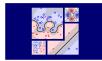
Machine Learning Techniques

(機器學習技法)



Lecture 1: Linear Support Vector Machine

Hsuan-Tien Lin (林軒田)

htlin@csie.ntu.edu.tw

Department of Computer Science & Information Engineering

National Taiwan University (國立台灣大學資訊工程系)



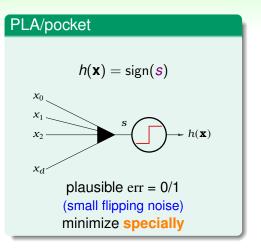
Roadmap

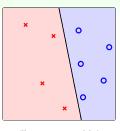
1 Embedding Numerous Features: Kernel Models

Lecture 1: Linear Support Vector Machine

- Large-Margin Separating Hyperplane
- Standard Large-Margin Problem
- Support Vector Machine
- Reasons behind Large-Margin Hyperplane
- 2 Combining Predictive Features: Aggregation Models
- 3 Distilling Implicit Features: Extraction Models

Linear Classification Revisited

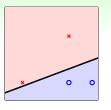


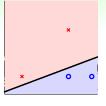


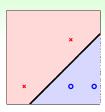
(linear separable)

linear (hyperplane) classifiers: $h(\mathbf{x}) = \text{sign}(\mathbf{w}^T \mathbf{x})$

Which Line Is Best?





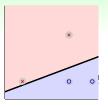


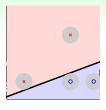
- PLA? depending on randomness
- VC bound? whichever you like!

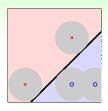
$$E_{\text{out}}(\mathbf{w}) \leq \underbrace{E_{\text{in}}(\mathbf{w})}_{0} + \underbrace{\Omega(\mathcal{H})}_{d_{\text{VC}} = d + 1}$$

You? rightmost one, possibly :-)

Why Rightmost Hyperplane?







informal argument

if (Gaussian-like) noise on future $\mathbf{x} \approx \mathbf{x}_n$:

 \mathbf{x}_n further from hyperplane

⇔ tolerate more noise

⇔ more robust to overfitting

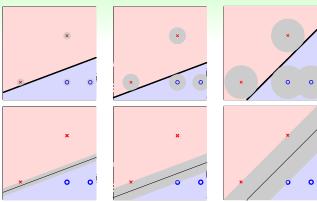
distance to closest \mathbf{x}_n

⇔ amount of noise tolerance

⇔ robustness of hyperplane

rightmost one: more robust because of larger distance to closest x_n

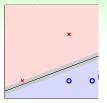
Fat Hyperplane

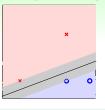


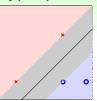
- robust separating hyperplane: fat
 —far from both sides of examples
- robustness \equiv **fatness**: distance to closest \mathbf{x}_n

goal: find fattest separating hyperplane

Large-Margin Separating Hyperplane







 $\max_{\mathbf{w}} \quad \text{fatness}(\mathbf{w})$

subject to

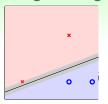
w classifies every (\mathbf{x}_n, y_n) correctly

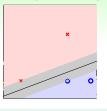
 $\frac{\mathsf{fatness}(\mathbf{w}) = \min_{n=1,\dots,N} \mathsf{distance}(\mathbf{x}_n, \mathbf{w})}{\mathsf{distance}(\mathbf{x}_n, \mathbf{w})}$

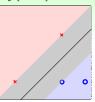
- fatness: formally called margin
- correctness: $y_n = sign(\mathbf{w}^T \mathbf{x}_n)$

goal: find largest-margin separating hyperplane

Large-Margin Separating Hyperplane







```
\max_{\mathbf{w}} \quad \mathbf{margin}(\mathbf{w})
subject to every y_n \mathbf{w}^T \mathbf{x}_n > 0
\mathbf{margin}(\mathbf{w}) = \min_{n=1,...,N} \mathsf{distance}(\mathbf{x}_n, \mathbf{w})
```

- fatness: formally called margin
- correctness: $y_n = sign(\mathbf{w}^T \mathbf{x}_n)$

goal: find largest-margin separating hyperplane

Consider two examples $(\mathbf{v},+1)$ and $(-\mathbf{v},-1)$ where $\mathbf{v}\in\mathbb{R}^2$ (without padding the $v_0=1$). Which of the following hyperplane is the largest-margin separating one for the two examples? You are highly encouraged to visualize by considering, for instance, $\mathbf{v}=(3,2)$.

- 1 $x_1 = 0$
- $2 x_2 = 0$

Consider two examples $(\mathbf{v},+1)$ and $(-\mathbf{v},-1)$ where $\mathbf{v}\in\mathbb{R}^2$ (without padding the $v_0=1$). Which of the following hyperplane is the largest-margin separating one for the two examples? You are highly encouraged to visualize by considering, for instance, $\mathbf{v}=(3,2)$.

- $\mathbf{1} x_1 = 0$
- $2 x_2 = 0$

Reference Answer: (3)

Here the largest-margin separating hyperplane (line) must be a perpendicular bisector of the line segment between \mathbf{v} and $-\mathbf{v}$. Hence \mathbf{v} is a normal vector of the largest-margin line. The result can be extended to the more general case of $\mathbf{v} \in \mathbb{R}^d$.

Distance to Hyperplane: Preliminary

$$\max_{\mathbf{w}} \quad \text{margin}(\mathbf{w})$$
subject to
$$\text{every } y_n \mathbf{w}^T \mathbf{x}_n > 0$$

$$\text{margin}(\mathbf{w}) = \min_{n=1,...,N} \frac{\text{distance}(\mathbf{x}_n, \mathbf{w})}{\text{distance}(\mathbf{x}_n, \mathbf{w})}$$

'shorten' x and w

distance needs w_0 and (w_1, \dots, w_d) differently (to be derived)

$$\begin{bmatrix} | \\ \mathbf{w} \\ | \end{bmatrix} = \begin{bmatrix} w_1 \\ \vdots \\ w_d \end{bmatrix} \quad ; \quad \begin{bmatrix} | \\ \mathbf{x} \\ | \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_d \end{bmatrix}$$

for this part: $h(\mathbf{x}) = \operatorname{sign}(\mathbf{w}^T \mathbf{x} + \mathbf{b})$

Distance to Hyperplane

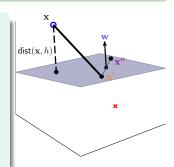
want: distance($\mathbf{x}, \mathbf{b}, \mathbf{w}$), with hyperplane $\mathbf{w}^T \mathbf{x}' + \mathbf{b} = 0$

consider x', x" on hyperplane

2 w ⊥ hyperplane:

$$\begin{pmatrix} \mathbf{w}^T & \underbrace{(\mathbf{x}'' - \mathbf{x}')} \\ \text{vector on hyperplane} \end{pmatrix} = 0$$

3 distance = project $(\mathbf{x} - \mathbf{x}')$ to \perp hyperplane



$$distance(\mathbf{x}, \mathbf{b}, \mathbf{w}) = \left| \frac{\mathbf{w}^T}{\|\mathbf{w}\|} (\mathbf{x} - \mathbf{x}') \right| \stackrel{\text{(1)}}{=} \frac{1}{\|\mathbf{w}\|} |\mathbf{w}^T \mathbf{x} + \mathbf{b}|$$

Distance to **Separating** Hyperplane

$$distance(\mathbf{x}, \mathbf{b}, \mathbf{w}) = \frac{1}{\|\mathbf{w}\|} |\mathbf{w}^T \mathbf{x} + \mathbf{b}|$$

separating hyperplane: for every n

$$y_n(\mathbf{w}^T\mathbf{x}_n+b)>0$$

distance to separating hyperplane:

distance
$$(\mathbf{x}_n, \mathbf{b}, \mathbf{w}) = \frac{1}{\|\mathbf{w}\|} \mathbf{y}_n(\mathbf{w}^T \mathbf{x}_n + \mathbf{b})$$

max
$$\underset{b,\mathbf{w}}{\text{margin}}(\mathbf{b},\mathbf{w})$$
subject to every $y_n(\mathbf{w}^T\mathbf{x}_n + \mathbf{b}) > 0$

$$\text{margin}(\mathbf{b},\mathbf{w}) = \min_{n=1,\dots,N} \frac{1}{\|\mathbf{w}\|} y_n(\mathbf{w}^T\mathbf{x}_n + \mathbf{b})$$

Margin of **Special** Separating Hyperplane

max
$$\underset{\boldsymbol{b}, \mathbf{w}}{\text{margin}}(\boldsymbol{b}, \mathbf{w})$$

subject to every $y_n(\mathbf{w}^T\mathbf{x}_n + \boldsymbol{b}) > 0$
margin $(\boldsymbol{b}, \mathbf{w}) = \min_{n=1,\dots,N} \frac{1}{\|\mathbf{w}\|} y_n(\mathbf{w}^T\mathbf{x}_n + \boldsymbol{b})$

- $\mathbf{w}^T \mathbf{x} + \mathbf{b} = 0$ same as $3\mathbf{w}^T \mathbf{x} + 3\mathbf{b} = 0$: scaling does not matter
- special scaling: only consider separating (b, w) such that

$$\min_{n=1,\dots,N} y_n(\mathbf{w}^T \mathbf{x}_n + b) = 1 \Longrightarrow \text{margin}(b, \mathbf{w}) = \frac{1}{\|\mathbf{w}\|}$$

$$\begin{array}{ll} \max \limits_{\boldsymbol{b}, \mathbf{w}} & \frac{1}{\|\mathbf{w}\|} \\ \text{subject to} & \text{every } y_n(\mathbf{w}^T\mathbf{x}_n + b) > 0 \\ & \min \limits_{n=1,\dots,N} & y_n(\mathbf{w}^T\mathbf{x}_n + b) = 1 \end{array}$$

Standard Large-Margin Hyperplane Problem

$$\max_{\mathbf{b},\mathbf{w}} \quad \frac{1}{\|\mathbf{w}\|} \quad \text{subject to} \min_{n=1,\dots,N} \quad y_n(\mathbf{w}^T \mathbf{x}_n + \mathbf{b}) = 1$$

necessary constraints: $y_n(\mathbf{w}^T\mathbf{x}_n + \mathbf{b}) \ge 1$ for all n

```
original constraint: \min_{n=1,...,N} y_n(\mathbf{w}^T \mathbf{x}_n + \mathbf{b}) = 1 want: optimal (\mathbf{b}, \mathbf{w}) here (inside)
```

if optimal (b, \mathbf{w}) outside, e.g. $y_n(\mathbf{w}^T\mathbf{x}_n + \mathbf{b}) > 1.126$ for all n—can scale (b, \mathbf{w}) to "more optimal" $(\frac{b}{1.126}, \frac{\mathbf{w}}{1.126})$ (contradiction!)

```
final change: \max \Longrightarrow \min, remove \sqrt{\phantom{a}}, add \frac{1}{2} \min_{\substack{b,\mathbf{w}\\b}} \quad \frac{1}{2}\mathbf{w}^T\mathbf{w} subject to y_n(\mathbf{w}^T\mathbf{x}_n + \mathbf{b}) \ge 1 for all n
```

Fun Time

Consider three examples $(\mathbf{x}_1, +1)$, $(\mathbf{x}_2, +1)$, $(\mathbf{x}_3, -1)$, where $\mathbf{x}_1 = (3, 0)$, $\mathbf{x}_2 = (0, 4)$, $\mathbf{x}_3 = (0, 0)$. In addition, consider a hyperplane $x_1 + x_2 = 1$. Which of the following is not true?

- the hyperplane is a separating one for the three examples
- 2 the distance from the hyperplane to \mathbf{x}_1 is 2
- 3 the distance from the hyperplane to \mathbf{x}_3 is $\frac{1}{\sqrt{2}}$
- $oldsymbol{4}$ the example that is closest to the hyperplane is $oldsymbol{x}_3$

Fun Time

Consider three examples $(\mathbf{x}_1, +1)$, $(\mathbf{x}_2, +1)$, $(\mathbf{x}_3, -1)$, where $\mathbf{x}_1 = (3, 0)$, $\mathbf{x}_2 = (0, 4)$, $\mathbf{x}_3 = (0, 0)$. In addition, consider a hyperplane $x_1 + x_2 = 1$. Which of the following is not true?

- 1 the hyperplane is a separating one for the three examples
- 2 the distance from the hyperplane to \mathbf{x}_1 is 2
- 3 the distance from the hyperplane to \mathbf{x}_3 is $\frac{1}{\sqrt{2}}$
- $oldsymbol{4}$ the example that is closest to the hyperplane is $oldsymbol{x}_3$

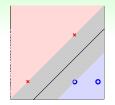
Reference Answer: 2

The distance from the hyperplane to \mathbf{x}_1 is $\frac{1}{\sqrt{2}}(3+0-1)=\sqrt{2}$.

Solving a Particular Standard Problem

$$\min_{\substack{b,\mathbf{w}}} \quad \frac{1}{2}\mathbf{w}^{T}\mathbf{w}$$

subject to
$$y_{n}(\mathbf{w}^{T}\mathbf{x}_{n} + \mathbf{b}) \geq 1 \text{ for all } n$$



$$X = \begin{bmatrix} 0 & 0 \\ 2 & 2 \\ 2 & 0 \\ 3 & 0 \end{bmatrix} \quad \mathbf{y} = \begin{bmatrix} -1 \\ -1 \\ +1 \\ +1 \end{bmatrix} \qquad \begin{array}{c} -b \ge 1 & (i) \\ -2w_1 - 2w_2 - b \ge 1 & (ii) \\ 2w_1 & +b \ge 1 & (iii) \\ 3w_1 & +b \ge 1 & (iv) \end{array}$$

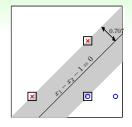
- $\left\{ \begin{array}{ccc} (i) & \& & (iii) & \Longrightarrow & w_1 \ge +1 \\ (ii) & \& & (iii) & \Longrightarrow & w_2 \le -1 \end{array} \right\} \Longrightarrow \frac{1}{2} \mathbf{w}^T \mathbf{w} \ge 1$
- $(w_1 = 1, w_2 = -1, b = -1)$ at **lower bound** and satisfies (i) (iv)

$$g_{SVM}(\mathbf{x}) = sign(x_1 - x_2 - 1)$$
: SVM? :-)

Support Vector Machine (SVM)

optimal solution:
$$(w_1 = 1, w_2 = -1, b = -1)$$

margin (b, \mathbf{w}) $= \frac{1}{\|\mathbf{w}\|} = \frac{1}{\sqrt{2}}$



- examples on boundary: 'locates' fattest hyperplane other examples: not needed
- call boundary example support vector (candidate)

support vector machine (SVM): learn fattest hyperplanes (with help of support vectors)

Solving General SVM

 $\min_{b,\mathbf{w}} \quad \frac{1}{2}\mathbf{w}^T\mathbf{w}$
subject to $y_n(\mathbf{w}^T\mathbf{x}_n + b) \ge 1 \text{ for all } n$

- not easy manually, of course :-)
- gradient descent? not easy with constraints
- luckily:
 - (convex) quadratic objective function of (b, \mathbf{w})
 - linear constraints of (b, w)
 - -quadratic programming

quadratic programming (QP):
 'easy' optimization problem

Quadratic Programming

optimal
$$(b, \mathbf{w}) = ?$$

$$\min_{b, \mathbf{w}} \quad \frac{1}{2} \mathbf{w}^T \mathbf{w}$$
subject to $y_n(\mathbf{w}^T \mathbf{x}_n + b) \ge 1$, for $n = 1, 2, ..., N$

optimal
$$\mathbf{u} \leftarrow \mathsf{QP}(\mathbf{Q}, \mathbf{p}, \mathbf{A}, \mathbf{c})$$

$$\min_{\mathbf{u}} \quad \frac{1}{2}\mathbf{u}^{T}\mathbf{Q}\mathbf{u} + \mathbf{p}^{T}\mathbf{u}$$
subject to
$$\mathbf{a}_{m}^{T}\mathbf{u} \geq c_{m},$$
for $m = 1, 2, \dots, M$

objective function:
$$\mathbf{u} = \begin{bmatrix} b \\ \mathbf{w} \end{bmatrix}$$
; $\mathbf{Q} = \begin{bmatrix} 0 & \mathbf{0}_d^T \\ \mathbf{0}_d & \mathbf{I}_d \end{bmatrix}$; $\mathbf{p} = \mathbf{0}_{d+1}$ constraints: $\mathbf{a}_n^T = \mathbf{y}_n \begin{bmatrix} 1 & \mathbf{x}_n^T \end{bmatrix}$; $\mathbf{c}_n = 1$; $M = N$

SVM with general QP solver: easy if you've read the manual :-)

SVM with QP Solver

Linear Hard-Margin SVM Algorithm

$$\mathbf{0} \quad \mathbf{Q} = \begin{bmatrix} \mathbf{0} & \mathbf{0}_d^T \\ \mathbf{0}_d & \mathbf{I}_d \end{bmatrix}; \mathbf{p} = \mathbf{0}_{d+1}; \mathbf{a}_n^T = y_n \begin{bmatrix} 1 & \mathbf{x}_n^T \end{bmatrix}; c_n = 1$$

- \odot return $b \otimes \mathbf{w}$ as g_{SVM}
 - hard-margin: nothing violate 'fat boundary'
 - linear: \mathbf{x}_n

want non-linear?

$$z_n = \Phi(x_n)$$
—remember? :-)

Fun Time

Consider two negative examples with $\mathbf{x}_1 = (0,0)$ and $\mathbf{x}_2 = (2,2)$; two positive examples with $\mathbf{x}_3 = (2,0)$ and $\mathbf{x}_4 = (3,0)$, as shown on page 14 of the slides. Define \mathbf{u} , \mathbf{Q} , \mathbf{p} , c_n as those listed on page 17 of the slides. What are \mathbf{a}_n^T that need to be fed into the QP solver?

1
$$\mathbf{a}_1^T = [-1, 0, 0]$$
 , $\mathbf{a}_2^T = [-1, 2, 2]$, $\mathbf{a}_3^T = [-1, 2, 0]$

$$\mathbf{a}_{2}^{T} = [-1, 2, 2]$$

,
$$\mathbf{a}_3^T = [-1, 2, 0]$$

,
$$\mathbf{a}_4^T = [-1, 3, 0]$$

, $\mathbf{a}_4^T = [-1, 3, 0]$

2
$$\mathbf{a}_1^T = [1, 0, 0]$$

,
$$\mathbf{a}_2^T = [1, -2, -2]$$
 , $\mathbf{a}_3^T = [-1, 2, 0]$

$$, \mathbf{a}_{4}^{T} = [1, 3, 0]$$

3
$$\mathbf{a}_1^T = [1,0,0]$$
 , $\mathbf{a}_2^T = [1,2,2]$, $\mathbf{a}_3^T = [1,2,0]$

$$\mathbf{a}_{4}^{T} = [1, 3, 0]$$

4
$$\mathbf{a}_1^T = [-1, 0, 0]$$

,
$$\boldsymbol{a}_2^T = [-1, -2, -2]$$
 , $\boldsymbol{a}_3^T = [1, 2, 0]$

Fun Time

Consider two negative examples with $\mathbf{x}_1 = (0,0)$ and $\mathbf{x}_2 = (2,2)$; two positive examples with $\mathbf{x}_3 = (2,0)$ and $\mathbf{x}_4 = (3,0)$, as shown on page 14 of the slides. Define \mathbf{u} , \mathbf{Q} , \mathbf{p} , c_n as those listed on page 17 of the slides. What are \mathbf{a}_n^T that need to be fed into the QP solver?

1
$$\mathbf{a}_{1}^{T} = [-1, 0, 0]$$
 , $\mathbf{a}_{2}^{T} = [-1, 2, 2]$, $\mathbf{a}_{3}^{T} = [-1, 2, 0]$

$$\mathbf{a}_{2}^{T} = [-1, 2, 2]$$

,
$$\mathbf{a}_3^T = [-1, 2, 0]$$

,
$$\mathbf{a}_{4}^{T} = [-1, 3, 0]$$

2
$$\mathbf{a}_1^T = [1,0,0]$$
 , $\mathbf{a}_2^T = [1,-2,-2]$, $\mathbf{a}_3^T = [-1,2,0]$

$$\mathbf{a}_{2}' = [1, -2,$$

$$, \mathbf{a}_{4}^{T} = [-1, 3, 0]$$
 $, \mathbf{a}_{4}^{T} = [1, 3, 0]$

$$\mathbf{a}_1 = [1,0,0]$$

3
$$\mathbf{a}_1^T = [1,0,0]$$
 , $\mathbf{a}_2^T = [1,2,2]$, $\mathbf{a}_3^T = [1,2,0]$

4
$$\mathbf{a}_{1}^{T} = [-1, 0, 0]$$
 , $\mathbf{a}_{2}^{T} = [-1, -2, -2]$, $\mathbf{a}_{3}^{T} = [1, 2, 0]$

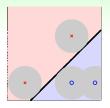
,
$$\mathbf{a}_4^T = [1, 3, 0]$$

Reference Answer: (4)

We need
$$\mathbf{a}_n^T = y_n \begin{bmatrix} 1 & \mathbf{x}_n^T \end{bmatrix}$$
.

Why Large-Margin Hyperplane?

 $\min_{b,\mathbf{w}} \quad \frac{1}{2}\mathbf{w}^{T}\mathbf{w}$
subject to $y_{n}(\mathbf{w}^{T}\mathbf{z}_{n}+b) \geq 1 \text{ for all } n$



	minimize	constraint
regularization	<i>E</i> in	$\mathbf{w}^T \mathbf{w} \leq C$
SVM	$\mathbf{w}^T \mathbf{w}$	$E_{\rm in}=0$ [and more]

SVM (large-margin hyperplane): 'weight-decay regularization' within $E_{\rm in}=0$

Large-Margin Restricts Dichotomies

consider 'large-margin algorithm' A_{ρ} :

either returns g with margin(g) $\geq \rho$ (if exists), or 0 otherwise

\mathcal{A}_0 : like PLA \Longrightarrow shatter 'general' 3 inputs









$\mathcal{A}_{1.126}$: more strict than SVM \Longrightarrow cannot shatter any 3 inputs









fewer dichotomies \Longrightarrow smaller 'VC dim.' \Longrightarrow better generalization

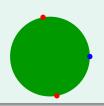
VC Dimension of Large-Margin Algorithm

fewer dichotomies ⇒ smaller 'VC dim.'

considers $d_{VC}(A_{\rho})$ [data-dependent, need more than VC] instead of $d_{VC}(\mathcal{H})$ [data-independent, covered by VC]

$d_{\sf VC}(\mathcal{A}_{\scriptscriptstyle ho})$ when \mathcal{X} = unit circle in \mathbb{R}^2

- $\rho = 0$: just perceptrons ($d_{VC} = 3$)
- $\rho > \frac{\sqrt{3}}{2}$: cannot shatter any 3 inputs $(d_{VC} < 3)$
 - —some inputs must be of distance $\leq \sqrt{3}$



generally, when \mathcal{X} in radius-R hyperball:

$$d_{\text{VC}}(\mathcal{A}_{\rho}) \leq \min\left(\frac{R^2}{\rho^2}, d\right) + 1 \leq \underbrace{d+1}_{d_{\text{VC}}(\text{perceptrons})}$$

Benefits of Large-Margin Hyperplanes

	large-margin hyperplanes	hyperplanes	hyperplanes + feature transform Φ
#	even fewer	not many	many
boundary	simple	simple	sophisticated

- not many good, for d_{VC} and generalization
- sophisticated good, for possibly better E_{in}

a new possibility: non-linear SVM large-margin hyperplanes + numerous feature transform Φ mot many boundary sophisticated

Fun Time

Consider running the 'large-margin algorithm' \mathcal{A}_{ρ} with $\rho=\frac{1}{4}$ on a \mathcal{Z} -space such that $\mathbf{z}=\mathbf{\Phi}(\mathbf{x})$ is of 1126 dimensions (excluding z_0) and $\|\mathbf{z}\|\leq 1$. What is the upper bound of $d_{\text{VC}}(\mathcal{A}_{\rho})$ when calculated by $\min\left(\frac{R^2}{\rho^2},d\right)+1$?

- **1** 5
- 2 17
- **3** 1126
- 4 1127

Fun Time

Consider running the 'large-margin algorithm' \mathcal{A}_{ρ} with $\rho=\frac{1}{4}$ on a \mathcal{Z} -space such that $\mathbf{z}=\mathbf{\Phi}(\mathbf{x})$ is of 1126 dimensions (excluding z_0) and $\|\mathbf{z}\|\leq 1$. What is the upper bound of $d_{\text{VC}}(\mathcal{A}_{\rho})$ when calculated by $\min\left(\frac{R^2}{\rho^2},d\right)+1$?

- **1** 5
- **2** 17
- **3** 1126
- **4** 1127

Reference Answer: 2

By the description, d = 1126 and R = 1. So the upper bound is simply 17.

Summary

1 Embedding Numerous Features: Kernel Models

Lecture 1: Linear Support Vector Machine

- Large-Margin Separating Hyperplane intuitively more robust against noise
- Standard Large-Margin Problem minimize ||w|| at special separating scale
- Support Vector Machine 'easy' via quadratic programming
- Reasons behind Large-Margin Hyperplane fewer dichotomies and better generalization
- next: solving non-linear Support Vector Machine
- 2 Combining Predictive Features: Aggregation Models
- 3 Distilling Implicit Features: Extraction Models