
 - Can be thought of as a speed up way to perform NN classification
 - Offer extremely fast prediction times
 - Can handle non-numeric, discrete, categorical features with ease
- Some challenges with decision trees
 - Can be bulky i.e. model size can be large
 - Deciding how to split a node can be time consuming
 - Learning the best decision tree is an intractable (NP hard) problem

Decision Boundaries

Some interesting discussion on Piazza

Earlier definition of decision boundary (points where classifier gets confused is simple but not general enough)

More robust definition of decision boundary: locations where classifier decision abruptly changes from one class to another class

All classifiers have such a decision boundary

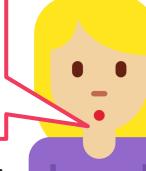
Easy to detect whether a test point is at decision boundary for linear classifiers – difficult to do so for most other classifiers, e.g. deep nets



Decision Boundaries

Some interesting discussion on Piazza

Indeed, since we would have to not only predict for that data point, but also for other data points around it!



Earlier definition of decision boundary (points where classifier gets confused is simple but not general enough)

More robust definition of decision boundary: locations where classifier decision abruptly changes from one class to another class

All classifiers have such a decision boundary

Easy to detect whether a test point is at decision boundary for linear classifiers – difficult to do so for most other classifiers, e.g. deep nets



It might still get confused if there are 4 points equally close 2 of them red and 2 green ©

For example, kNN will never get confused if k = 3 (or some odd number) and 2 classes

Keep appearing again and again in various methods LwP with 2 classes, Euclidean metric always gives a linear classifier Even if Mahalanobis metric used, still LwP gives a linear classifier

Decision stumps with a single feature also give a linear classifier

Extremely popular in ML

Very small model size – just one vector (and one bias value)

Very fast $\mathcal{O}(d)$ prediction time

Used to build DTs, deep nets etc



Linear Classifiers

Keep appearing again and ag LwP with 2 classes, Euclide: Even if Mahalanobis metric Decision stumps with a single reature also give a linear classif

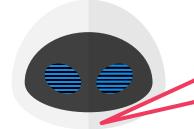
Before going forward, recall that linear classifiers are those that have a line or a plane as the decision boundary. A linear classifier is given by a model that looks like (\mathbf{w}, b) and it makes predictions by looking at whether $\mathbf{w}^{\mathsf{T}}\mathbf{x} + b > 0$ or not

Extremely popular in ML

Very small model size – just one vector (and one bias value)

Very fast O(d) prediction time Used to build DTs, deep nets etc

Learning classifiers directly will allow us to control many useful properties about them!



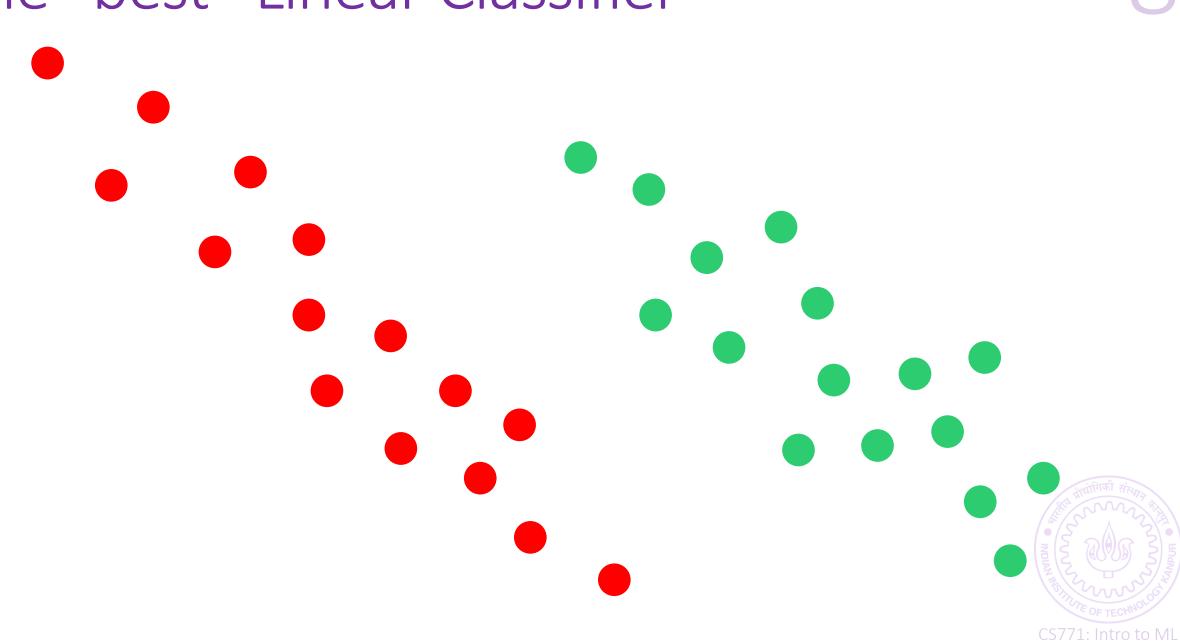
That is exactly what we will do today!

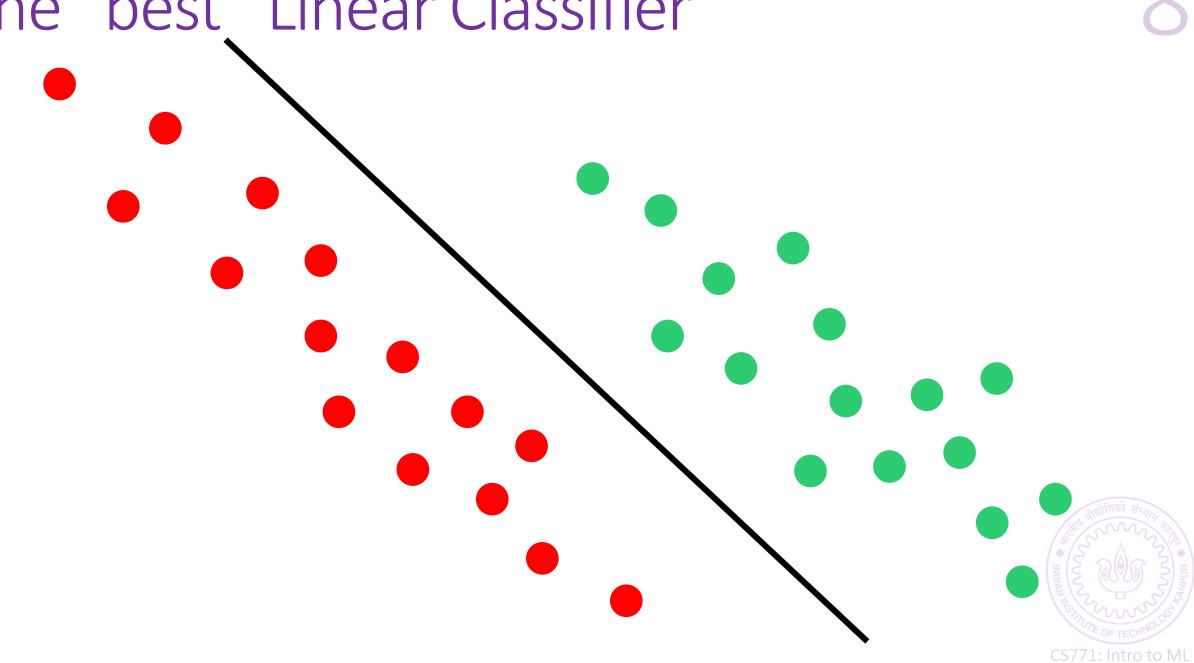
Instead of indirectly getting a linear classifier via LwP + Mahalanobis etc etc, can't we learn one directly?

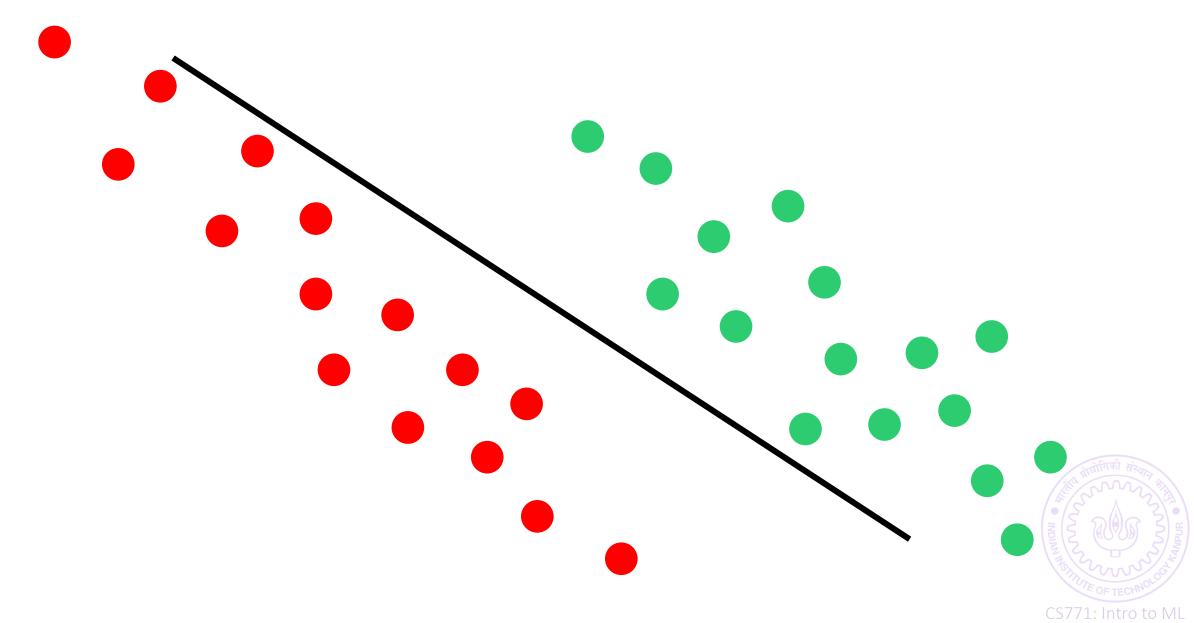


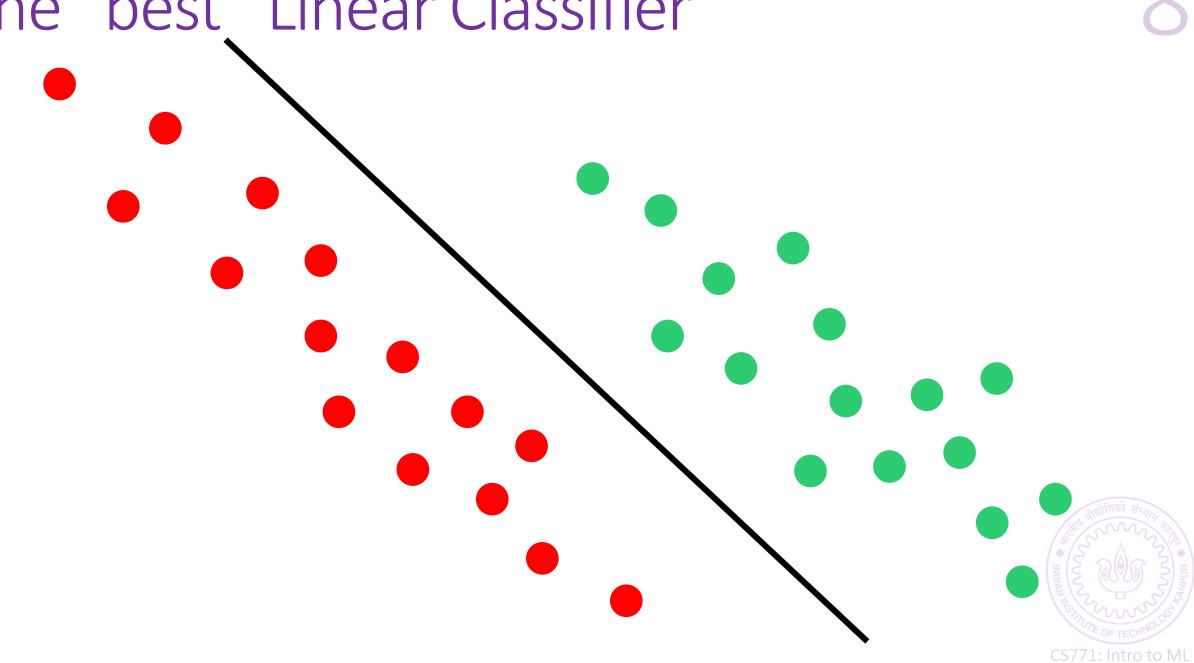




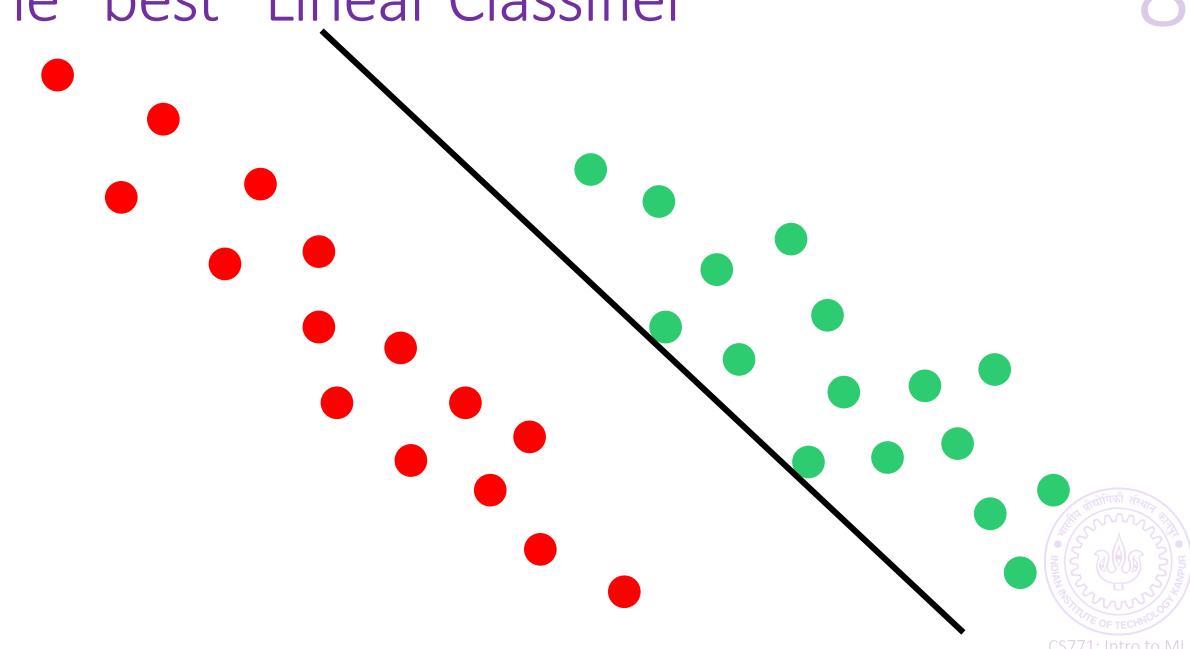




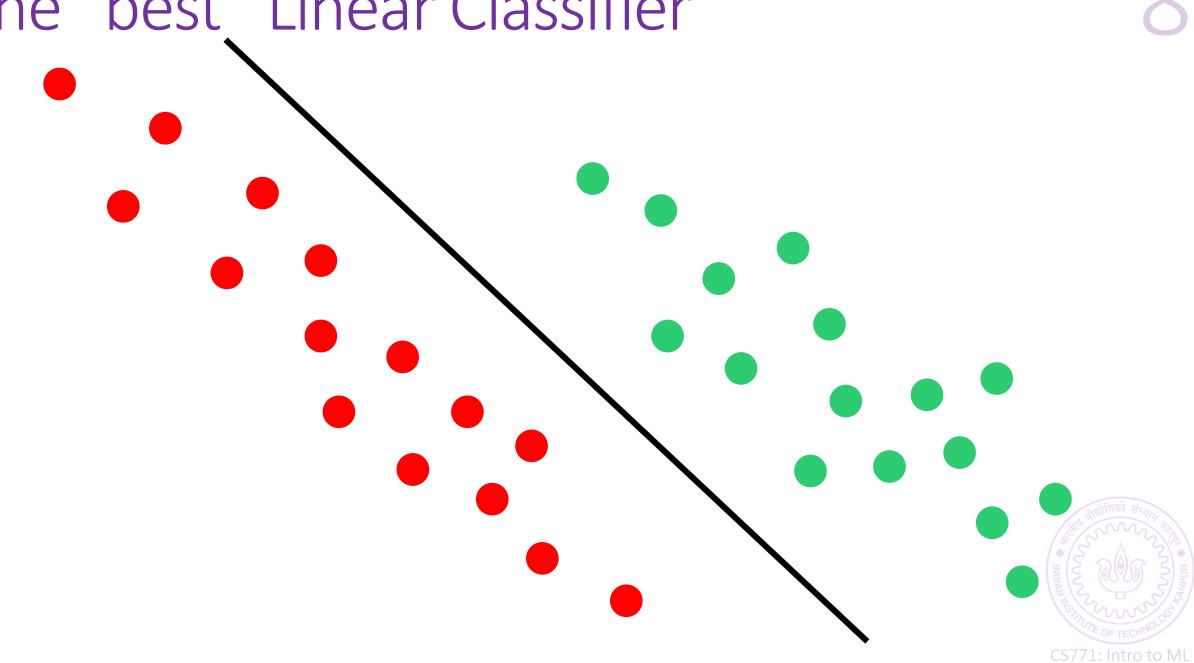




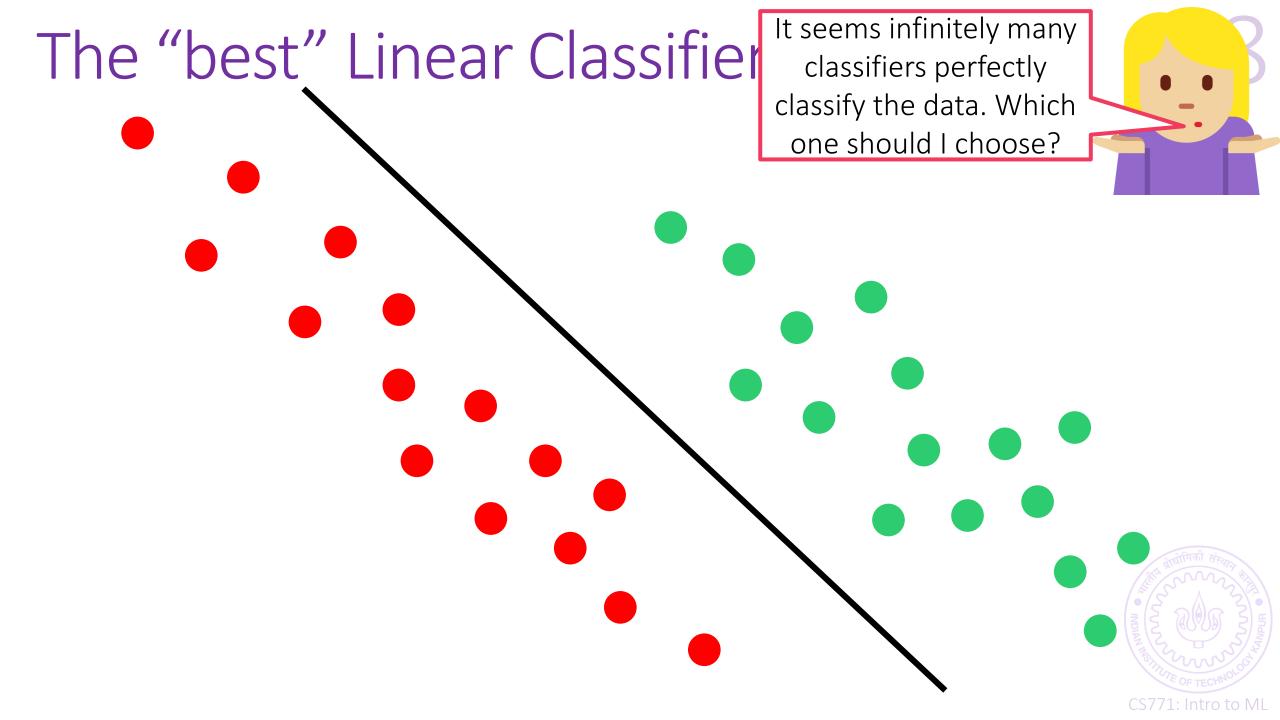
CS771: Intro to ML

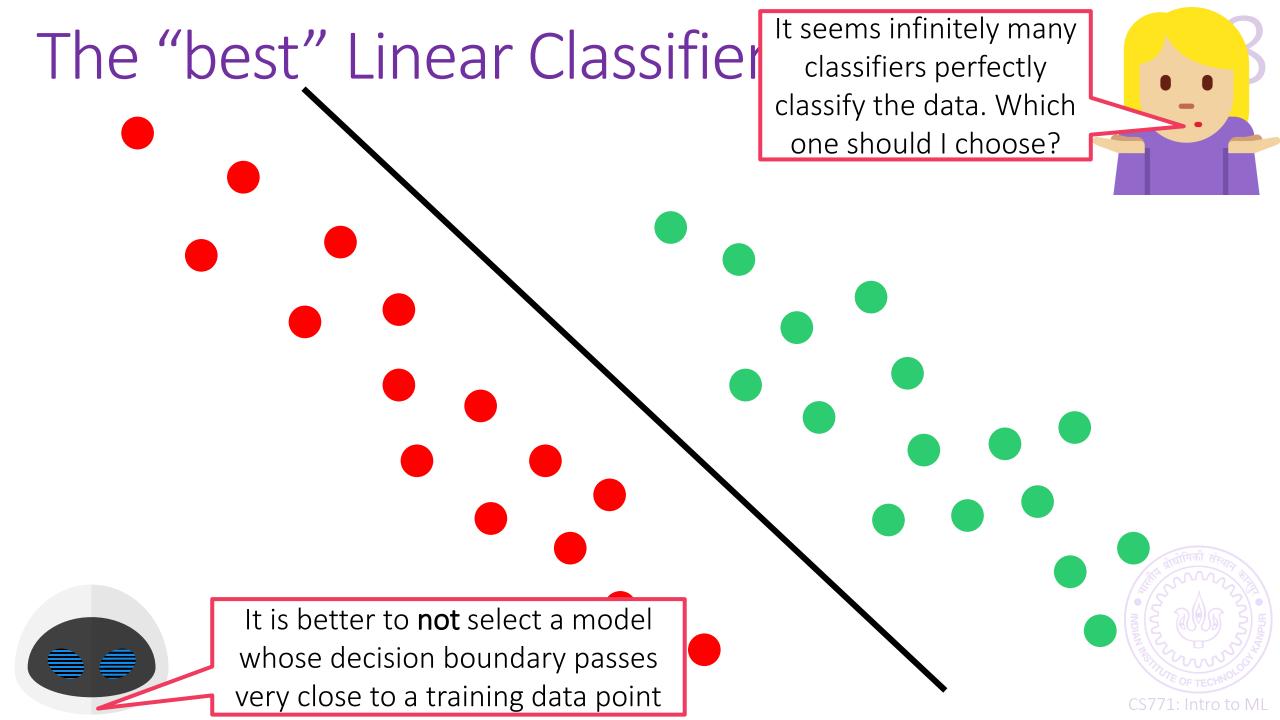


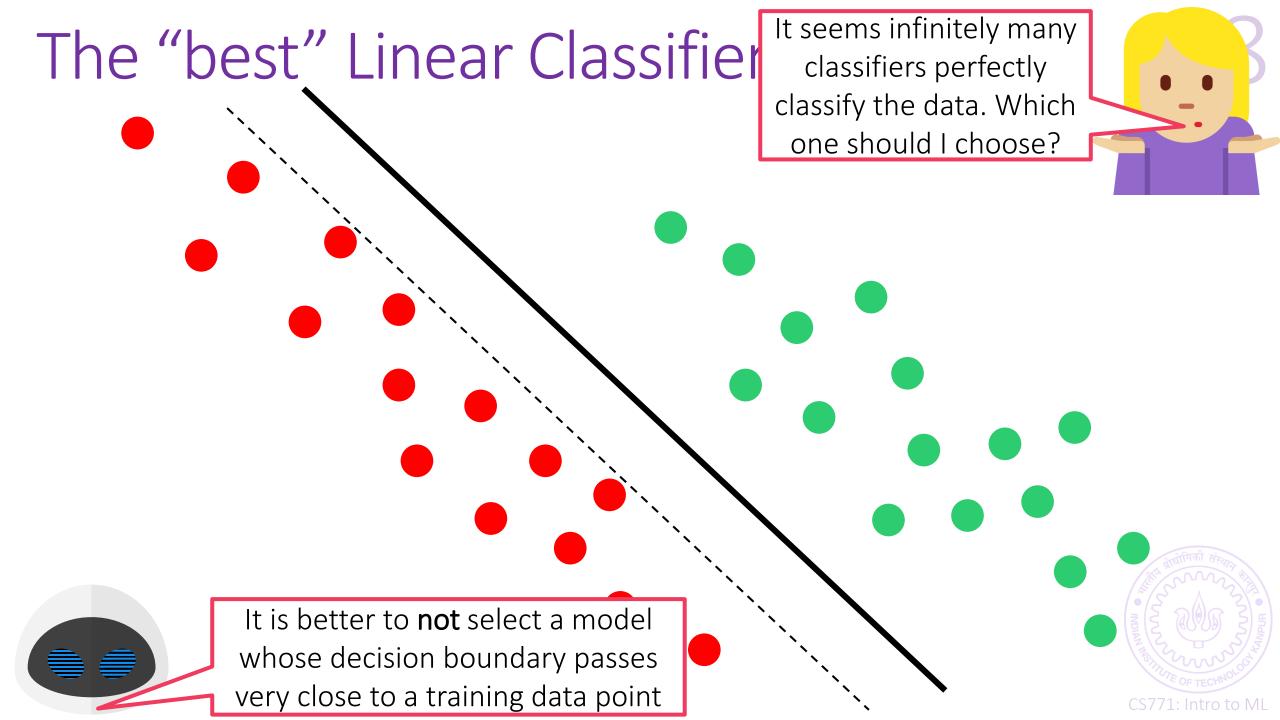
CS771: Intro to ML

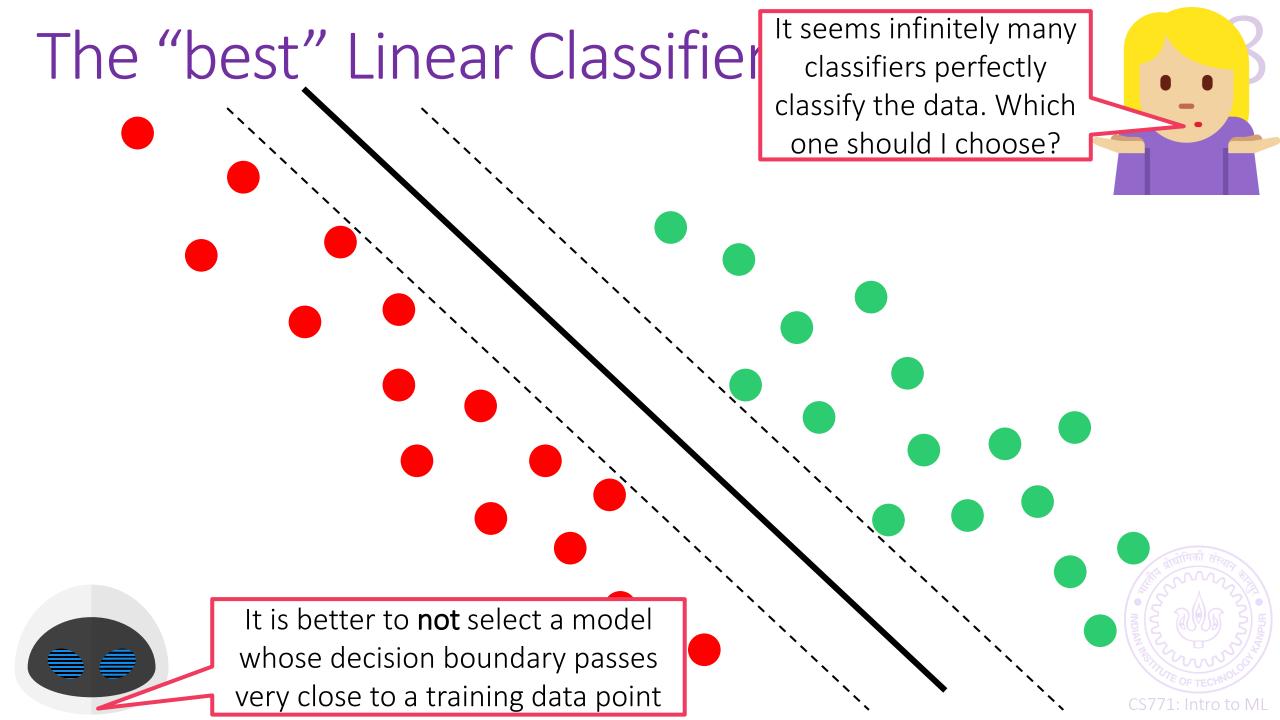


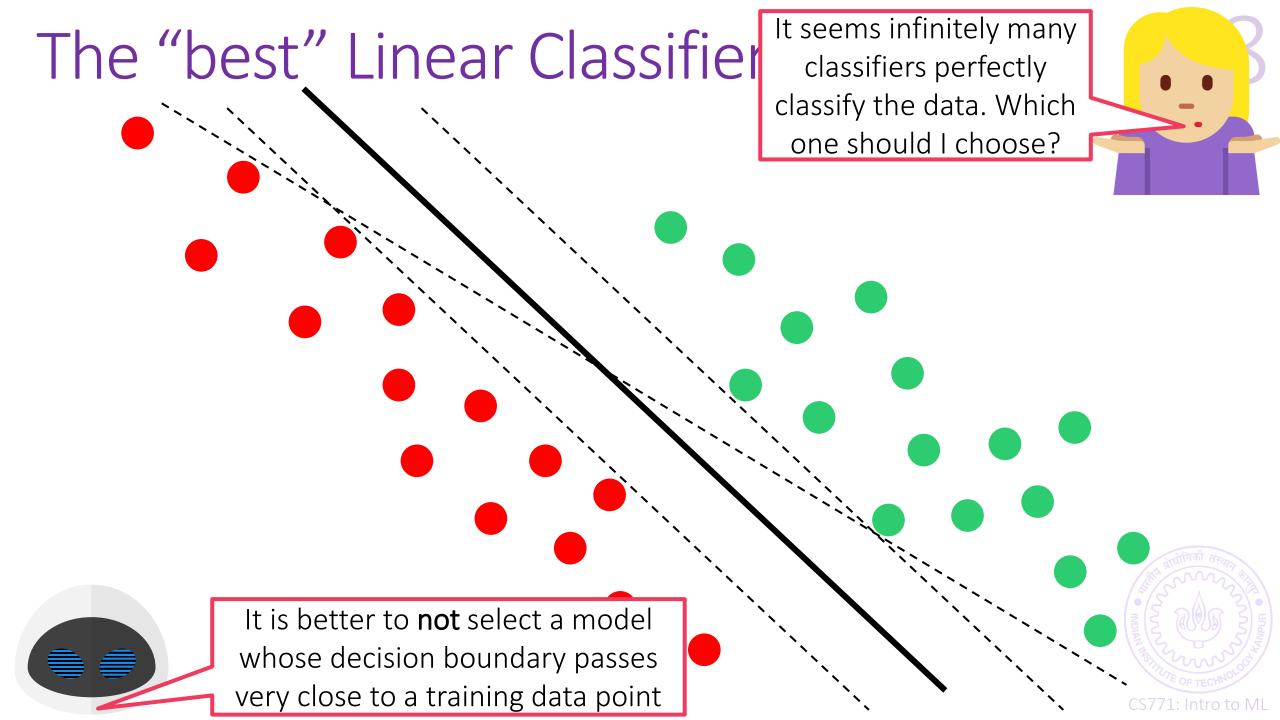
The "best" Linear Classifier CS771: Intro to ML

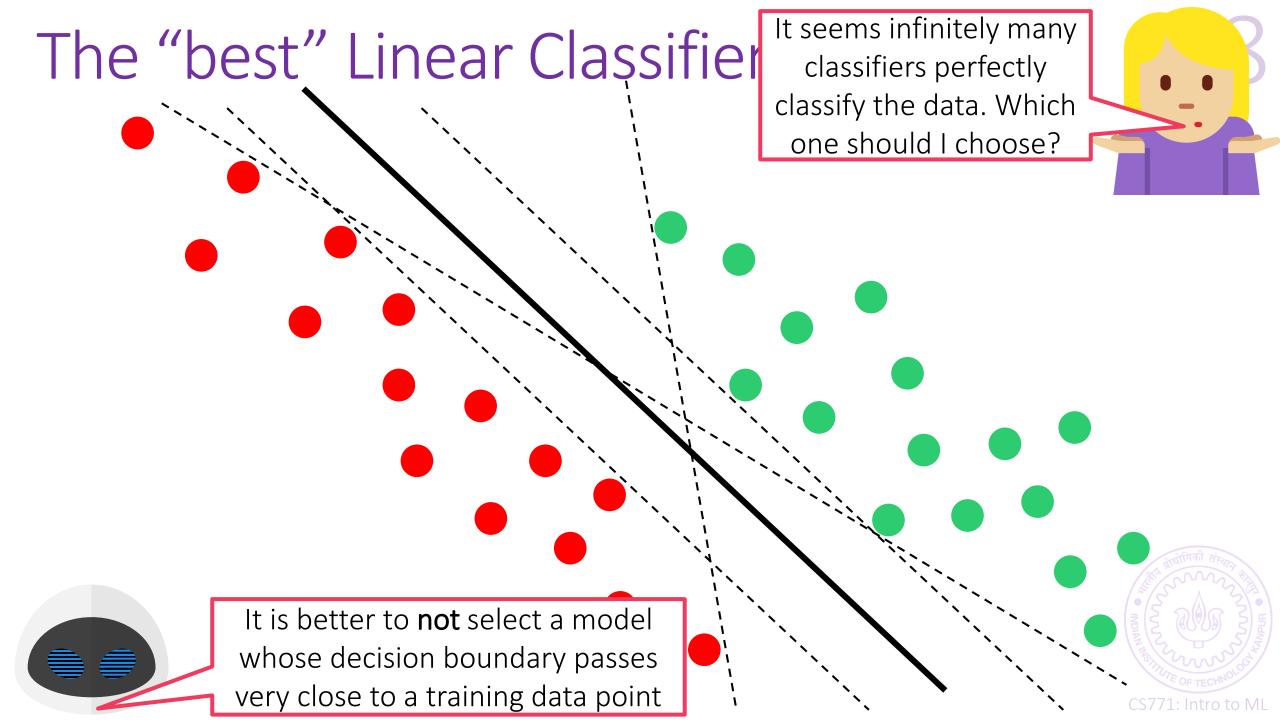


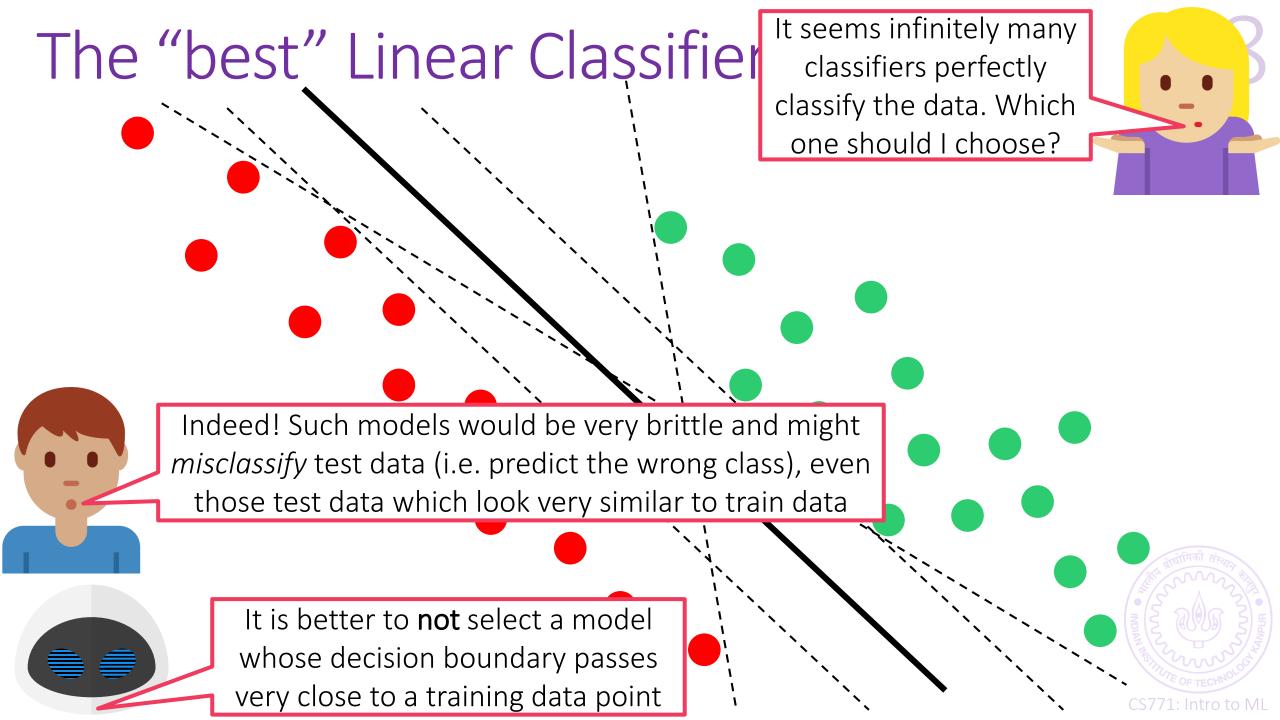


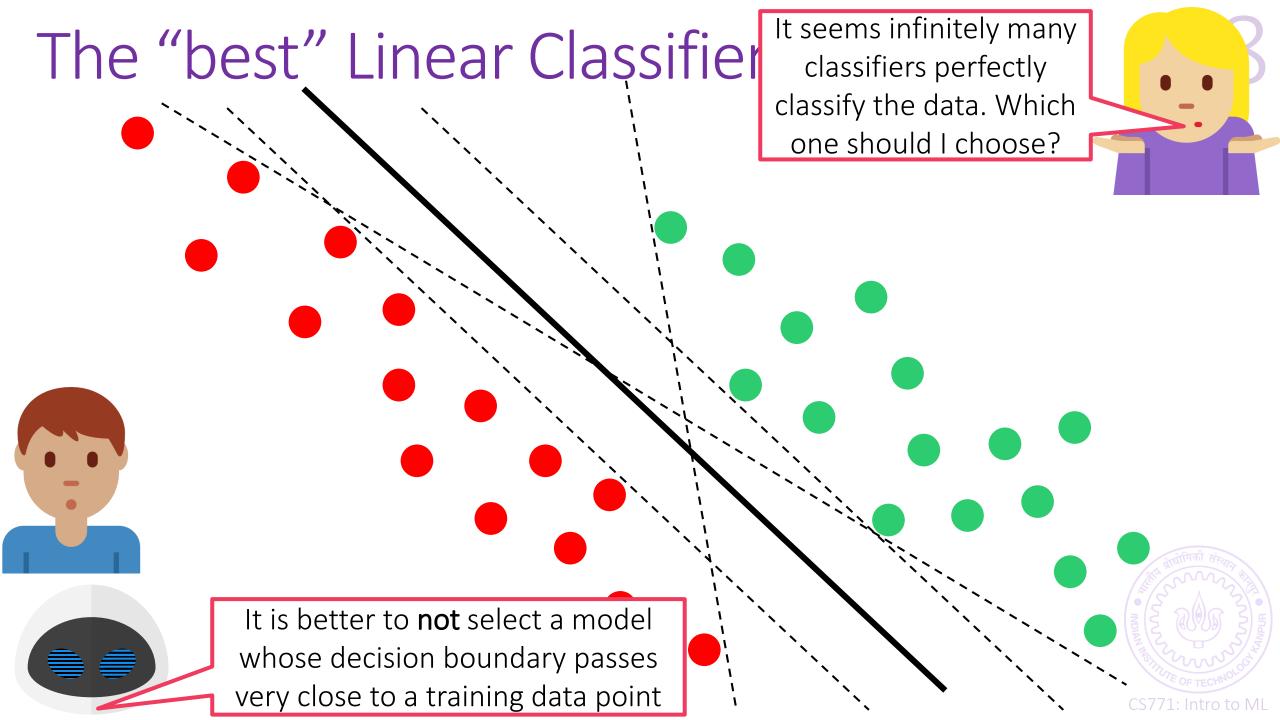


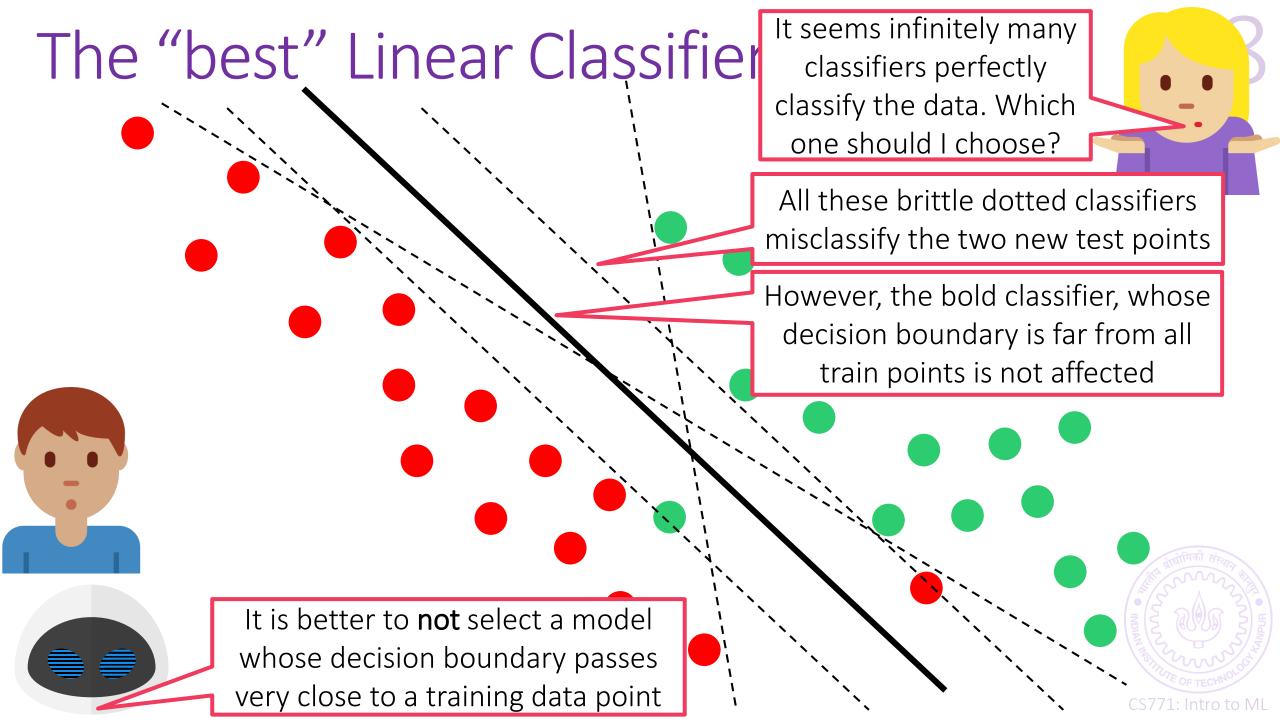




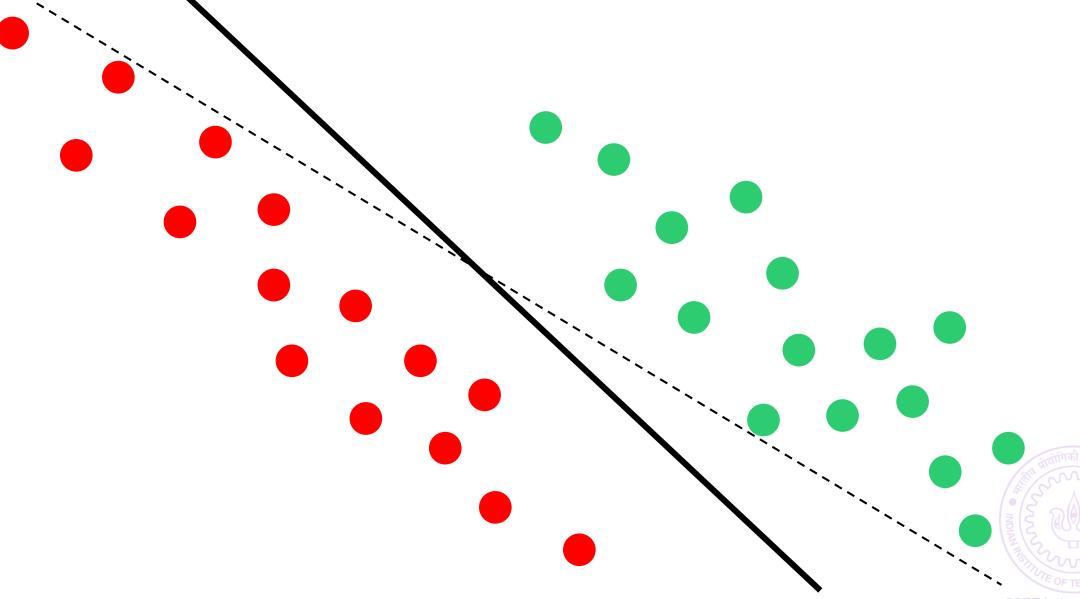


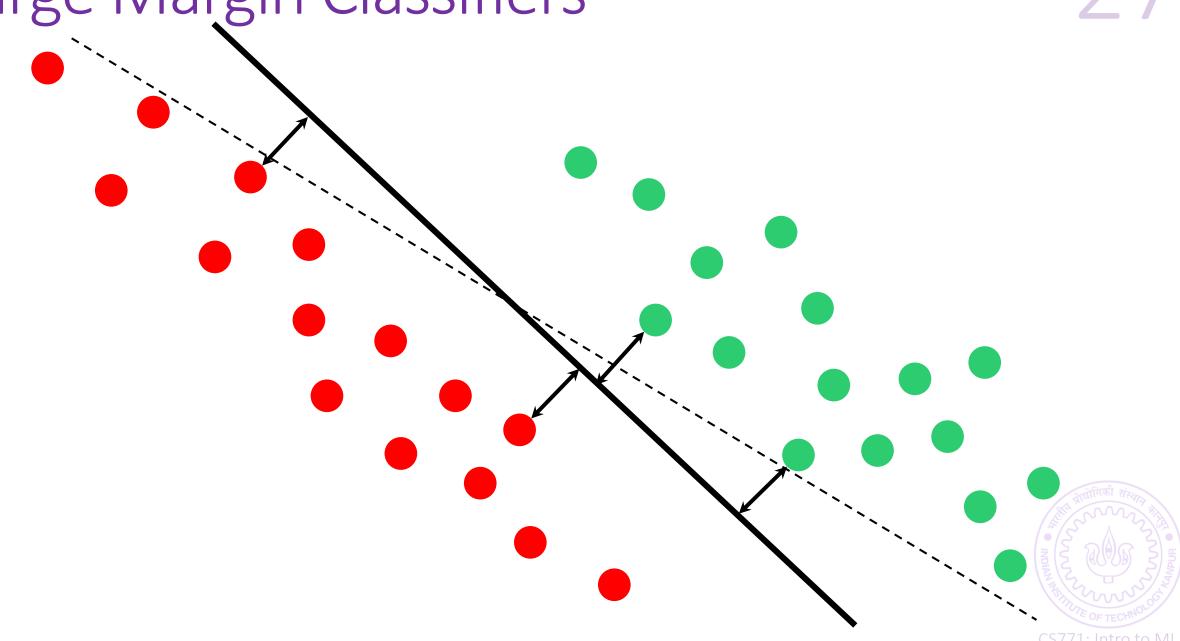




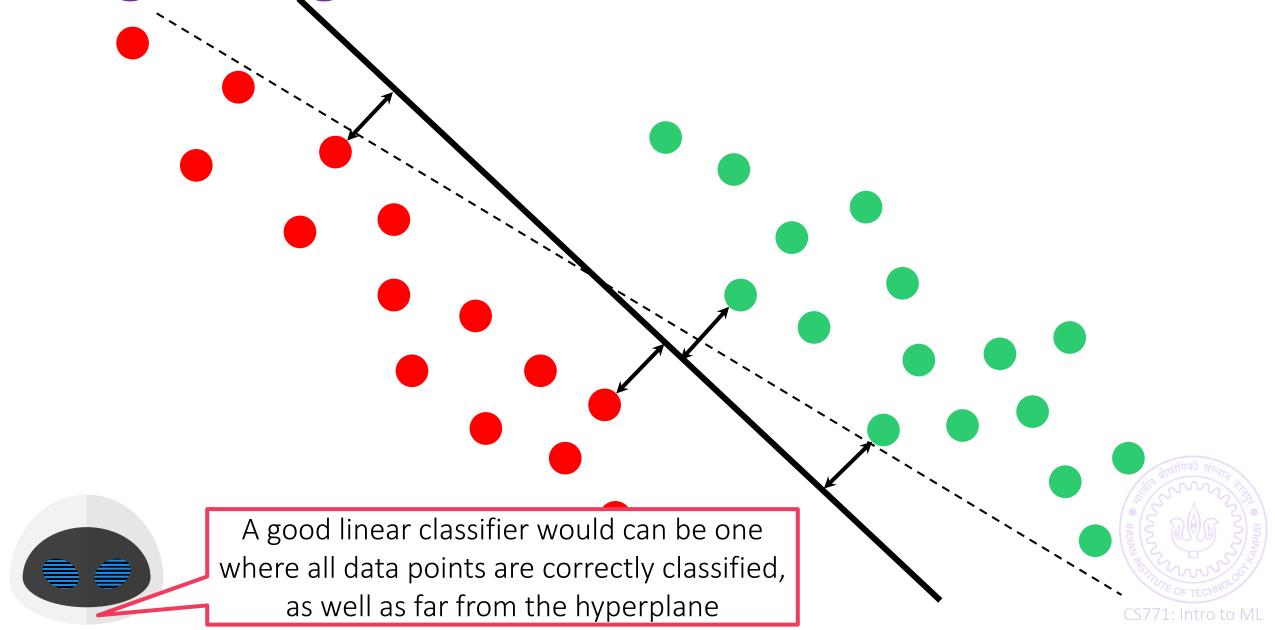




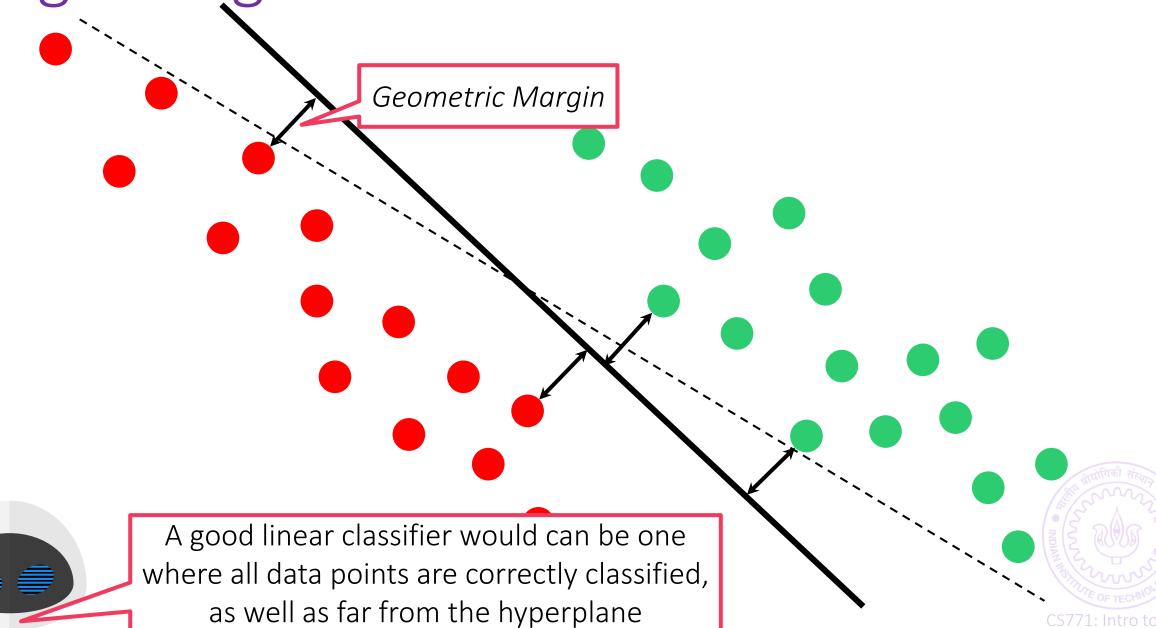






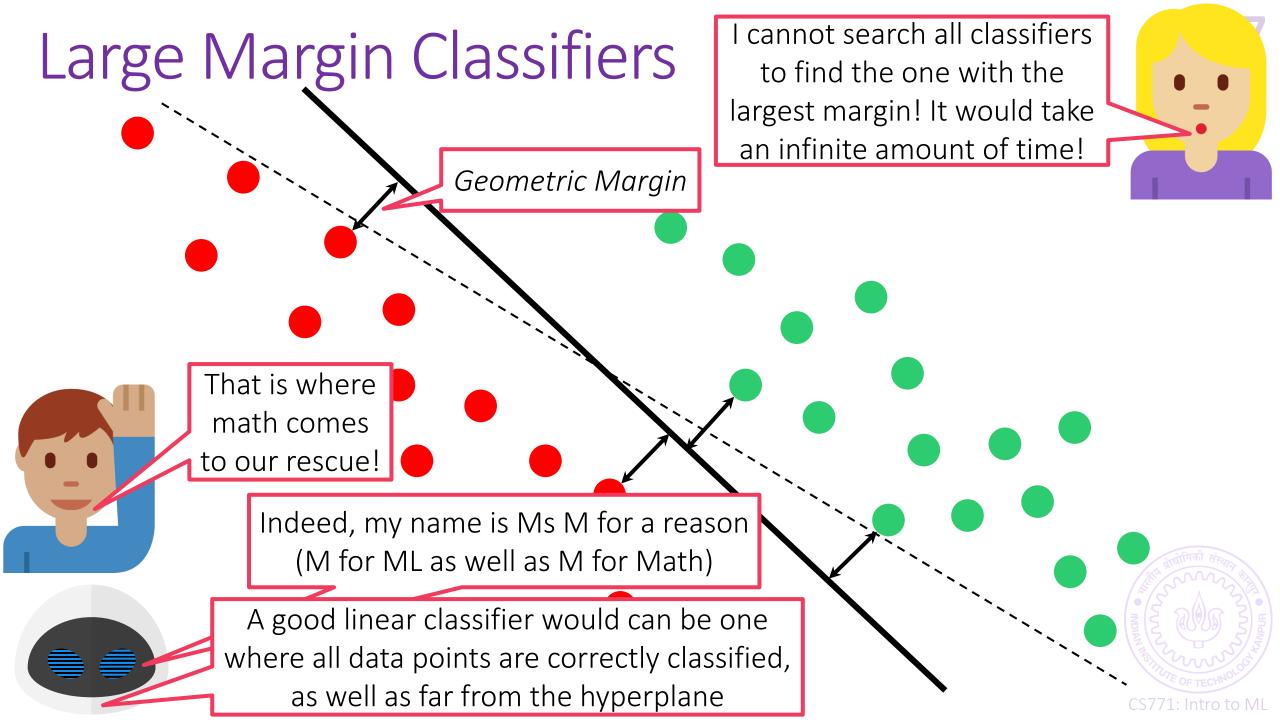


27



Large Margin Classifiers Geometric Margin A good linear classifier would can be one where all data points are correctly classified, as well as far from the hyperplane

cannot search all classifiers Large Margin Classifiers to find the one with the largest margin! It would take an infinite amount of time! Geometric Margin A good linear classifier would can be one where all data points are correctly classified, as well as far from the hyperplane



The distance of origin from hyperplane $\mathbf{w}^{\mathsf{T}}\mathbf{x} + b = 0$ is $|b|/||\mathbf{w}||_2$ The distance of a point **p** from this hyperplane is $\|\mathbf{w}^{\mathsf{T}}\mathbf{p} + b\|/\|\mathbf{w}\|_2$ Given train data for a binary classification problem $\{(\mathbf{x}^i, y^i)\}_{i=1}^n$ where $\mathbf{x}^i \in \mathbb{R}^d$ and $y^i \in \{-1,1\}$, we want two things from a classifier It should classify every point correctly – how to ask this politely? One way: demand that for all $i = 1 \dots n$, $\operatorname{sign}(\mathbf{w}^{\mathsf{T}}\mathbf{x}^i + b) = y^i$ Easier way: demand that for all i = 1 ... n, $y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + \mathbf{b}) \ge 0$ It should not let any data point come close to the boundary Demand that $\min_{i=1}^{n} |\mathbf{w}^{\mathsf{T}} \mathbf{x}^{i} + b|/||\mathbf{w}||_{2}$ be as large as possible

Just a fancy way of saying

Please find me a linear classifier that perfectly classifies the train data while keeping data points as far away from the hyperplane as possible

The mathematical way of writing this request is the following

Constraints

$$\max_{\mathbf{w},b} \left\{ \min_{i=1...n} |\mathbf{w}^{\mathsf{T}} \mathbf{x}^{i} + b| / ||\mathbf{w}||_{2} \right\}$$

Objective

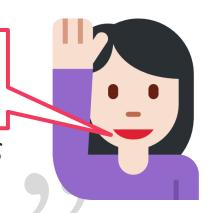
such that $y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + \mathbf{b}) \ge 0$ for all $i = 1 \dots n$



Support Vector Machines

Just a fancy way of saying

Please find me a linear classification problem classifies the train data while keeping data points as far away from the hyperplane as possible



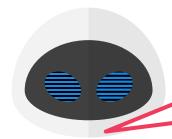
The mathematical way of writing this request is the following

Constraints

$$\max_{\mathbf{w},b} \left\{ \min_{i=1...n} |\mathbf{w}^{\mathsf{T}} \mathbf{x}^{i} + b| / ||\mathbf{w}||_{2} \right\}$$

Objective

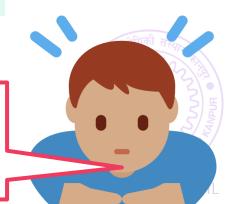
such that $y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + \mathbf{b}) \ge 0$ for all $i = 1 \dots n$



This is known as an optimization problem with an objective and lots of constraints

This looks so complicated, how will I ever find a solution to this optimization problem?

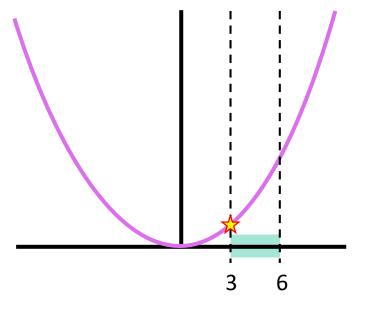
Let us simplify this



Constrained Optimization 101

HOW WE MUST COPY TO MS M Objective Constraints $\min_{x} f(x)$ such that p(x) < 0and q(x) > 0 etc. etc.

 $\min_{x} x^{2}$ s.t. $x \le 6$ and $x \ge 3$



HOW WE SPEAK TO A HUMAN

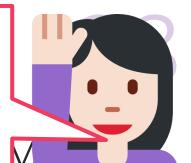
I want to find an unknown x that gives me the *best* value according to this function f

Oh! btw, not any x would do! x must satisfy these conditions

All I am saying is, of the values of x that satisfy my conditions, find me the one that gives the best value according to f

Constrained Optimi

Constraints are usually specified using math equations. The set of points that satisfy all the constraints is called the feasible set of the optimization problem



HOW WE MUST SPEAK TO MS

Objective

Constraints

 $\min_{x} f(x)$ such that p(x) < 0and q(x) > 0 etc. etc.



 $\min_{x} x^{2}$ s.t. $x \le 6$ and $x \ge 3$

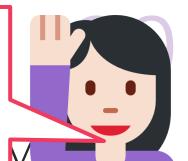
Feasible set is the interval [3,6]

I want to find an unknown xFor your specified constraints, the optimal (least) value of f is 9 and it is achieved at x=3 Id do! must satisfy these conditions

All I am saying is, of the values of x that satisfy my conditions, find me the one that gives the best value according to f

Constrained Optimi

Constraints are usually specified using math equations. The set of points that satisfy *all* the constraints is called the *feasible set* of the optimization problem



HOW WE MUST COLLY TO MS

Objective

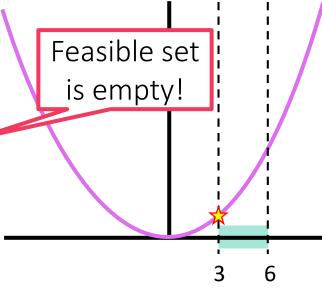
Constraints

 $\min_{x} f(x)$

such that p(x) < 0

and q(x) > 0 etc. etc.

 $\min_{x} x^{2}$ s.t. $x \ge 6$ and $x \le 3$



I want to find an unknown xYou optimization problem has no solution since no point satisfies all your constraints \otimes Id do

must satisfy these conditions

All I am saying is, of the values of x that satisfy my conditions, find me the one that gives the best value according to f

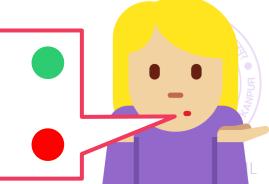
Back to SVMs

Assume there do exist models that perfectly classify all train data Consider one such model (\mathbf{w}, b) which classifies train data perfectly Now, $|\mathbf{w}^{\mathsf{T}}\mathbf{x}^{i} + b|/||\mathbf{w}||_{2} = |y^{i} \cdot (\mathbf{w}^{\mathsf{T}}\mathbf{x}^{i} + b)|/||\mathbf{w}||_{2} \text{ as } y^{i} \in \{-1,1\}$ Thus, geometric margin is same as $\min_{i=1...n} |y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + b)| / ||\mathbf{w}||_2 = \min_{i=1...n} y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + b) / ||\mathbf{w}||_2$ since model has perfect classification!

We will use this useful fact to greatly simplify the optimization problem



What if train data is *non-linearly* separable i.e no linear classifier can perfectly classify it? For example



Support Vector Mach

Called the *functional margin*. Note that geometric margin = functional margin/ $\|\mathbf{w}\|_2$

Let i_0 be the data point that comes closest to the hyperplane i.e.

$$\left(\min_{i=1\dots n} y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + b)\right) = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$

Recall that all this discussion holds only for a perfect classifier (\mathbf{w}, b)

Let
$$\epsilon = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$
 and consider $\widetilde{\mathbf{w}} = \mathbf{w}/\epsilon$, $\widetilde{b} = b/\epsilon$

Note this gives us
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$ as well as $\min_{i=1\dots n} y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) / \|\widetilde{\mathbf{w}}\|_2 = 1 / \|\widetilde{\mathbf{w}}\|_2$ (as $y^{i_0} \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^{i_0} + \widetilde{b}) = 1$)

Thus, instead of searching for (\mathbf{w}, b) , easier to search for $(\widetilde{\mathbf{w}}, \widetilde{b})$

$$\max_{\widetilde{\mathbf{w}},\widetilde{b}} \{1/\|\widetilde{\mathbf{w}}\|_2\}$$

such that
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$



Support Vector Mach

Called the *functional margin*. Note that geometric margin = functional margin/ $\|\mathbf{w}\|_2$

Let i_0 be the data point that comes closest to the hyperplane i.e.

$$\left(\min_{i=1\dots n} y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + b)\right) = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$

Recall that all this discussion holds only for a perfect classifier (\mathbf{w}, b)

Let
$$\epsilon = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$
 and consider $\widetilde{\mathbf{w}} = \mathbf{w}/\epsilon$, $\widetilde{b} = b/\epsilon$

Note this gives us
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$ as well as $\min_{i=1\dots n} y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) / \|\widetilde{\mathbf{w}}\|_2 = 1 / \|\widetilde{\mathbf{w}}\|_2$ (as $y^{i_0} \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^{i_0} + \widetilde{b}) = 1$)

Thus, instead of searching for (\mathbf{w}, b) , easier to search for $(\widetilde{\mathbf{w}}, \widetilde{b})$

$$\min_{\widetilde{\mathbf{w}},\widetilde{b}}\{\|\widetilde{\mathbf{w}}\|_2\}$$

such that
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$



Support Vector Mach

Called the *functional margin*. Note that geometric margin = functional margin/ $\|\mathbf{w}\|_2$

Let i_0 be the data point that comes closest to the hyperplane i.e.

$$\left(\min_{i=1\dots n} y^i \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^i + b)\right) = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$

Recall that all this discussion holds only for a perfect classifier (\mathbf{w}, b)

Let
$$\epsilon = y^{i_0} \cdot (\mathbf{w}^\mathsf{T} \mathbf{x}^{i_0} + b)$$
 and consider $\widetilde{\mathbf{w}} = \mathbf{w}/\epsilon$, $\widetilde{b} = b/\epsilon$

Note this gives us
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$ as well as $\min_{i=1\dots n} y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) / \|\widetilde{\mathbf{w}}\|_2 = 1 / \|\widetilde{\mathbf{w}}\|_2$ (as $y^{i_0} \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^{i_0} + \widetilde{b}) = 1$)

Thus, instead of searching for (\mathbf{w}, b) , easier to search for $(\widetilde{\mathbf{w}}, \widetilde{b})$

$$\min_{\widetilde{\mathbf{w}},\widetilde{b}}\{\|\widetilde{\mathbf{w}}\|_2^2\}$$

such that
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1$$
 for all $i = 1 \dots n$



The C-SVM Technique

For linearly separable cases where we suspect a perfect classifier exists

$$\min_{\widetilde{\mathbf{w}}, \widetilde{b}} \frac{1}{2} \|\widetilde{\mathbf{w}}\|_{2}^{2}$$

s.t. $y^{i} \cdot (\widetilde{\mathbf{w}}^{\mathsf{T}} \mathbf{x}^{i} + \widetilde{b}) \geq 1$ for all $i \in [n]$

If a linear classifier cannot perfectly classify data, then find model using

$$\min_{\widetilde{\mathbf{w}}, \widetilde{b}, \{\xi_i\}} \frac{1}{2} ||\widetilde{\mathbf{w}}||_2^2 + C \sum_{i=1}^n \xi_i$$
s.t. $y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1 - \xi_i$ for all $i \in [n]$ as well as $\xi_i \ge 0$ for all $i \in [n]$



The C-SVM Te What prevents me from misusing the slack variables to learn a model that misclassifies every data point?

For linearly separable cases v

The C term prevents you from doing so. If we set C to be a large value (it is a hyper-parameter), then it will penalize s.t. $y^i \cdot (\widetilde{\mathbf{w}}^T \mathbf{x} + v) \leq 1$ for all $\iota \in [n]$

s.t.
$$y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T}$$

If a linear classifier cannot perfectly classify data, then find mo

$$\min_{\widetilde{\mathbf{w}},\widetilde{b},\{\xi_i\}} \frac{1}{2} ||\widetilde{\mathbf{w}}||_2^2 + C\sum_{i=1}^n$$
 Having the constraint $\xi_i \geq 0$ prevents us from misusing slack

s.t. $y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \geq 1 - \xi_i$ to artificially inflate the margin

as well as $\xi_i \geq 0$ for all $i \in [n]$

Recall English phrase "cut me some slack"

The ξ_i terms are called *slack variables*. They allow some data points to come close to the hyperplane or be misclassified altogether



We can further simplify the previous optimization problem

Note ξ_i basically allows us to have $y^i \cdot \left(\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}\right) < 1$ (even < 0)

Thus, the amount of slack we want is just $\xi_i = 1 - y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b})$

However, recall that we must also satisfy $\xi_i \geq 0$

Another way of saying that if you already have $y^i \cdot \left(\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}\right) \geq 1$, then you don't need any slack i.e. you should have $\xi_i = 0$ in this case

Thus, we need only set $\xi_i = \left[1 - y^i \cdot \left(\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}\right)\right]_+$

The above is nothing but the popular hinge loss function!



We can further simplify the previous optimization problem

Note ξ_i basically allows us to have $y^i \cdot \left(\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}\right) < 1$ (even < 0)

Thus, the amount of slack we want is just $\xi_i = 1 - y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b})$

However, recall that we must also satisfy $\xi_i \geq 0$

Another way of saying that if you already have $y^i \cdot (\widetilde{\mathbf{w}}[x]_+ = \max\{x, 0\}$ then you don't need any slack i.e. you should have ξ_i

Thus, we need only set $\xi_i = \left[1 - y^i \cdot \left(\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}\right)\right]_+$

The above is nothing but the popular hinge loss function!



Hinge Loss

Captures how well as a classifier classified a data point

Suppose on a data point $(\mathbf{x}, y), y \in \{-1,1\}$, a model gives prediction score of s (for a linear model (\mathbf{w}, b) , we have $s = \mathbf{w}^\mathsf{T} \mathbf{x} + b$)

We obviously want $s \cdot y \ge 0$ for correct classification but we also want $s \cdot y \gg 0$ for large margin – hinge loss function captures both

$$\ell_{\text{hinge}}(s, y) = [1 - s \cdot y]_{+} = \begin{cases} 0 & \text{if } s \cdot y \ge 1 \\ 1 - s \cdot y & \text{if } s \cdot y < 1 \end{cases}$$

Note that hinge loss not only penalizes misclassification but also correct classification if the data point gets too close to the hyperplane!

Final Form of C-SVM

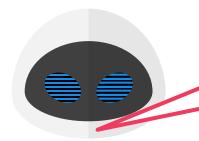
Recall that the C-SVM optimization finds a model by solving

$$\min_{\widetilde{\mathbf{w}}, \widetilde{b}, \{\xi_i\}} \frac{1}{2} \|\widetilde{\mathbf{w}}\|_2^2 + C \sum_{i=1}^n \xi_i$$

s.t. $y^i \cdot (\widetilde{\mathbf{w}}^\mathsf{T} \mathbf{x}^i + \widetilde{b}) \ge 1 - \xi_i$ for all $i \in [n]$
as well as $\xi_i \ge 0$ for all $i \in [n]$

Using the previous discussion, we can rewrite the above very simply

$$\min_{\widetilde{\mathbf{w}},\widetilde{b}} \frac{1}{2} \|\widetilde{\mathbf{w}}\|_{2}^{2} + C \sum_{i=1}^{n} \ell_{\text{hinge}} (\widetilde{\mathbf{w}}^{\mathsf{T}} \mathbf{x}^{i} + \widetilde{b}, y^{i})$$



This is where calculus and some more math comes in ©

Agreed this is simpler than before but I still don't know how to use this to find the model





Emoticons from Flaticon, designed by Twitter https://www.flaticon.com/packs/smileys-and-people-9 Licensed under CC BY 3.0