

CSCI567 Machine Learning (Spring 2021)

Sirisha Rambhatla

University of Southern California

Feb 24, 2021

Outline

- 1 Logistics
- 2 Review of last lecture
- 3 Support vector machines (primal formulation)
- 4 Quiz 1 Specifics

Outline

- 1 Logistics
- 2 Review of last lecture
- 3 Support vector machines (primal formulation)
- 4 Quiz 1 Specifics

Logistics

- HW 3 was assigned.
- We will discuss quiz specifics at the end of the lecture today.

Outline

- 1 Logistics
- 2 Review of last lecture**
- 3 Support vector machines (primal formulation)
- 4 Quiz 1 Specifics

Kernel functions

Definition: a function $k : \mathbb{R}^D \times \mathbb{R}^D \rightarrow \mathbb{R}$ is called a *(positive semidefinite) kernel function* if there exists a function $\phi : \mathbb{R}^D \rightarrow \mathbb{R}^M$ so that for any $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^D$,

$$k(\mathbf{x}, \mathbf{x}') = \phi(\mathbf{x})^T \phi(\mathbf{x}')$$

Kernel functions

Definition: a function $k : \mathbb{R}^D \times \mathbb{R}^D \rightarrow \mathbb{R}$ is called a *(positive semidefinite) kernel function* if there exists a function $\phi : \mathbb{R}^D \rightarrow \mathbb{R}^M$ so that for any $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^D$,

$$k(\mathbf{x}, \mathbf{x}') = \phi(\mathbf{x})^T \phi(\mathbf{x}')$$

Examples we have seen

$$k(\mathbf{x}, \mathbf{x}') = (\mathbf{x}^T \mathbf{x}')^2$$

$$k(\mathbf{x}, \mathbf{x}') = \sum_{d=1}^D \frac{\sin(2\pi(x_d - x'_d))}{x_d - x'_d}$$

$$k(\mathbf{x}, \mathbf{x}') = (\mathbf{x}^T \mathbf{x}' + c)^d \quad \text{(polynomial kernel)}$$

$$k(\mathbf{x}, \mathbf{x}') = e^{-\frac{\|\mathbf{x} - \mathbf{x}'\|_2^2}{2\sigma^2}} \quad \text{(Gaussian/RBF kernel)}$$

Kernelizing ML algorithms

Feasible as long as **only inner products are required**:

- regularized linear regression (dual formulation)

$$\phi(\mathbf{x})^T \mathbf{w}^* = \phi(\mathbf{x})^T \Phi^T (\mathbf{K} + \lambda \mathbf{I})^{-1} \mathbf{y} \quad (\mathbf{K} = \Phi \Phi^T \text{ is } \textit{kernel matrix})$$

- nearest neighbor classifier with L2 distance

$$\|\phi(\mathbf{x}) - \phi(\mathbf{x}')\|_2^2 = k(\mathbf{x}, \mathbf{x}) + k(\mathbf{x}', \mathbf{x}') - 2k(\mathbf{x}, \mathbf{x}')$$

- perceptron, logistic regression, SVM, ...

Outline

- 1 Logistics
- 2 Review of last lecture
- 3 Support vector machines (primal formulation)**
- 4 Quiz 1 Specifics

Support vector machines (SVM)

- One of the most commonly used classification algorithms
- Works well with the kernel trick
- Strong theoretical guarantees

Support vector machines (SVM)

- One of the most commonly used classification algorithms
- Works well with the kernel trick
- Strong theoretical guarantees

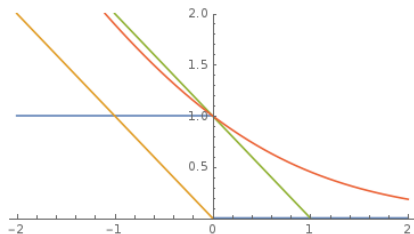
We focus on **binary classification** here.

Primal formulation

In one sentence: linear model with L2 regularized hinge loss.

Primal formulation

In one sentence: linear model with L2 regularized hinge loss. Recall



- **perceptron loss** $l_{\text{perceptron}}(z) = \max\{0, -z\} \rightarrow$ Perceptron
- **logistic loss** $l_{\text{logistic}}(z) = \log(1 + \exp(-z)) \rightarrow$ logistic regression
- **hinge loss** $l_{\text{hinge}}(z) = \max\{0, 1 - z\} \rightarrow$ **SVM**

Primal formulation

For a linear model (\mathbf{w}, b) , this means

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

Primal formulation

For a linear model (\mathbf{w}, b) , this means

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

- recall $y_n \in \{-1, +1\}$

Primal formulation

For a linear model (\mathbf{w}, b) , this means

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

- recall $y_n \in \{-1, +1\}$
- a nonlinear mapping ϕ is applied

Primal formulation

For a linear model (\mathbf{w}, b) , this means

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

- recall $y_n \in \{-1, +1\}$
- a nonlinear mapping ϕ is applied
- the bias/intercept term b is used explicitly (think about why after this lecture)

Primal formulation

For a linear model (\mathbf{w}, b) , this means

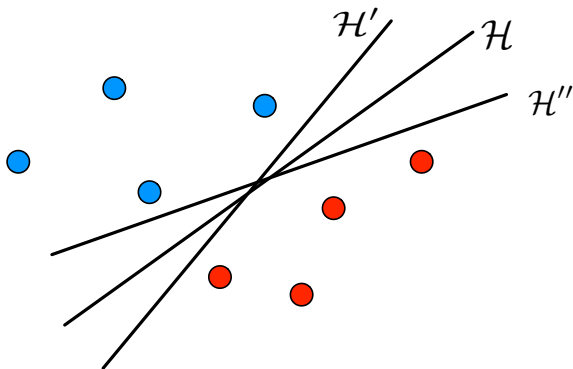
$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

- recall $y_n \in \{-1, +1\}$
- a nonlinear mapping ϕ is applied
- the bias/intercept term b is used explicitly (think about why after this lecture)

So why L2 regularized hinge loss?

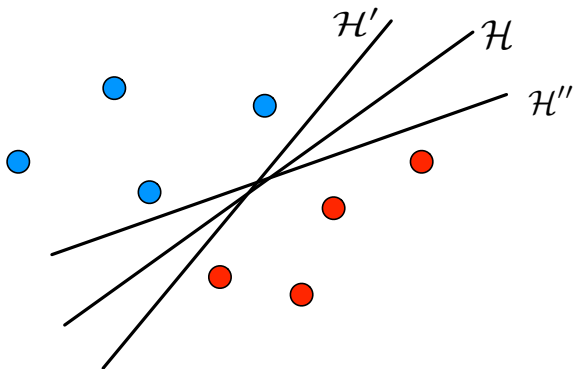
Geometric motivation: separable case

When data is **linearly separable**, there are *infinitely many hyperplanes with zero training error*:



Geometric motivation: separable case

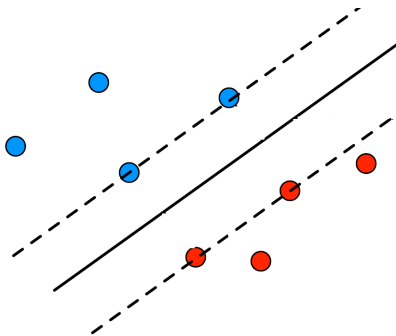
When data is **linearly separable**, there are *infinitely many hyperplanes with zero training error*:



So which one should we choose?

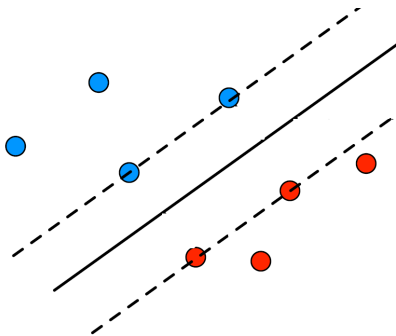
Intuition

The further away from data points the better.



Intuition

The further away from data points the better.



How to formalize this intuition?

Distance to hyperplane

What is the **distance** from a point \mathbf{x} to a hyperplane $\{\mathbf{x} : \mathbf{w}^T \mathbf{x} + b = 0\}$?

Distance to hyperplane

What is the **distance** from a point \mathbf{x} to a hyperplane $\{\mathbf{x} : \mathbf{w}^T \mathbf{x} + b = 0\}$?

Assume the **projection** is $\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2}$, then

$$0 = \mathbf{w}^T \left(\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2} \right) + b = \mathbf{w}^T \mathbf{x} - \ell \|\mathbf{w}\| + b$$

and thus $\ell = \frac{\mathbf{w}^T \mathbf{x} + b}{\|\mathbf{w}\|_2}$.

Distance to hyperplane

What is the **distance** from a point \mathbf{x} to a hyperplane $\{\mathbf{x} : \mathbf{w}^T \mathbf{x} + b = 0\}$?

Assume the **projection** is $\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2}$, then

$$0 = \mathbf{w}^T \left(\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2} \right) + b = \mathbf{w}^T \mathbf{x} - \ell \|\mathbf{w}\| + b$$

and thus $\ell = \frac{\mathbf{w}^T \mathbf{x} + b}{\|\mathbf{w}\|_2}$.

Therefore the distance is

$$\frac{|\mathbf{w}^T \mathbf{x} + b|}{\|\mathbf{w}\|_2}$$

Distance to hyperplane

What is the **distance** from a point \mathbf{x} to a hyperplane $\{\mathbf{x} : \mathbf{w}^T \mathbf{x} + b = 0\}$?

Assume the **projection** is $\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2}$, then

$$0 = \mathbf{w}^T \left(\mathbf{x} - \ell \frac{\mathbf{w}}{\|\mathbf{w}\|_2} \right) + b = \mathbf{w}^T \mathbf{x} - \ell \|\mathbf{w}\| + b$$

and thus $\ell = \frac{\mathbf{w}^T \mathbf{x} + b}{\|\mathbf{w}\|_2}$.

Therefore the distance is

$$\frac{|\mathbf{w}^T \mathbf{x} + b|}{\|\mathbf{w}\|_2}$$

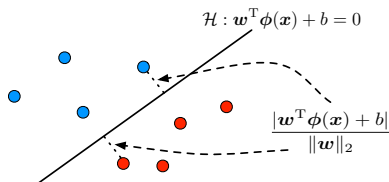
For a hyperplane that correctly classifies (\mathbf{x}, y) , the distance becomes

$$\frac{y(\mathbf{w}^T \mathbf{x} + b)}{\|\mathbf{w}\|_2}$$

Maximizing margin

Margin: the *smallest* distance from all training points to the hyperplane

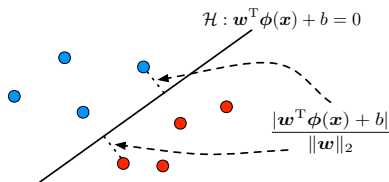
$$\text{MARGIN OF } (\mathbf{w}, b) = \min_n \frac{y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)}{\|\mathbf{w}\|_2}$$



Maximizing margin

Margin: the *smallest* distance from all training points to the hyperplane

$$\text{MARGIN OF } (\mathbf{w}, b) = \min_n \frac{y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)}{\|\mathbf{w}\|_2}$$



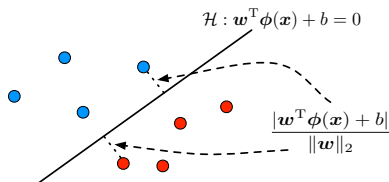
The intuition “**the further away the better**” translates to solving

$$\max_{\mathbf{w}, b} \min_n \frac{y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)}{\|\mathbf{w}\|_2}$$

Maximizing margin

Margin: the *smallest* distance from all training points to the hyperplane

$$\text{MARGIN OF } (\mathbf{w}, b) = \min_n \frac{y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)}{\|\mathbf{w}\|_2}$$



The intuition “**the further away the better**” translates to solving

$$\max_{\mathbf{w}, b} \min_n \frac{y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)}{\|\mathbf{w}\|_2} = \max_{\mathbf{w}, b} \frac{1}{\|\mathbf{w}\|_2} \min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)$$

Rescaling

Note: rescaling (\boldsymbol{w}, b) does not change the hyperplane at all.

Rescaling

Note: rescaling (\mathbf{w}, b) does not change the hyperplane at all.

We can thus always scale (\mathbf{w}, b) s.t. $\min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$

Rescaling

Note: rescaling (\mathbf{w}, b) does not change the hyperplane at all.

We can thus always scale (\mathbf{w}, b) s.t. $\min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$

The margin then becomes

$$\begin{aligned} & \text{MARGIN OF } (\mathbf{w}, b) \\ &= \frac{1}{\|\mathbf{w}\|_2} \min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \\ &= \frac{1}{\|\mathbf{w}\|_2} \end{aligned}$$

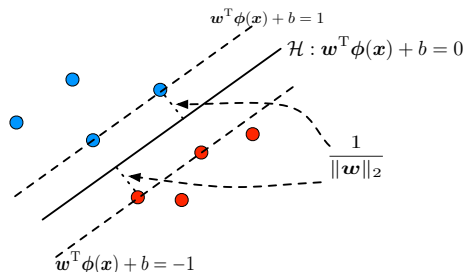
Rescaling

Note: rescaling (\mathbf{w}, b) does not change the hyperplane at all.

We can thus always scale (\mathbf{w}, b) s.t. $\min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$

The margin then becomes

$$\begin{aligned} \text{MARGIN OF } (\mathbf{w}, b) &= \frac{1}{\|\mathbf{w}\|_2} \min_n y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \\ &= \frac{1}{\|\mathbf{w}\|_2} \end{aligned}$$



Summary for separable data

For a separable training set, we aim to solve

$$\max_{\mathbf{w}, b} \frac{1}{\|\mathbf{w}\|_2} \quad \text{s.t.} \quad \min_n y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$$

Summary for separable data

For a separable training set, we aim to solve

$$\max_{\mathbf{w}, b} \frac{1}{\|\mathbf{w}\|_2} \quad \text{s.t.} \quad \min_n y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$$

This is equivalent to

$$\begin{aligned} \min_{\mathbf{w}, b} \quad & \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1, \quad \forall n \end{aligned}$$

Summary for separable data

For a separable training set, we aim to solve

$$\max_{\mathbf{w}, b} \frac{1}{\|\mathbf{w}\|_2} \quad \text{s.t.} \quad \min_n y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) = 1$$

This is equivalent to

$$\begin{aligned} \min_{\mathbf{w}, b} \quad & \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1, \quad \forall n \end{aligned}$$

SVM is thus also called *max-margin* classifier. The constraints above are called *hard-margin* constraints.

General non-separable case

If data is not linearly separable, the previous constraint

$$y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1, \quad \forall n$$

is obviously *not feasible*.

General non-separable case

If data is not linearly separable, the previous constraint

$$y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1, \quad \forall n$$

is obviously *not feasible*.

To deal with this issue, we relax them to **soft-margin** constraints:

$$y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1 - \xi_n, \quad \forall n$$

where we introduce **slack variables** $\xi_n \geq 0$.

SVM Primal formulation

We want ξ_n to be as small as possible too.

SVM Primal formulation

We want ξ_n to be as small as possible too. The objective becomes

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & \frac{1}{2} \|\mathbf{w}\|_2^2 + C \sum_n \xi_n \\ \text{s.t.} \quad & y_n (\mathbf{w}^T \phi(\mathbf{x}_n) + b) \geq 1 - \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

where C is a hyperparameter to balance the two goals.

Equivalent form

Formulation

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

Equivalent form

Formulation

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

is equivalent to

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & \max\{0, 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b)\} = \xi_n, \quad \forall n \end{aligned}$$

Equivalent form

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} = \xi_n, \quad \forall n \end{aligned}$$

is equivalent to

$$\min_{\mathbf{w}, b} C \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{1}{2} \|\mathbf{w}\|_2^2$$

Equivalent form

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} = \xi_n, \quad \forall n \end{aligned}$$

is equivalent to

$$\min_{\mathbf{w}, b} C \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{1}{2} \|\mathbf{w}\|_2^2$$

and

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

with $\lambda = 1/C$.

Equivalent form

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} = \xi_n, \quad \forall n \end{aligned}$$

is equivalent to

$$\min_{\mathbf{w}, b} C \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{1}{2} \|\mathbf{w}\|_2^2$$

and

$$\min_{\mathbf{w}, b} \sum_n \max \{0, 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b)\} + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

with $\lambda = 1/C$. *This is exactly minimizing L2 regularized hinge loss!*

Optimization

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

- It is a convex (**quadratic** in fact) problem

Optimization

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

- It is a convex (**quadratic** in fact) problem
- thus can apply any convex optimization algorithms, e.g. SGD

Optimization

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \boldsymbol{\phi}(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

- It is a convex (**quadratic** in fact) problem
- thus can apply any convex optimization algorithms, e.g. SGD
- there are **more specialized and efficient** algorithms

Optimization

$$\begin{aligned} \min_{\mathbf{w}, b, \{\xi_n\}} \quad & C \sum_n \xi_n + \frac{1}{2} \|\mathbf{w}\|_2^2 \\ \text{s.t.} \quad & 1 - y_n(\mathbf{w}^T \phi(\mathbf{x}_n) + b) \leq \xi_n, \quad \forall n \\ & \xi_n \geq 0, \quad \forall n \end{aligned}$$

- It is a convex (**quadratic** in fact) problem
- thus can apply any convex optimization algorithms, e.g. SGD
- there are **more specialized and efficient** algorithms
- but usually we apply kernel trick, which requires solving the *dual problem*

Outline

- 1 Logistics
- 2 Review of last lecture
- 3 Support vector machines (primal formulation)
- 4 Quiz 1 Specifics**

Logistics

- Quiz 1 is scheduled for March 3, 2021 from 10:00 – 12:00 PM. It is an in-class, open book and notes exam (no other resources are allowed).
- We will be using CrowdMark and WebEx to administer the exam.
- CrowdMark link: <https://app.crowdmark.com/sign-in/usc>
- We'll be releasing some questions (and solutions) for the topics covered in HW3 on Friday using CrowdMark. *Make sure you get familiar with the platform.*
- **Topics:** All topics covered till the next lecture.

On Quiz day

- Join ~15 min prior to the class time.
- We'll assign the exam 5 minutes before 10:00 AM on CrowdMark.
- You will have 10:00 – 11:45 AM for the exam, and the last 15 minutes are for you to upload your solutions.
- You will upload the pictures for each question separately.
- Join via the WebEx link on DEN@USC, *required to have video ON*.
- We'll be recording the video via WebEx.
- You may ask your questions privately to the teaching staff using WebEx chat, cannot communicate with fellow students in any way.