

Lecture: Machine Learning for Data Science

Winter semester 2021/22

Lectures 7: Classification (Support vector machines)

Prof. Dr. Eirini Ntoutsi

Outline

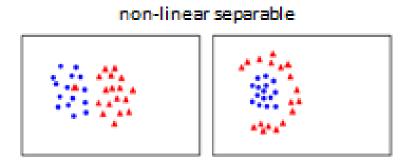
- Class of linear classifiers
- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

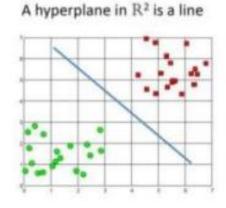
Basic idea

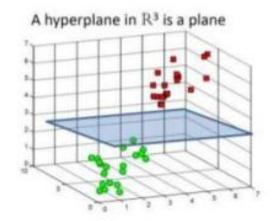
Assumption: The classes are linearly separable

linear separable

- Goal: find a classifier that will separate the data based on their class
 - In 2D, this is just a straight line
 - □ In higher dimensions, a hyperplane





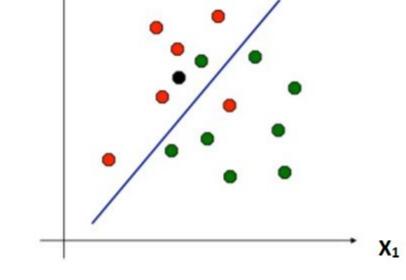


A hyperplane in Rn is an n-1 dimensional subspace

- Consider a simple binary classification problem.
 - Let training set, $D=\{(\overrightarrow{x_i},y_i)\}$ and each instance is described in the d-dimensional feature space: $(X_1,X_2,...,X_d)$
 - Let class Y = {-1,1}
- The decision function is linear in the features:

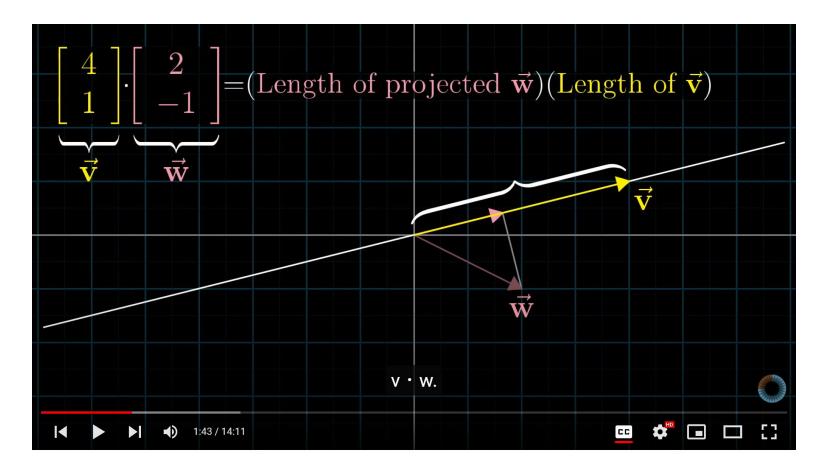
$$f(x) = w \cdot x + b = \sum_{i=1}^{a} w_i x_i + b$$

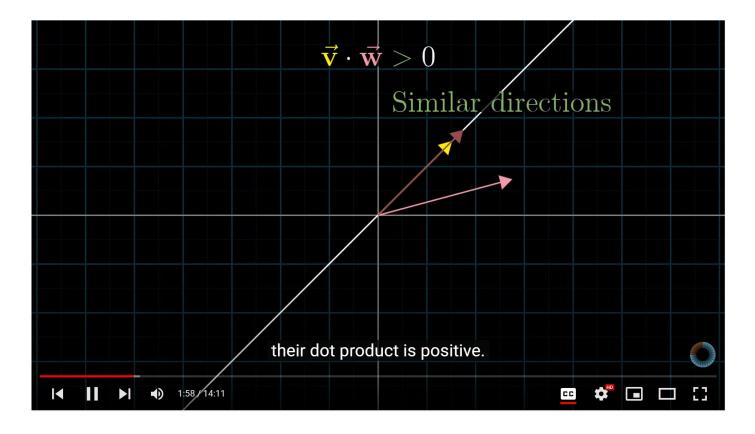
- orientation is defined by w
 - w is a d-dimensional vector (the weight vector)
- \Box offset from origin is defined by b (bias)
 - b is a scalar
- $w \cdot x$ is the dot product

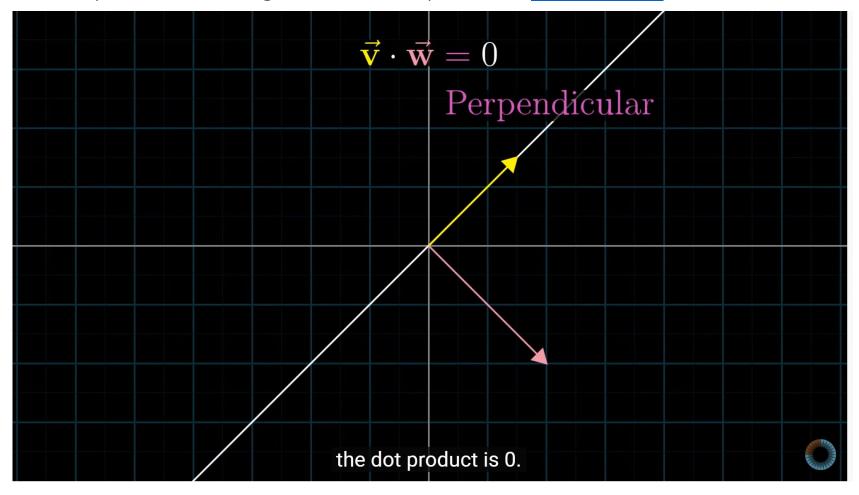


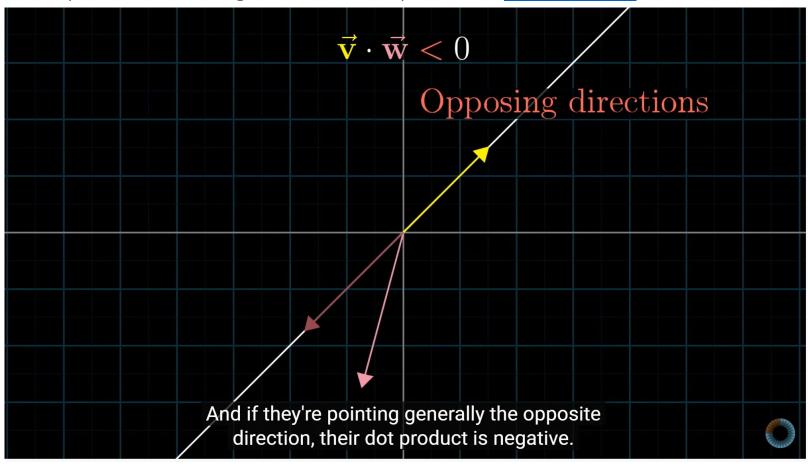
X₂ †

w and b are the parameters of the model (to be learned)







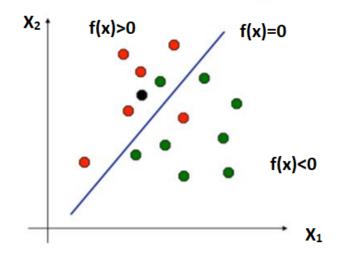


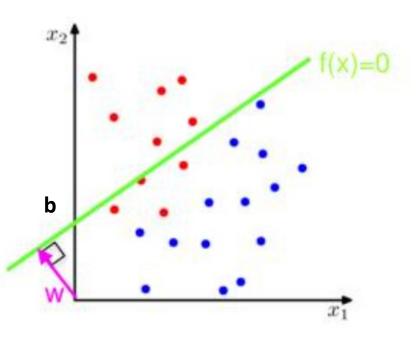
• Classification is based on the sign of f(x)

$$f(x) = \begin{cases} +1, & \text{if } \sum_{i=1}^{d} w_i x_i + b > 0 \\ -1, & \text{if } \sum_{i=1}^{d} w_i x_i + b < 0 \end{cases}$$

The decision boundary is a (d-1)-dimensional hyper-plane orthogonal to w given by

$$f(x) = 0 \Rightarrow w \cdot x + b = 0 \Rightarrow \sum_{i=1}^{d} w_i x_i + b = 0$$





Class of linear classifiers

• The class of linear classifiers (also called, halfspaces) H₁ is a class of functions of the form

$$f(x) = w \cdot x + b = \sum_{i=1}^{a} w_i x_i + b$$

- A very important class of predictors as the weights indicate the importance of the different features in the prediction
- Remember the Pacman example from the AI lecture
 - Instances refer to states and we could describe a state through different features
 - Distance to closest ghost → f₁
 - Distance to closest dot → f₂
 - Number of ghosts \rightarrow f_3
 - **...**
 - Goal was to find whether a state is good or not

$$V(s) = w_1 f_1(s) + w_2 f_2(s) + \dots + w_n f_n(s) = \sum_{i=1}^n w_i f_i(s)$$

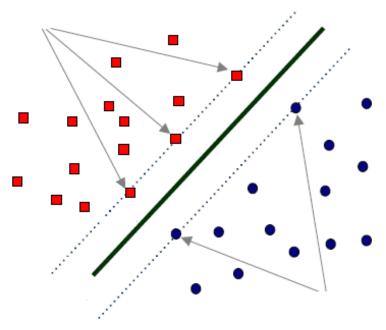


Outline

- Class of linear classifiers
- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

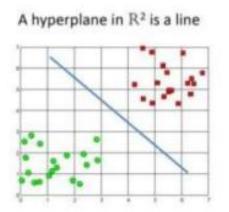
Support Vector Machines (SVM)

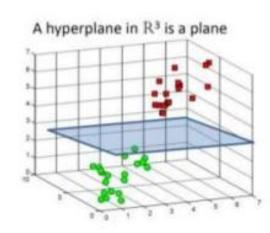
- A popular classification method
- Its roots are in statistical learning theory
- Promising results in many applications, e.g., handwritten text classification, text categorization
- The decision boundary is represented using a subset of the training instances, the so-called support vectors.



Basic idea: Class separation by hyperplanes

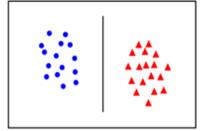
- Lets start with a simple 2 class problem and lets assume linear separability (we will relax this later)
- Goal: find a decision boundary (hyperplane) that will separate the data based on their class
 - In 2D, this is just a straight line
 - In higher dimensions, a hyperplane

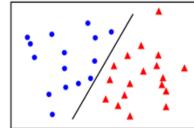




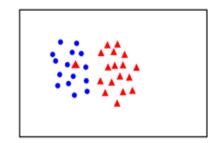
A hyperplane in Rn is an n-1 dimensional subspace

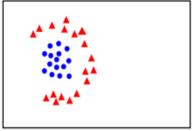
linear separable





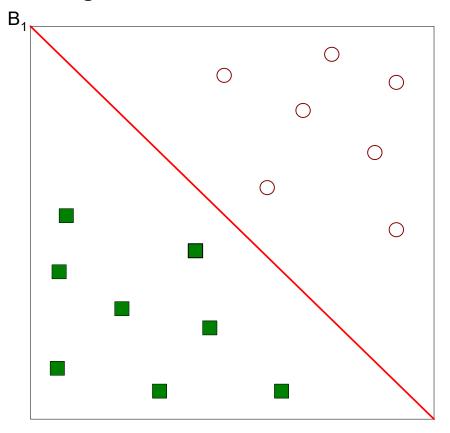
non-linear separable





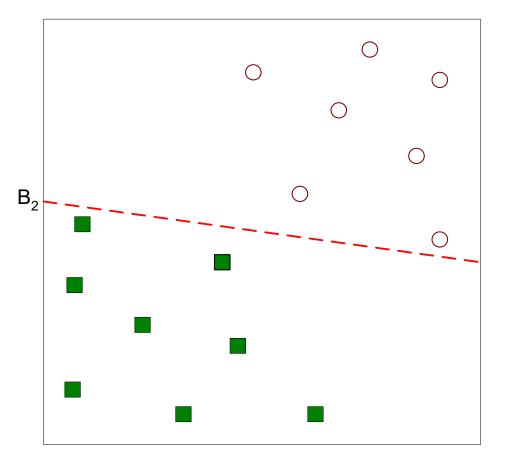
Finding a separating hyperplane

- Consider the following running example (2D for simplicity, so the hyperplane is a line)
- A possible solution is the following:



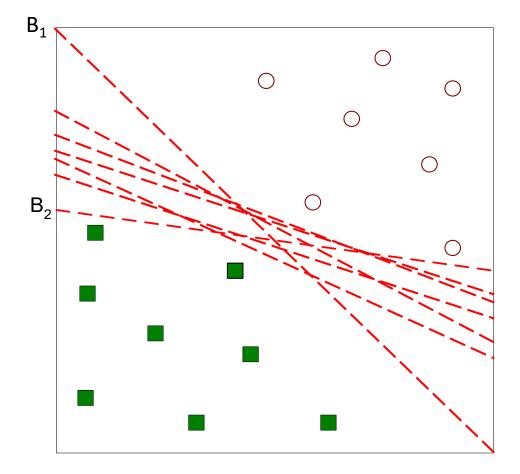
Finding a separating hyperplane

Another possible solution



Finding a separating hyperplane

- Lots of possible solutions
- All with 0 error in the training data
- But we want to choose a hyperplane that is expected to work well on future unseen instances of the population.
 - □ i.e., a hyperplane that can generalize

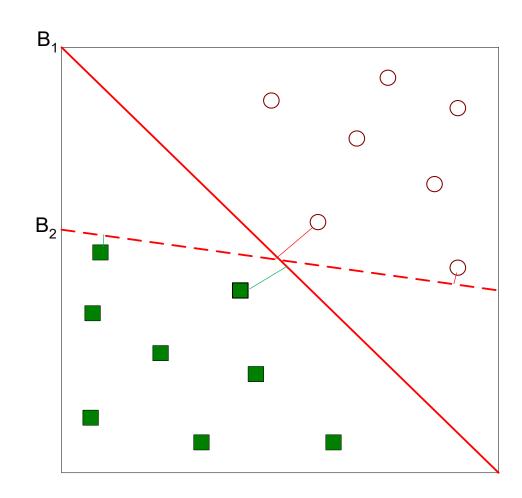


Choosing the best hyperplane

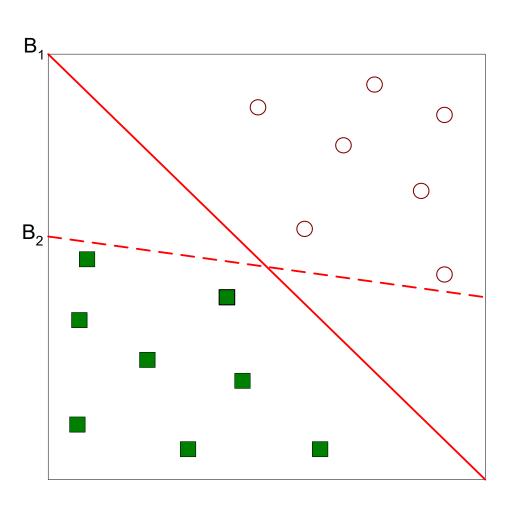
• Which hyperplane is better B_1 or B_2 ?

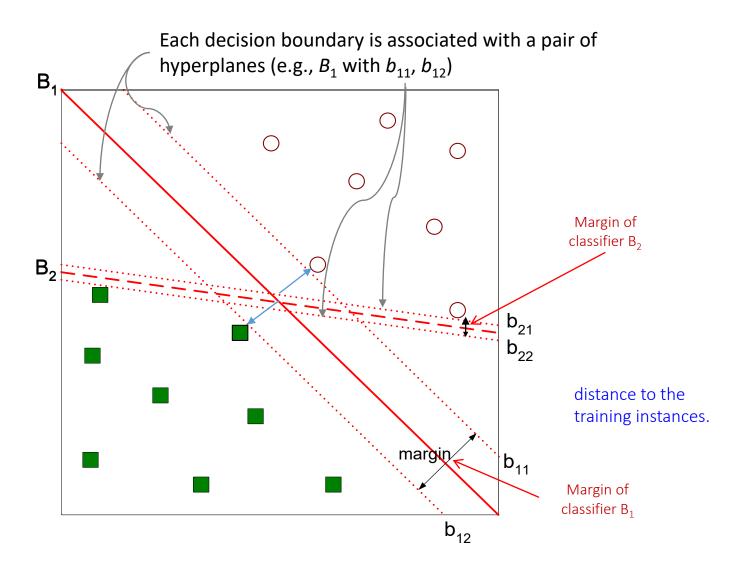


- How to define better? We need to evaluate somehow the hyperplanes/ lines.
 - Intuitively, a line is bad if it passes too close to the training instances
 - because it will be noise sensitive and will generalize poorly.
 - Therefore, our goal should be to find the line (hyperplane in general) that results in the largest minimum distance to the training instances.
 - Twice this distance is called margin.



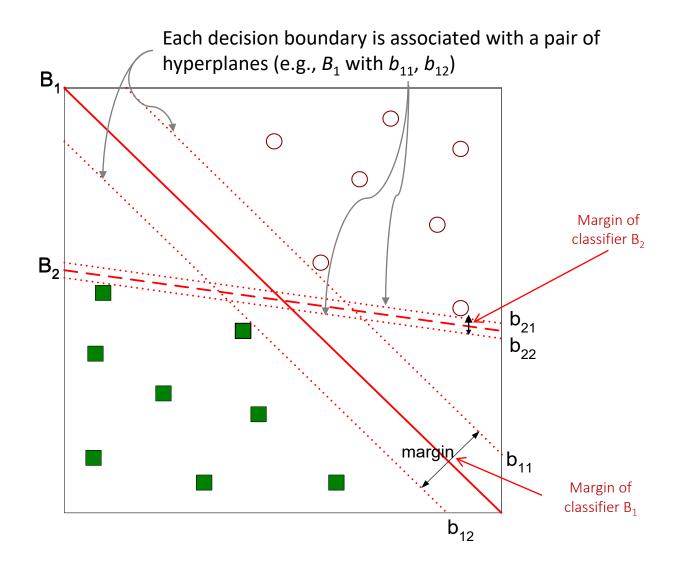
Choosing the best hyperplane





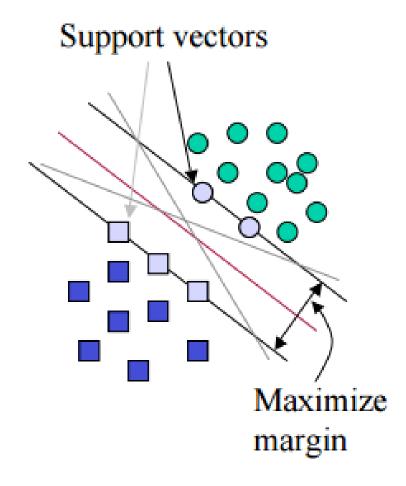
Choosing the best hyperplane

- Goal: Find the hyperplane that <u>maximizes</u> the margin (represents largest class separation)
- In our example, which hyperplane is better B_1 or B_2 ?
 - B_1 is better than B_2



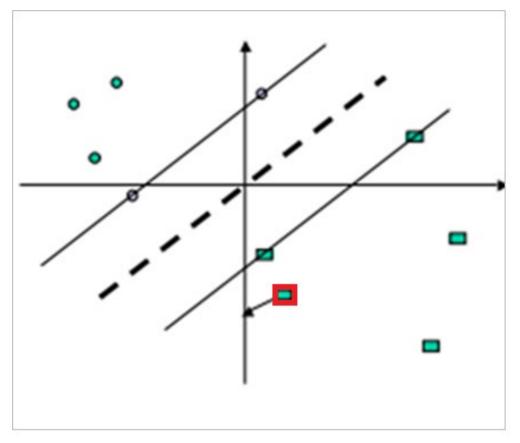
Support vectors

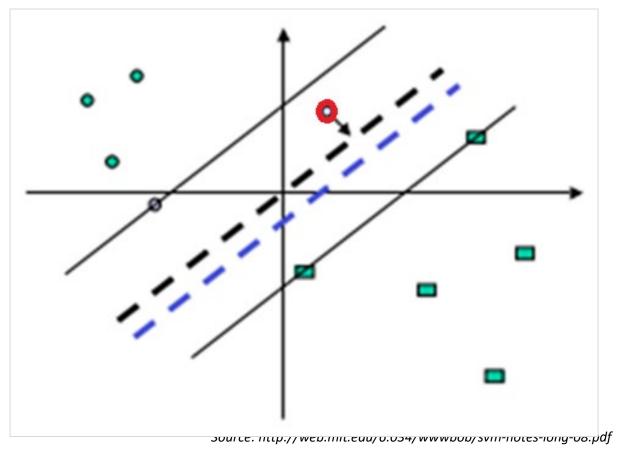
- SVMs maximize the margin (Winston terminology: the 'street') around the separating hyperplane
- The decision function is fully specified by a (usually very small) subset of training samples, the support vectors.
- Support vectors are the data points that lie closest to the decision boundary
 - They are the most difficult to classify
- Support vectors are critical elements
 - If removed, they would change the position of the dividing hyperplane



The criticality of support vectors

- Moving the non-support vectors has no effect on the decision boundary
- Moving a support vector moves the decision boundary





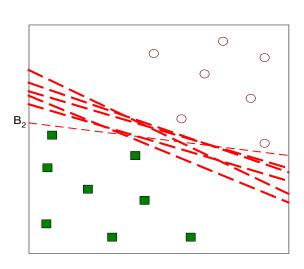
Outline

- Class of linear classifiers
- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

- A linear SVM searches for a hyperplane that maximizes the margin (maximal margin classifier)
- Consider a simple binary classification problem. Let training set, $D = \{(\vec{x_i}, y_i)\}$ and
 - Each instance is described in the d-dimensional feature space: $(X_1, X_2, ..., X_d)$
 - Let class Y = {-1,1}
- The decision boundary of a linear classifier can be written as follows:

$$w \cdot x_i + b = 0$$

- w is a weight vector
- x_i is the input vector (instance)
- b is a scalar (bias)
- w and b are the parameters of the model



 The linear classifier is the hyperplane H characterized by parameters w and b

$$w \cdot x_i + b = 0$$

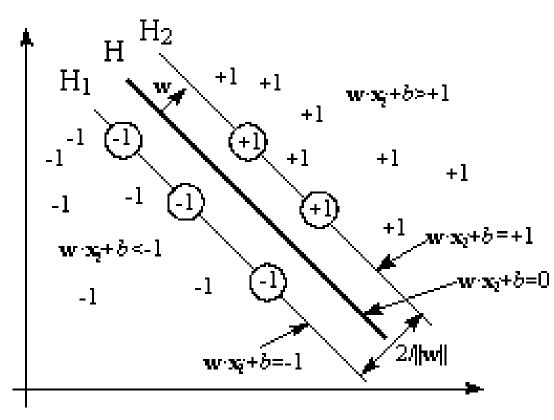
• For any instance x_i in the training set, the decision boundary H must satisfy the following inequalities:

$$w \cdot x_i + b \ge +1$$
 when $y_i = +1$
 $w \cdot x_i + b \le -1$ when $y_i = -1$

For the associated hyperplanes H_1 and H_2 it holds:

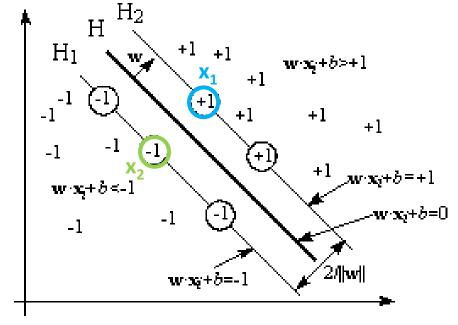
$$H_2$$
: $w \cdot x_i + b = +1$
 H_1 : $w \cdot x_i + b = -1$

- The points on the planes H_1 , H_2 are the support vectors
- The aforementioned conditions are also applicable to any linear classifiers, SVMs imposes an additional requirement regarding the margin



Source: http://www.support-vector-machines.org/SVM_osh.html

- The margin of hyperplane H is given by the distance between the two hyperplanes H_1, H_2 .
- Let x_1 , x_2 be two points in H_2 , H_1 respectively.
 - $w \cdot x_1 + b = +1$
 - $w \cdot x_2 + b = -1$
- From geometry, distance of point x_i from hyperplane: $\frac{|\mathbf{x}_i \cdot \mathbf{w} + b|}{\|\mathbf{w}\|}$
- Distance of x_1 from H: = $\frac{1}{\|w\|}$
- Distance of x_2 from H: $=\frac{1}{\|w\|}$



Source: http://www.support-vector-machines.org/SVM_osh.html

- So the margin which we want to maximize is given by

 $\| w \| = \sqrt{w \cdot w}$ is the Euclidean norm/length:

So, we want to maximize

Margin
$$d = \frac{2}{\|w\|}$$

- In order to maximize d, we need to minimize $\| w \|$
 - actually, we minimize the following:

$$\min_{w} \frac{\|w\|}{2} \iff \min_{w} \frac{\|w\|^2}{2}$$

but, subject to the following constraints

//This allows us to perform quadratic programming optimization latter on

$$\mathbf{y}_{i} = \begin{cases} +1, & if \ \mathbf{w} \cdot \mathbf{x}_{i} + b \ge +1 \\ -1, & if \ \mathbf{w} \cdot \mathbf{x}_{i} + b \le -1 \end{cases}$$

(i.e., there are no data points between H_1 and H_2)



or, alternatively

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

Definition: (Hard Margin) Linear SVM: Separable case

$$\min_{w} \frac{\|w\|^2}{2}$$

subject to

$$y_i(\boldsymbol{w} \cdot \boldsymbol{x}_i + b) \ge 1, x_i \in D$$

- This is a constrained optimization problem
 - The objective function is quadratic
 - The constraints are linear on model parameters w, b
 - This is convex optimization problem, which can be solved using the <u>Lagrange multiplier method</u>
 - A technique that lets you find the maximum or minimum of a multivariable function when there is some constraint on the input values you are allowed to use.

- Goal: Minimize $\min_{w} \frac{\|w\|^2}{2}$ subject to $y_i(w \cdot x_i + b) \ge 1$
- Introduce Langrange multipliers $a_i \ge 0 \ \forall i$; there is an a_i for each training instance
- Define the auxiliary objective function L_P

$$L_P = \frac{1}{2} ||\mathbf{w}||^2 - \sum_{i=1}^n \alpha_i (y_i(\mathbf{x}_i, \mathbf{w} + b) - 1)$$

• Minimize L_P w.r.t. w, b.

$$\frac{\partial L}{\partial \mathbf{w}} = \left(\mathbf{w} - \sum_{i=1}^{n} \alpha_{i} y_{i} \mathbf{x}_{i}\right) = 0$$

$$\frac{\partial L}{\partial b} = \sum_{i=1}^{n} \alpha_{i} y_{i} = 0$$

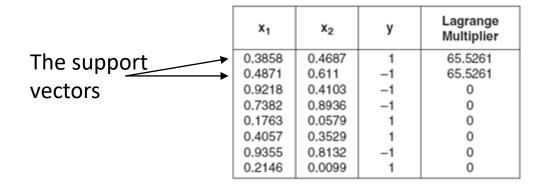
- Points with α_i >0 are called support vectors and lie on H_1 or H_2 .
- Points with $\alpha_i=0$ lie beyond margin planes and are irrelevant to the solution.

- The solution (trained SVM) consists of:
 - □ The support vectors x_i (those instances with $\alpha_i > 0$)
- Based on which, we can also compute the parameters w, b of the decision boundary
- The plane is a linear combination of the training vectors:

$$\boldsymbol{w} = \sum_{i=1}^{n} \alpha_{i} y_{i} \boldsymbol{x}_{i}$$

 b can be computed using the plane equation for each support vector:

$$f(x_i) = wx_i + b \rightarrow b = f(x_i) - wx_i$$



Linear SVM – an example of computing model parameters

- Find a linear SVM for the given 2D dataset:
 - \Box After we find the support vectors α_i :
 - We compute the parameters of the plane:

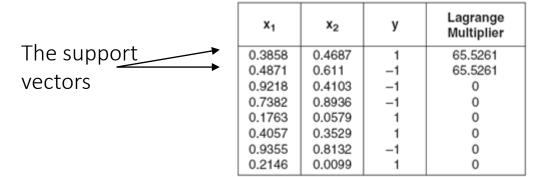
$$\boldsymbol{w} = \sum_{i=1}^n \alpha_i y_i \boldsymbol{x}_i$$

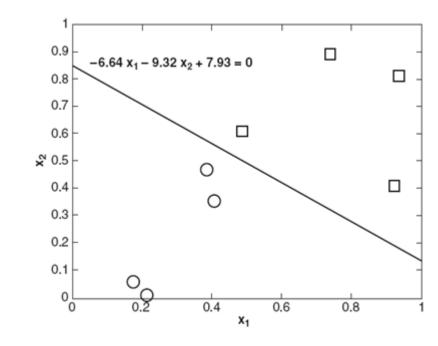
Computing w:

$$w_1 = \sum_{i=1}^{N} \alpha_i y_i x_{i1} = 65.5621 * 1 * 0,3858 + 65.5621 * -1 * 0,4871 = -6,64$$

$$w_2 = \sum_{i=1}^{N} \alpha_i y_i x_{i2} = 65.5621 * 1 * 0,4687 + 65.5621 * -1 * 0,611 = -9,32$$

- Computing b:
 - $f(x_i) = wx_i + b \implies b = f(x_i) wx_i$ $b^{(1)} = 1 wx_1 = 1 (-6,64)(0,3858) (-9,32)(0,4687)$ $b^{(2)} = -1 wx_2 = \dots$ $b = avg(b^{(1)}, b^{(2)})$





Linear SVM – Classifying new instances

- How can we classify a new instance x_i ?
- Let $Ns \subseteq D$ be the set of support vectors, with $s_i = x_i$
- The classification of a new point x_i is given by the sign of:

$$f(x_j) = sign(wx_j + b)$$

$$w = \sum_{i=1}^{n} \alpha_i y_i x_i$$

$$f(x_j) = sign(\sum_{i=1}^{N_s} \alpha_i y_i s_i \cdot x_j + b)$$

- a_i : Lagrange multipliers
- s_i : is the support vector
- y_i : is the class of s_i

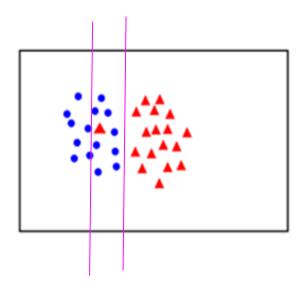
Note that the decision relies on the inner product between x_i and the support vectors $s_i=x_i$

Outline

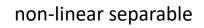
- Class of linear classifiers
- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

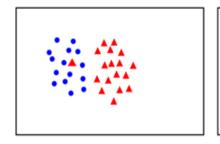
Linear SVM nonseparable cases

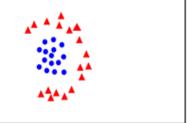
- What if the problem is not linearly separable?
 - There is no hyperplane that makes no mistakes on training data



linear separable

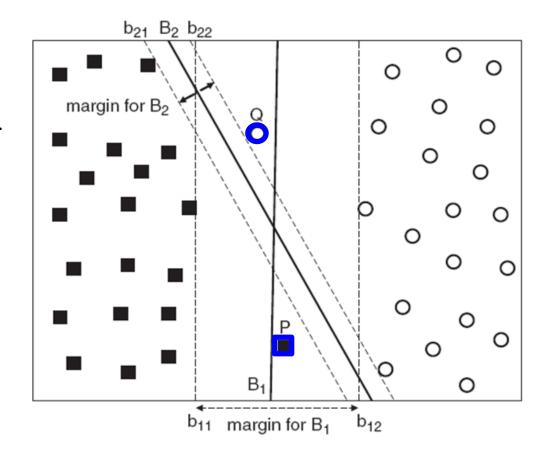






Even in linear separable cases

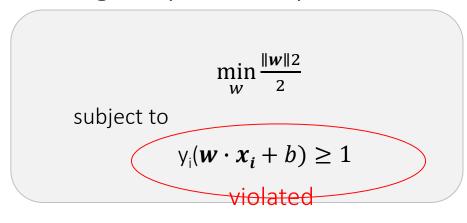
- **?** Which hyperplane is better B_1 or B_2 ?
 - We might prefer a solution that better separates the bulk of the data while ignoring a few weird noise points.
 - B_1 should be preferred over B_2
 - □ it has a wider margin → less susceptible to overfitting
 - but, the so far SVM formulation is error free
 - → Soft margin approach
 - Allows the margin to make some mistakes



Soft margin approach

- Learn a decision boundary that is tolerable to small training errors
- Allows SVM to construct a decision boundary even in cases where the classes are not linearly separable
- Idea: trade-off between the width of the margin and the misclassification errors committed by the linear decision boundary.

Original optimization problem



Idea:

- Relax the constraints to accommodate small training errors
- Introduce positive-valued slack variables ξ_i

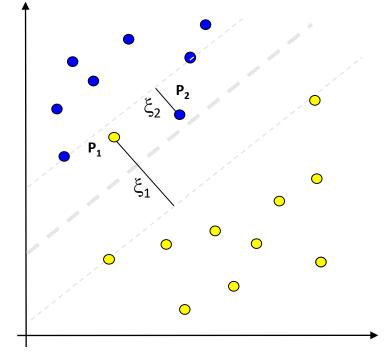
Soft margin approach

Relaxing by introducing slack variables ξ_i , $\xi_i \ge 0$

$$\mathbf{y_i} = \begin{cases} +1, & if \ \mathbf{w} \cdot \mathbf{x_i} + b \ge +1 \\ -1, & if \ \mathbf{w} \cdot \mathbf{x_i} + b \le -1 \end{cases}$$

$$\mathbf{y_i} = \begin{cases} +1, & if \ \mathbf{w} \cdot \mathbf{x_i} + b \ge +1 - \xi_i \\ -1, & if \ \mathbf{w} \cdot \mathbf{x_i} + b \le -1 + \xi_i \end{cases}$$

- The slack variable ξ_i provide an estimate of the error of the decision boundary on training instance x_i
- Intuitively, data points on the incorrect side of the margin boundary have a penalty that increases with the distance from it.
 - This allows x_i to not meet the margin requirement at a cost proportional to the value of ξ_i .
- Goal: find a line that penalize points in the "wrong side".



Soft margin approach

Original optimization problem

$$\min_{w} \frac{\|w\|^2}{2}$$

subject to

$$y_i(\boldsymbol{w} \cdot \boldsymbol{x}_i + b) \ge 1$$

Definition: Soft margin linear SVM

Need to minimize:

$$\min_{w} \frac{\|w\|^2}{2} + C\left(\sum_{i=1}^{n} \xi_i^k\right)$$

subject to the following constraints:

$$\mathbf{y}_{i} = \begin{cases} +1, & \text{if } \mathbf{w} \cdot \mathbf{x}_{i} + b \geq +1 - \xi_{i} \\ -1, & \text{if } \mathbf{w} \cdot \mathbf{x}_{i} + b \leq -1 + \xi_{i} \end{cases}$$

If no constrains on # mistakes, we might end up with a very wide margin with many misclassification errors

C, k are user-specified parameters representing the penalty of misclassifying the training instances

Relaxed constraints

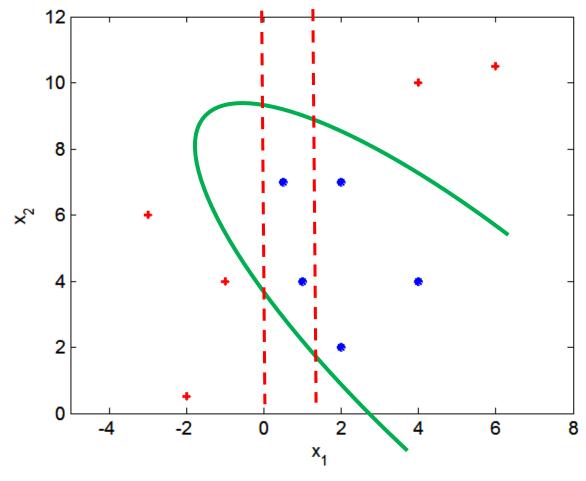
- Can be solved used quadratic programming
 - □ This way we can learn the parameters *w, b* of the decision boundary

Outline

- Class of linear classifiers
- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

Nonlinear SVM

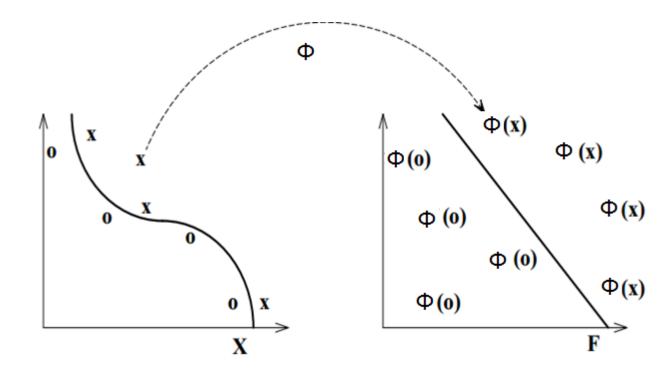
What if the decision boundary is not linear?



Machine Learning for Data Science: Lecture 6 - Classification (SVMs)

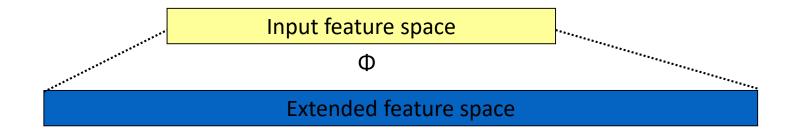
Transformation to separate

- Trick: transform the data from its original space X into a new space $\Phi(X)$ so that a linear decision boundary can be used to separate the instances in the transformed space
- In $\Phi(X)$, we can apply the same methodology as before to find a linear decision boundary

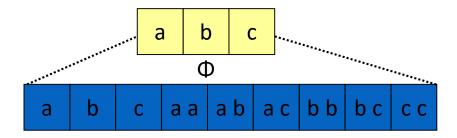


Transformation

Intuitively, we extend the hypothesis space



■ e.g.,



An example 1/2

Data is generated as follows:

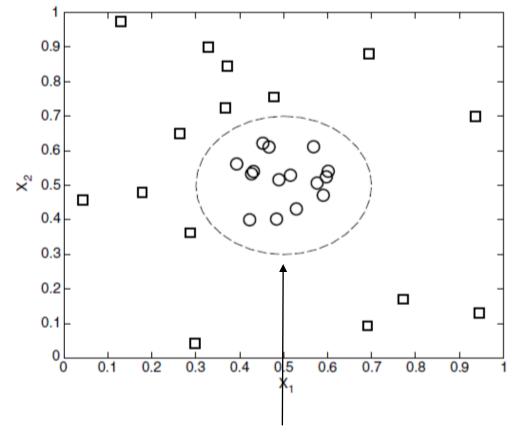
$$y(x_1, x_2) = \begin{cases} 1 & \text{if } \sqrt{(x_1 - 0.5)^2 + (x_2 - 0.5)^2} > 0.2, \\ -1 & \text{otherwise.} \end{cases}$$

The decision boundary can be written as:

$$\sqrt{(x_1 - 0.5)^2 + (x_2 - 0.5)^2} = 0.2,$$

or, alternatively:

$$x_1^2 - x_1 + x_2^2 - x_2 = -0.46.$$



Decision boundary in the original space is elliptical

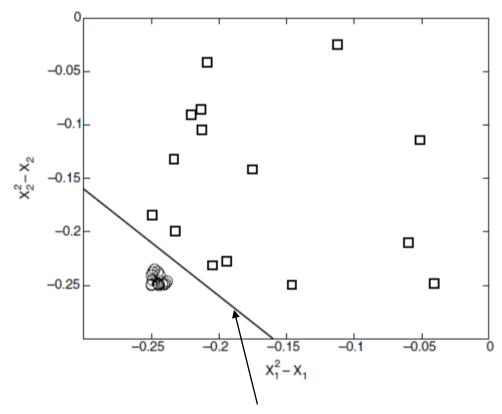
An example 2/2

 A non-linear transformation Φ maps the data into a new space.

$$\Phi: (x_1, x_2) \longrightarrow (x_1^2, x_2^2, \sqrt{2}x_1, \sqrt{2}x_2, 1)$$

• In the transformed space, we can find the parameters of the boundary $w = (w_1, w_2, w_3, w_4)$

$$w_4x_1^2 + w_3x_2^2 + w_2\sqrt{2}x_1 + w_1\sqrt{2}x_2 + w_0 = 0.$$



In the transformed space, the decision boundary becomes linear

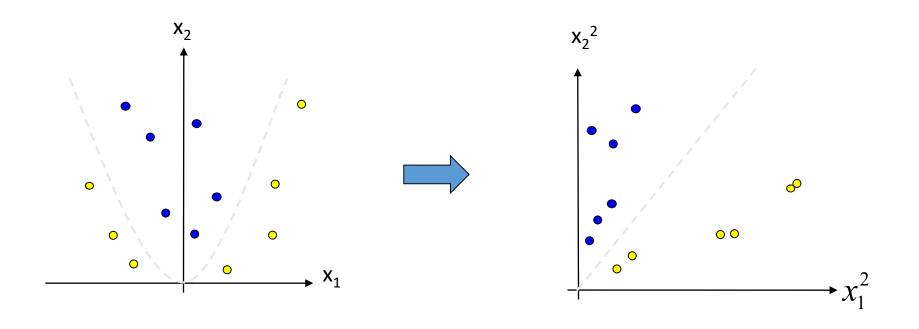
Another example

Input space (2D):

Extended space (6D):

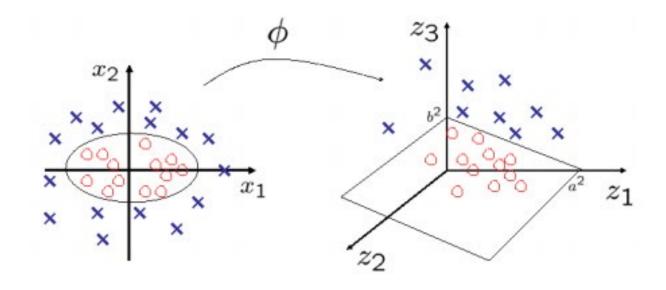
$$\vec{x} = (x_1, x_2)$$

$$\phi(\vec{x}) = (x_1^2, x_2^2, \sqrt{2} \cdot x_1, \sqrt{2} \cdot x_2, \sqrt{2} \cdot x_1 \cdot x_2, 1)$$



Another example

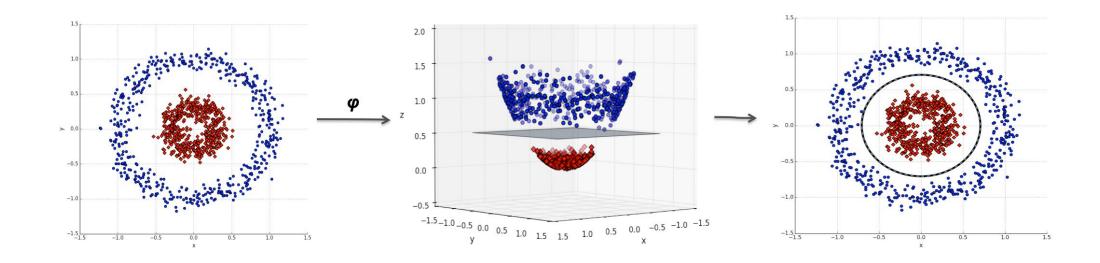
Elliptical boundary in the input space becomes linear in the transformed space



$$\phi: [x_1, x_2]^T \to [x_1^2, \sqrt{2}x_1x_2, x_2^2]^T$$

Another example

The data is linearly separable in the transformed space



Nonlinear SVM definition

Updated definition

Need to minimize:

$$\min_{w} \frac{\|w\|^2}{2}$$

subject to the following constraints:

$$y_i(\mathbf{w} \cdot \Phi(\mathbf{x}_i) + b) \ge 1$$

Original optimization problem

$$\min_{w} \frac{\|w\|^2}{2}$$
 subject to

$$y_i(\boldsymbol{w} \cdot \boldsymbol{x}_i + b) \ge 1$$

We work in the transformed space

Original boundary wx + b = 0

- Can be solved used quadratic programming
 - This way we can learn the parameters w, b of the decision boundary

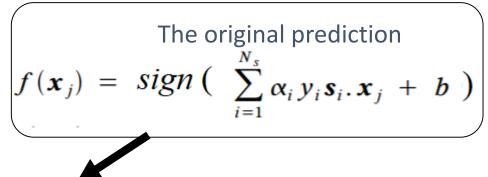
Transformed boundary $w\Phi(x) + b = 0$

Nonlinear SVM definition

- How can we classify a new instance x_i ?
- Main idea: Use the transformed space

$$f(x_j) = sign(\mathbf{w} \cdot \mathbf{\Phi}(\mathbf{x}_j) + b) = sign(\sum_{i=1}^n a_i \mathbf{y}_i \mathbf{\Phi}(\mathbf{x}_i) \mathbf{\Phi}(\mathbf{x}_j) + b)$$

- Involves calculating of the dot product(similarity) in the transformed space
 - computational problem (very large vectors)
 - curse of dimensionality



Kernel trick

- The kernel trick is a method for computing similarity between two instances in the transformed feature space using the original attribute set.
 - e.g., consider transformation

$$\Phi: (u_1, u_2) \to (u_1^2, u_2^2, \sqrt{2}u_1, \sqrt{2}u_2, \sqrt{2}u_1u_21)$$

□ The dot product between 2 input vectors *u*, *v* in the transformed space is:

$$\Phi(\mathbf{u}) \cdot \Phi(\mathbf{v}) = (u_1^2, u_2^2, \sqrt{2}u_1, \sqrt{2}u_2, \sqrt{2}u_1u_2, 1) \cdot (v_1^2, v_2^2, \sqrt{2}v_1, \sqrt{2}v_2, \sqrt{2}v_1v_2, 1)
= u_1^2 v_1^2 + u_2^2 v_2^2 + 2u_1 v_1 + 2u_2 v_2 + 2u_1 u_2 v_1 v_2 + 1
= (\mathbf{u} \cdot \mathbf{v} + 1)^2$$

So, we can express the dot product in $\mathcal{O}(x)$ in terms of a similarity function in the original feature

space kernel function

$$K(u,v) = \Phi(u)\Phi(v) = (uv+1)^2$$

A function that returns the dot product between the images of two vectors.

Kernels

- The main requirement for a kernel function in nonlinear SVM
- There must exist a transformation such that the kernel function computed for two vectors is equivalent to the dot product between these vectors in the transformed space.

$$K(u,v) = \Phi(u)\Phi(v)$$

Popular kernel functions

Linear

$$K(\vec{x}, \vec{y}) = \langle \vec{x}, \vec{y} \rangle$$

Polynomial

$$K(\vec{x}, \vec{y}) = \left(\left\langle \vec{x}, \vec{y} \right\rangle + c \right)^d$$

Gaussian kernel

$$K(\vec{x}, \vec{y}) = \exp\left(-\frac{\|\vec{x} - \vec{y}\|^2}{2\sigma^2}\right)$$

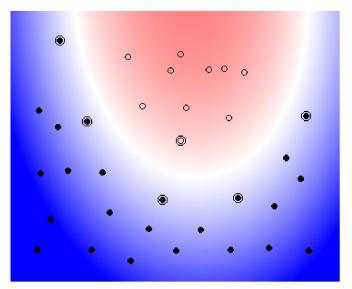
Radial basis function (RBF) kernel

$$K(\vec{x}, \vec{y}) = \exp\left(-\gamma \cdot \left| \vec{x} - \vec{y} \right|^2\right)$$

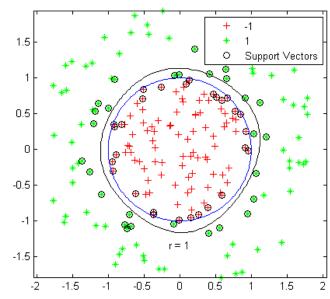
....

Choosing the right kernel depends on the problem at hand

Polynomial kernel (degree 2)



Gaussian kernel



SVM overview

- High accuracy classifiers
- Relatively weak tendency to overfitting
- Efficient classification of new objects
- Compact models
- Costly implementation
 - sometimes long training times
 - learned models difficult to interpret

Outline

- Support vector machines Basic intuition and basic notions
- (Hard-margin) Linear SVM
- Soft-margin linear SVM
- Non-linear SVM
- Things you should know from this lecture & reading material

Overview and Reading

Overview

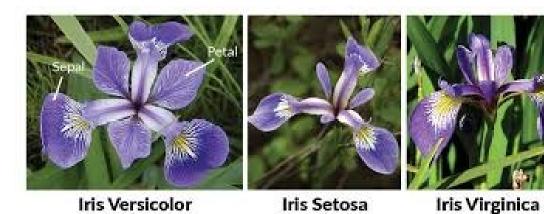
- Hard-margin linear SVMs
- Soft-margin linear SVMs
- Non-linear SVMs

Reading

- Chapter 15: Support Vector Machines, Understanding Machine Learning book by Shai Shalev-Schwartz and Shai Ben-David
- Dot products and duality | Chapter 9, Essence of linear algebra <u>Youtube</u>

Hands on experience

- Consider the favorite Iris dataset (or choose your favorite dataset)
- Experiment with different kernels and their parameters (if any)
- Plot the decision boundary
- Compare the results



Acknowledgements

- The slides are based on
 - □ KDD I lecture at LMU Munich (Johannes Aßfalg, Christian Böhm, Karsten Borgwardt, Martin Ester, Eshref Januzaj, Karin Kailing, Peer Kröger, Eirini Ntoutsi, Jörg Sander, Matthias Schubert, Arthur Zimek, Andreas Züfle)
 - □ Introduction to Data Mining book slides at http://www-users.cs.umn.edu/~kumar/dmbook/
 - Pedro Domingos Machine Lecture course slides at the University of Washington
 - Machine Learning book by T. Mitchel slides at http://www.cs.cmu.edu/~tom/mlbook-chapter-slides.html
 - C. Burges, A Tutorial on Support Vector Machines for Pattern Recognition, DMKD 1998
 - Thank you to all TAs contributing to their improvement, namely Vasileios Iosifidis, Damianos Melidis, Tai Le Quy, Han Tran.

Thank you

Questions/Feedback/Wishes?