# Support Vector Machines

COMP5318 Machine Learning and Data Mining

semester 2, 2024, week 6a

**Nguyen Hoang Tran**

Based on slides prepared by Irena Koprinska (irena.koprinska@sydney.edu.au)

Reference: Tan ch.4.9, Witten ch.7.2: 252-256

# Outline

- Maximum margin hyperplane
- Linear SVM
- Non-linear SVM

# Separation by a hyperplane

- Given is the following training data (2 class problem: squares and circles):

- Find a linear boundary (line, hyperplane) that separates the data
- Is the data linearly separable?

# Separation by a hyperplane (2)

- One possible decision boundary

Another possible decision boundary

# Separation by a hyperplane (3)

- Other possible decision boundaries – there are many options

# Margin of a hyperplane and support vectors

- A decision boundary B1:

*Support vectors* are the examples (data points) that lie closest to the decision boundary; remove them will change the decision boundary

*Margin* – the separation between the boundary and the closest examples

The boundary is in the middle of the margin

# Support vectors

The support vectors just touch the margin of the decision boundary

It is possible to have more than 1 support vector for each class

For our example: 5 support vectors, 3 for class square and 2 for class circle

# Support vectors (2)

Why “vectors”?

On the previous slides we saw only the tips of the support vectors; here we can see the actual vectors

Remember that the given training examples are vectors (input vectors) where each dimension corresponds to 1 feature

The support vectors are a subset of the input vectors => they are also vectors

# Which hyperplane is better?

- Which hyperplane should we select - B1 or B2?
- Which one is likely to classify more accurately new data**?**

Choose $B_1$ since $B_1$ has bigger margin

Goal:

我们要选择有最大 margin 的 support vectors

也叫 maximum margin hyperplane

- The hyperplane with the bigger margin, B1

# Maximum margin hyperplane

- The hyperplane with the biggest margin is called the *maximum margin hyperplane*
- It is the hyperplane with the highest possible distance to the training examples
- SVM selects the maximum margin hyperplane

Goal

- Decision boundaries with <u>large margins</u> (i.e. farthest away from the training data) <u>are better</u> than those with small margins as they typically are more accurate on new examples

# Maximum margin hyperplane - rationale

- If the margin is small, then any slight change in the hyperplane or the training examples at the boundary is more likely to affect the classification as there is very narrow room to allow data perturbations

Why we need bigger margin

- => small margin is more susceptible to overfitting
- On the other hand, if the margin is big, there is more leeway to be robust to minor changes in the data
- => likely to have better generalization performance

- There is also justification from statistical learning theory, the so called structural risk minimization principle

# Linear decision boundary

- Binary classification problem, *N* training examples (input vectors)
- x is the input vector, y is the class value

$$(\mathbf{x}_i, y_i), i = 1,..,N$$

$$\mathbf{x}_i = (x_{i1},...,x_{im})^T, y_i = \{-1,1\}$$

*Training data example*:

$$\mathbf{x}_1 = (2,2), y_1 = 1$$

$$\mathbf{x}_2 = (0.5,1), y_2 = -1, etc.$$

- A decision boundary of a linear classifier is

$$\mathbf{w} \cdot \mathbf{x} + b = 0$$

parameters

$$x_1 + 0.5x_2 - 1 = 0$$

$m=2$ $b=-1$

$w=[1, 0.5]$

Learning a linear model is equivalent to finding **w** and *b*

# Linear model – classifying new examples

- If we know the decision boundary, we can easily classify a new example **x** by calculating f = wx+b and determining the sign

$$\text{if } \mathbf{x} \text{ is above the decision boundary}: \mathbf{w}\cdot\mathbf{x}+b>0$$

$$\text{if } \mathbf{x} \text{ is below the decision boundary}: \mathbf{w}\cdot\mathbf{x}+b<0$$

$$= sign(\mathbf{w}\cdot\mathbf{x}+b)$$

How to use the classifier for "linear case"

不允许出现 data point locate on f=wx+b

出现就表明不准确

# SVM - problem statement

- Our separating hyperplane is *H*
- *H* is in the middle of 2 other hyperplanes, *H1* and *H2*, defined as:

$$H_1: \mathbf{w}\cdot\mathbf{x}+b=1$$

$$H2: \mathbf{w}\cdot\mathbf{x}+b=-1$$

$H : wx+b=0$

- The points laying on *H1* and *H2* are the support vectors
- *d* is the margin of *H*
- It can be shown that: $d = \dfrac{2}{\|\mathbf{w}\|}$

$\max d \Rightarrow \min \frac{1}{2}\|w\|^2$

- To <u>maximize</u> the margin *d*, we need to <u>minimize</u> ||w||
- This is equivalent to <u>minimizing</u> the quadratic function: $\frac{1}{2}\|\mathbf{w}\|^2$

# Learning a maximum margin hyperplane in linear SVM

- Given: a set of labelled training examples
- Learn: the maximum margin hyperplane such as all training examples are classified correctly
- This could be formulated as a constraint optimization problem:
  - Given N training examples $(\mathbf{x}_i, y_i), i = 1,..,N$

    $\mathbf{x}_i = (x_{i1},\ldots,x_{im})^T, y_i = \{-1,1\}$

    training vector class
  - Minimize $\frac{1}{2}\|\mathbf{w}\|^2$ ← Maximizing the margin
  - Subject to $y_i(\mathbf{w}\cdot\mathbf{x}_i + b) \geq 1, \forall i$ 对于每个 data point 都要满足

    负数表示 predict wrong

    Another way of expressing correct classification of all training examples i=1..N

# The optimization problem

- This is an optimization problem that can be solved using Quadratic Programming (QP) and the Lagrange multiplier method
- Firstly, the problem is transformed into an equivalent form using Lagrange multipliers λ :

$$\max \mathbf{w}(\lambda) = \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j=1}^{N} \lambda_i \lambda_j y_i y_j \mathbf{x}_i \cdot \mathbf{x}_j$$

Dot product of pairs of training vectors

Class value of the training vectors

$$subject\ to\ \lambda_i \geq 0, \sum_{i=1}^{N} \lambda_i y_i = 0$$

- The values of λs are found using QP
- The solution (i.e. the optimal decision boundary) is given by:

$$\boxed{\mathbf{w} = \sum_{i=1}^{N} \lambda_i y_i \mathbf{x}_i}$$

classifier, we need to max W

Equation

# Properties of the solution

$$\mathbf{w} = \sum_{i=1}^{N} \lambda_i y_i \mathbf{x}_i$$

$\lambda_i > 0 \Rightarrow$ data point is support vector

$\lambda_i = 0 \Rightarrow$ data point is not support vector so majority is 0

- The optimal decision boundary (the maximum margin hyperplane) w is a linear combination (coefficient $\lambda$ * target value*training vector) of the training examples
- But many of the $\lambda$s are 0 -> linear combination of a small number of training examples
- The training examples $x_i$ with non-zero $\lambda_i$ are the *support vectors* and they are the examples closest to the decision boundary w
- => the optimal decision boundary w is a linear combination of support vectors

# Classifying new examples

$$\mathbf{w} = \sum_{i=1}^{N} \lambda_i y_i \mathbf{x}_i$$ maximum margin hyperplane

How to use classifiers

- To classify a new example z:

$$\boxed{f = \mathbf{w} \cdot \mathbf{z} + b = \sum_{i=1}^{N} \lambda_i y_i \mathbf{x}_i \cdot \mathbf{z} + b}$$

Dot product of the new vector and the support vectors

$$sign(f)$$

i.e. the new example belongs to class 1, if $f > 0$ or class -1 if $f < 0$

# Example

| features $x_1$ | features $x_2$ | class $y$ | Lagrange Multiplier |
|---|---|---|---|
| 0.3858 | 0.4687 | 1 | 65.5261 $\lambda_1$ |
| 0.4871 | 0.611 | −1 | 65.5261 $\lambda_2$ |
| 0.9218 | 0.4103 | −1 | 0 $\lambda_3$ |
| 0.7382 | 0.8936 | −1 | 0 |
| 0.1763 | 0.0579 | 1 | 0 |
| 0.4057 | 0.3529 | 1 | 0 |
| 0.9355 | 0.8132 | −1 | 0 |
| 0.2146 | 0.0099 | 1 | 0 |

x1
x2

because they are support vectors

- 8 2-dim. training examples; 2 classes: -1,1
- After solving the problem with QP we find the λs
- Only 2 λs are non-zero (x1 & x2) and they correspond to the support vectors
- Using the λs , the weights (defining the decision boundary are):

$$w_1 = \sum_{i=1}^{2} \lambda_i y_i \mathbf{x}_{i1} = 65.5261(1*0.3858 - 1*0.4871) = -6.64$$

$$w_2 = \sum_{i=1}^{2} \lambda_i y_i \mathbf{x}_{i2} = 65.5261(1*0.4687 - 1*0.611) = -9.32$$

$b = 7.93$ //there is a formula for b (not shown)

- Classifying new examples:
  - above the decision boundary: class 1
  - below: class -1

Classifier = $-6.64x_1 - 9.32x_2 + 7.93$

# SVM with soft-margin

- The method we discussed so far constructs decision boundaries that are free of misclassifications. We can allow some misclassifications.
- Ex.: B1 is better than B2 as its margin is bigger but now 2 new examples are added; B1 misclassifies them but B2 still classifies them correctly

- This does not mean that B2 is better as the new examples may be noise
- B1 should still be preferred as it has a bigger margin and is less sensitive to overfitting and noise
- We can modify our method to allow some misclassifications, i.e. by considering the trade-off between the margin width and the number of misclassifications
- As a result, the modified method will construct linear boundary even if the data is not linearly separable

# Soft-margin solution

- The optimisation problem formulation is similar but there is an additional parameter $C$ in the definition of the optimization function
- Large $C$: more emphasis on minimizing the training error than maximizing the margin

- The old formulation:

Find $\mathbf{w}$ and b such that
$\mathbf{\Phi}(\mathbf{w}) = \mathbf{w}^{\mathrm{T}}\mathbf{w}$ is minimized
and for all $(\mathbf{x}_i, y_i)$, $i=1..n$ : $y_i(\mathbf{w}^{\mathbf{T}}\mathbf{x}_i + b) \geq 1$

- Modified formulation incorporates slack variables:

Find $\mathbf{w}$ and b such that
$\mathbf{\Phi}(\mathbf{w}) = \mathbf{w}^{\mathrm{T}}\mathbf{w} + C\Sigma\xi_i$ is minimized
and for all $(\mathbf{x}_i, y_i)$, $i=1..n$ : $y_i(\mathbf{w}^{\mathbf{T}}\mathbf{x}_i + b) \geq 1 - \xi_i$, $\xi_i \geq 0$

- Parameter $C$ can be viewed as a way to control overfitting: it "trades off" the relative importance of maximizing the margin and fitting the training data.

# Non-linear SVM

- In practice most problems are linearly non-separable
- SVM can further be extended to find a non-linear boundary

The decision boundary is non-linear

# Non-linear SVM - Idea

- Transform the data from its original feature space to a new space where a linear boundary can be used to separate the data
- If the transformation is non-linear and to a higher dimensional space, it is more likely than a linear decision boundary can be found in it

- The learned linear decision boundary in the new feature space is mapped back to the original feature space, resulting in a non-linear decision boundary in the original space

# Example

- Non-linearly separable data in the original space

$\phi$

- Becomes linearly separable in the new space

transformation from old to new space:

$$\phi = (x_1, x_2) \rightarrow ({x_1}^2 - x_1, {x_2}^2 - x_2)$$

# Non-linear SVM - Idea

# Learning non-linear SVM

- What type of mapping function $\Phi$ should we use?
- Even if we know $\Phi$ , how can we do the computation in the new space efficiently?
  - The new space is typically with higher dimensionality
  - Computing dot products of vectors in high dimensional space is computationally expensive
  - Recall that to find the decision boundary we compute dot products of input vectors

$$\max W(\lambda) = \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j=1}^{N} \lambda_i \lambda_j y_i y_j \mathbf{x}_i \cdot \mathbf{x}_j$$

in the original space

$$\mathbf{x}_i \xrightarrow{\Phi} \Phi(\mathbf{x}_i), \mathbf{x}_j \xrightarrow{\Phi} \Phi(\mathbf{x}_j)$$

$$\Phi(\mathbf{x}_i) \cdot \Phi(\mathbf{x}_j)$$

in the new space – higher dim vectors

- How to effectively compute dot products in high dimensional space?
- Solution: *kernel trick*

# Kernel trick

- Method for computing the dot product of a pair of vectors in the new space without first computing the transformation of each vector from the original to the new space

- We need the dot product of the features in the new space: $\Phi(\mathbf{x}_i) \cdot \Phi(\mathbf{x}_j)$

- We will <u>not</u> firstly transform the features in the new space and then compute their dot product

$$1)\ \mathbf{x}_i \xrightarrow{\Phi} \Phi(\mathbf{x}_i), \mathbf{x}_j \xrightarrow{\Phi} \Phi(\mathbf{x}_j)$$

$$2)\ \Phi(\mathbf{x}_i).\Phi(\mathbf{x}_j)$$

- We will compute the dot product of the original features and use it in a function (called kernel function) to determine the dot product of the transformed features
- The kernel function specifies the relationship between the dot products in the original and transformed space

# Kernel trick - example

- 2 dim original and 3 dim new space: $\Phi:(x_1,x_2)=(x_1^2,\sqrt{2}x_1x_2,x_2^2)$

- u, v – vectors in the original space (2-dim)
- Φ(u), Φ(v) – transformed vectors u and v in the new space (3-dim)

$$\mathbf{u}\xrightarrow{\Phi}\Phi(\mathbf{u}),\mathbf{v}\xrightarrow{\Phi}\Phi(\mathbf{v})$$

- Let's calculate the dot product of Φ(u) and Φ(v)

$$\Phi(\mathbf{u})\cdot\Phi(\mathbf{v})=(u_1^2,\sqrt{2}u_1u_2,u_2^2)\cdot(v_1^2,\sqrt{2}v_1v_2,v_2^2)=$$
$$=u_1^2v_1^2+2u_1u_2v_1v_2+u_2^2v_2^2=(u_1v_1)^2+(u_2v_2)^2+2u_1u_2v_1v_2=$$
$$=(u_1v_1+u_2v_2)^2=(\mathbf{u}\cdot\mathbf{v})^2$$

- The dot product in the new space can be expressed via the dot product in the original space!
- This relationship is specified by the kernel function: $\Phi(\mathbf{u})\cdot\Phi(\mathbf{v})=(\mathbf{u}\cdot\mathbf{v})^2$

$$\boxed{K(\mathbf{u},\mathbf{v})=\Phi(\mathbf{u})\cdot\Phi(\mathbf{v})=(\mathbf{u}\cdot\mathbf{v})^2}$$

kernel trick

# Kernel function

- Kernel function for our example:

$$K(\mathbf{u},\mathbf{v}) = (\mathbf{u}\cdot\mathbf{v})^2$$

- Kernel functions allow the dot product in the new space to be computed without first computing $\Phi$ for each input vector
- As they specify the relationship between the dot products in the original and new feature space, we can compute a function of dot product in the original space and use it to evaluate the dot product in the new spaces
- Hence, we learn in higher dimensional space by computing kernel functions in lower dimensional space

$$K(\mathbf{u},\mathbf{v}) = \Phi(\mathbf{u})\cdot\Phi(\mathbf{v}) = (\mathbf{u}\cdot\mathbf{v})^2$$

# Mercer's theorem

- The special property of the kernel function for our example

$$K(\mathbf{u},\mathbf{v}) = \Phi(\mathbf{u})\cdot\Phi(\mathbf{v}) = (\mathbf{u}\cdot\mathbf{v})^2$$

- Functions K for which this is true (i.e. such $\Phi$ exist) need to satisfy the Mercer's Theorem, i.e. this restricts the class of functions K we can use

- We specify *K* (should satisfy Mercer's Theorem), i.e. we specify $\Phi$ indirectly, instead of choosing $\Phi$

- We perform the dot product computation in the original space which has smaller dimensionality

# Frequently used kernel functions

- Some kernels satisfying the Mercer's Theorem are

$$K(\mathbf{x},\mathbf{y}) = (\mathbf{x}\cdot\mathbf{y}+1)^p - polynomial\,kernel$$

$$K(\mathbf{x},\mathbf{y}) = e^{-\frac{\|x-y\|^2}{2\sigma^2}} - RBF$$ (Radial Basis Function)

$$K(\mathbf{x},\mathbf{y}) = \tanh(k\mathbf{x}\cdot\mathbf{y}-\theta) - tanget\ hyperbolic$$

$$(satisfies\ Mercer's\,Th.only\ for\ some\,k\ and\ \theta)$$

# SVM training and classification using kernel functions

- Training:

How to train classifier

$$\max \mathbf{w}(\lambda) = \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j=1}^{N} \lambda_i \lambda_j y_i y_j K(\mathbf{x}_i, \mathbf{x}_j)$$

$$subject\, to\, \lambda_i \geq 0, \sum_{i=1}^{N} \lambda_i y_i = 0$$

- Optimal hyperplane in the new space: $\mathbf{w} = \sum_{i=1}^{N} \lambda_i y_i \Phi(\mathbf{x}_i)$

classifier

- Classifying new example z:

$$\boxed{f = \mathbf{w} \cdot \mathbf{z} + b = \sum_{i=1}^{N} \lambda_i y_i K(\mathbf{x}_i, \mathbf{z}) + b}$$

use classifier

# SVM – summary

- Very popular classification method
- Can form arbitrary decision boundaries (both linear and non-linear)
- Three key concepts:
  - The decision boundary is the maximum margin hyperplane – the task is formulated as an optimization problem
  - Transform data into a new (typically higher dimensional space) where it is more likely to be linearly separable
  - Kernel trick – do the calculations in the original, not in the new higher dimensional space

- Can be applied to multi-class classification problems too – they are transformed into 2-class problems
- There is an extension for regression tasks – Support Vector Regression

# References

- SVMs were introduced by Cortes and Vapnik (1995)
  https://link.springer.com/article/10.1007/BF00994018

- Tutorial by Christopher Burges:
  https://drive.google.com/open?id=0B6x5IP0EWft1RFZGYWpodDlGZXc