SE125 Machine Learning

Support Vector Machines

Yue Ding
School of Software, Shanghai Jiao Tong University
dingyue@sjtu.edu.cn

References and Acknowledgement

The slides in this lecture are mainly from Prof. Weinan Zhang's machine learning course for ACM class (CS420, Spring 2020)

- http://wnzhang.net/teaching/cs420/slides/3-svm-kernel.pdf
- http://wnzhang.net

课程难度:



掌握程度:



Recall--Linear Regression

Linear regression model

$$y = f_{\theta}(x) = \theta_0 + \sum_{j=1}^{d} \theta_j x_j = \theta^{\top} x$$

 $x = (1, x^1, x^2, \dots, x^d)$

Objective function to minimize

$$J_{\theta} = \frac{1}{2N} \sum_{i=1}^{N} (y_i - f_{\theta}(x_i))^2 \qquad \min_{\theta} J_{\theta}$$

Optimization--SGD

$$\theta_{\text{new}} = \theta_{\text{old}} + \eta (y_i - f_{\theta}(x_i)) x_i$$

Optimization--matrix form

$$\hat{\boldsymbol{\theta}} = (\boldsymbol{X}^{\top} \boldsymbol{X} + \boldsymbol{\lambda} \boldsymbol{I})^{-1} \boldsymbol{X}^{\top} \boldsymbol{y}$$

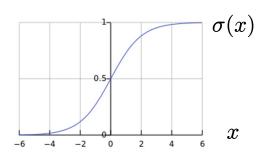
What if it's a classification problem?

Logistic Regression

Logistic regression is a binary classification model

$$p_{\theta}(y = 1|x) = \sigma(\theta^{\top}x) = \frac{1}{1 + e^{-\theta^{\top}x}}$$

$$p_{\theta}(y = 0|x) = \frac{e^{-\theta^{\top}x}}{1 + e^{-\theta^{\top}x}}$$



Cross entropy loss function

$$\mathcal{L}(y,x,p_{ heta}) = -y\log\sigma(heta^ op x) - (1-y)\log(1-\sigma(heta^ op x))$$

Gradient

$$\frac{\partial \mathcal{L}(y, x, p_{\theta})}{\partial \theta} = -y \frac{1}{\sigma(\theta^{\top} x)} \sigma(z) (1 - \sigma(z)) x - (1 - y) \frac{-1}{1 - \sigma(\theta^{\top} x)} \sigma(z) (1 - \sigma(z)) x$$

$$= (\sigma(\theta^{\top} x) - y) x$$

$$\theta \leftarrow \theta + \eta(y - \sigma(\theta^{\top} x)) x$$

$$\frac{\partial \sigma(z)}{\partial z} = \sigma(z) (1 - \sigma(z))$$

Label Decision

Logistic regression provides the probability

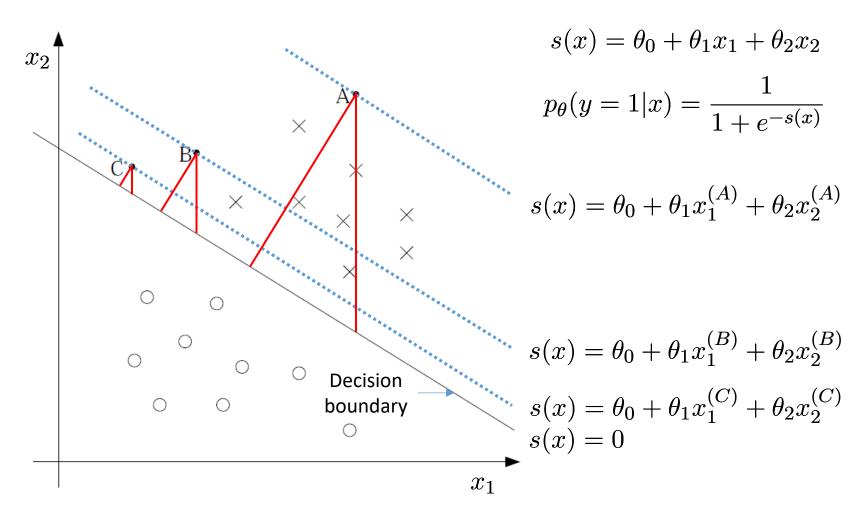
$$p_{\theta}(y = 1|x) = \sigma(\theta^{\top}x) = \frac{1}{1 + e^{-\theta^{\top}x}}$$

$$p_{\theta}(y = 0|x) = \frac{e^{-\theta^{\top}x}}{1 + e^{-\theta^{\top}x}}$$

• The final label of an instance is decided by setting a threshold \boldsymbol{h}

$$\hat{y} = \begin{cases} 1, & p_{\theta}(y = 1|x) > h \\ 0, & \text{otherwise} \end{cases}$$

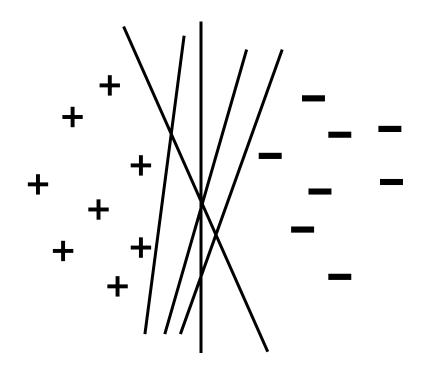
Logistic Regression Scores



The higher score, the larger distance to the decision boundary, the higher confidence

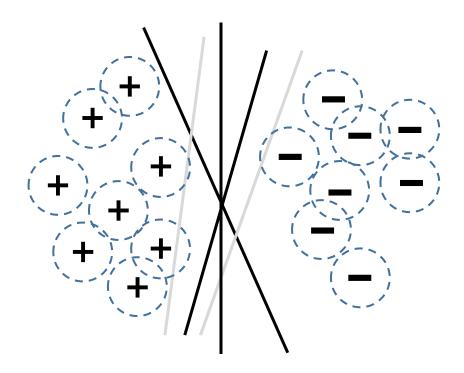
Linear Classification

 For linear separable cases, we have multiple decision boundaries



Linear Classification

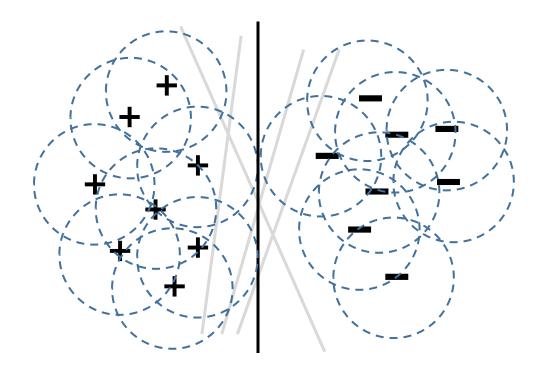
 For linear separable cases, we have multiple decision boundaries



Ruling out some separators by considering data noise

Linear Classification

 For linear separable cases, we have multiple decision boundaries



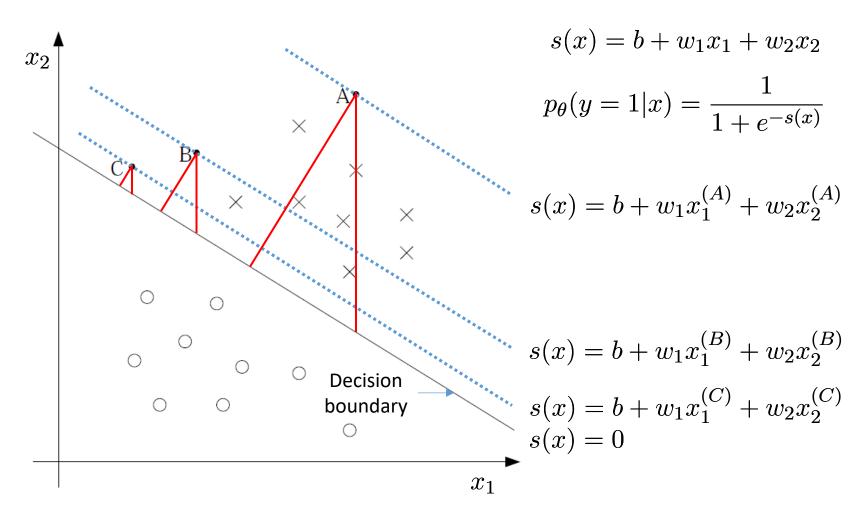
• The intuitive optimal decision boundary: the largest margin

Notations for SVMs

- Feature vector x
- Class label $y \in \{-1, 1\}$
- Parameters
 - Intercept b
 - ullet Feature weight vector w
- Label prediction

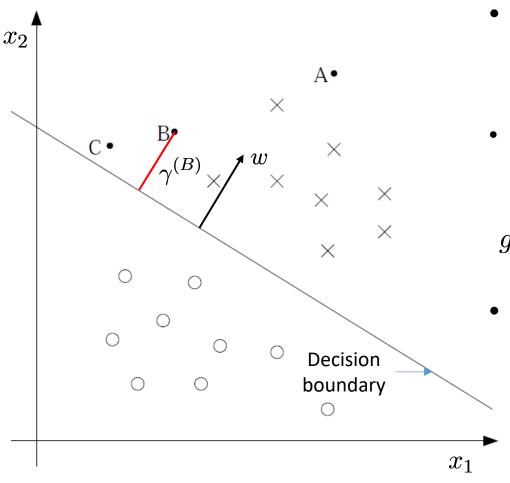
$$h_{w,b}(x) = g(w^{\top}x + b)$$
$$g(z) = \begin{cases} +1 & z \ge 0\\ -1 & \text{otherwise} \end{cases}$$

Logistic Regression Scores



The higher score, the larger distance to the separating hyperplane, the higher confidence

Margins



Functional margin

$$\hat{\gamma}^{(i)} = y^{(i)}(w^{\top}x^{(i)} + b)$$

 Note that the separating hyperplane won't change with the magnitude of (w, b)

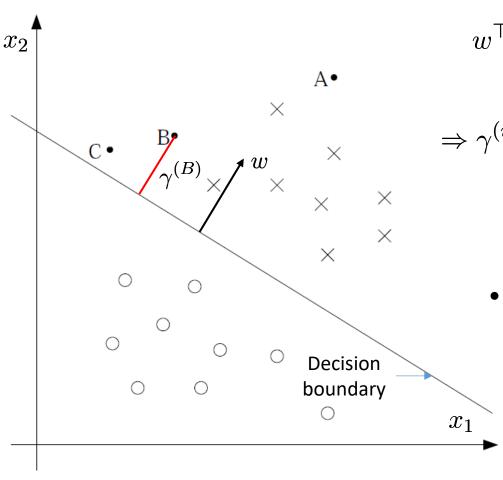
$$g(w^{\top}x + b) = g(2w^{\top}x + 2b)$$

Geometric margin

$$\gamma^{(i)} = y^{(i)}(w^{\top}x^{(i)} + b)$$

where $||w||^2 = 1$

Margins



Decision boundary

$$w^{\top} \left(x^{(i)} - \gamma^{(i)} y^{(i)} \frac{w}{\|w\|} \right) + b = 0$$

$$\Rightarrow \gamma^{(i)} = y^{(i)} \frac{w^{\top} x^{(i)} + b}{\|w\|}$$
$$= y^{(i)} \left(\left(\frac{w}{\|w\|} \right)^{\top} x^{(i)} + \frac{b}{\|w\|} \right)$$

Given a training set

$$S = \{(x_i, y_i)\}_{i=1...m}$$

the smallest geometric margin

$$\gamma = \min_{i=1\dots m} \gamma^{(i)}$$

Objective of an SVM

Find a separable hyperplane that maximizes the minimum geometric margin

$$\max_{\gamma,w,b} \ \gamma$$
 s.t. $y^{(i)}(w^{\top}x^{(i)}+b) \geq \gamma, \ i=1,\ldots,m$
$$\|w\|=1 \quad \text{(non-convex constraint)}$$

Equivalent to normalized functional margin

$$\max_{\hat{\gamma}, w, b} \frac{\hat{\gamma}}{\|w\|}$$
 (non-convex objective) s.t. $y^{(i)}(w^{\top}x^{(i)} + b) \geq \hat{\gamma}, \ i = 1, \dots, m$

Lagrangian for Convex Optimization

A convex optimization problem

$$\min_{w} f(w)$$
s.t. $h_i(w) = 0, \quad i = 1, \dots, l$

The Lagrangian of this problem is defined as

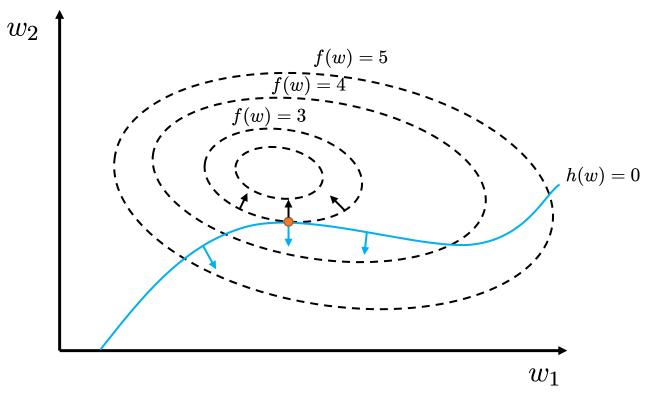
$$\mathcal{L}(w, \beta) = f(w) + \sum_{i=1}^l \beta_i h_i(w)$$
 Lagrangian multipliers

Solving

$$\frac{\partial \mathcal{L}(w,\beta)}{\partial w} = 0 \qquad \frac{\partial \mathcal{L}(w,\beta)}{\partial \beta} = 0$$

yields the solution of the original optimization problem.

Lagrangian for Convex Optimization



$$\mathcal{L}(w,\beta) = f(w) + \beta h(w)$$

$$\frac{\partial \mathcal{L}(w,\beta)}{\partial w} = \frac{\partial f(w)}{\partial w} + \beta \frac{\partial h(w)}{\partial w} = 0$$

i.e., two gradients on the same direction

With Inequality Constraints

A convex optimization problem

$$\min_{w} f(w)$$
s.t. $g_{i}(w) \leq 0, \quad i = 1, ..., k$
 $h_{i}(w) = 0, \quad i = 1, ..., l$

The Lagrangian of this problem is defined as

$$\mathcal{L}(w,\alpha,\beta) = f(w) + \sum_{i=1}^k \alpha_i g_i(w) + \sum_{i=1}^l \beta_i h_i(w)$$
 Lagrangian multipliers

Primal Problem

A convex optimization

$$\min_{w} \quad f(w)$$
s.t. $g_i(w) \leq 0, \quad i = 1, \dots, k$
 $h_i(w) = 0, \quad i = 1, \dots, l$

The Lagrangian

$$\mathcal{L}(w,lpha,eta) = f(w) + \sum_{i=1}^k lpha_i g_i(w) + \sum_{i=1}^l eta_i h_i(w)$$

• The primal problem

$$\theta_{\mathcal{P}}(w) = \max_{\alpha, \beta: \alpha_i \ge 0} \mathcal{L}(w, \alpha, \beta)$$

ullet If a given w violates any constraints, i.e.,

$$g_i(w) > 0$$
 or $h_i(w) \neq 0$

• Then $\theta_{\mathcal{P}}(w) = +\infty$

Primal Problem

A convex optimization

$$\min_{w} \quad f(w)$$
s.t. $g_i(w) \leq 0, \quad i = 1, \dots, k$
 $h_i(w) = 0, \quad i = 1, \dots, l$

The Lagrangian

$$\mathcal{L}(w,lpha,eta) = f(w) + \sum_{i=1}^k lpha_i g_i(w) + \sum_{i=1}^l eta_i h_i(w)$$

The primal problem

$$\theta_{\mathcal{P}}(w) = \max_{\alpha, \beta: \alpha_i \ge 0} \mathcal{L}(w, \alpha, \beta)$$

- ullet Conversely, if all constraints are satisfied for w
- Then $\theta_{\mathcal{P}}(w) = f(w)$

$$\theta_{\mathcal{P}}(w) = \begin{cases} f(w) & \text{if } w \text{ satisfies primal constraints} \\ +\infty & \text{otherwise} \end{cases}$$

Primal Problem

$$\theta_{\mathcal{P}}(w) = \begin{cases} f(w) & \text{if } w \text{ satisfies primal constraints} \\ +\infty & \text{otherwise} \end{cases}$$

The minimization problem

$$\min_{w} \theta_{\mathcal{P}}(w) = \min_{w} \max_{\alpha, \beta: \alpha_i \ge 0} \mathcal{L}(w, \alpha, \beta)$$

is the same as the original problem

$$\min_{w} f(w)$$
s.t. $g_{i}(w) \leq 0, \quad i = 1, \dots, k$
 $h_{i}(w) = 0, \quad i = 1, \dots, l$

• Define the value of the primal problem $p^* = \min_w \theta_{\mathcal{P}}(w)$

Dual Problem

A slightly different problem

$$\theta_{\mathcal{D}}(\alpha, \beta) = \min_{w} \mathcal{L}(w, \alpha, \beta)$$

Define the dual optimization problem

$$\max_{\alpha,\beta:\alpha_i\geq 0} \theta_{\mathcal{D}}(\alpha,\beta) = \max_{\alpha,\beta:\alpha_i\geq 0} \min_{w} \mathcal{L}(w,\alpha,\beta)$$

Min & Max exchanged compared to the primal problem

$$\min_{w} \theta_{\mathcal{P}}(w) = \min_{w} \max_{\alpha, \beta: \alpha_{i} > 0} \mathcal{L}(w, \alpha, \beta)$$

Define the value of the dual problem

$$d^* = \max_{\alpha,\beta:\alpha_i>0} \min_{w} \mathcal{L}(w,\alpha,\beta)$$

Primal Problem vs. Dual Problem

$$d^* = \max_{\alpha, \beta: \alpha_i \ge 0} \min_{w} \mathcal{L}(w, \alpha, \beta) \le \min_{w} \max_{\alpha, \beta: \alpha_i \ge 0} \mathcal{L}(w, \alpha, \beta) = p^*$$

Proof

$$\min_{w} \mathcal{L}(w, \alpha, \beta) \le \mathcal{L}(w, \alpha, \beta), \forall w, \alpha \ge 0, \beta$$

$$\Rightarrow \max_{\alpha,\beta:\alpha\geq 0} \min_{w} \mathcal{L}(w,\alpha,\beta) \leq \max_{\alpha,\beta:\alpha\geq 0} \mathcal{L}(w,\alpha,\beta), \forall w$$

$$\Rightarrow \max_{\alpha,\beta:\alpha\geq 0} \min_{w} \mathcal{L}(w,\alpha,\beta) \leq \min_{w} \max_{\alpha,\beta:\alpha\geq 0} \mathcal{L}(w,\alpha,\beta)$$

• But under certain condition $d^* = p^*$

Karush-Kuhn-Tucker (KKT) Conditions

- If f and g_i 's are convex and h_i 's are affine, and suppose g_i 's are all strictly feasible
- then there must exist w^* , α^* , θ^*
 - w* is the solution of the primal problem
 - α^* , θ^* are the solutions of the dual problem
 - and the values of the two problems are equal $p^* = d^* = \mathcal{L}(w^*, \alpha^*, \beta^*)$
- And w^* , α^* , θ^* satisfy the KKT conditions

$$\frac{\partial}{\partial w_i}\mathcal{L}(w^*,\alpha^*,\beta^*)=0,\ i=1,\dots,n$$

$$\frac{\partial}{\partial \beta_i}\mathcal{L}(w^*,\alpha^*,\beta^*)=0,\ i=1,\dots,l$$
 KKT dual complementarity $\longrightarrow \alpha_i^*g_i(w^*)=0,\ i=1,\dots,k$ condition

KKT dual

condition

$$g_i(w^*) \le 0, \ i = 1, \dots, k$$

 $\alpha^* > 0, \ i = 1, \dots, k$

- Moreover, if some w^* , α^* , θ^* satisfy the KKT conditions, then it is also a solution to the primal and dual problems.
- More details please refer to Boyd "Convex optimization" 2004.

Now Back to SVM Problem

Objective of an SVM

SVM objective: finding the optimal margin classifier

$$\min_{w,b} \frac{1}{2} ||w||^2$$

s.t. $y^{(i)}(w^{\top}x^{(i)} + b) \ge 1, i = 1, ..., m$

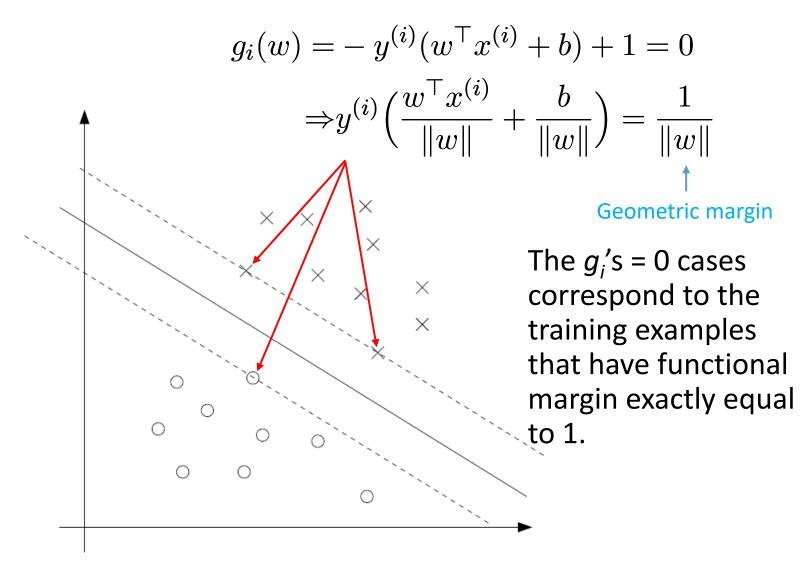
Re-wright the constraints as

$$g_i(w,b) = -y^{(i)}(w^{\top}x^{(i)} + b) + 1 \le 0$$

so as to match the standard optimization form

$$\min_{w} f(w)$$
s.t. $g_{i}(w) \leq 0, \quad i = 1, ..., k$
 $h_{i}(w) = 0, \quad i = 1, ..., l$

Equality Cases



Objective of an SVM

• SVM objective: finding the optimal margin classifier

$$\min_{w,b} \frac{1}{2} ||w||^2$$
s.t. $-y^{(i)}(w^{\top}x^{(i)} + b) + 1 \le 0, i = 1, ..., m$

Lagrangian

$$\mathcal{L}(w, b, \alpha) = \frac{1}{2} \|w\|^2 - \sum_{i=1}^{m} \alpha_i [y^{(i)}(w^{\top} x^{(i)} + b) - 1]$$

• No θ or equality constraints in SVM problem

Solving

$$\mathcal{L}(w, b, \alpha) = \frac{1}{2} \|w\|^2 - \sum_{i=1}^{m} \alpha_i [y^{(i)}(w^{\top} x^{(i)} + b) - 1]$$

Derivatives

$$\frac{\partial}{\partial w} \mathcal{L}(w, b, \alpha) = w - \sum_{i=1}^{m} \alpha_i y^{(i)} x^{(i)} = 0 \quad \Rightarrow \quad w = \sum_{i=1}^{m} \alpha_i y^{(i)} x^{(i)}$$
$$\frac{\partial}{\partial b} \mathcal{L}(w, b, \alpha) = \sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

Then Lagrangian is re-written as

$$\mathcal{L}(w, b, \alpha) = \frac{1}{2} \left\| \sum_{i=1}^{m} \alpha_i y^{(i)} x^{(i)} \right\|^2 - \sum_{i=1}^{m} \alpha_i [y^{(i)} (w^{\top} x^{(i)} + b) - 1]$$

$$= \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)} - b \sum_{i=1}^{m} \alpha_i y^{(i)} \right\|_{=0}^{=0}$$

Solving α^*

Dual problem

$$\max_{\alpha \geq 0} \theta_{\mathcal{D}}(\alpha) = \max_{\alpha \geq 0} \min_{w,b} \mathcal{L}(w, b, \alpha)$$

$$\max_{\alpha} W(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)}$$
s.t. $\alpha_i \geq 0, \ i = 1, \dots, m$

$$\sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

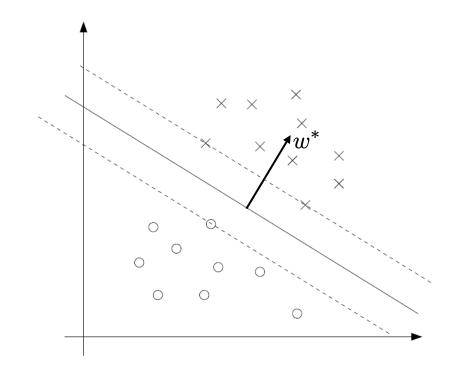
- To solve α^* with some methods e.g. SMO
 - We will get back to this solution later

Solving w^* and b^*

• With α^* solved, w^* is obtained by

$$w = \sum_{i=1}^{m} \alpha_i y^{(i)} x^{(i)}$$

- Only supporting vectors with $\alpha > 0$
- With w* solved, b* is obtained by



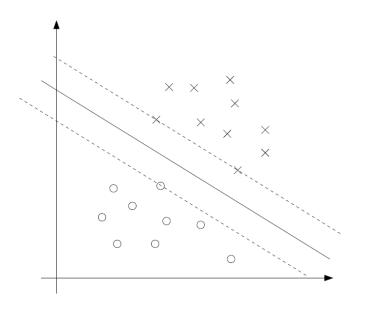
$$b^* = -\frac{\max_{i:y^{(i)}=-1} w^{*\top} x^{(i)} + \min_{i:y^{(i)}=1} w^{*\top} x^{(i)}}{2}$$

Predicting Values

• With the solutions of w^* and b^* , the predicting value (i.e. functional margin) of each instance is

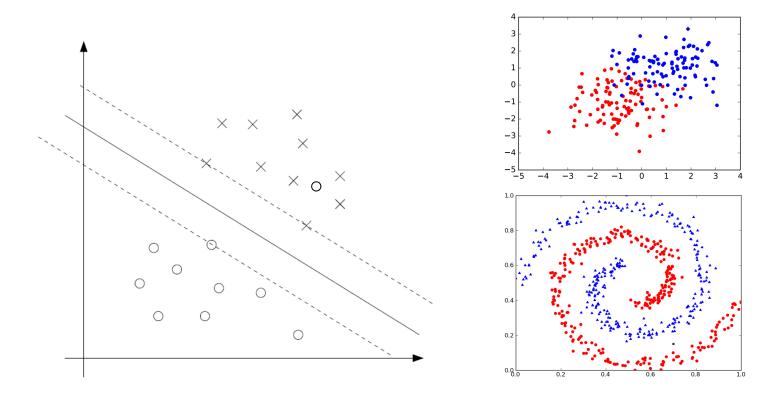
$$w^{*^{\top}}x + b^{*} = \left(\sum_{i=1}^{m} \alpha_{i} y^{(i)} x^{(i)}\right)^{\top} x + b^{*}$$
$$= \sum_{i=1}^{m} \alpha_{i} y^{(i)} \langle x^{(i)}, x \rangle + b^{*}$$

 We only need to calculate the inner product of x with the supporting vectors



Non-Separable Cases

- The derivation of the SVM as presented so far assumes that the data is linearly separable.
- More practical cases are linearly non-separable.



Dealing with Non-Separable Cases

Add slack variables

$$\min_{w,b} \ \frac{1}{2} \|w\|^2 + C \sum_{i=1}^m \xi_i \longleftarrow \text{L1 regularization}$$
 s.t. $y^{(i)}(w^\top x^{(i)} + b) \ge 1 - \xi_i, \ i = 1, \dots, m$

s.t.
$$y^{(i)}(w^{\top}x^{(i)} + b) \ge 1 - \xi_i, i = 1, \dots, m$$

 $\xi_i \ge 0, i = 1, \dots, m$

Lagrangian

$$\mathcal{L}(w, b, \xi, \alpha, r) = \frac{1}{2} w^{\top} w + C \sum_{i=1}^{m} \xi_i - \sum_{i=1}^{m} \alpha_i [y^{(i)}(x^{\top} w + b) - 1 + \xi_i] - \sum_{i=1}^{m} r_i \xi_i$$

Dual problem

$$\max_{\alpha} W(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)}$$

s.t.
$$0 \le \alpha_i \le C, i = 1, ..., m$$

Surprisingly, this is the only change

$$\sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

Efficiently solved by SMO algorithm

SVM Hinge Loss vs. LR Loss

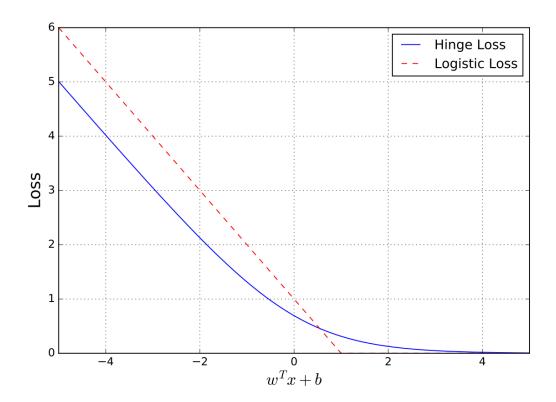
SVM Hinge loss

$$\frac{1}{2} \|w\|^2 + C \sum_{i=1}^m \max(0, 1 - y_i(w^\top x_i + b)) \qquad -y_i \log \sigma(w^\top x_i + b) - (1 - y_i) \log(1 - \sigma(w^\top x_i + b))$$

• LR log loss

$$-y_i \log \sigma(w^{\top} x_i + b) - (1 - y_i) \log(1 - \sigma(w^{\top} x_i + b))$$

• If y = 1



Now Back to Solve α^*

Dual problem

$$\max_{\alpha} W(\alpha) = \sum_{i=1}^{m} \alpha_{i} - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_{i} \alpha_{j} x^{(i)^{\top}} x^{(j)}$$
s.t. $0 \le \alpha_{i} \le C, \ i = 1, \dots, m$

$$\sum_{i=1}^{m} \alpha_{i} y^{(i)} = 0$$

• With α^* solved, w and b are solved easily

Coordinate Ascent (Descent)

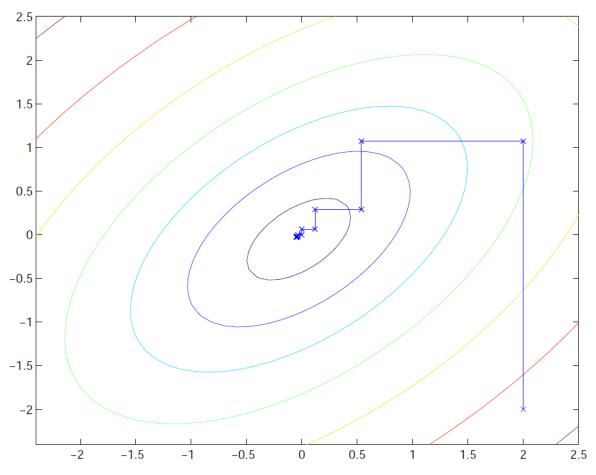
For the optimization problem

$$\max_{\alpha} W(\alpha_1, \alpha_2, \dots, \alpha_m)$$

Coordinate ascent algorithm

```
Loop until convergence: {
    For i=1,\ldots,m {
    \alpha_i:=\arg\max_{\hat{\alpha}_i}W(\alpha_1,\ldots,\alpha_{i-1},\hat{\alpha}_i,\alpha_{i+1},\ldots,\alpha_m)
    }
}
```

Coordinate Ascent (Descent)



A two-dimensional coordinate ascent example

- SMO: sequential minimal optimization
- SVM optimization problem

$$\max_{\alpha} \quad W(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)}$$
s.t. $0 \le \alpha_i \le C, \ i = 1, \dots, m$

$$\sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

Cannot directly apply coordinate ascent algorithm because

$$\sum_{i=1}^m lpha_i y^{(i)} = 0 \; \Rightarrow \; lpha_i y^{(i)} = -\sum_{j \neq i} lpha_j y^{(j)}$$

Update two variable each time

```
Loop until convergence {
    1. Select some pair \alpha_i and \alpha_j to update next
    2. Re-optimize W(\alpha) w.r.t. \alpha_i and \alpha_j
}
```

- Convergence test: whether the change of $W(\alpha)$ is smaller than a predefined value (e.g. 0.01)
- Key advantage of SMO algorithm is the update of α_i and α_i (step 2) is efficient

$$\max_{\alpha} W(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)}$$
s.t. $0 \le \alpha_i \le C, i = 1, \dots, m$

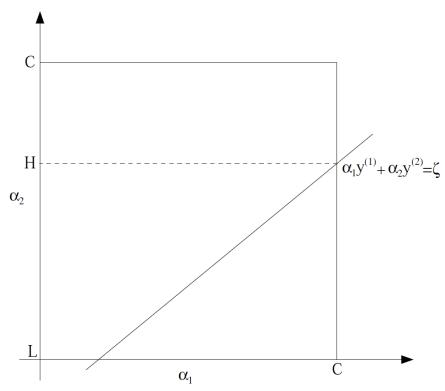
$$\sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

• Without loss of generality, hold $\alpha_3 \dots \alpha_m$ and optimize $W(\alpha)$ w.r.t. α_1 and α_2

$$lpha_1 y^{(1)} + lpha_2 y^{(2)} = -\sum_{i=3}^m lpha_i y^{(i)} = \zeta$$

$$\Rightarrow \quad \alpha_2 = -\frac{y^{(1)}}{y^{(2)}} lpha_1 + \frac{\zeta}{y^{(2)}}$$

$$lpha_1 = (\zeta - lpha_2 y^{(2)}) y^{(1)}$$



• With $\alpha_1 = (\zeta - \alpha_2 y^{(2)}) y^{(1)}$, the objective is written as

$$W(\alpha_1, \alpha_2, \dots, \alpha_m) = W((\zeta - \alpha_2 y^{(2)}) y^{(1)}, \alpha_2, \dots, \alpha_m)$$

• Thus the original optimization problem

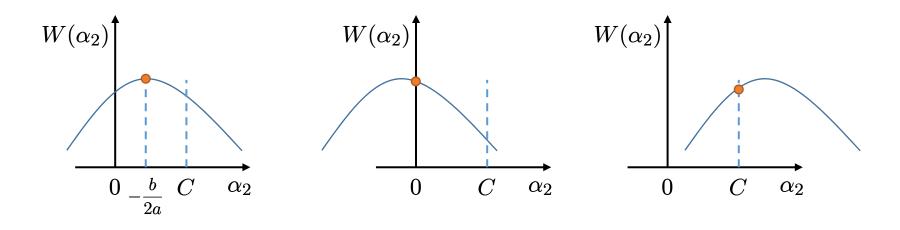
$$\max_{\alpha} \quad W(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y^{(i)} y^{(j)} \alpha_i \alpha_j x^{(i)^{\top}} x^{(j)}$$
s.t. $0 \le \alpha_i \le C, \ i = 1, \dots, m$

$$\sum_{i=1}^{m} \alpha_i y^{(i)} = 0$$

is transformed into a quadratic optimization problem w.r.t. α_2

$$\max_{\alpha_2} W(\alpha_2) = a\alpha_2^2 + b\alpha_2 + c$$
s.t. $0 \le \alpha_2 \le C$

Optimizing a quadratic function is much efficient



$$\max_{\alpha_2} W(\alpha_2) = a\alpha_2^2 + b\alpha_2 + c$$

s.t. $0 \le \alpha_2 \le C$