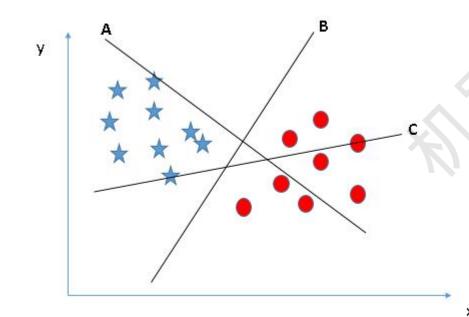
机器学习导论第五章

本章概要

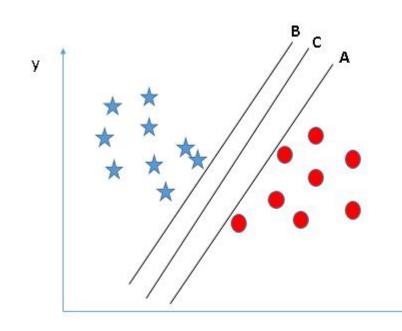
- ▶ 支持向量机 (Support Vector Machine, SVM)
 - ▶ 硬间隔支持向量机
 - ▶ 软间隔支持向量机
 - ▶非线性支持向量机
- ▶ 支持向量回归(Support Vector Regression,SVR)
- ▶ Scikit-Learn代码实现

▶ 给定训练样本集 $D = \{(x_1, y_1), (x_2, y_2), ..., (x_m, y_m), y_i \in \{-1, +1\}, 分类学习最近本的想法就是基于训练集D在样本空间中找到一个划分超平面,将不同类别的样本分开。$



对于图有A、B、C三个超平面, 很明显应该选择超平面B,也 就是说超平面首先应该能满足 将两类样本点分开。

▶ 能将训练样本分开的划分超平面可能有很多,应该如何选择?



- · 直观上看,应该去找位于两类训练样本 "正中间"的划分超平面,即红色的那个
- 因为该划分超平面对训练样本局部扰动的 "容忍"性最好
- 例如,由于训练集的局限性或噪声的干扰, 训练集外的样本可能比图中的训练样本更 接近两个类目前的分隔界,在分类决策的 时候就会出现错误,而超平面C受影响最小
 - 也就是说超平面C所产生的分类结果是最 鲁棒性的、是最可信的,对未见样本的泛 化能力最强。

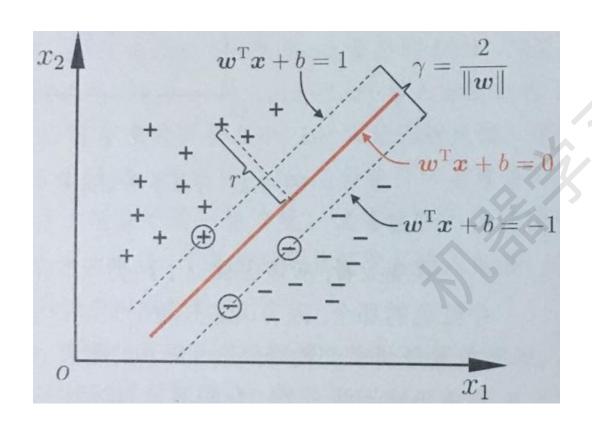
ightharpoonup 在样本空间中,划分超平面可通过以下线性方程来描述: $w^Tx+b=0$

其中 $\mathbf{w} = (w_1, w_2, ..., w_d)$ 为法向量,决定了超平面的方向; b为位移项,决定了超平面与原点之间的距离,将超平面记为 (\mathbf{w}, b)

▶ 样本空间中任意点X到超平面(W,b)的距离可写为:

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

假设超平面(w,b)能将训练样本正确分类,即对于(x_i , y_i) $\in D$,若 $y_i = +1$,则有 $w^Tx_i + b > 0$;若 $y_i = -1$,则有 $w^Tx_i + b < 0$ 。令 $\begin{cases} w^Tx_i + b \geq +1, \ y_i = +1 \\ w^Tx_i + b \leq -1, \ y_i = -1 \end{cases}$



$$\begin{cases} \mathbf{w}^{T} \mathbf{x}_{i} + b \ge + 1, & y_{i} = + 1 \\ \mathbf{w}^{T} \mathbf{x}_{i} + b \le - 1, & y_{i} = - 1 \end{cases}$$

距离最佳超平面 最近的几个训练样本点使上式中的等号成立,它们被称为"支持向量" (support vector)

D 记起平面 $\mathbf{w}^T \mathbf{x}_i + b = +1$ 和 $\mathbf{w}^T \mathbf{x}_i + b = -1$ 之间的距离为 γ ,该距离又被称为"问隔" (margin):

$$\gamma = \frac{2}{\|\boldsymbol{w}\|}$$

- > SVM的核心之一就是想办法将"间隔" γ最大化
- ▶ 也即

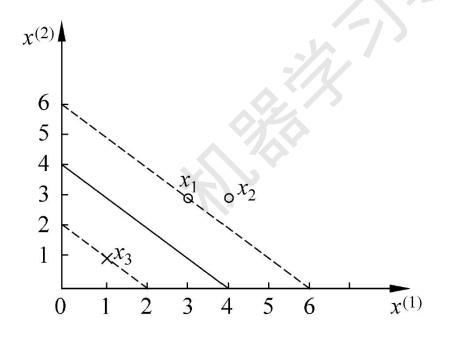
$$\max_{w,b} \frac{2}{\|w\|}$$
s.t. $y_i(w^T x_i + b) \ge 1$, $i = 1,2,...,m$

上 式等价于

$$\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2$$
s.t. $y_i(\mathbf{w}^T \mathbf{x}_i + b) \ge 1$, $i = 1,2,...,m$

这是支持向量基的基本型

例:已知一个如图所示的训练数据集,其正例点是 $x_1=(3,3)^T$, $x_2=(4,3)^T$ 负例点是 $x_3=(1,1)^T$,试求最大间隔分离超平面。



根据训练数据集构造约束最优化问题:

$$\min_{w,b} \frac{1}{2} (w_1^2 + w_2^2)$$
s.t. $3w_1 + 3w_2 + b \ge 1$
 $4w_1 + 3w_2 + b \ge 1$
 $-w_1 - w_2 - b \ge 1$

求得此最优化问题的解 $w_1=w_2=\frac{1}{2},\ b_1=-2$ 。于是最大问隔分离超平面为 $\frac{1}{2}x^{(1)}+\frac{1}{2}x^{(2)}-2=0$

其中 $x_1 = (3,3)^T n x_3 = (1,1)^T 为 支持向量。$

- ▶ 上一页PPT的公式是一个凸二次规划问题,我们可以将该凸二次规划问题 通过拉格朗日对偶性来解决
- ▶ 对上一页PPT的公式的每条约束添加拉格朗日乘子 $\alpha_i \geq 0$,则该问题的拉格朗日函数可写为:

$$L(\mathbf{w}, b, \alpha) = \frac{1}{2} \|\mathbf{w}\|^2 + \sum_{i=1}^{m} \alpha_i (1 - y_i(\mathbf{w}^T \mathbf{x}_i + b))$$

▶ 令 $L(w,b,\alpha)$ 对w和b的偏导为0可得:

$$\mathbf{w} = \sum_{i=1}^{m} \alpha_i y_i \mathbf{x}_i$$
$$0 = \sum_{i=1}^{m} \alpha_i y_i$$

▶ 可得支持向量基的基本型的对偶问题:

的基本型的对偶问题:
$$\max_{\alpha} \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_i \alpha_j y_i y_j \mathbf{x}_i^T \mathbf{x}_j$$

$$s.t. \sum_{i=1}^{m} \alpha_i y_i = 0$$

$$\alpha_i \ge 0, \ i = 1, 2, ..., m$$

解出α后,求出W和b即可得到模型

$$f(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + b = \sum_{i=1}^m \alpha_i y_i \mathbf{x}_i^T \mathbf{x} + b$$

》 例:与上例的训练数据集相同,其正例点是 $x_1=(3,3)^T$, $x_2=(4,3)^T$ 负例点是 $x_3=(1,1)^T$,试用算法求线性可分支持向量机。

▶ 根据所给数据,对偶问题是

$$\begin{aligned} \min_{\alpha} \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_{i} \alpha_{j} y_{i} y_{j} x_{i}^{T} x_{j} - \sum_{i=1}^{m} \alpha_{i} \\ &= \frac{1}{2} (18\alpha_{1}^{2} + 25\alpha_{2}^{2} + 2\alpha_{3}^{2} + 42\alpha_{1}\alpha_{2} - 12\alpha_{1}\alpha_{3} - 14\alpha_{2}\alpha_{3}) - \alpha_{1} - \alpha_{2} - \alpha_{3} \\ & \text{s. t. } \alpha_{1} + \alpha_{2} + \alpha_{3} = 0 \\ & \alpha_{i} \geq 0, \ i = 1, 2, 3 \end{aligned}$$

▶ 将 $\alpha_3 = \alpha_1 + \alpha_2$ 代入目标函数并记为:

$$s(\alpha_1, \alpha_2) = 4\alpha_1^2 + \frac{13}{2}\alpha_2^2 + 10\alpha_1\alpha_2 - 2\alpha_1 - 2\alpha_2$$

▶ 对 α_1 , α_2 求偏导数并令其为 α_2 , 可得 α_2)在点($\frac{3}{2}$, α_2),取极值,但该点不满足约束条件 $\alpha_2 \geq 0$,所以最小值应在边界上达到。

- ▶ 计算得

$$w_1 = w_2 = \frac{1}{2}$$

$$b = -2$$

▶ 分离超平面为

$$\frac{1}{2}x^{(1)} + \frac{1}{2}x^{(2)} - 2 = 0$$

▶ 分类决策函数为

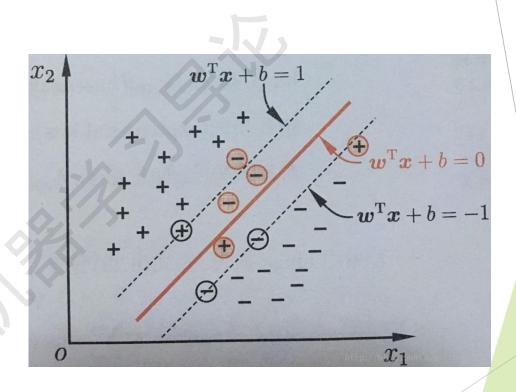
$$f(\mathbf{x}) = sign(\frac{1}{2}x^{(1)} + \frac{1}{2}x^{(2)} - 2)$$

▶ 在式中有不等式约束,因此上述过程满足Karush-Kuhn-Tucker(KKT)条件:

$$\begin{cases} \alpha_i \ge 0 \\ y_i f(\mathbf{x}_i) - 1 \ge 0 \\ \alpha_i (y_i f(\mathbf{x}_i) - 1) = 0 \end{cases}$$

- ▶ 于是,对任意训练样本 (x_i, y_i) ,总有 $\alpha_i = 0$ 或 $y_i f(x_i) = 1$ 。若 $\alpha_i = 0$,则该样本不会在 $f(x) = \sum_{i=1}^m \alpha_i y_i x_i^T x + b$ 的求和中出现,也就不会对f(x)有任何影响;若 $\alpha_i > 0$,则必有 $y_i f(x_i) = 1$,所对应的样本点位于最大间隔边界上,是一个支持向量。
- 这写实处支持向量机的一个重要性质:训练完成后,大部分的训练样本不需要保留,最终模型仅与支持向量有关。
- 上例中的 $\alpha_1=\alpha_3=\frac{1}{4}$,对应的实例点 x_1 , x_3 是支持向量。

- 在现实任务中很难找到一个超平面将不同类别的样本完全划分开,即很难找到合适的核函数使得训练样本在特征空间中线性可分。
- 退一步说,即使找到了一个可以使训练集在特征空间中完全分开的核函数, 也很难确定这个线性可分的结果是不 是由于过拟合导致的。
- P解决该问题的办法是在一定程度上运行SVM在一些样本上出错,为此引入了"软间隔"(soft margin)的概念



- \blacktriangleright 硬间隔支持向量机要求所有的样本均被最佳超平面正确划分,而软间隔支持向量机允许某些样本点不满足间隔大于等于1的条件 $y_i(\mathbf{w}^T\mathbf{x}_i+b)\geq 1$
- ▶ 在最大化间隔的时候也要限制不满足间隔大于等于1的样本的个数使之尽可能的少
- ▶ 引入一个惩罚系数 C>0,并对每个样本点 (x_i,y_i) 引入一个松弛变量 (slack variables) $\xi \geq 0$

$$\min_{\mathbf{w},b} \left(\frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^m \xi_i \right)$$
s.t. $y_i(\mathbf{w}^T \mathbf{x}_i + b) \ge 1 - \xi_i, \quad i = 1, 2, ..., m$
 $\xi_i \ge 0$

- ▶ 上式中约束条件改为 $y_i(\mathbf{w}^T \mathbf{x}_i + b) \ge 1 \xi_i$,表示问隔加上松弛变量大于等于1
- ▶ 优化目标改为 $\min_{w,b} \left(\frac{1}{2}||w||^2 + C\sum_{i=1}^m \xi_i\right)$,表示对每个松弛变量都要有一个代价损失 $C\xi_i$, C越大对误分类的惩罚越大、C越小对误分类的惩罚越小。

- \blacktriangleright 假设求解软间隔支持向量机间隔最大化问题得到的最佳超平面 $\mathbf{w}^T\mathbf{x} + b = 0$,对应的分类决策函数为 $\mathrm{sign}(\mathbf{w}^T\mathbf{x} + b)$,称为软间隔支持向量机
- ▶ 利用拉格朗日乘子法可得到上式的拉格朗日函数:

$$L(\mathbf{w}, b, \alpha, \xi, \mu) = \frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^{m} \xi_i - \sum_{i=1}^{m} \alpha_i (y_i(\mathbf{w}^T \mathbf{x}_i + b) - 1 + \xi_i) - \sum_{i=1}^{m} \mu_i \xi_i$$

其中 $\alpha_i \geq 0$, $\mu_i \geq 0$ 是拉格朗日乘子

ト 令 $L(w, b, \alpha, \xi, \mu)$ 分别对 w, b, ξ 求偏导并将偏导数为零可得:

$$\begin{cases} \mathbf{w} = \sum_{i=1}^{m} \alpha_i y_i \mathbf{x} \\ \sum_{i=1}^{m} \alpha_i y_i = 0 \\ \mathbf{C} = \alpha_i + \mu_i \end{cases}$$

▶ 可得到对偶问题:

$$\max_{\alpha} \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_i \alpha_j y_i y_j \mathbf{x}_i^T \mathbf{x}_j$$

$$s. t. \sum_{i=1}^{m} \alpha_i y_i = 0$$

$$0 \le \alpha_i \le C, \ i = 1, 2, ..., m$$

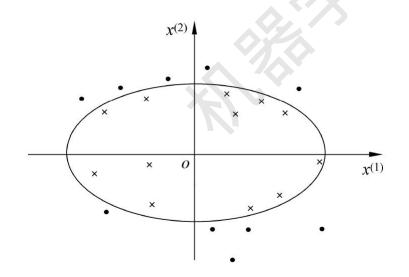
▶ 对比软间隔支持向量机的对偶问题和硬间隔支持向量机的对偶问题可发现二者的唯一差别就在于对偶变量的约束不同,软间隔支持向量机对对偶变量的约束是 $0 \le \alpha_i \le C$,硬间隔支持向量机对对偶变量的约束是 $0 \le \alpha_i$,于是可采用和硬间隔支持向量机相同的解法求解。

▶ 对于软间隔支持向量机,KKT条件要求:

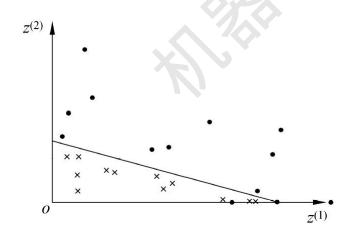
$$\begin{cases} \alpha_{i} \geq 0, \mu_{i} \geq 0 \\ y_{i}f(x_{i}) - 1 + \xi_{i} \geq 0 \\ \alpha_{i}(y_{i}f(x_{i}) - 1 + \xi_{i}) = 0 \\ \xi_{i} \geq 0, \ \mu_{i}\xi_{i} = 0 \end{cases}$$

- ▶ 同硬间隔支持向量机类似,对任意训练样本 (x_i, y_i) ,总有 $\alpha_i = 0$ 或 $y_i f(x_i) 1 + \xi_i = 0$,若 $\alpha_i = 0$,则该样本不会对最佳决策面有任何影响;若 $\alpha_i > 0$ 则必有 $y_i f(x_i) = 1 \xi_i$,也就是说该样本是支持向量。
- ► 若 $\alpha_i < C$ 则 $\mu_i > 0$ 进而有 $\xi_i = 0$,即该样本处在最大间隔边界上;若 $\alpha_i = C$ 则 $\mu_i = 0$ 此时如果 $\xi_i \leq 1$ 则该样本处于最大间隔内部,如果 $\xi_i > 1$ 则该样本处于最大间隔外部即被分错了。由此也可看出,软间隔支持向量机的最终模型仅与支持向量有关。

- 对解线性分类问题,线性分类支持向量机是一种非常有效的方法、但是,有时分类问题是非线性的,这时可以使用非线性支持向量机
- ▶ 如图,是一个分类问题。由图可见,无法用直线(线性模型)将正负实例正确分开,但可以用一条椭圆曲线(非线性模型)将它们正确分开



- ▶ 非线性问题往往不好求解,所以希望能用解线性分类问题的方法解决这个问题、
- 所采取的方法是进行一个非线性变换,将非线性问题变换为线性问题,通过解变换后的线性问题的方法求解原来的非线性问题。
- 对上图所示的例子,通过变换,将左图中椭圆变换成右图中的直线,将 非线性分类问题变换为线性分类问题。



- ▶ 设原空问为 $\mathcal{X} \subset R^2$, $\mathbf{x} = \left(x^{(1)}, x^{(2)}\right)^T \in \mathcal{X}$, 新空问为 $\mathbf{Z} \subset R^2$, $\mathbf{z} = \left(z^{(1)}, z^{(2)}\right)^T \in \mathcal{Z}$ 。
- ▶ 定义从原空间到新空间的变换(映射):

$$z = \phi(x) = ((x^{(1)})^2, (x^{(2)})^2)^T$$

经过变换 $Z = \phi(x)$,原空间 $X \subset R^2$ 变换为新空间 $Z \subset R^2$,原空间中的点相应地变换为新空间中的点,原空间中的椭圆

$$w_1(x^{(1)})^2 + w_2(x^{(2)})^2 + b = 0$$

变换成为新空间中的直线

$$w_1 z^{(1)} + w_2 z^{(2)} + b = 0$$

将φ(x)表示将x映射后的特征向量,在特征空间划分超平面所对应的模型 可表示为

$$f(\mathbf{x}) = \mathbf{w}^T \phi(\mathbf{x}) + b$$

▶ 优化问题为:

$$\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2$$
s.t. $y_i(\mathbf{w}^T \phi(\mathbf{x}_i) + b) \ge 1$, $i = 1,2,...,m$

▶ 其对偶问题为

$$\max_{\alpha} \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_i \alpha_j y_i y_j \phi(\mathbf{x}_i)^T \phi(\mathbf{x}_j)$$

$$s. t. \sum_{i=1}^{m} \alpha_i y_i = 0$$

$$\alpha_i \ge 0, i = 1, 2, ..., m$$

▶ 引入核函数 (kernel function)

$$\kappa(x_i, x_j) = \langle \phi(x_i), \phi(x_j) \rangle = \phi(x_i)^T \phi(x_j)$$

▶ 对偶问题可写为:

対:
$$\max_{\alpha} \sum_{i=1}^{m} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_{i} \alpha_{j} y_{i} y_{j} \kappa(\mathbf{x}_{i}, \mathbf{x}_{j})$$

$$s.t. \sum_{i=1}^{m} \alpha_{i} y_{i} = 0$$

$$\alpha_{i} \geq 0, \quad i = 1, 2, ..., m$$

▶ 求解后可得到:

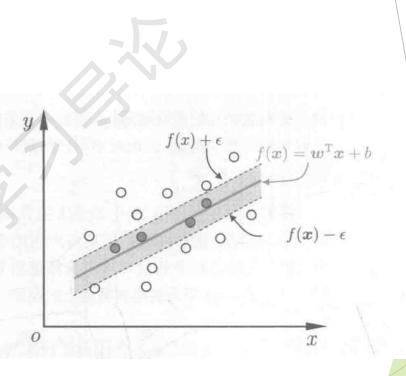
$$f(\mathbf{x}) = \mathbf{w}^T \phi(\mathbf{x}) + b = \sum_{i=1}^m \alpha_i y_i \kappa(\mathbf{x}_i, \mathbf{x}_j) + b$$

常用核函数

名称	表达式	参数
线性核	$\kappa(\overrightarrow{x_i},\overrightarrow{x_j}) = \overrightarrow{x_i}^T\overrightarrow{x_j}$	
多项式核	$\kappa(\overrightarrow{x_i},\overrightarrow{x_j})=(\overrightarrow{x_i}^T\overrightarrow{x_j})^n$	$n \geq 1$ 为多项式的次数
高斯核(RBF)	$\kappa(\overrightarrow{x_i},\overrightarrow{x_j}) = exp(-rac{\ \overrightarrow{x_i}-\overrightarrow{x_j}\ ^2}{2\sigma^2})$	$\sigma>0$ 为高斯核的带宽
拉普拉斯核	$\kappa(\overrightarrow{x_i},\overrightarrow{x_j}) = exp(-rac{\ x_i-x_j\ }{\sigma})$	σ>0
Sigmoid核	$\kappa(\overrightarrow{x_i},\overrightarrow{x_j}) = tanh(eta \overrightarrow{x_i}^T \overrightarrow{x_j} + heta)$	thah为双曲正切函数

支持向量回归

- ▶ 给定训练样本集 $D = \{(x_1, y_1), (x_2, y_2), ..., (x_m, y_m), y_i \in \mathbb{R}, \hat{\pi} \\ 望学得一个回归模型<math>f(x) = \mathbf{w}^T x + b$,使得f(x)与y尽可能接近, \mathbf{w} 和b是待确定的模型参数
- ▶ 对样本(x,y),传统回归模型基于模型输出 f(x)与真实输出y之间的差别来计算损失, 当且仅当f(x)与y完全相同时,损失才为0
- 支持向量回归假设我们能容忍f(x)与y之间最多有€的偏差,即仅当f(x)与y之间的差别绝对值大于€时才计算损失。



支持向量回归

▶ SVR的问题可形式化为

$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^{m} l_{\epsilon} (f(\mathbf{x}_i) - y_i))$$

▶ l_{ϵ} 是 ϵ 不敏感损失函数:

$$l_{\epsilon}(z) = \begin{cases} 0, & \text{if } |z| \leq \epsilon \\ |z| - \epsilon, & \text{otherwise} \end{cases}$$

▶ 线性支持向量机

```
import numpy as np
from sklearn import datasets
from sklearn.pipeline import Pipeline
from sklearn.preprocessing import StandardScaler
from sklearn.svm import LinearSVC
iris = datasets.load_iris()
X = iris["data"][:, (2, 3)] # petal length, petal width
y = (iris["target"] == 2).astype(np.float64) # Iris virginica
svm_clf = Pipeline([
        ("scaler", StandardScaler()),
        ("linear_svc", LinearSVC(C=1, loss="hinge")),
    ])
svm_clf.fit(X, y)
>>> svm_clf.predict([[5.5, 1.7]])
array([1.])
```

▶ 非线性支持向量机(多项式内核)

让我们在卫星数据集上进行测试:这是一个用于二元分类的小数据集,其中数据点的形状为两个交织的半圆

超参数coefO控制的是模型受高阶多项式还是低阶多项式影响的程度

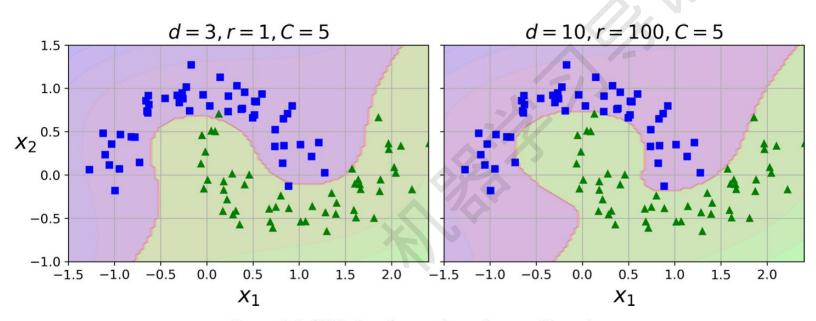


Figure 5-7. SVM classifiers with a polynomial kernel

非线性支持向量机(高斯RBF内核)

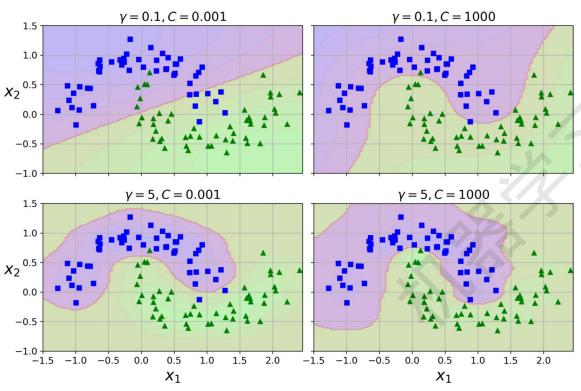
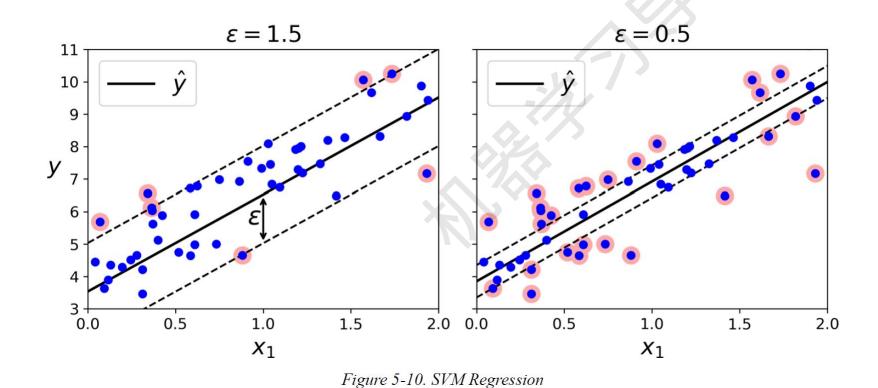


Figure 5-9. SVM classifiers using an RBF kernel

- 增加Y值会使钟形曲线变得更窄(左图),因此每个实例的影响范围随之变小:决策边界变得更不规则,开始围着单个实例绕弯。
- 反过来,减小γ值使钟形曲线 变得更宽,因而每个实例的影 响范围增大,决策边界变得更 平坦。所以γ就像是一个正则 化的超参数:模型过拟合,就 降低它的值,如果欠拟合则提 升它的值

> 支持向量回归



▶ 支持向量回归

线性

```
from sklearn.svm import LinearSVR
svm_reg = LinearSVR(epsilon=1.5)
svm_reg.fit(X, y)
```

非线性

```
from sklearn.svm import SVR

svm_poly_reg = SVR(kernel="poly", degree=2, C=100, epsilon=0.1)
svm_poly_reg.fit(X, y)
```

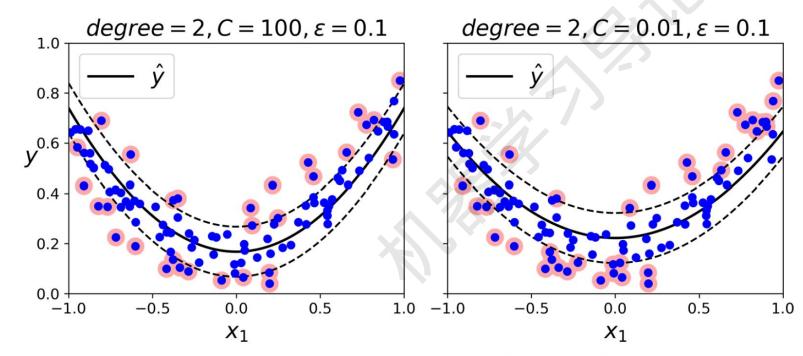


Figure 5-11. SVM Regression using a second-degree polynomial kernel