

Lecture Outline:

- -Introduction to SVM : History and motivation
- -Problem definition
- -The SVM approach: The Linear separable case
- -SVM: Non Linear separable case:
 - VC Dimension
 - The kernel Trick: discussion on Kernel functions.
 - -Soft margin: introducing the slack variables and discussing the trade-off parameter "C".
 - -Procedure for choosing an SVM model that best fits our problem ("K-fold").
- -Some Applications of SVM.
- -Conclusion: The Advantages and Drawbacks of SVM.
- -Software: Popular implementations of SVM
- -References

2

Before Starting

Before starting:

- 1- throughout the lecture if you see <u>underlined red colored</u> text then click on this text for farther information.
- 2- let me introduce you to "Nodnikit": She is an outstanding student. Although she asks many questions but sometimes these questions are key questions that help us understand the material more in depth. Also the notes that she gives are very helpful.



Introduction to SVM: History and motivation



- -Support Vector Machine (SVM) is a <u>supervised learning</u> algorithm developed by <u>Vladimir Vapnik</u> and it was first heard in 1992, introduced by Vapnik, Boser and Guyon in COLT-92.[3]
- -(it is said that <u>Vladimir Vapnik</u> has mentioned its idea in 1979 in one of his paper but its major development was in the 90's)
- For many years Neural Networks was the ultimate champion ,it was the most effective learning algorithm.

TILL SVM CAME!

5

Introduction to SVM: History and motivation cont'

- -SVM became popular because of its success in handwritten digit recognition (in NIST (1998)). it gave accuracy that is comparable to sophisticated and carefully constructed neural networks with elaborated features in a handwriting recognition task .[1]
- -Much more effective "off the shelf" algorithm than Neural Networks: It generalize good on unseen data and is easier to train and doesn't have any local optima in contrast to neural networks that may have many local optima and takes a lot of time to converge.[4]

Introduction to SVM: History and motivation cont'

- -SVM has successful applications in many complex, realworld problems such as text and image classification, hand-writing recognition, data mining, bioinformatics, medicine and biosequence analysis and even stock market!
- -In many of these applications SVM is the best choice.
- -We will further elaborate on some of these applications latter in this lecture.

7

Problem definition:

-We are given a set of n points (vectors):

 x_1, x_2, \dots, x_n such that x_i is a vector of length m, and each belong to one of two classes we label them by "+1" and "-1".

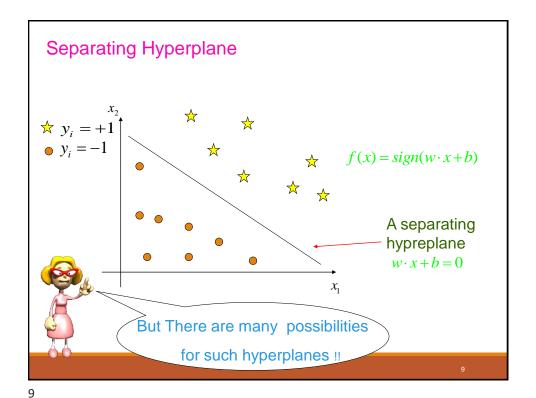
-So our training set is: $(x_1, y_1), (x_2, y_2), (x_n, y_n)$ $\forall i \ x_i \in \mathbb{R}^m, \ y_i \in \{+1, -1\}$

So the decision function will be $f(x) = sign(w \cdot x + b)$

- We want to find a separating hyperplane $w \cdot x + b = 0$ that separates these points into the two classes.

"The positives" (class "+1") and "The negatives" (class "-1").

(Assuming that they are linearly separable)

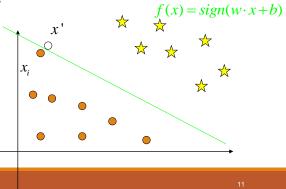


Choosing a separating hyperplane:

- -Suppose we choose the hypreplane (seen below) that is close to some sample x_i .
- Now suppose we have a new point x' that should be in class
- "-1" and is close to x_i . Using our classification function $\mathcal{F}(x)$ this point is misclassified!

Poor generalization!

(Poor performance on unseen data)

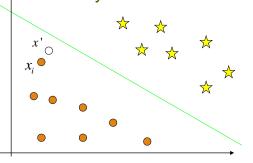


11

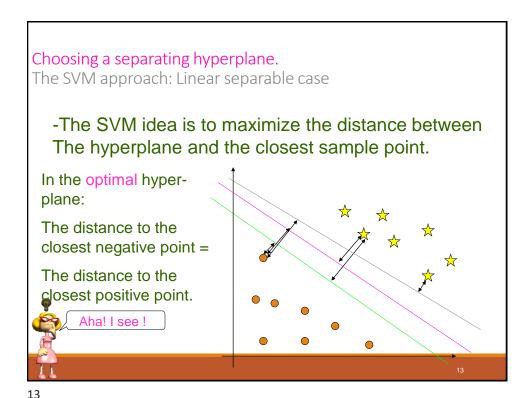
Choosing a separating hyperplane:

- -Hyperplane should be as far as possible from any sample point.
- -This way a new data that is close to the old samples will be classified correctly.

Good generalization!



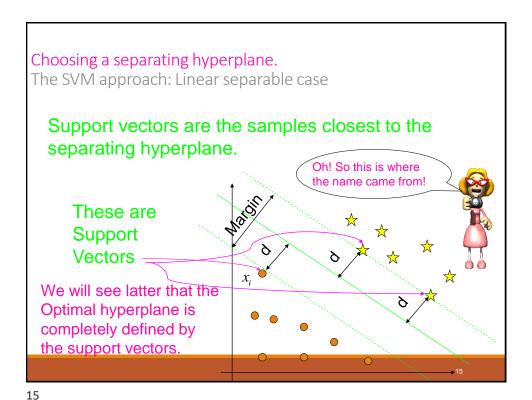
1



Choosing a separating hyperplane.
The SVM approach: Linear separable case

SVM's goal is to maximize the Margin which is twice the distance "d" between the separating hyperplane and the closest sample.

Why it is the best?
-Robust to outliners as we saw and thus strong generalization ability.
-It proved itself to have better performance on test data in both practice and in theory.



Formula for the Margin

Let us look at our decision boundary: This separating hyperplane equation is: $w^t x + b = 0$

Where $w \in R^m, x \in R^m, b \in R$

Note that $\frac{w}{\|w\|}$ is orthogonal to the separating hyperplane and its length is 1.

Let γ_i be the distance between the hyperplane and Some training example x_i . So γ_i is the length of the segment from **p** to x_i .

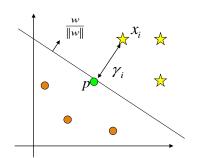
Formula for the Margin cont'

p is point on the hypreplane so $w^t p + b = 0$. On the other hand $p = x_i - \gamma_i \cdot \frac{w}{\|w\|}$.

$$w^{t}(x_{i}-\gamma_{i}\frac{w}{\|w\|})+b=0$$

$$\gamma_i = \frac{\left\| w' \cdot x_i + b \right\|}{\left\| w \right\|}$$

define $d = \min_{i \in 1..n} \gamma_i = \min_{i \in 1..n} \frac{\left\| w^t x_i + b \right\|}{\left\| w \right\|}$



Note that if we changed w to αw and b to αb this will not affect d since $\frac{\|\alpha w'x + \alpha b\|}{\|\alpha w'x + \alpha b\|} = \frac{\|w'x + b\|}{\|\alpha w + \alpha b\|}$.

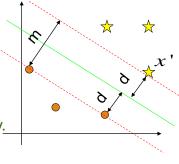
17

SVM: Linear separable case.

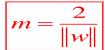
Formula for the Margin cont'

-Let x be a sample point closet to The boundary. Set $\|w^t x' + b\| = 1$ (we can rescale w and b).

-For uniqueness set $\|w^i x_i + b\| = 1$ for any sample x_i closest to the boundary. So now



$$d = \frac{\|w'x' + b\|}{\|w\|} = \frac{1}{\|w\|}$$
 The Margin



Finding the optimal hyperplane:

To find the optimal separating hyperplane, SVM aims to maximize the margin:

-Maximize $m = \frac{2}{\|w\|}$

such that:
For
$$y_i = +1$$
, $\mathbf{w}^T \mathbf{x}_i + b \ge 1$
For $y_i = -1$, $\mathbf{w}^T \mathbf{x}_i + b \le -1$

 $\frac{1}{2}\|w\|^2$ **Minimize** such that:

$$y_i(\mathbf{w}^T\mathbf{x}_i+b) \ge 1$$

We transformed the problem into a form that can be efficiently solved. We got an optimization problem with a convex quadratic objective with only linear constrains and always has a single global minimum.

19

SVM: Linear separable case.

The optimization problem:

-Our optimization problem so far:

do remember the Lagrange Multipliers from Calculus!

minimize
$$\frac{1}{2} \|\mathbf{w}\|^2$$

s.t.
$$y_i(\mathbf{w}^T\mathbf{x}_i+b) \ge 1$$



-We will solve this problem by introducing Lagrange multipliers α_i associated with the constrains:

minimize
$$L_p(w,b,\alpha) = \frac{1}{2} \|w\|^2 - \sum_{i=1}^n \alpha_i (y_i(x_i \cdot w + b) - 1)$$

$$s.t \quad \alpha_i \ge 0$$

The optimization problem cont':

So our primal optimization problem now:

minimize
$$L_p(w,b,\alpha) = \frac{1}{2} \|w\|^2 - \sum_{i=1}^n \alpha_i (y_i(x_i \cdot w + b) - 1)$$

$$s.t \quad \alpha_i \ge 0$$

We star solving this problem:

$$\frac{\partial L_p}{\partial \mathbf{w}} = 0 \qquad \mathbf{w} = \sum_{i=1}^n \alpha_i y_i \mathbf{x}_i$$

$$\frac{\partial L_p}{\partial b} = 0 \qquad \sum_{i=1}^n \alpha_i y_i = 0$$

21

21

SVM: Linear separable case.

Inroducing The Legrangin Dual Problem.

By substituting the above results in the primal problem and doing some math manipulation we get: Lagrangian Dual Problem:

$$\begin{aligned} \text{maximaize } L_D(\alpha) &= \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=0}^n \sum_{j=0}^n \alpha_i \alpha_j y_i y_j x_i^t x_j \\ s.t & \alpha_i \geq 0 \ \ and \ \sum_{i=1}^n \alpha_i y_i = 0 \end{aligned}$$

 $\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ are now our variables, one for each sample point x_i .

Finding "w" and "b" for the boundary $w^t x + b$:

Using the KKT (Karush-Kuhn-Tucker) condition:

$$\forall i \ \alpha_i \left(y_i (\mathbf{w}^T \mathbf{x}_i + b) - 1 \right) = 0$$

-We can calculate "b" by taking "i" such that $\alpha_i > 0$:

Must be
$$y_i(w^t x_i + b) - 1 = 0 \Rightarrow b = \frac{1}{y_i} - w^t x_i = \underline{y_i - w^t x_i}$$
 $(y_i \in \{1, -1\})$

- -Calculating "w" will be done using what we have found above : $w = \sum_{i} \alpha_{i} y_{i} x_{i}$
- -Usually ,Many of the α_i -s are zero so the calculation of "w" has a low complexity.

23

23

SVM: Linear separable case.

The importance of the Support Vectors:

- -Samples with $\alpha_i > 0$ are the Support Vectors: the closest samples to the separating hyperplane.
- -So $\mathbf{w} = \sum_{i=1}^{n} \alpha_i y_i \mathbf{x}_i = \sum_{i=SV} \alpha_i y_i \mathbf{x}_i$.
- -And $b = y_i w^t x_i$ such that x_i is a support vector.
- -We see that the separating hyperplane $w^t x + b$ is completely defined by the support vectors.
- -Now our Decision Function is:

$$f(x) = sign(w^{t}x + b) = sign(\sum_{i \in SV} \alpha_{i} y_{i} x_{i} \cdot x + b)$$

Some notes on the dual problem:

$$\begin{aligned} \text{maximaize } L_D(\alpha) &= \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=0}^n \sum_{j=0}^n \alpha_i \alpha_j y_i y_j x_i^t x_j \\ st & \alpha_i \ge 0 \quad and \quad \sum_{i=1}^n \alpha_i y_i = 0 \end{aligned}$$

-This is a quadratic programming (QP) problem. A global maximum of $\ L_{\scriptscriptstyle D}(\alpha)$ can always be found

 $L_D(\alpha)$ Can be optimized using a QP software. Some examples are Loqo, cplex, etc. (see http://www.numerical.rl.ac.uk/qp/qp.html)

-But for SVM the most popular QP is Sequential Minimal Optimization (SMO): It was introduced by John C. Platt in 1999. And it is widely used because of its efficiency. [4]

25

25

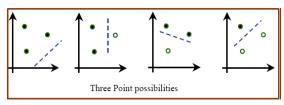
VC (Vapnik-Chervonenkis) Dimension

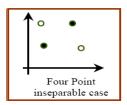


What if the sample points are not linearly separable ?!

Definition: "The VC dimension of a class of functions {fi} is the maximum number of points that can be separated (shattered) into two classes in all possible ways by {fi}." [6]

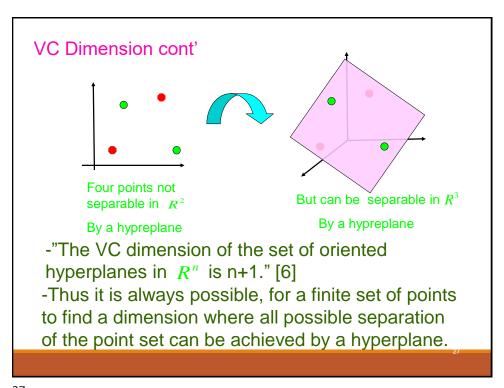
-if we look at any (non-collinear) three points in 2d plane they can be Linearly separated:

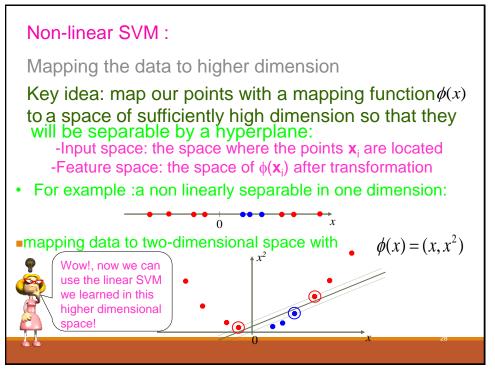




These images above are taken from....

 \rightarrow The VC dimension for a set of oriented lines in \mathbb{R}^2 is 3.





Non Linear SVM:

Mapping the data to higher dimension cont'

-To solve a non linear classification problem with a linear classifier all we have to do is to substitute $\phi(x)$ Instead of x everywhere where x appears in the optimization problem:

maximize
$$L_D(\alpha) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j y_i y_j x_i^t x_j$$
 s.t $\alpha_i \ge 0$ $\sum_{i=1}^n y_i \alpha_i = 0$ Now it will be:

maximize
$$L_D(\alpha) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j y_i y_j \phi(x_i^t) \phi(x_j)$$
 s.t $\alpha_i \ge 0$ $\sum_{i=1}^n y_i \alpha_i = 0$

The decision function will be: $g(x) = f(\phi(x)) = sign(w^t \cdot \phi(x) + b)$

29

Non Linear SVM : An illustration of the algorithm: feature Space The solution in the input space

The Kernel Trick:

But Computations in the feature space can be costly because it may be high dimensional!

That's right! Working in high dimensional space is computationally expensive.

But luckily the kernel trick comes to rescue:

If we look again at the optimization problem:

maximize
$$L_D(\alpha) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j y_i y_j \phi(x_i^t) \phi(x_j)$$
 s.t $\alpha_i \ge 0$ $\sum_{i=1}^n y_i \alpha_i = 0$ And the decision function:

$$f(\phi(x)) = sign(w^t \phi(x) + b) = sign(\sum_{i=1}^{n} \alpha_i y_i \phi(x_i^t) \phi(x) + b)$$

No need to know this mapping explicitly nor do we need to know the dimension of the new space, because we only use the dot product of feature vectors in both the training and test.

31

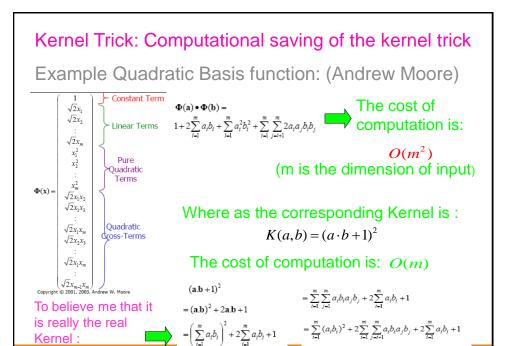
31

The Kernel Trick:

A *kernel function* is defined as a function that corresponds to a dot product of two feature vectors in some expanded feature space:

$$K(\mathbf{x}_i, \mathbf{x}_j) \equiv \phi(\mathbf{x}_i)^T \phi(\mathbf{x}_j)$$

Now we only need to compute $K(x_i, x_j)$ and we don't need to perform computations in high dimensional space explicitly. This is what is called the Kernel Trick.



Kernel:

Higher Order Polynomials (From Andrew Moore)

Poly- nomial	φ <i>(x)</i>	Cost to build Q_{kl} matrix tradition ally	Cost if m=100	ф <i>(а).</i> ф <i>(b)</i>	Cost to build Q_{kl} matrix sneakily	Cost if m=100
Quadratic	All <i>m</i> ² /2 terms up to degree 2	m² R² /4	2,500 <i>R</i> ²	(a.b+1)²	mR ² /2	50 <i>R</i> ²
Cubic	All m³/6 terms up to degree 3	m³ R²/12	83,000 <i>R</i> ²	(a.b+1) ³	mR ² /2	50 R ²
Quartic	All m4/24 terms up to degree 4	m4 R2 /48	1,960,000 R ²	(a.b+1)⁴	mR ² /2	50 <i>R</i> ²

R is the number of samples, m is the dimension of the sample points.

$$Q_{kl} = y_k y_l \phi(x_k) \phi(x_l) \qquad 1 \le k, l \le R$$

The Kernel Matrix

(a.k.a. the Gram matrix):

$$\mathsf{K} = \begin{bmatrix} \mathsf{K}(1,1) & \mathsf{K}(1,2) & \mathsf{K}(1,3) & \dots & \mathsf{K}(1,\mathsf{m}) \\ \mathsf{K}(2,1) & \mathsf{K}(2,2) & \mathsf{K}(2,3) & \dots & \mathsf{K}(2,\mathsf{m}) \\ & & & & & & \\ \vdots & & & & & & \\ \mathsf{K}(\mathsf{m},1) & \mathsf{K}(\mathsf{m},2) & \mathsf{K}(\mathsf{m},3) & \dots & \mathsf{K}(\mathsf{m},\mathsf{m}) \\ \end{bmatrix}$$

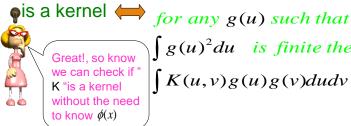
- -The central structure in kernel machines
- -Information 'bottleneck': contains all necessary information for the learning algorithm.
- -one of its most interesting properties: Mercer's Theorem.

based on notes from www.support-vectors.com

35

Mercer's Theorem:

- -A function $K(x_i, x_i)$ is a kernel (there exists a $\phi(x)$ such that $K(\mathbf{x}_i, \mathbf{x}_i) \equiv \phi(\mathbf{x}_i)^T \phi(\mathbf{x}_i)$ The Kernel matrix is Symmetric Positive Semi-definite.
 - -Another version of mercer's theorem that isn't related to the kernel matrix is: $K(x_i, x_i)$ function



$$\int g(u)^2 du \quad is finite then$$

$$\int K(u,v)g(u)g(v)dudv \ge 0$$

Examples of Kernels:

- -Some common choices (the first two always satisfying Mercer's condition):
- -Polynomial kernel $K(x_i, x_j) = (x_i^t x_j + 1)^p$
- -Gaussian Radial Basis Function "RBF" (data is lifted to infinite dimension): $K(x_i, x_j) = \exp(-\frac{1}{2\sigma^2} ||x_i x_j||^2)$
- -Sigmoidal: $K(x_i, x_j) = \tanh(kx_i \cdot x_j \delta)$ (it is not a kernel for every k and δ).
- -In fact, SVM model using a sigmoid kernel function is equivalent to a two-layer, feed-forward neural network.

37

37

Making Kernels:

Suppose

- lacksquare K_1 and K_2 are both kernels over $X \times X, X \subseteq \mathbb{R}^d$
- f is a real-valued function over X
- lacksquare Φ is a feature map from X to \mathbb{R}^m
- K_3 is a kernel over $\mathbb{R}^m \times \mathbb{R}^m$
- B is a positive semi-definite $d \times d$ matrix

Then the following are all kernels:

$$K(\mathbf{a}, \mathbf{b}) = K_1(\mathbf{a}, \mathbf{b}) + K_2(\mathbf{a}, \mathbf{b})$$

$$K(\mathbf{a}, \mathbf{b}) = \alpha K_1(\mathbf{a}, \mathbf{b})$$

$$K(\mathbf{a}, \mathbf{b}) = K_1(\mathbf{a}, \mathbf{b})K_2(\mathbf{a}, \mathbf{b})$$

$$K(\mathbf{a}, \mathbf{b}) = f(\mathbf{a})f(\mathbf{b})$$

$$K(\mathbf{a}, \mathbf{b}) = K_3(\Phi(\mathbf{a}), \Phi(\mathbf{b}))$$

$$K(\mathbf{a}, \mathbf{b}) = \mathbf{a}^T B \mathbf{b}$$

Now we can make complex kernels from simple ones:

Modularity!

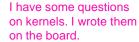


Taken from (CSI 5325) SVM

cture [7]

3

Important Kernel Issues:



How to know which Kernel to use?

-This is a good question and actually still an open question, many researches have been working to deal with this issue but still we don't have a firm answer. It is one of the weakness of SVM. We will see an approach to this issue latter.

How to verify that rising to higher dimension using a specific kernel will map the data to a space in which they are linearly separable?

For most of the kernel function we don't know the corresponding mapping function $\phi(x)$ so we don't know to which dimension we rose the data. So even though rising to higher dimension increases the likelihood that they will be separable we can't guarantee that . We will see a compromising solution for this problem.

39

39

Important Kernel Issues:

We saw that the Gaussian Radial Basis Kernel lifts the data to infinite dimension so our data is always separable in this space so why don't we always use this kernel?

First of all we should decide which σ to use in this kernel ($\exp(-\frac{1}{2\sigma^2}||x_i-x_j||^2)$).

Secondly, A strong kernel, which lifts the data to infinite dimension, sometimes may lead us the severe problem of Overfitting:

Symptoms of overfitting:

- 1) Low margin → poor classification performance.
- 2) Large number of support vectors → Slows down the computation.

Important Kernel Issues:

3) If we look at the kernel matrix then it is almost diagonal. This means that the points are orthogonal and only similar to itself.

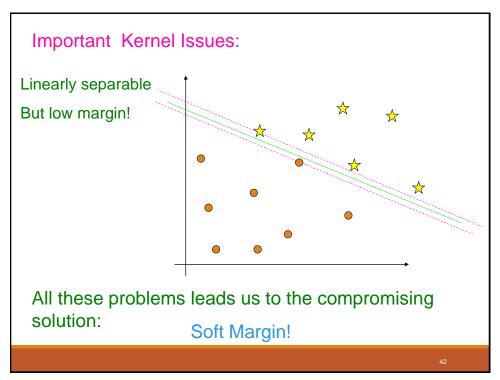
All these things lead us to say that our kernel function is not really adequate. Since it does not generalize good over the data.

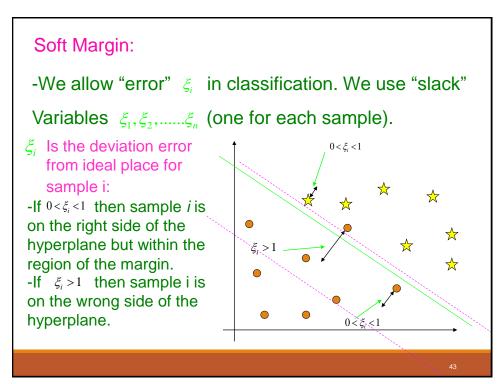
-It is good to say that Gaussian radial basis function (RBF) is widely used, BUT not alone because their got to be a tool to release some pressure of this strong kernel.

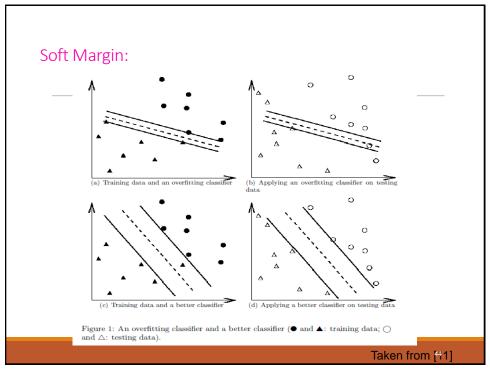
In addition to the above problems, another problem is that sometimes the points are linearly separable but the margin is Low:

41

41







Soft Margin:

The primal optimization problem

-We change the constrains to $y_i(w^ix_i+b) \ge 1-\xi_i \quad \forall i \quad \xi_i \ge 0$ instead of $y_i(w^ix_i+b) \ge 1 \quad \forall i$.

Our optimization problem now is:

$$\text{minimize } \frac{1}{2} \left\| \mathbf{w} \right\|^2 + C \sum_{i=1}^n \xi_i$$

Such that: $y_i(w^t x_i + b) \ge 1 - \xi_i \quad \forall i \quad \xi_i \ge 0$

 $C > O_n$ is a constant. It is a kind of penalty on the term $\sum_{i=1}^{n} \xi_i$. It is a tradeoff between the margin and the training error. It is a way to control overfitting along with the maximum margin approach[1].

45

Soft Margin:

The Dual Formulation.

Our dual optimization problem now is:

maximize
$$\sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j \mathbf{x}_i^T \mathbf{x}_j$$

Such that:

$$0 \le \alpha_i \le C \quad \forall i \quad and \quad \sum_{i=1}^n \alpha_i y_i = 0$$

-We can find "w" using : $w = \sum_{i=1}^{n} \alpha_i y_i x_i$

-To compute "b" we take any $0 < \alpha_i < C$ and solve for "b".

$$\alpha_i[y_i(w^t x_i + b) - 1] = 0$$

$$\alpha_i = 0 \Rightarrow y_i(w^T x_i + b) > 1$$

$$0 < \alpha_i < C \Rightarrow y_i(w^T x_i + b) = 1$$

Which value for "C" should we choose.

 $\alpha_i = C \Rightarrow y_i(w^T x_i + b) < 1 \quad \text{(points with } \xi_i > 0\text{)}$

Soft Margin:

The "C" Problem

- -"C" plays a major role in controlling overfitting.
- -Finding the "Right" value for "C" is one of the major problems of SVM:
- -Larger C → less training samples that are not in ideal position (which means less training error that affects positively the Classification Performance (CP)) But smaller margin (affects negatively the (CP)). C large enough may lead us to overfitting (too much complicated classifier that fits only the training set)
- -Smaller C → more training samples that are not in ideal position (which means more training error that affects negatively the Classification Performance (CP)) But larger Margin (good for (CP)). C small enough may lead to underffiting (naïve classifier)

47

