

# Machine Learning and Intelligent Systems

Support Vector Machines

Maria A. Zuluaga

Nov 17, 2023

EURECOM - Data Science Department

#### Table of contents

Recap: The Perceptron

Maximum Margin Classifiers

Formalization

Linear Algebra of a Hyperplane

The Learning Process

Quadratic Optimization Function

Support Vectors

Recap

Recap: The Perceptron

## The Perceptron

#### **Data Assumptions:**

- Binary classification :  $y_i \in \{-1, 1\}$
- Data is linearly separable

#### **Model Assumption:**

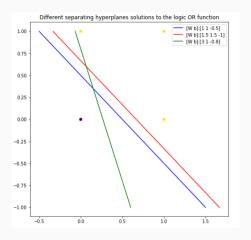
• The decision boundary is a hyperplane:

$$\mathcal{H} = \{ \mathbf{x} : \hat{w}^T \mathbf{x} + b = 0 \}$$

- w: Weight vector that defines the hyperplane
- b: bias

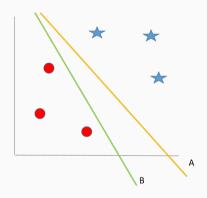
**Goal:** Find a separating hyperplane by minimizing the number of errors, i.e. number of points in the "wrong" side of the decision boundary

#### Initialization



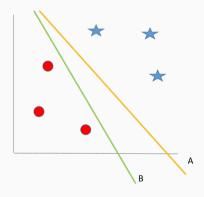
Different initializations lead to different solutions

## Training set



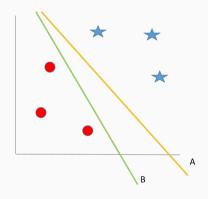
• Which of these to boundaries is a valid solution for the perceptron?

## Training set



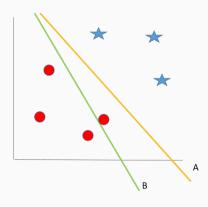
- Which of these to boundaries is a valid solution for the perceptron?
  - Answer: Both are valid as the perceptron loss is zero

Training set



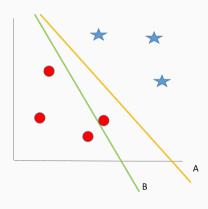
- Which of these to boundaries is a valid solution for the perceptron?
  - Answer: Both are valid as the perceptron loss is zero
- Which one is best according to you?

## Training set and a test point



- Which of these to boundaries is a valid solution for the perceptron?
  - Answer: Both are valid as the perceptron loss is zero
- Which one is best according to you?

#### Training set and a test point



- Which of these to boundaries is a valid solution for the perceptron?
  - Answer: Both are valid as the perceptron loss is zero
- Which one is best according to you?
  - Answer: Boundary A seems more "reliable"
- Intuition: The best boundary is the one that is as far as possible from both classes

## **Support Vector Machines and The Percetron**

- A Support Vector Machine (SVM) makes predictions exactly like the perceptron
- SVMS, however, try to find a boundary that is as far as possible from both classes
- SVM also differs in the way in which it learns the parameters

## **Support Vector Machines and The Percetron**

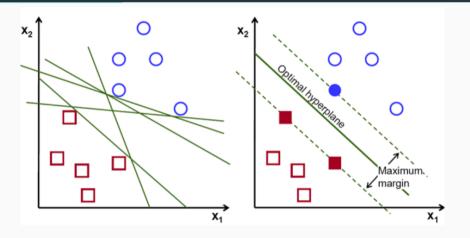
- A Support Vector Machine (SVM) makes predictions exactly like the perceptron
- SVMS, however, try to find a boundary that is as far as possible from both classes
- SVM also differs in the way in which it learns the parameters
- Reminder

$$E_p(\mathbf{w}) = -\sum_{i \in \mathcal{M}} \mathbf{w}^T \mathbf{x}_i \mathbf{y}_i$$

The perceptron criterion

**Maximum Margin Classifiers** 

# **Maximum Margin Classification**



SVMs aim to find the boundary that maximizes the margin between the classes

# **Assumptions and Definitions**

#### **Data Assumptions:**

- Binary classification :  $y_i \in \{-1, 1\}$
- Data is linearly separable

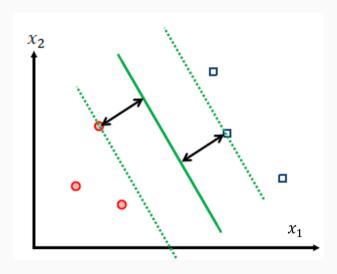
#### Goal:

• Maximize the margin width

#### **Definitions:**

- Margin width: Distance between the decision boundary and the nearest points on either class
- Support vectors: Points that define the location of the decision boundary

# **Support Vectors**



# Parenthesis: Linear Algebra of a Hyperplane

#### $\mathcal{H}\colon$ Hyperplane or affine set defined by:

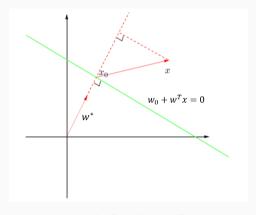
$$\mathcal{H} = \{ \mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0 \}$$

#### Key properties:

1. For any  $x_1$ ,  $x_2 \in \mathcal{H}$ 

$$\mathbf{w}^T(\mathbf{x}_1 - \mathbf{x}_2) = 0$$

so, 
$$\mathbf{w}^* = \frac{\mathbf{w}^T}{\|\mathbf{w}\|}$$
 is the vector normal to  $\mathcal{H}$ 



Adapted from Fig 4.15 Hastie et al. ESL

# Parenthesis: Linear Algebra of a Hyperplane

 $\mathcal{H}\colon \mathsf{Hyperplane}$  or affine set defined by:

$$\mathcal{H} = \{ \mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0 \}$$

#### **Key properties:**

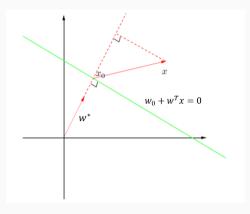
1. For any  $\mathbf{x}_1$ ,  $\mathbf{x}_2 \in \mathcal{H}$ 

$$\mathbf{w}^T(\mathbf{x}_1 - \mathbf{x}_2) = 0$$

so, 
$$\mathbf{w}^* = \frac{\mathbf{w}^T}{\|\mathbf{w}\|}$$
 is the vector normal to  $\mathcal{H}$ 

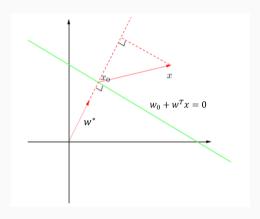
2. For any  $x_0 \in \mathcal{H}$ ,

$$\mathbf{w}^T \mathbf{x}_0 = -w_0$$



Adapted from Fig 4.15 Hastie et al. ESL

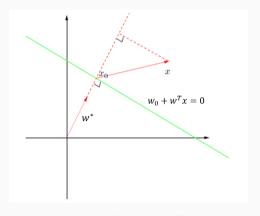
The signed distance of any point  $\mathbf{x}$  to  $\mathcal{H}$  is the projection of a vector  $\mathbf{v}$  into the normal vector.



Adapted from Fig 4.15 Hastie et al. ESL

The signed distance of any point  $\mathbf{x}$  to  $\mathcal{H}$  is the projection of a vector  $\mathbf{v}$  into the normal vector.

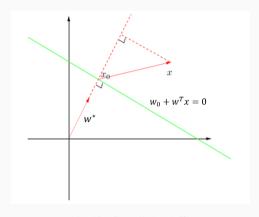
$$\mathbf{w}^* \cdot \mathbf{v} = \frac{\mathbf{w}^T}{\|\mathbf{w}\|} (\mathbf{x} - \mathbf{x}_0)$$
 (key property 1)



Adapted from Fig 4.15 Hastie et al. ESL

The signed distance of any point  $\mathbf{x}$  to  $\mathcal{H}$  is the projection of a vector  $\mathbf{v}$  into the normal vector.

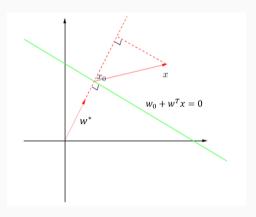
$$\mathbf{w}^* \cdot \mathbf{v} = \frac{\mathbf{w}^T}{\|\mathbf{w}\|} (\mathbf{x} - \mathbf{x}_0) \qquad \text{(key property 1)}$$
$$= \frac{1}{\|\mathbf{w}\|} (\mathbf{w}^T \mathbf{x} - \mathbf{w}^T \mathbf{x}_0) \quad \text{(key property 2)}$$



Adapted from Fig 4.15 Hastie et al. ESL

The signed distance of any point  $\mathbf{x}$  to  $\mathcal{H}$  is the projection of a vector  $\mathbf{v}$  into the normal vector.

$$\mathbf{w}^* \cdot \mathbf{v} = \frac{\mathbf{w}^T}{\|\mathbf{w}\|} (\mathbf{x} - \mathbf{x}_0) \qquad \text{(key property 1)}$$
$$= \frac{1}{\|\mathbf{w}\|} (\mathbf{w}^T \mathbf{x} - \mathbf{w}^T \mathbf{x}_0) \quad \text{(key property 2)}$$
$$= \frac{1}{\|\mathbf{w}\|} (\mathbf{w}^T \mathbf{x} + \mathbf{w}_0)$$

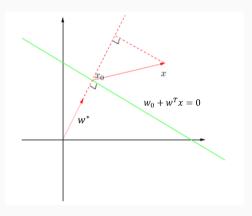


Adapted from Fig 4.15 Hastie et al. ESL

The signed distance of any point  $\mathbf{x}$  to  $\mathcal{H}$  is the projection of a vector  $\mathbf{v}$  into the normal vector.

$$\mathbf{w}^* \cdot \mathbf{v} = \frac{\mathbf{w}^T}{\|\mathbf{w}\|} (\mathbf{x} - \mathbf{x}_0) \qquad \text{(key property 1)}$$
$$= \frac{1}{\|\mathbf{w}\|} (\mathbf{w}^T \mathbf{x} - \mathbf{w}^T \mathbf{x}_0) \quad \text{(key property 2)}$$
$$= \frac{1}{\|\mathbf{w}\|} (\mathbf{w}^T \mathbf{x} + \mathbf{w}_0)$$

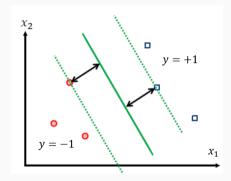
Signed distance to 
$$\mathcal{H}$$
:  $\frac{1}{\|\mathbf{w}\|}(\mathbf{w}^T\mathbf{x} + \mathbf{w}_0)$ 



Adapted from Fig 4.15 Hastie et al. ESL

## **Data Assumptions:**

- $\bullet$  Training set  ${\cal D}$  with  $\mathbf{x} \in \mathbb{R}^D, \, \mathbf{y} \in \{-1,1\}$
- Data is linearly separable



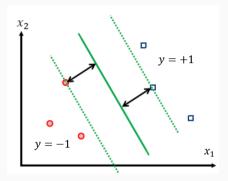
## **Data Assumptions:**

- Training set  $\mathcal{D}$  with  $\mathbf{x} \in \mathbb{R}^D$ ,  $\mathbf{y} \in \{-1, 1\}$
- Data is linearly separable

#### **Model Assumptions:**

- The y<sub>i</sub>s encode the side of the perfect decision boundary each x<sub>i</sub> is on
- Our model:

$$\hat{\mathbf{y}} = \mathbf{h}(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + w_0$$



#### **Data Assumptions:**

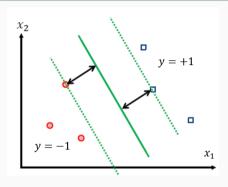
- $\bullet$  Training set  ${\color{red}\mathcal{D}}$  with  $\mathbf{x} \in \mathbb{R}^D,\, {\color{red}\mathbf{y}} \in \{-1,1\}$
- Data is linearly separable

#### **Model Assumptions:**

- The y<sub>i</sub>s encode the side of the perfect decision boundary each x<sub>i</sub> is on
- Our model:

$$\hat{\mathbf{y}} = \mathbf{h}(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + w_0$$

Question: Have you seen this before?



#### **Data Assumptions:**

- Training set  $\mathcal{D}$  with  $\mathbf{x} \in \mathbb{R}^D, \ \mathbf{y} \in \{-1, 1\}$
- Data is linearly separable

## **Model Assumptions:**

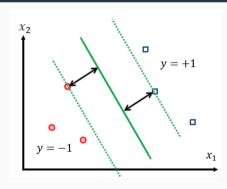
- The y<sub>i</sub>s encode the side of the perfect decision boundary each x<sub>i</sub> is on
- Our model:

$$\hat{\mathbf{y}} = \mathbf{h}(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + w_0$$

Question: Have you seen this before?

• Correctly classified points satisfy:

$$\mathbf{y}_i(\mathbf{w}^T\mathbf{x}_i + w_0) > 0$$



#### **Data Assumptions:**

- Training set  $\mathcal{D}$  with  $\mathbf{x} \in \mathbb{R}^D$ ,  $\mathbf{y} \in \{-1, 1\}$
- Data is linearly separable

#### **Model Assumptions:**

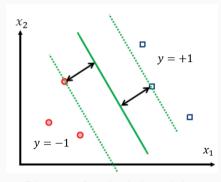
- The y<sub>i</sub>s encode the side of the perfect decision boundary each x<sub>i</sub> is on
- Our model:

$$\hat{\mathbf{y}} = \mathbf{h}(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + w_0$$

Question: Have you seen this before?

Correctly classified points satisfy:

$$\mathbf{y}_i(\mathbf{w}^T\mathbf{x}_i + w_0) > 0$$



Distance for the i-th training sample to the decision boundary:

$$d(\mathbf{x}_i, \mathcal{H}) = \frac{|\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0|}{\|\mathbf{w}\|}$$

## The Learning Process: Maximum Margin

• Margin width  $\gamma$ : Distance from the decision boundary to the closest point

$$\gamma(\mathbf{w}, w_0) = \min_{\mathbf{x}_i \in \mathcal{D}} d(\mathbf{x}_i, \mathcal{H}) = \min_{\mathbf{x}_i \in \mathcal{D}} \frac{|\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0|}{\|\mathbf{w}\|}$$

ullet If the hyperplane is such that  $\gamma$  is maximized, it must be equidistant to the two classes

## The Learning Process: Maximum Margin

• Margin width  $\gamma$ : Distance from the decision boundary to the closest point

$$\gamma(\mathbf{w}, w_0) = \min_{\mathbf{x}_i \in \mathcal{D}} d(\mathbf{x}_i, \mathcal{H}) = \min_{\mathbf{x}_i \in \mathcal{D}} \frac{|\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0|}{\|\mathbf{w}\|}$$

- ullet If the hyperplane is such that  $\gamma$  is maximized, it must be equidistant to the two classes
- We want to find the margin as large as possible (maximization)

## The Learning Process: Maximum Margin

• Margin width  $\gamma$ : Distance from the decision boundary to the closest point

$$\gamma(\mathbf{w}, w_0) = \min_{\mathbf{x}_i \in \mathcal{D}} d(\mathbf{x}_i, \mathcal{H}) = \min_{\mathbf{x}_i \in \mathcal{D}} \frac{|\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0|}{\|\mathbf{w}\|}$$

- ullet If the hyperplane is such that  $\gamma$  is maximized, it must be equidistant to the two classes
- We want to find the margin as large as possible (maximization)
- SVM seeks to maximize, as a function of  $\{\mathbf{w}, w_0\}$ , the quantity:

$$\underset{\mathbf{w},w_0}{\arg\max} \ \gamma(\mathbf{w},w_0)$$

Question: Do you see a problem?

## The Learning Process: Constrained Optimization

 To guarantee that the data gets properly classified, we need to add a constraint to the optimization problem:

$$\begin{aligned} &\underset{\mathbf{w}, w_0}{\text{arg max}} & & \gamma(\mathbf{w}, w_0) \\ &\text{subject to} & & \mathbf{y}_i(\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \end{aligned}$$

## The Learning Process: Constrained Optimization

• To guarantee that the data gets properly classified, we need to add a constraint to the optimization problem:

• Let's replace  $\gamma$ :

## The Learning Process: Constrained Optimization

 To guarantee that the data gets properly classified, we need to add a constraint to the optimization problem:

• Let's replace  $\gamma$ :

• and reorganize a bit:

$$\underset{\mathbf{w}, w_0}{\text{arg max}} \quad \frac{1}{\|\mathbf{w}\|} \underset{\mathbf{x}_i \in \mathcal{D}}{\text{min}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0|$$

$$\text{subject to} \quad \underbrace{\mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0)} > 0$$

# Non-Unique Representation

• The hyperplane is scale invariant, i.e.  $\mathcal{H} = \{\mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0\}$  is equivalent to  $\mathcal{H} = \{\mathbf{x} : \beta \mathbf{w}^T \mathbf{x} + \beta w_0 = 0\} \ \forall \beta \neq 0$ 

## **Non-Unique Representation**

- The hyperplane is scale invariant, i.e.  $\mathcal{H} = \{\mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0\}$  is equivalent to  $\mathcal{H} = \{\mathbf{x} : \beta \mathbf{w}^T \mathbf{x} + \beta w_0 = 0\} \ \forall \beta \neq 0$
- In words: The same boundary (the classifier) can be expressed in infinite ways
- We can use this property to simplify the optimization problem

#### Non-Unique Representation

- The hyperplane is scale invariant, i.e.  $\mathcal{H} = \{\mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0\}$  is equivalent to  $\mathcal{H} = \{\mathbf{x} : \beta \mathbf{w}^T \mathbf{x} + \beta w_0 = 0\} \ \forall \beta \neq 0$
- In words: The same boundary (the classifier) can be expressed in infinite ways
- We can use this property to simplify the optimization problem
- Idea: The scale is not important, so we can fix it to an arbitrary value

$$\begin{aligned} & \underset{\mathbf{w}, w_0}{\text{arg max}} & & \frac{1}{\|\mathbf{w}\|} \min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| \\ & \text{subject to} & & \forall i \ y_i (\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \end{aligned}$$

#### Non-Unique Representation

- The hyperplane is scale invariant, i.e.  $\mathcal{H} = \{\mathbf{x} : \mathbf{w}^T \mathbf{x} + w_0 = 0\}$  is equivalent to  $\mathcal{H} = \{\mathbf{x} : \beta \mathbf{w}^T \mathbf{x} + \beta w_0 = 0\} \ \forall \beta \neq 0$
- In words: The same boundary (the classifier) can be expressed in infinite ways
- We can use this property to simplify the optimization problem
- Idea: The scale is not important, so we can fix it to an arbitrary value

$$\begin{aligned} \underset{\mathbf{w}, w_0}{\text{arg max}} \quad & \frac{1}{\|\mathbf{w}\|} \min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| \\ \text{subject to} \quad & \forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0) > 0 \\ & \min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1 \end{aligned}$$

### The Learning Process: Back to the Objective Function

$$\arg \max_{\mathbf{w}, w_0} \frac{1}{\|\mathbf{w}\|} \frac{\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0}{\|\mathbf{w}\|^T \mathbf{x}_i + \mathbf{w}_0} > 0$$

$$\min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1$$

## The Learning Process: Back to the Objective Function

arg max 
$$\frac{1}{\|\mathbf{w}\|} \frac{\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0}{\|\mathbf{w}\|_{\mathbf{x}_i \in \mathcal{D}}}$$
subject to 
$$\forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0) > 0$$
$$\min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1$$

As we prefer to do minimization rather than maximization we can use the fact that maximizing  $\|\mathbf{w}\|^{-1}$  is equivalent to minimizing  $\|\mathbf{w}\|^2$ 

### The Learning Process: Back to the Objective Function

arg max 
$$\frac{1}{\|\mathbf{w}\|} \frac{\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0}{\|\mathbf{w}\|_{\mathbf{x}_i \in \mathcal{D}}}$$
subject to 
$$\forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0) > 0$$
$$\min_{\mathbf{x}_i \in \mathcal{D}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1$$

As we prefer to do minimization rather than maximization we can use the fact that maximizing  $\|\mathbf{w}\|^{-1}$  is equivalent to minimizing  $\|\mathbf{w}\|^2$ 

$$\begin{aligned} & \underset{\mathbf{w}, w_0}{\text{arg min}} & & \frac{1}{2} \|\mathbf{w}\|^2 \\ & \text{subject to} & & \forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \\ & & \underset{\mathbf{x}_i \in \mathcal{D}}{\text{min}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1 \end{aligned}$$

• We can further simplify the optimization problem by simplifying the constraints.

- We can further simplify the optimization problem by simplifying the constraints.
- The two original constraints:

$$\begin{aligned} & \underset{\mathbf{w}, w_0}{\text{arg min}} & & \frac{1}{2} \|\mathbf{w}\|^2 \\ & \text{subject to} & & \forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \\ & & & \underset{\mathbf{x}_i \in \mathcal{D}}{\text{min}} \left| \mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0 \right| = 1 \end{aligned}$$

- We can further simplify the optimization problem by simplifying the constraints.
- The two original constraints:

$$\begin{aligned} & \underset{\mathbf{w}, w_0}{\text{arg min}} & & \frac{1}{2} \|\mathbf{w}\|^2 \\ & \text{subject to} & & \forall i \ \mathbf{y}_i(\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \\ & & & \underset{\mathbf{x}_i \in \mathcal{D}}{\text{min}} |\mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0| = 1 \end{aligned}$$

• are equivalent to:

• Exercise: Can you proof that these are equivalent?

- We can further simplify the optimization problem by simplifying the constraints.
- The two original constraints:

$$\begin{aligned} & \underset{\mathbf{w}, w_0}{\text{arg min}} & & \frac{1}{2} \|\mathbf{w}\|^2 \\ & \text{subject to} & & \forall i \ \mathbf{y}_i (\mathbf{w}^T \mathbf{x}_i + w_0) > 0 \\ & & \underset{\mathbf{x}_i \in \mathcal{D}}{\text{min}} \left| \mathbf{w}^T \mathbf{x}_i + \mathbf{w}_0 \right| = 1 \end{aligned}$$

• are equivalent to:

• Exercise: Can you proof that these are equivalent?

In words: Find the simplest hyperplane (smaller  $|\mathbf{w}|^2$ ) such that all inputs lie at least 1 unit away from the hyperplane on the correct side.

#### **Quadratic Optimization Function**

This formulation is a quadratic optimization problem: The objective is quadratic and the constraints are linear.

An advantage of these type of problems is that they can be efficiently solved with quadratic program solvers. This made SVMs very popular for many years.

Another interesting property is that it has a unique solution whenever a hyperplane exists.

# Support Vectors

#### **Support Vectors**

- We defined a support vector as a point defining the location of the decision boundary
- The support vectors would be those points in the training set strictly satisfying

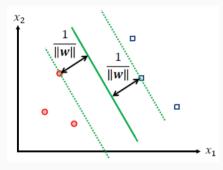
$$\mathbf{y}_i(\mathbf{w}^T\mathbf{x}_i+w_0)=1$$

#### Support Vectors

- We defined a support vector as a point defining the location of the decision boundary
- The support vectors would be those points in the training set strictly satisfying

$$\mathbf{y}_i(\mathbf{w}^T\mathbf{x}_i + w_0) = 1$$

- They determine the shape of the hyperplane: If one is removed and the SVM is retrained, the resulting hyperplane will be different.
- The opposite occurs with non-support vectors
- Support vectors will become more important during the Kernels lecture



Hard SVM: No points allowed within the margin

Recap

#### Recap

- We have introduced support vector machines (SVMs) as maximum margin classifiers
- We derived the hard margin SVM objective
- We reviewed the concept of constrained optimization
- We introduced the concept of support vector

#### **Key Concepts**

- Hyperplane
- Maximum Margin Classifiers
- Support Vectors
- Constrained Optimization



## Further Reading and Useful Material

Source	Notes
Support Vector Networks - Cortes and Vapnik	original publication (link)
Pattern Recognition and Machine Learning	Ch 7
The Elements of Statistical Learning	Sec. 4.5, Ch 12
Distance to a plane	Applet (link)