# Midterm Review

## Topics we covered

#### **Machine Learning**

#### Optimization

- Basics of optimization
  - Convexity
  - Unconstrained: GD, SGD
  - Constrained: Lagrange, KKT
  - Duality
- Linear Methods
  - Perceptrons
  - Support Vector Machines
  - Kernels

#### **Statistics**

- Basics of probability
  - Tail bounds
  - Density Estimation
  - Exponential Families
- Graphical Models



## Basics of Machine Learning

- Supervised/Unsupervised Learning?
  - Classification, Regression, Clustering
- Training error/Test error?
- Model Complexity: Overfitting/Underfitting
- True error Bayes Optimal Error

#### Bias-Variance Tradeoff

 When estimating a quantity θ, we evaluate the performance of an estimator by computing its risk – expected value of a loss function

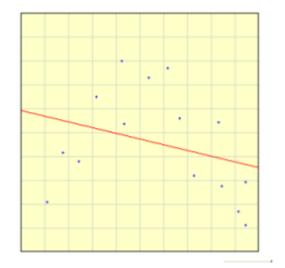
• 
$$R(\theta, \hat{\theta}) = E L(\theta, \hat{\theta})$$
, where *L* could be

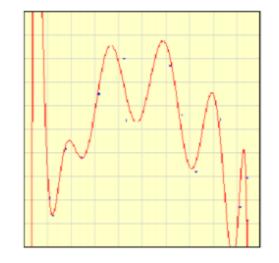
- Mean Squared Error Loss
- 0/1 Loss
- Hinge Loss (used for SVMs)
- Bias-Variance Decomposition:  $Y = f(x) + \varepsilon$   $Err(x) = E[f(x) - \hat{f}(x)^2]$  $= (E[\hat{f}(x)] - f(x))^2 + E[\hat{f}(x) - E[\hat{f}(x)]]^2 + \sigma_{\varepsilon}^2$

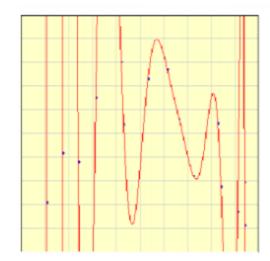
## **Bias-Variance Tradeoff**

 The choice of hypothesis class introduces a learning bias
 More complex class: less bias and more

variance.







# Training error

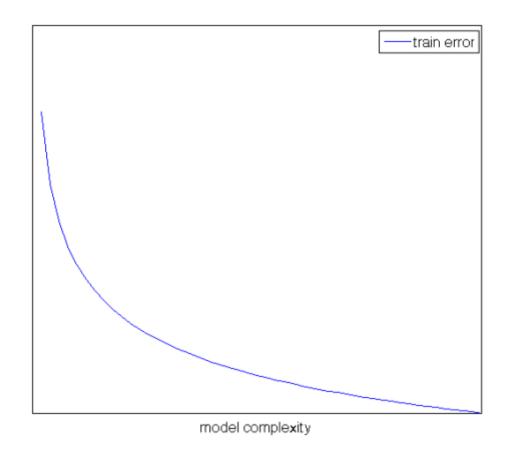
Given a dataset

Chose a loss function (L<sub>2</sub> for regression for example)

#### • Training set error:

$$error_{train} = \frac{1}{N_{train}} \sum_{\substack{j=1\\N_{train}}}^{N_{train}} \left( I(y_i \neq h(x)) \right)$$
$$error_{train} = \frac{1}{N_{train}} \sum_{\substack{j=1\\j=1}}^{N_{train}} \left( y_i - w.\mathbf{x_i} \right)^2$$

# Training error as a function of complexity

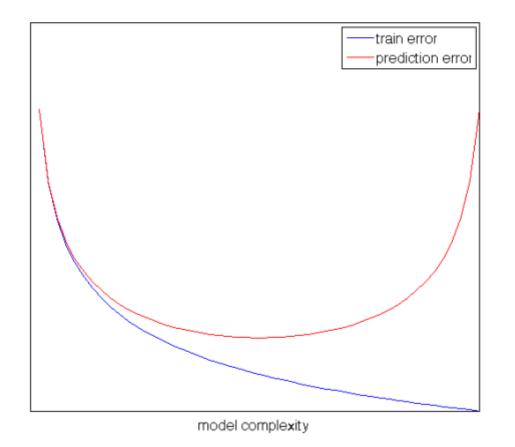


#### **Prediction error**

- Training error is not necessary a good measure
- We care about the error over all inputs points:

$$error_{true} = E_x \Big( I(y \neq h(x)) \Big)$$

# Prediction error as a function of complexity



#### **Train-test**

#### In practice:

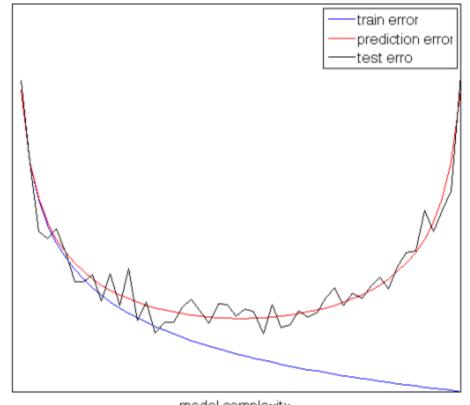
Randomly divide the dataset into test and train.

#### • Use training data to optimize parameters.

• Test error:  

$$error_{test} = \frac{1}{N_{test}} \sum_{i=1}^{N_{test}} \left( I(y_i \neq h(x_i)) \right)$$

## Test error as a function of complexity



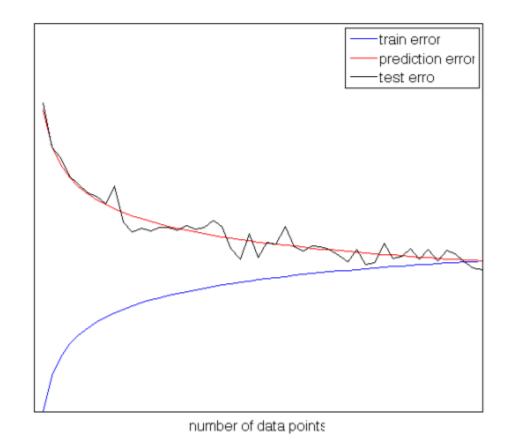
model complexity

# Overfitting

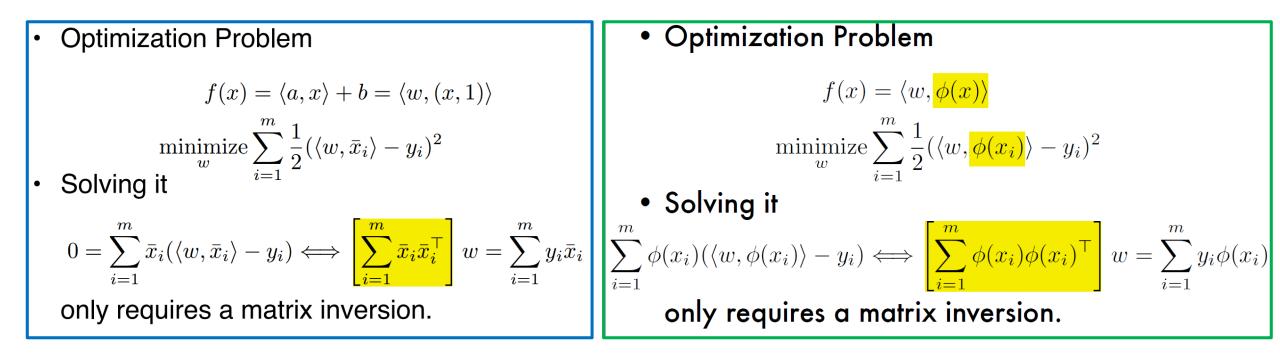
Overfitting happens when we obtain a model h when there exist another solution h' such that:

 $[error_{train}(h) < error_{train}(h')] \land [error_{true}(h) > error_{true}(h')]$ 

# Error as a function of data size for fixed complexity



## Regression



## Optimization

#### Convexity

- Convex Sets
- Convex Functions
- 2 Unconstrained Convex Optimization
  - First-order Methods
  - Newton's Method
- Constrained Optimization
  - Primal and dual problems
  - KKT conditions

#### **Convex Sets**

Definition

For  $x, x' \in X$  it follows that  $\lambda x + (1 - \lambda)x' \in X$  for  $\lambda \in [0, 1]$ 

- Examples
  - Empty set  $\emptyset$ , single point  $\{x_0\}$ , the whole space  $\mathbb{R}^n$
  - Hyperplane:  $\{x \mid a^{\top}x = b\}$ , halfspaces  $\{x \mid a^{\top}x \leq b\}$
  - Euclidean balls:  $\{x \mid ||x x_c||_2 \le r\}$
  - Positive semidefinite matrices: S<sup>n</sup><sub>+</sub> = {A ∈ S<sup>n</sup> | A ≥ 0} (S<sup>n</sup> is the set of symmetric n × n matrices)
- Convex Set C, D
  - Translation  $\{x + b \mid x \in C\}$
  - Scaling  $\{\lambda x \mid x \in C\}$
  - Affine function  $\{Ax + b \mid x \in C\}$
  - Intersection  $C \cap D$
  - Set sum  $C + D = \{x + y \mid x \in C, y \in D\}$

#### **Convex Functions**



**dom** f is convex,  $\lambda \in [0, 1]$  $\lambda f(x) + (1 - \lambda)f(y) \ge f(\lambda x + (1 - \lambda)y)$ 

• First-order condition: if f is differentiable,

 $f(y) \geq f(x) + \nabla f(x)^{\top}(y-x)$ 

• Second-order condition: if f is twice differentiable,

$$\nabla^2 f(x) \succeq 0$$

• Strictly convex:  $\nabla^2 f(x) \succ 0$ Strongly convex:  $\nabla^2 f(x) \succeq dI$  with d > 0

Copied from: Xuezhi Wang

#### Convex Functions – Examples

- Exponential.  $e^{ax}$  convex on  $\mathbb{R}$ , any  $a \in \mathbb{R}$
- Powers.  $x^a$  convex on  $\mathbb{R}_{++}$  when  $a \ge 1$  or  $a \le 0$ , and concave for  $0 \le a \le 1$ .
- Powers of absolute value.  $|x|^p$  for  $p \ge 1$ , convex on  $\mathbb{R}$ .
- Logarithm. log x concave on  $\mathbb{R}_{++}$ .
- Norms. Every norm on  $\mathbb{R}^n$  is convex.
- $f(x) = \max\{x_1, ..., x_n\}$  convex on  $\mathbb{R}^n$
- Log-sum-exp.  $f(x) = \log(e^{x_1} + ... + e^{x_n})$  convex on  $\mathbb{R}^n$ .

## Useful Observations

- A function is convex if and only if its epigraph is a convex set.
- Below-Sets of Convex Functions is a convex set
- Convex functions cannot have local minima

## Gradient Descent



**given** a starting point  $x \in \text{dom} f$ .

#### repeat

- 1.  $\Delta x := -\nabla f(x)$
- 2. Choose step size t via exact or backtracking line search.

3. update.  $x := x + t\Delta x$ .

Until stopping criterion is satisfied.

- Key idea
  - Gradient points into descent direction
  - Locally gradient is good approximation of objective function

#### Newton's Method

Goal: 
$$\phi : \mathbb{R} \to \mathbb{R}$$
  
 $\phi(x^*) = 0$   
 $x^* = ?$ 

**Linear Approximation (1**<sup>st</sup> order Taylor approx):

$$\phi(\underbrace{x + \Delta x}_{\mathsf{x}^*}) = \phi(x) + \phi'(x)\Delta x + o(|\Delta x|)$$

$$\underbrace{\mathsf{x}^*}_{\mathsf{\Phi}(\mathsf{x}^*) = 0}$$

Therefore,

$$0 \approx \phi(x) + \phi'(x) \Delta x$$
$$x^* - x = \Delta x = -\frac{\phi(x)}{\phi'(x)}$$
$$x_{k+1} = x_k - \frac{\phi(x)}{\phi'(x)}$$

Copied from: Prof Barnabas

#### Newton's Method

 $f: \mathbb{R}^n \to \mathbb{R}, \ f \text{ is differentiable.}$  $\min_{x \in \mathbb{R}^n} f(x)$ 

We need to find the roots of  $\nabla f(x) = 0_n$  $\nabla f : \mathbb{R}^n \to \mathbb{R}^n$ 

Newton system:  $\nabla f(x) + \nabla^2 f(x) \Delta x = 0_n$ 

Newton step:  $\Delta x = x_{k+1} - x_k = -[\nabla^2 f(x)]^{-1} \nabla f(x)$ 

Iterate until convergence, or max number of iterations exceeded

Copied from: Prof Barnabas

# Duality

**Primal problem:** 

$$\min_{x \in \mathbb{R}^n} f(x)$$
  
subject to  $h_i(x) \le 0, i = 1, \dots, m$ 

Lagrangian:

$$L(x, u) = f(x) + \sum_{i=1}^{m} u_i h_i(x)$$

where  $u \in \mathbb{R}^m$  and  $u \ge 0$ . Lagrange dual function:

$$g(u) = \min_{x \in \mathbb{R}^n} L(x, u)$$

# Duality

Dual problem:

 $\max_{u} g(u)$ <br/>subject to  $u \ge 0$ 

- Dual problem is a convex optimization problem, since g is always concave (even if primal problem is not convex)
- The primal and dual optimal values always satisfy weak duality:  $f^* \ge g^*$
- Slater's condition: for convex primal, if there is an x such that  $h_1(x) < 0, ..., h_m(x) < 0$  and  $l_1(x) = 0, ..., l_r(x) = 0$  then strong duality holds:  $f^* = g^*$ . Or equivalently Karlin's or strict constraint qualification.

### **KKT** Conditions

If  $x^*, u^*, v^*$  are primal and dual solutions, with zero duality gap (strong duality holds), then  $x^*, u^*, v^*$  satisfy the KKT conditions:

- stationarity:  $0 \in \partial f(x^*) + \sum u_i^* \partial h_i(x^*)$
- complementary slackness:  $u_i^* h_i(x^*) = 0$  for all i
- primal feasibility:  $h_i(x^*) \leq 0$  for all i
- dual feasibility:  $u_i^* \ge 0$  for all i

#### Perceptrons

```
initialize w = 0 and b = 0
repeat
if y_i [\langle w, x_i \rangle + b] \le 0 then
w \leftarrow w + y_i x_i and b \leftarrow b + y_i
end if
until all classified correctly
```

- Nothing happens if classified correctly
- Weight vector is linear combination  $w = \sum y_i x_i$

 $i \in I$ 

• Classifier is linear combination of inner products  $f(x) = \sum_{i \in I} y_i \langle x_i, x \rangle + b$ 

## Convergence of Perceptrons

• If there exists some  $(w^*, b^*)$  with unit length and  $y_i [\langle x_i, w^* \rangle + b^*] \ge \rho$  for all *i* 

then the perceptron converges to a linear separator after a number of steps bounded by

$$(b^{*2}+1)(r^2+1)\rho^{-2}$$
 where  $||x_i|| \le r$ 

- Dimensionality independent
- Order independent (i.e. also worst case)
- Scales with 'difficulty' of problem

#### Back to Optimization

 A typical machine learning problem has a penalty/regularizer + loss form

$$\min_{w} F(w) = g(w) + \frac{1}{n} \sum_{i=1}^{n} f(w; y_i, x_i),$$

 $x_i, w \in \mathbb{R}^p$ ,  $y_i \in \mathbb{R}$ , both g and f are convex

- Today we only consider differentiable f, and let g = 0 for simplicity
- ► For example, let f(w; y<sub>i</sub>, x<sub>i</sub>) = log p(y<sub>i</sub>|x<sub>i</sub>, w), we are trying to maximize the log likelihood, which is

$$\max_{w} \frac{1}{n} \sum_{i=1}^{n} \log p(y_i | x_i, w)$$

#### Gradient Descent

• choose initial  $w^{(0)}$ , repeat

$$w^{(t+1)} = w^{(t)} - \eta_t \cdot \nabla F(w^{(t)})$$

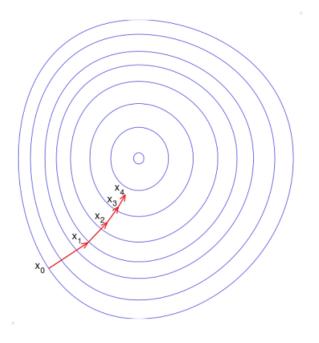
until stop

•  $\eta_t$  is the learning rate, and

$$\nabla F(w^{(t)}) = \frac{1}{n} \sum_{i} \nabla_{w} f(w^{(t)}; y_{i}, x_{i})$$

• How to stop?  $||w^{(t+1)} - w^{(t)}|| \le \epsilon$  or  $||\nabla F(w^{(t)})|| \le \epsilon$ 

# Two dimensional example:



#### Stochastic Gradient Descent

We name <sup>1</sup>/<sub>n</sub> ∑<sub>i</sub> f(w; y<sub>i</sub>, x<sub>i</sub>) the empirical loss, the thing we hope to minimize is the expected loss

$$f(w) = \mathbb{E}_{y_i, x_i} f(w; y_i, x_i)$$

Suppose we receive an infinite stream of samples (y<sub>t</sub>, x<sub>t</sub>) from the distribution, one way to optimize the objective is

$$w^{(t+1)} = w^{(t)} - \eta_t \nabla_w f(w^{(t)}; y_t, x_t)$$

- On practice, we simulate the stream by randomly pick up (y<sub>t</sub>, x<sub>t</sub>) from the samples we have
- Comparing the average gradient of GD  $\frac{1}{n} \sum_{i} \nabla_{w} f(w^{(t)}; y_{i}, x_{i})$

#### SGD and Perceptron

Recall Perceptron: initialize w, repeat

$$w = w + \begin{cases} y_i x_i & \text{if } y_i \langle w, x_i \rangle < 0 \\ 0 & \text{otherwise} \end{cases}$$

Fix learning rate  $\eta = 1$ , let  $f(w; y, x) = \max(0, -y_i \langle w, x_i \rangle)$ , then

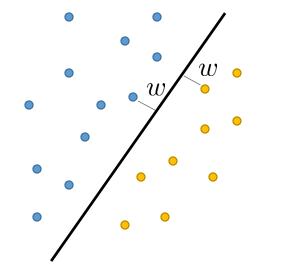
$$\nabla_w f(w; y, x) = \begin{cases} -y_i x_i & \text{if } y_i \langle w, x_i \rangle < 0\\ 0 & \text{otherwise} \end{cases}$$

we derive Perceptron from SGD

## SVM Primal

Find maximum margin hyper-plane

$$f(x) = \langle w, x \rangle + b = 0$$



Hard Margin

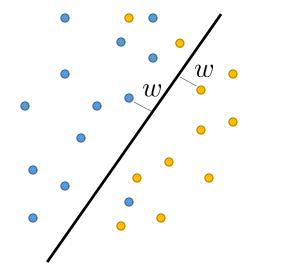
 $\min_{w,b} ||w||^2$ subject to  $(\langle w, x_i \rangle + b)y_i \ge 1$ 

## SVM Primal

Find maximum margin hyper-plane

$$f(x) = \langle w, x \rangle + b = 0$$

Soft Margin

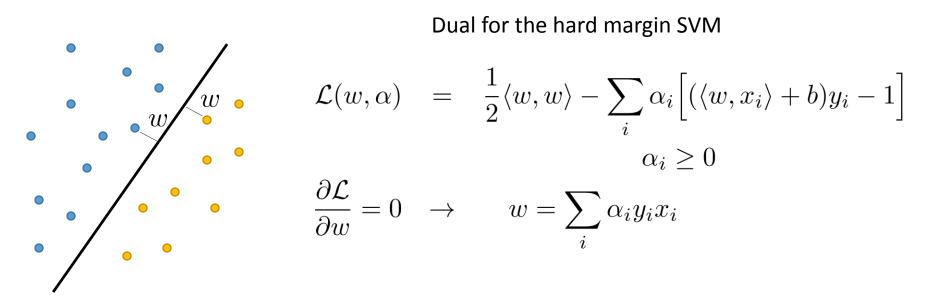


$$\min_{w,b} ||w||^2 + C \sum_i \xi_i$$
  
subject to  $(\langle w, x_i \rangle + b)y_i \ge 1$   
 $\xi_i \ge 0$ 

### SVM Dual

Find maximum margin hyper-plane

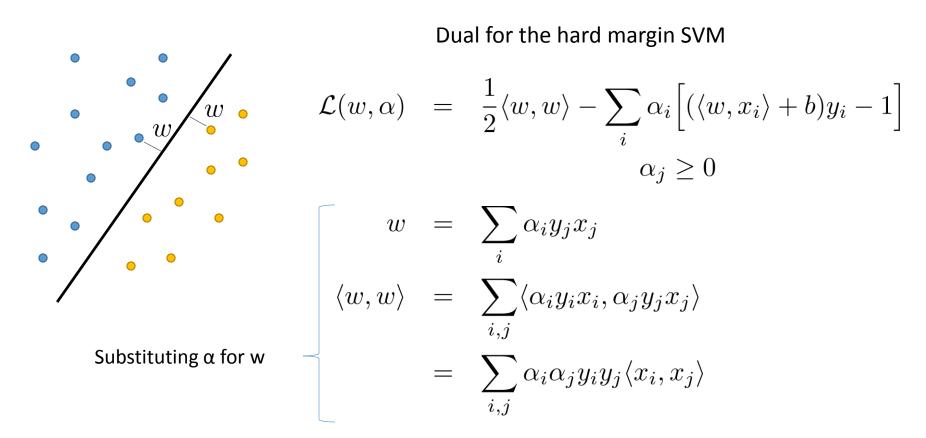
 $f(x) = \langle w, x \rangle + b = 0$ 



### SVM Dual

Find maximum margin hyper-plane

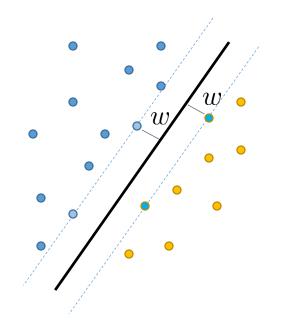
 $f(x) = \langle w, x \rangle + b = 0$ 



### SVM Dual

Find maximum margin hyper-plane

 $\mathcal{L}$ 



$$f(x) = \langle w, x \rangle + b = 0$$

Dual for the hard margin SVM

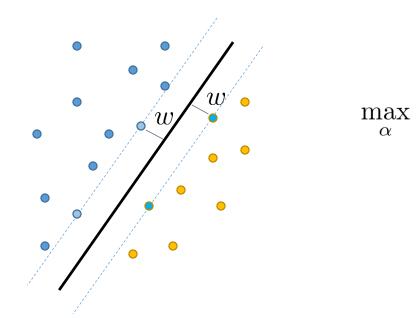
$$(w, \alpha) = \frac{1}{2} \langle w, w \rangle - \sum_{i} \alpha_{i} \Big[ (\langle w, x_{i} \rangle + b) y_{i} - 1 \Big]$$
$$\alpha_{j} \ge 0$$

The constraints are active for the support vectors

$$\forall k \text{ s.t. } a_k > 0 \qquad b = y_k - \langle w, x_k \rangle$$

#### SVM Dual

Find maximum margin hyper-plane



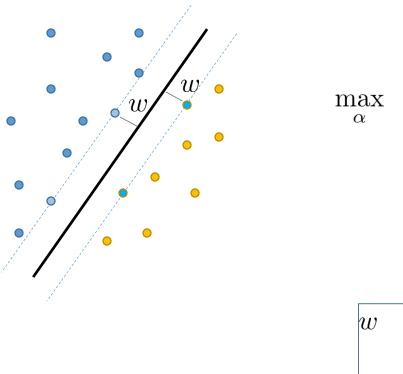
$$f(x) = \langle w, x \rangle + b = 0$$

Dual for the hard margin SVM

$$-\frac{1}{2}\sum_{i} \alpha_{i}\alpha_{j}y_{i}y_{j}\langle x_{i}, x_{j}\rangle + \sum_{i} \alpha_{i}$$
$$\sum_{i} \alpha_{i}y_{i} = 0$$
$$\alpha_{i} \ge 0$$

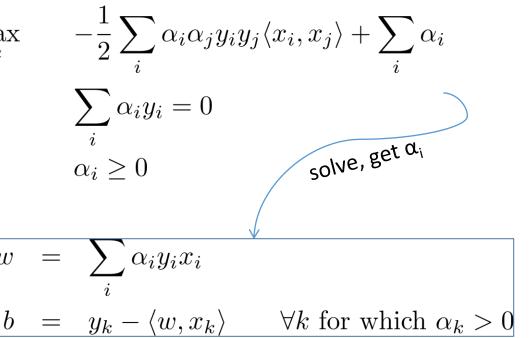
## SVM – Computing w

Find maximum margin hyper-plane



 $f(x) = \langle w, x \rangle + b = 0$ 

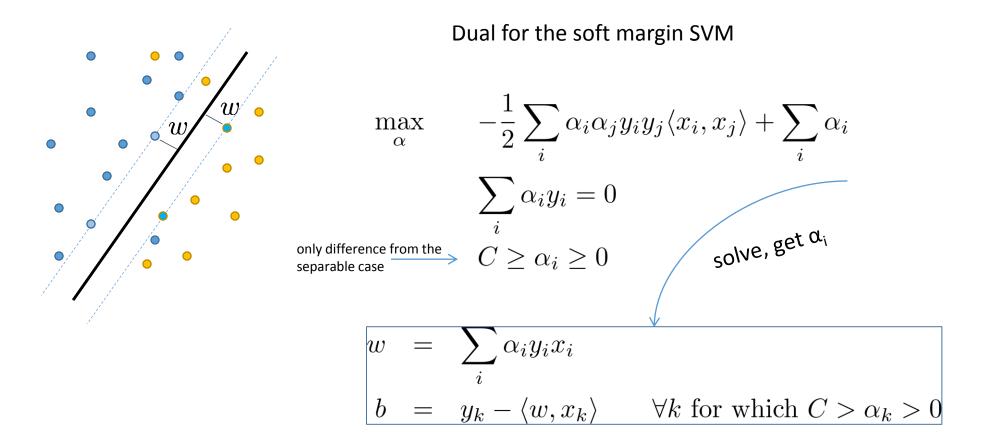
Dual for the hard margin SVM



## SVM – Computing w

Find maximum margin hyper-plane

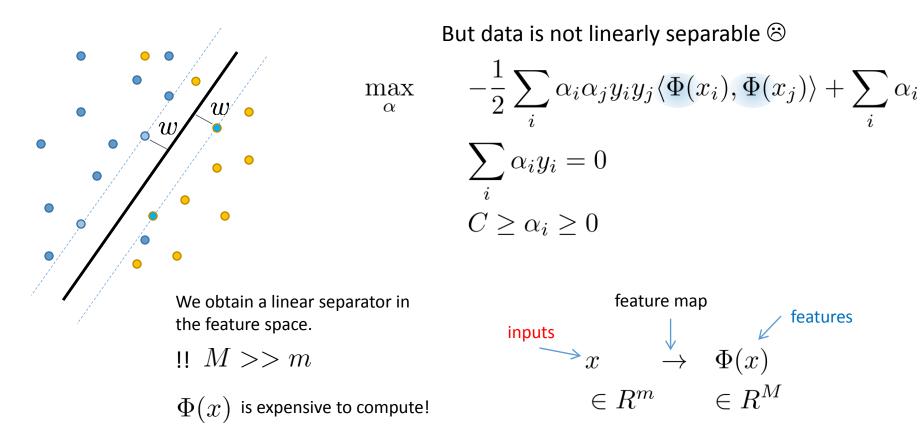
 $f(x) = \langle w, x \rangle + b = 0$ 



### SVM – the feature map

Find maximum margin hyper-plane

 $f(x) = \langle w, \Phi(x) \rangle + b = 0$ 

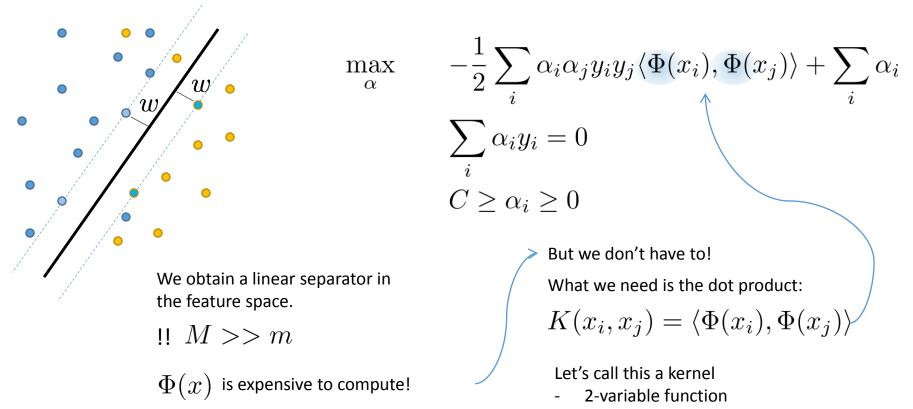


Copied from: Junier Oliva

40

# Introducing the kernel

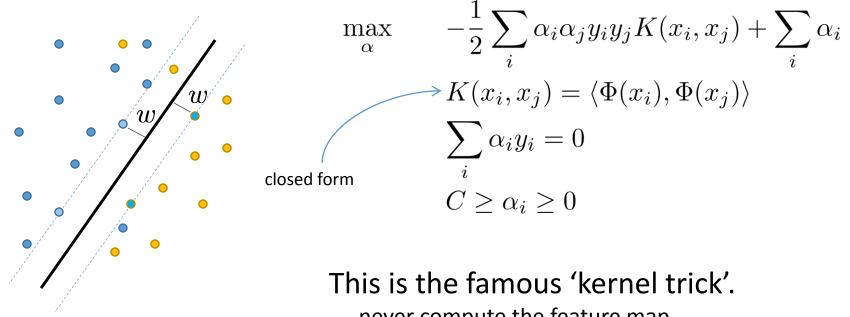
The dual formulation no longer depends on w, only on a dot product!



- can be written as a dot product

#### Kernel SVM

The dual formulation no longer depends on w, only on a dot product!



- never compute the feature map
- learn using the closed form K
- constant time for HD dot products

#### Kernel SVM – Run time

What happens when we need to classify some  $x_0$ ?

Recall that w depends on  $\boldsymbol{\alpha}$ 

$$w = \sum_{i} \alpha_{i} y_{i} \Phi(x_{i})$$
  

$$b = y_{k} - \langle w, \Phi(x_{k}) \rangle$$
  

$$\forall k \text{ s.t. } C > \alpha_{k} > 0$$

Our classifier for  $\mathbf{x}_0$  uses w  $sign(\langle w, \Phi(x_0) \rangle + b)$ 

#### Kernel SVM – Run time

What happens when we need to classify some  $x_0$ ?

Recall that w depends on  $\alpha$ 

$$w = \sum_{i} \alpha_{i} y_{i} \Phi(x_{i})$$
  

$$b = y_{k} - \langle w, \Phi(x_{k}) \rangle$$
  

$$\forall k \text{ s.t. } C > \alpha_{k} > 0$$

Our classifier for  $x_0$  uses w  $sign(\langle w, \Phi(x_0) \rangle + b)$ 

Who needs w when we've got dot products?

$$w, \Phi(x_0)\rangle = \sum_i \alpha_i y_i K(x_0, x_i)$$
  
 $b = y_k - \sum_i \alpha_i y_i K(x_k, x_i)$   
 $k \rightarrow \text{ support vectors}$ 

### Kernel SVM Recap

Pick kernel

Solve the optimization to get  $\boldsymbol{\alpha}$ 

$$\max_{\alpha} \quad -\frac{1}{2} \sum_{i} \alpha_{i} \alpha_{j} y_{i} y_{j} K(x_{i}, x_{j}) + \sum_{i} \alpha_{i}$$
$$K(x_{i}, x_{j}) = \langle \Phi(x_{i}), \Phi(x_{j}) \rangle$$
$$\sum_{i} \alpha_{i} y_{i} = 0$$
$$C \ge \alpha_{i} \ge 0$$

Compute b using the support vectors

$$b = y_k - \sum_i \alpha_i y_i K(x_k, x_i)$$

Classify as

$$sign\left(\sum_{i} \alpha_{i} y_{i} K(x_{0}, x_{i}) + b\right)$$

## Reminder on Kernels

• Remember Kernels are nothing but implicit feature maps  $\phi: \mathcal{X} \to \mathbb{R}^d$ 

• Gram Matrix

- of a set of vectors  $x_1 \dots x_n$  in the inner product space defined by the kernel K
- $G_{ij} = K(x_i, x_j) = \langle \phi(x_i), \phi(x_j) \rangle \quad \forall i, j \in 1 \dots n$
- Gram Matrix is always positive definite

# Bayes Rule

Joint Probability

 $\Pr(X, Y) = \Pr(X|Y) \Pr(Y) = \Pr(Y|X) \Pr(X)$ 

Bayes Rule

$$\Pr(X|Y) = \frac{\Pr(Y|X) \cdot \Pr(X)}{\Pr(Y)}$$

- Hypothesis testing
- Reverse conditioning

# Law of Large Numbers

- Random variables  $x_i$  with mean  $\mu = \mathbf{E}[x_i]$
- Empirical average  $\hat{\mu}_n := \frac{1}{n} \sum_{i=1}^n x_i$
- Weak Law of Large Numbers

 $\lim_{n \to \infty} \Pr\left(|\hat{\mu}_n - \mu| \le \epsilon\right) = 1 \text{ for any } \epsilon > 0$ 

Strong Law of Large Numbers

$$\Pr\left(\lim_{n \to \infty} \hat{\mu}_n = \mu\right) = 1$$

this means convergence in probability

## Central Limit Theorem

- Independent random variables  $x_i$  with mean  $\mu_i$  and standard deviation  $\sigma_i$
- The random variable  $z_n := \left[\sum_{i=1}^n \sigma_i^2\right]^{-\frac{1}{2}} \left[\sum_{i=1}^n x_i - \mu_i\right]$ converges to a Normal Distribution  $\mathcal{N}(0, 1)$
- Special case IID random variables & average

$$\frac{\sqrt{n}}{\sigma} \left[ \frac{1}{n} \sum_{i=1}^{n} x_i - \mu \right] \to \mathcal{N}(0, 1)$$
$$O\left( n^{-\frac{1}{2}} \right) \text{convergence}$$

#### Tail Bounds

**Markov Inequality:** If X is any nonnegative integrable random variable and a > 0, then

$$\Pr\left(X > a\right) \le \frac{\mathbb{E}[X]}{a}$$

**Chebyshev Inequality:** If X is any random variable with mean  $\mu$  and variance  $\sigma^2$ . Then for any  $\epsilon > 0$ , we have

$$\Pr\left(|X - \mu| > \epsilon\right) \le \frac{\sigma^2}{\epsilon^2}$$

#### More Tail Bounds

**The Chernoff Bound:** Suppose  $Y_1, ..., Y_r$  are i.i.d. random variables, taking values in  $\{0, 1\}$ . Let  $p = E[Y_i]$  and > 0. Then

$$\Pr\left(\sum_{i} Y_i > nq\right) \le \exp(-rD(q||p))$$

**Hoeffding's Inequality:** Suppose  $Y_1, ..., Y_r$  are i.i.d. random variables, taking values in  $(a_i, b_i)$ . Then

$$\Pr\left(\left|\sum_{i} (Y_i - \mathbb{E}[Y_i] \right| > t\right) \le 2 \exp\left(-\frac{2t^2}{\sum_{i=1}^r (b_i - a_i)^2}\right)$$

**Union Bound:** set of events  $A_1, A_2, A_3, ...,$  we have

$$\Pr\left(\bigcup_{i} A\right) \le \sum_{i} \Pr(A_i)$$



# A/B testing