CS 559: Machine Learning Fundamentals & Applications

Lecture 8: Supportive Vector Machine

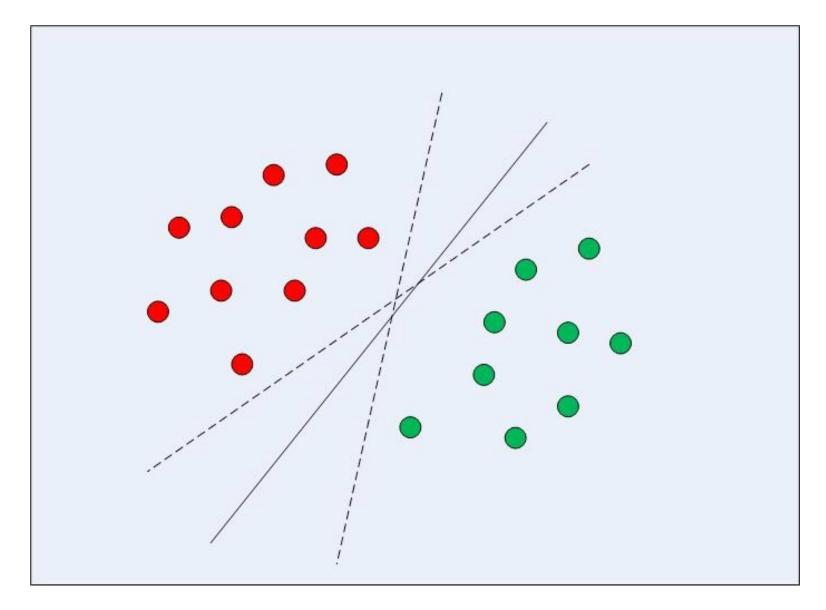




8.1. Motivation

8.1. Motivation





Lecture 8 - Support Vector Machine

8.1. Motivation



Recall the perceptron algorithm.

- 1. It guarantees to find a solution in a finite number of steps.
- 2. The solution of parameters depends on the *initially chosen values*.
- There can be multiple solutions all of which classify the training data set perfectly.
- Then what is the best model among them?
- We want to select the one that gives the smallest generalization error.



- 1870
- SVM was invented in 1963 by Vapnik and Chervonenkis to solve a classification problem.
- It was extended to solve nonlinear problems by applying *kernel methods* in 1992.
- Then, it became one of the popular classifiers (and regressions).

How does it work?

- It determines the **maximum margin** (the smallest perpendicular distance between the decision boundary and the closest data points) to a convex optimization problem.
- The solution is **globally** optimized.



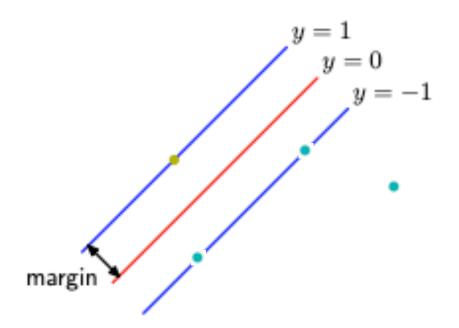
- Let the training data set compromises $\mathbf{x} = \{x_1, x_2, ..., x_N\}$ with corresponding target values $\mathbf{t} = \{t_1, ..., t_N\}$ where $t_n \in \{-1, 1\}$.
- Consider a linear binary classifier

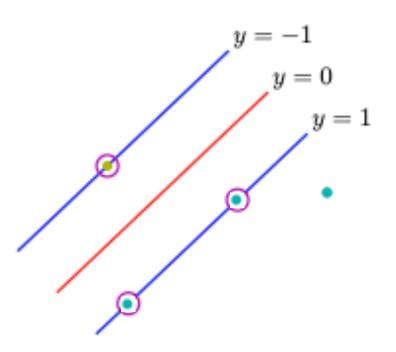
$$y(x) = \mathbf{w}^T \phi(x) + b.$$

• If the training data set is **linearly separable**, the solution for **w** and **b** is found that satisfies

$$t_n = \begin{cases} +1 & \text{if } y(x) > 0 \\ -1 & \text{if } y(x) < 0 \end{cases}.$$

- 1870
- In SVM, the decision boundary (hyperplane) is chosen for one with *maximized margin*.
- The hyperplane is determined by the subset of data points that lies on the margin and they are called **support vectors** (SVs).







- We are only interested only in SVs.
- For points that are correctly classified, $t_n y(x_n) > 0$ for all n, the distance of a point x_n to the hyperplane is

$$\frac{t_n y(\mathbf{x}_n)}{||\mathbf{w}||} = \frac{t_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b)}{||\mathbf{w}||}.$$

Eq. 8 - 1

• The *maximized margin* is found by solving

$$\underset{\boldsymbol{w},b}{\operatorname{argmax}} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$
Eq. 8 - 2

where the factor $\frac{1}{||w||}$ is taken outside of the optimization over n since w is independent of n.



Since for all correctly classified points will satisfy

$$t_n(w^T\phi(x_n)+b)\geq 1,$$

we can use all points that is closest to the surface

$$t_n(w^T\phi(x_n)+b)=1.$$

• This simplifies the requirement that we maximize $|w|^{-1}$ which is equivalent to minimizing $|w|^2$ that is to solve the optimization

$$\underset{\boldsymbol{w},b}{\operatorname{argmax}} \frac{1}{2} ||\boldsymbol{w}||^2.$$

Eq. 8 - 3





- In order to solve this, we need to introduce *Lagrange multipliers*.
- Lagrange multipliers, also known as *undetermined multipliers*, are used to find the *stationary points* of a function of several variables subject to one or more constraints.
- Consider the problem of finding the maximum of a function $f(x_1, x_2)$ subject to a constraint relating x_1 and x_2 , in form of

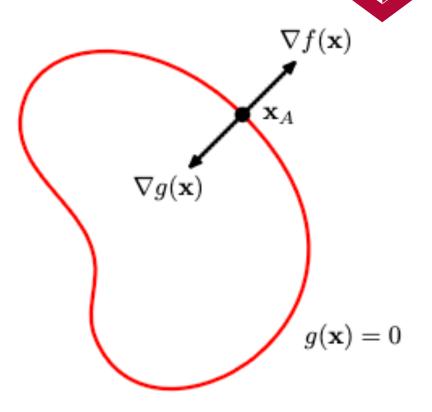
$$g(x_1, x_2) = 0.$$

• The analytical approach is not easy. Hence, we can approach geometrically.

- Consider a *D*-dimensional variable x with components x_1, \dots, x_D .
- The constrain equation g(x) = 0 represents a (D-1)-dimensional surface in x-space.
- At any point on the constraint surface, $\nabla g(x)$ will be **orthogonal** to the surface. Consider a point x lies on the constraint surface and a nearby point $x + \epsilon$ lies on the surface. A Taylor expansion around x gives

$$g(\mathbf{x} + \boldsymbol{\epsilon}) \approx g(\mathbf{x}) + \boldsymbol{\epsilon}^T \nabla g(\mathbf{x}).$$

- In the limit $||\epsilon|| \to 0$, we have $\epsilon^T \nabla g(x) = 0$ is parallel to the constrain surface where g(x) = 0, ∇g is normal to the surface.
- If there is a point x^* maximizes f(x), then the gradient of f(x) also should be **orthogonal to the surface** in the opposite direction.





• Since ∇f and ∇g are *anti-parallel*, there must be a non-zero Lagrange multiplier λ exist such that

$$\nabla f + \lambda \nabla g = 0.$$

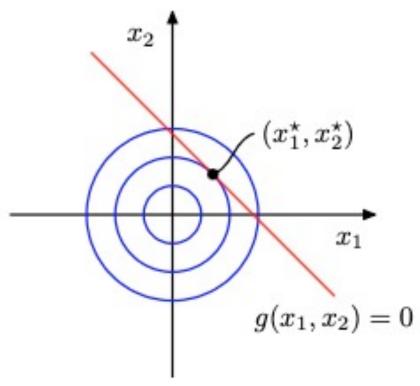
Eq. 8 - 4

• The Lagrangian function, $L(x, \lambda)$, is then defined as

$$L(\mathbf{x},\lambda) = f(\mathbf{x}) + \lambda g(\mathbf{x}).$$

• By setting $\nabla_x L = 0$, the constrained condition Eq. 8-4 can be obtained.





• Suppose we want to find the stationary point of

$$f(x_1, x_2) = 1 - x_1^2 - x_2^2$$

subject to the constraint $g(x_1, x_2) = x_1 + x_2 - 1 = 0$.

• The corresponding Lagrangian function is

$$L(x,\lambda) = 1 - x_1^2 - x_2^2 + \lambda(x_1 + x_2 - 1).$$

• The conditions to be stationary w.r.t. x_1, x_2 , and λ give the following equations:

$$-2x_1 + \lambda = 0$$

-2x_2 + \lambda = 0
x_1 + x_2 - 1 = 0.

• The solution of the stationary point $(x_1^*, x_2^*) = (\frac{1}{2}, \frac{1}{2})$ for $\lambda = 1$.



Two possible solutions can be obtained:

- Inactive solution the constrained stationary point lies in the region g(x) > 0.
 - The function g(x) does not play a role, and the stationary condition is $\nabla f(x) = 0$ and $\lambda = 0$.
- Active solution the constrained stationary point lies on the boundary g(x) = 0.
 - o The sign (+|−) of λ is crucial since f(x) will be at a maximum if $\nabla f(x) = -\lambda \nabla g(x)$ for some $\lambda > 0$.

• Either case, $\lambda g(x) = 0$.

- 1870
- Thus, the solution to the problem of maximizing f(x) subject to $g(x) \ge 0$ is obtained by optimizing Eq. 8-5, $L = f + \nabla g$, w.r.t. x and λ :

$$g(x) \ge 0$$
$$\lambda \ge 0$$
$$\lambda g(x) = 0.$$

- This solution is also known as the *Karush-Kuhn-Tucker (KKT)* condition.
- If f(x) is to be maximized f(x) subject to $g_j(x) = 0$ for j = 1, ..., J, and $h_k(x) \ge 0$ for k = 1, ..., K, the Lagrangian function is

$$L(\mathbf{x}, \{\lambda_j\}, \{\mu_k\}) = f(\mathbf{x}) + \sum_{\text{Lecture 8 - Supplier}}^{J} \lambda_j g_j(\mathbf{x}) + \sum_{k=1}^{K} \mu_k h_k(\mathbf{x}).$$



• To optimize the solution for Eq. 8-3, the Lagrangian function can be form as

$$L(\mathbf{w}, b, \mathbf{a}) = \frac{1}{2} ||\mathbf{w}||^2 - \sum_{n=1}^{N} a_n \{t_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) - 1\}$$
 Eq. 8 - 6

where the Lagrange multipliers $\boldsymbol{a} = (a_1, ..., a_N)^T$ with $a_n \ge 0$.

• We are going to minimize Eq. 8-6 w.r.t. w and b, and maximize w.r.t. a.

1870

• Setting $\nabla_{w,b}L = 0$ will have two conditions

$$\frac{\partial L(\mathbf{w}, b, \mathbf{a})}{\partial \mathbf{w}} = \mathbf{w} - \sum_{n=1}^{N} a_n t_n \phi(\mathbf{x}_n) = 0 \to \mathbf{w} = \sum_{n=1}^{N} a_n t_n \phi(\mathbf{x}_n)$$

Eq. 8 - 7

$$\frac{\partial L(\mathbf{w}, b, \mathbf{a})}{\partial b} = \sum_{n=1}^{N} a_n t_n = 0$$

Eq. 8 - 8

$$\frac{\partial L(\boldsymbol{w}, b, \boldsymbol{a})}{\partial \boldsymbol{a}} = -\sum_{n=1}^{N} \{t_n(\boldsymbol{w}^T \phi(\boldsymbol{x}_n) + b) - 1\} = 0 \rightarrow \boldsymbol{b} = t_n - \boldsymbol{w}^T \phi(\boldsymbol{x}_n)$$





Eliminating w and b from Eq. 8-6 using conditions, substituting Eq. 8-7 and -8 into Eq. 8-6, the dual representation of the maximum margin problem becomes

$$L(\mathbf{w}, b, \mathbf{a}) = \frac{1}{2} ||\mathbf{w}||^2 - \sum_{n=1}^{N} a_n \{t_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) - 1\}$$

$$\mathbf{w} = \sum_{n=1}^{N} a_n t_n \phi(\mathbf{x}_n)$$

$$\sum_{n=1}^{N} a_n t_n = 0$$

$$\tilde{L}(\mathbf{a}) = \frac{1}{2} \sum_{n=1}^{N} a_n t_n \phi_n \sum_{m=1}^{N} a_m t_m \phi_m - \sum_{n=1}^{N} \sum_{m=1}^{N} a_n t_m \phi_m a_m t_m \phi_m - b \sum_n a_n \phi_n + \sum_n a_n$$



Then the maximum margin dual representation becomes

$$\tilde{L}(\boldsymbol{a}) = \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m k(\boldsymbol{x}_n, \boldsymbol{x}_m)$$

Eq. 8 - 9

w.r.t. a subject to the constraints

$$\sum_{n=1}^{N} a_n t_n = 0.$$

Eq. 8 - 10

Eq. 8 - 11

Eq. 8-9 becomes a *non-parametric* SVM using *kernel* method.



To classify **new data points** using the training model, we evaluate the sign of y(x) by expressing using Eq. 8-7 to give

$$y(\mathbf{x}) = \sum_{n=1}^{N} a_n t_n k(\mathbf{x}, \mathbf{x}_n) + b.$$

It satisfies the KKT conditions,

$$a_n \ge 0$$

$$t_n y(\mathbf{x}_n) - 1 \ge 0$$

$$a_n \{t_n y(\mathbf{x}_n) - 1\} = 0.$$

The data points satisfying $t_n y(x_n) = 1$ are SVs.



Once the value for a is found, the threshold parameter b can be determined,

$$t_n \left(\sum_{m \in \mathcal{S}} a_m t_m k(\mathbf{x}_n, \mathbf{x}_m) + b \right) = 1$$

where S is the set of indices of SVs.

The average over all SVs gives

$$b = \frac{1}{N_{\mathcal{S}}} \sum_{n \in \mathcal{S}} \left(t_n - \sum_{m \in \mathcal{S}} a_m t_m k(\mathbf{x}_n, \mathbf{x}_m) \right)$$

where N_S is the total number of SVs.



• The maximum-margin classifier in terms of the minimization of an error function with a quadratic regularizer is

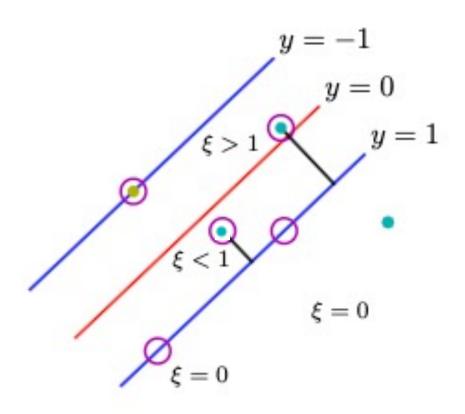
$$\sum_{n=1}^{N} E_{\infty}(y(\boldsymbol{x}_n)t_n - 1) + \lambda ||\boldsymbol{w}||^2$$

Eq. 8 - 12

where $E_{\infty}(z)$ is a function that is 0 if $z \ge 0$ and ∞ otherwise.



The class-conditional distributions may overlap in which the exact separation the training data can lead to poor generalization.

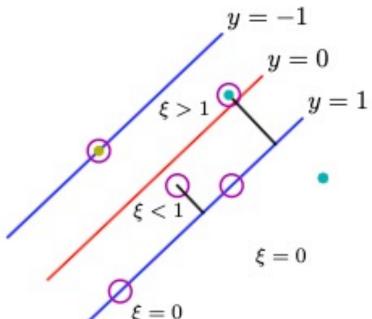


Eq. 8-12 needs to be modified by introducing slack variables $\xi_n \ge 0$ with one slack variable for each data point.

- For $\xi_n = 1$, a point on the boundary and classified correctly.
- For $0 < \xi \le 1$, a point lies *inside the margin* and on the correct side of the decision boundary.
- For $\xi_n > 1$, a point is *misclassified* and the exact classification constrains then can be replaced with

$$t_n y(x_n) \ge 1 - \xi_n$$
. Eq. 8 - 13





1870

The goal is to maximize margin while *softly penalizing* points that **lie on the wrong side of the boundary**

$$C\sum_{n=1}^{N} \xi_n + \frac{1}{2} ||w||^2$$

Eq. 8 - 14

where C > 0 controls the trade-off between the slack variable penalty and the margin, C = 1/||w||.



We need to minimize Eq. 8-14 subject to Eq. 8-13 together with $\xi_n \ge 0$. The corresponding Lagrangian is given by

$$L(\mathbf{w}, b, \mathbf{a}) = \frac{1}{2} ||\mathbf{w}||^2 + C \sum_{n=1}^{N} \xi_n - \sum_{n=1}^{N} a_n \{t_n y(\mathbf{x}_n) - 1 + \xi_n\} - \sum_{n=1}^{N} \mu_n \xi_n \quad Eq. \ 8 - 15$$

where $\{a_n \ge 0\}$ and $\{\mu_n \ge 0\}$ are Lagrange multipliers.

The corresponding KKT conditions are

$$a_n, \mu_n, \xi_n \ge 0$$

$$t_n y(x_n) - 1 + \xi \ge 0$$

$$a_n(t_n y(x_n) - 1 + \xi) = 0$$

$$\mu_n \xi_n = 0$$

where n = 1, ..., N.



The optimization of w, b, and $\{\xi_n\}$ gives

$$\frac{\partial L}{\partial \mathbf{w}} = 0 \to \mathbf{w} = \sum_{n=1}^{N} a_n t_n \phi(\mathbf{x}_n)$$

$$\frac{\partial L}{\partial b} = 0 \to \sum_{n=1}^{N} a_n t_n = 0$$

$$\frac{\partial L}{\partial \xi_n} = 0 \to a_n = C - \mu_n.$$

Since $\mu_n \ge 0$, it is known as **box constrains** that $0 \le a_n \le C$.





• For $a_n > 0$, the data points must satisfy

$$t_n y(\mathbf{x}_n) = 1 - \xi_n.$$

- If $a_n < C$, then $a_n = C \mu_n$ implies that $\mu_n > 0$ and $\xi_n = 0$.
- If $a_n = C$, points lie inside the margin and can either be correctly classified if $\xi \le 1$ or misclassified if $\xi > 1$.



• The support vectors for $0 < a_n < C$ having $\xi_n = 0$ and $t_n y(x_n) = 1$ will satisfy

$$t_n\left(\sum_{m\in\mathcal{S}}a_mt_mk(x_n,x_m)+b\right)=1.$$

• The parameter b is the averaging of those points

$$b = \frac{1}{N_{\mathcal{M}}} \sum_{n \in \mathcal{M}} \left(t_n - \sum_{m \in \mathcal{S}} a_m t_m k(x_n, x_m) \right).$$

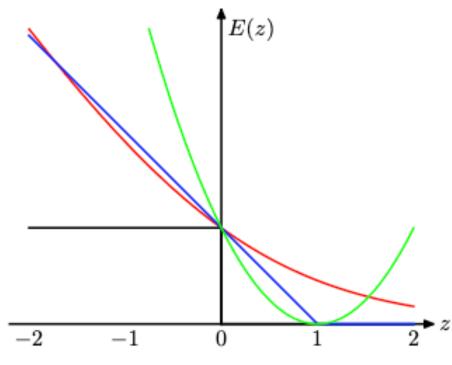
• The objective function can be written as

$$\sum_{n=1}^{N} E_{SV}(y_n, t_n) + \lambda ||\mathbf{w}||^2$$

where $\lambda = (2C)^{-1}$ and $E_{SV}(\cdot)$ is the **hinge** error function defined as

$$E_{SV}(y_n t_n) = [1 - y_n t_n]_+$$

and $[\cdot]_+$ denotes the positive part.





The constrain can be written more concisely as

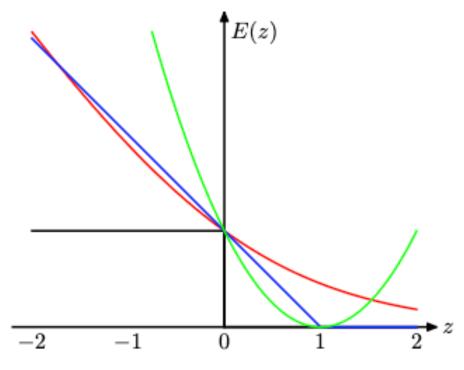
$$y_n t_n \ge 1 - \xi_n.$$

With $\xi_n > 0$,

$$\xi_n = \max(0.1 - y_n t_n).$$

The learning problem is equivalent to the unconstrained optimization over **w**:

$$\min_{w,b} \frac{||w||^2}{2} + \lambda \sum_{n=1}^{N} \max(0,1 - y_n t_n)$$







In simple linear regression, a regularized error function is

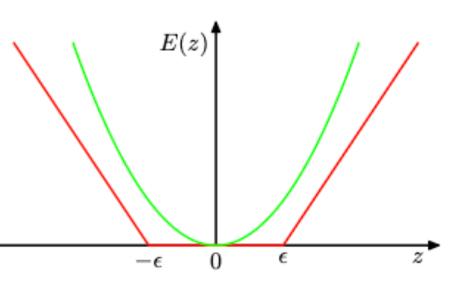
$$\frac{1}{2} \sum_{n=1}^{N} \{y_n - t_n\}^2 + \frac{\lambda}{2} ||\mathbf{w}||^2.$$

To obtain sparse solutions, the error function is replaced by an ϵ -insensitive *error function*:

$$E_{\epsilon}(y(x) - t) = \begin{cases} 0 & \text{if } |y(x) - t| < \epsilon \\ |y(x) - t| - \epsilon & \text{otherwise} \end{cases}.$$

We minimize a regularized error function given by

$$C\sum_{n=1}^{N} E_{\epsilon}(y(x_n) - t_n) + \frac{1}{2}||w||^2.$$





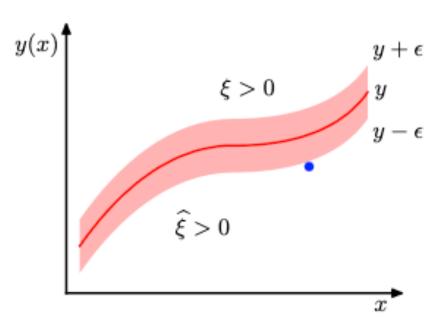
For each data point x_n , there are two slack variables $\xi_n \ge 0$ and $\widehat{\xi_n} \ge 0$.

- $\xi_n > 0$ corresponds to a point $t_n > y(x_n) + \epsilon$.
- $\widehat{\xi_n} > 0$ corresponds to a point $t_n < y(x_n) \epsilon$.

The condition for a target point to lie inside the ϵ tube $y_n - \epsilon \le t_n \le y_n + \epsilon$ with the corresponding conditions

$$t_n \le y(\mathbf{x}_n) + \epsilon + \xi_n$$

 $t_n \ge y(\mathbf{x}_n) - \epsilon - \widehat{\xi_n}$.





The error function for support vector regression can be written as

$$C\sum_{n=1}^{N}(\xi_n+\widehat{\xi_n})+\frac{1}{2}||w||^2$$

which must be minimized subject to the constraints
$$\xi_n \ge 0$$
 and $\widehat{\xi_n} \ge 0$.
$$L = C \sum_{n=1}^{N} (\xi_n + \widehat{\xi_n}) + \frac{1}{2} ||\mathbf{w}||^2 - \sum_{n=1}^{N} (\mu_n \xi_n + \widehat{\mu_n} \widehat{\xi_n}) - \sum_{n=1}^{N} a_n (\epsilon + \xi_n + y_n - t_n) - \sum_{n=1}^{N} \widehat{a_n} (\epsilon + \widehat{\xi_n} - y_n + t_n).$$

Eq. 8 - 16

Setting the derivative of Eq. 8-16 w.r.t. \boldsymbol{w} , b, ξ_n , and $\widehat{\xi_n}$ to zero gives

$$\frac{\partial L}{\partial \mathbf{w}} = 0 \to \mathbf{w} = \sum_{n=1}^{N} (a_n - \widehat{a_n}) \phi(\mathbf{x}_n)$$

$$\frac{\partial L}{\partial b} = 0 \to \sum_{n=1}^{N} (a_n - \widehat{a_n}) = 0$$

$$\frac{\partial L}{\partial \xi_n} = 0 \to a_n + \mu_n = C$$

$$\frac{\partial L}{\partial \widehat{\xi_n}} = 0 \to \widehat{a_n} + \widehat{\mu_n} = C.$$



Eq. 8 - 17



Using the result to eliminate the corresponding variables from Eq.6-16, the dual maximization becomes

$$\widetilde{L}(a,\widehat{a}) = -\frac{1}{2} \sum_{n,m} (a_n - \widehat{a_n})(a_m - \widehat{a_m})k(x_n, x_m) - \epsilon \sum_n (a_n - \widehat{a_n}) + \sum_n (a_n - \widehat{a_n})t_n$$

with the box constraints

$$0 \le a_n \le C$$
$$0 \le \widehat{a_n} \le C.$$

Substituting Eq. 8-17 to the model, the prediction for new inputs can be made as

$$y(x) = \sum_{n} (a_n - \widehat{a_n})k(x, x_n) + b.$$

Eq. 8 - 18

The bias parameter b can be found for a data point with $0 < a_n < C$ and $\xi_n = 0$ which must satisfy $\epsilon + y_n - t_n = 0$. Using Eq.6-18, b is

$$b = t_n - \epsilon - \sum_m (a_m - \widehat{a_m}) k(\mathbf{x}_n, \mathbf{x}_m).$$



8.8. Example

8.8. Example



Recall the perceptron example, we found the model $x_2 = 2x_1 - 1.667$.

```
import pandas as pd
          import matplotlib.pyplot as plt
          X = pd.DataFrame({'X1': [1,2,3,2,3,4], 'X2': [2,3,4.9,1,2,3.9], 'Y': [1,1,1,-1,-1,-1]})
      ✓ 1.6s
        1 import numpy as np
           Wp = 2
        3 \times 1 = \text{np.arange}(1,4.5,0.5)
        4 \times 2p = Wp*x1-1.667
        5 x2p
[2]
      ✓ 0.3s
    array([0.333, 1.333, 2.333, 3.333, 4.333, 5.333, 6.333])
```

8.8. Example

In this example, assume $a_n = 1$. The parameter w can be determined by

$$\mathbf{w} = \sum_{i} a_i t_i \mathbf{x}_i .$$

For x_1 ,

$$w_1 = \sum_{i} a_i t_i x_{1i}$$

$$= 1 \cdot 1(1+2+3) - 1 \cdot 1(2+3+4)$$

$$= -3$$

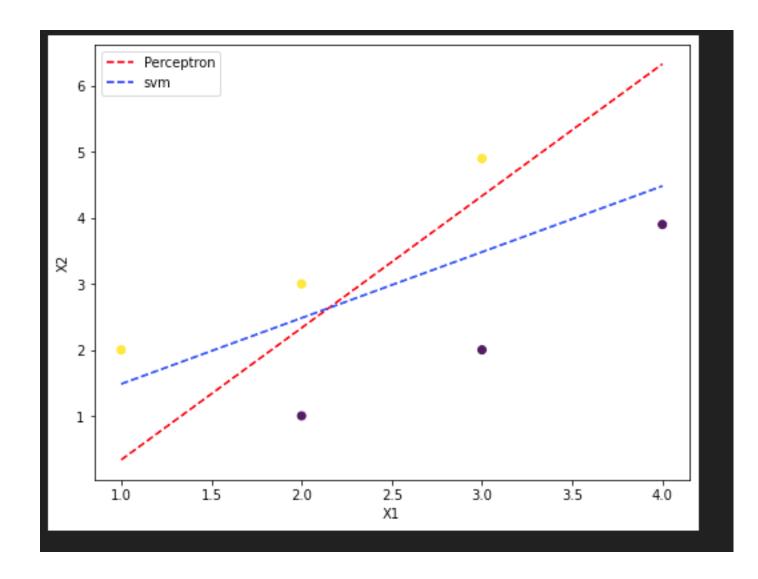
The bias parameter can be determined by

$$b = \frac{1}{N} \sum_{i,t \in 1} y_i - \mathbf{w}^T \mathbf{x}$$
$$= -1.45$$

The model is then $y = -3x_1 + 3x_2 - 1.45$ and it leads to $x_2 = x_1 + 0.483$.

Example







8.9. Example

8.9. Conclusion



- SVM was originally invented from linearly separable binary classification.
- SVM is the extension version of perceptron to find the best hyperplane.
- SVM is powerful.
 - o SVM is a parametric model when a data is linearly separable.
 - SVM uses kernel method and becomes a non-parametric model for non-linear data.