机器学习 Machine Learning

北京航空航天大学计算机学院 School of Computer Science and Engineering, Beihang University 刘庆杰 陈佳鑫

> 2025年春季学期 Spring 2025

5.1 支持向量机

- 支持向量机的发展简史
- 支持向量机的基本思想

支持向量机 (Support Vector Machine)

- ●什么是支持向量机 (SVM)
 - ▶支持向量机是基于统计学习理论 (Statistical Learning Theory, SLT) 发展起来的一种机器学习的方法
 - > 统计学习理论主要创立者是Vladimir N. Vapnik

1964年-1990年 莫斯科控制科学学院 曾担任计算机科学与研究系主任

1991年-2001年 美国AT&T贝尔实验室 发明支持向量机理论

2002年-2014年 NEC实验室(美国) 从事机器学习研究

2014年-2016年 美国Facebook公司 从事人工智能研究

2016年 美国Vencore实验室 继续研究工作

2006年 入选美国国家工程院院士。

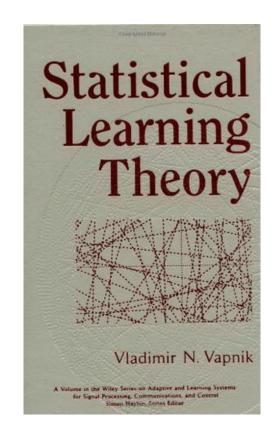


Vladimir N. Vapnik (1936 -)

支持向量机 (Support Vector Machine)

● V. Vapnik对于统计机器学习做出了巨大贡献

- ▶ 1968年,Vapnik和Chervonenkis提出了VC熵和VC维的概念,这些是统计学习理论的核心概念。同时,他们发现了泛函空间的大数定理,得到了关于收敛速度的非渐进界的主要结论。
- ▶ 1974年,Vapnik和Chervonenkis提出了结构风险最小化归纳原则。
- ▶ 1989年,Vapnik和Chervonenkis发现了经验风险最小化归纳原则和最大似然方法一致性的充分必要条件,完成了对经验风险最小化归纳推理的分析。
- > 90年代中期,有限样本情况下的机器学习理论研究逐渐成熟起来, Vapnik对统计学习理论进行了较完善的总结,其中详细叙述了 SVM理论。



支持向量机发展简史

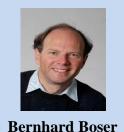
• 支持向量机的发展简史

1963年,Vapnik首 次提出了支持向量方 法,实现对特征子集 的划分等价于对整个 数据集的划分。





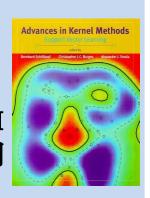
Grace Wahba





1990年, Grace、Boser和 Vapnik等开始了SVM的研究

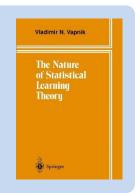
1999年, MIT出 版了《Advances in Kernel Method», SVM 理论的研究与应用 推向了一个高潮。



1971年, Kimeldorf提出使 用线性不等约束重 新构造支持向量的 核空间



1995年,Vapnik的书 «The Nature of Statistical Learning Theory》出版,详细叙述 了SVM理论



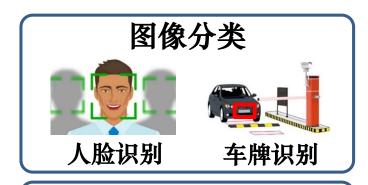
之后,SVM的研究主要集中 在对SVM本身性质的研究和 完善,和加大SVM应用的深 度和广度两方面。

支持向量机的应用

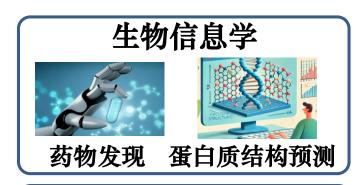
- 支持向量机的应用
 - ▶ 2000年~2010年, SVM被应用于诸多行业:









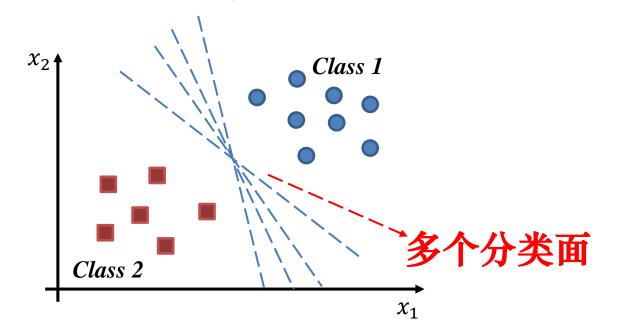


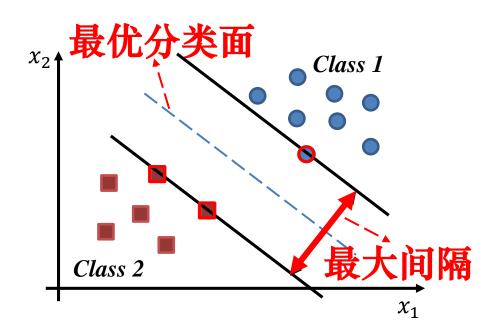


➢ 当前,由于SVM对样本规模要求少,仍然被用于一些样本受限的研究领域,如疾病诊断、基因表达分析等。

支持向量机的基本思想

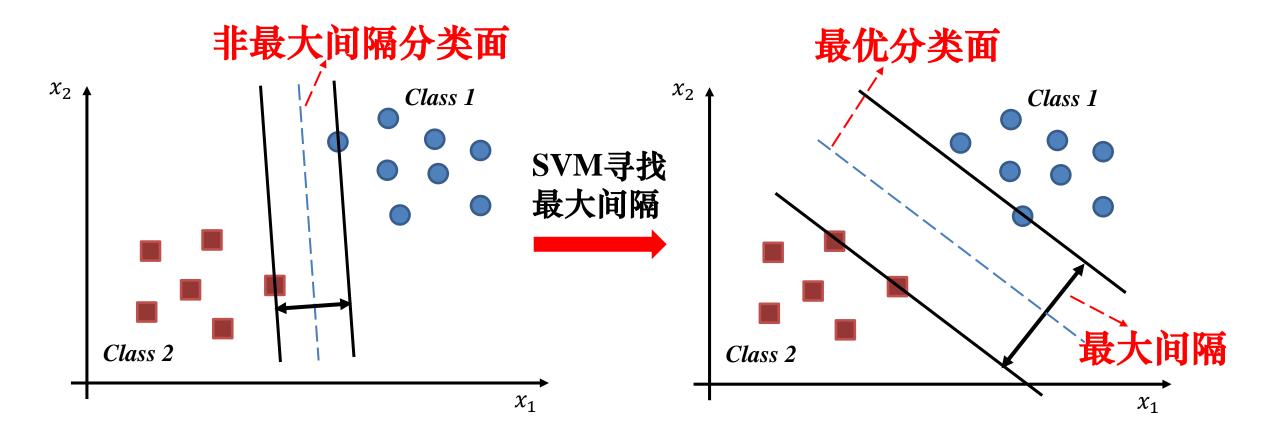
- SVM从线性可分情况下的最优分类面发展而来
 - > 分类面可能存在多个,但是哪一个是最优的分类平面?
- ▶最优分类面:要求分类面不但能将两类正确分开(训练错误率为0),且使分类间隔最大,这里的最优分类面是一个硬间隔分类面
 - ▶间隔 (Margin): 距离分类面最近的两个异类样本到分类面的距离之和





支持向量机的基本思想

- SVM如何求取最优分类面
 - >SVM考虑寻找一个满足分类要求的超平面,使训练集中的点距离分类面尽可能的远,即SVM是通过寻找最大间隔来求取最优分类面

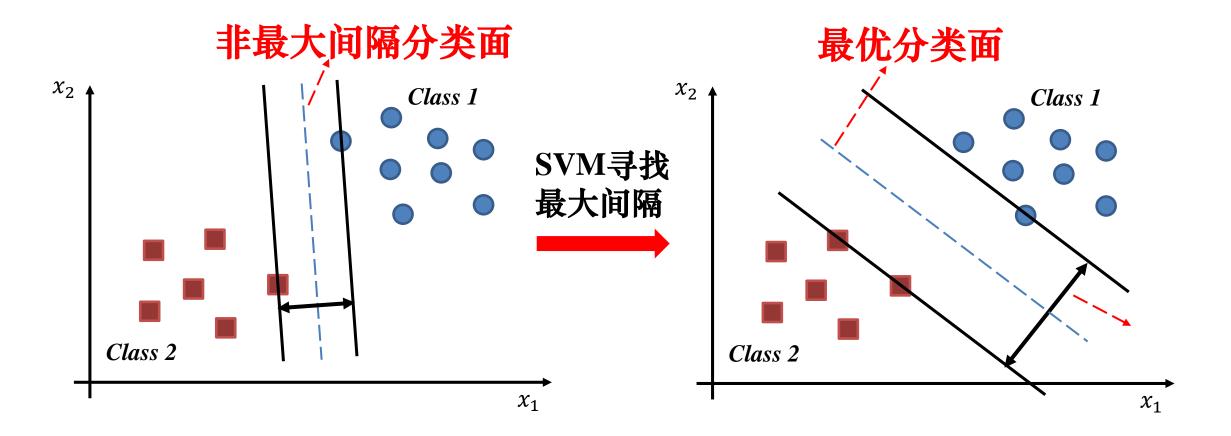


5.2 线性支持向量机

- 支持向量机的建模方法
- 支持向量机的模型推导

线性支持向量机

- 支持向量机如何求取最优分类面?
 - > SVM通过寻找最大间隔来求取最优分类面



线性支持向量机建模方法

● 线性支持向量机建模

- **芦样本集:** $\{x_n, t_n\}, n = 1, 2, ..., N, x_n \in \mathbb{R}^d, t_n \in \{-1, 1\}$
- 分类超平面: $y(x) = w^T x + b$

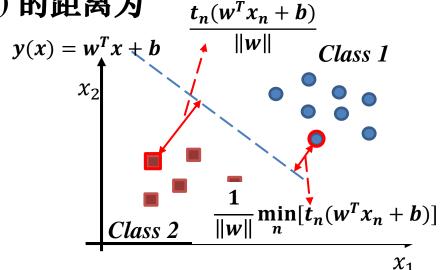
当分类超平面可以将训练样本正确分类时,有 $t_n = \begin{cases} +1, & w^T x_n + b > 0 \\ -1, & w^T x_n + b < 0 \end{cases}$,即 $t_n y(x_n) > 0$

样本集上任意一点 x_n 到分类超平面(满足 $t_n y(x_n) > 0$)的距离为

$$\frac{t_n y(x_n)}{\|w\|} = \frac{t_n (w^T x_n + b)}{\|w\|}$$

距离超平面最近的样本到分类超平面的距离为

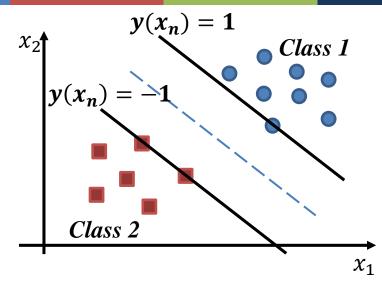
$$\frac{1}{\|\mathbf{w}\|} \min_{n} [t_n(\mathbf{w}^T \mathbf{x}_n + \mathbf{b})]$$



线性支持向量机建模方法

- 线性支持向量机建模
 - > 求解有最大间隔的分类超平面的目标函数为

$$\max_{w,b} \{ \frac{1}{\|w\|} \min_{n} [t_n(w^T x_n + b)] \} \quad \Rightarrow \quad 求解复杂$$



由于 $w \rightarrow kw, b \rightarrow kb$ 不影响求解目标,则令距离超平面最近的点为

$$t_n(w^Tx_n+b)=1$$

样本集中所有点满足 $t_n(w^Tx_n + b) \ge 1$

则求解原问题可以转为求解一个更简单的问题:

$$\max_{w,b} \{ \frac{1}{\|w\|} \min_{n} [t_n(w^T x_n + b)] \} \qquad \Rightarrow \qquad \max_{w,b} \frac{1}{\|w\|} \\ s.t. \quad t_n(w^T x_n + b) \ge 1$$

- 优化问题求解
 - > 原优化问题转化为二次规划问题

$$\max_{\substack{w,b}} \frac{1}{\|w\|}$$
 二次规划问题
$$\min_{\substack{w,b}} \frac{1}{2} \|w\|^2$$
 $s.t.$ $t_n(w^Tx_n + b) \ge 1$ (5-2-1)

- >使用拉格朗日乘子法将上述二次规划问题转化为等价的对偶问题来简化求解
- ▶该问题的拉格朗日函数可以表示为

$$L(w,b,a) = \frac{1}{2} \|w\|^2 - \sum_{n=1}^{N} a_n \{t_n(w^T x_n + b) - 1\}, \quad a_n \ge 0$$
 (5-2-2)

拉格朗日乘子

- 优化问题求解
 - > 分别对变量求导

$$\frac{\partial L(w,b,a)}{\partial w} = w - \sum_{n=1}^{N} a_n t_n x_n = 0, \quad \frac{\partial L(w,b,a)}{\partial b} = \sum_{n=1}^{N} a_n t_n = 0$$
 (5-2-3)

>带入拉格朗日函数,得到(5-2-1)的对偶形式

$$\max_{a} \sum_{n=1}^{N} a_{n} - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_{n} a_{m} t_{n} t_{m} x_{n}^{T} x_{m}$$
s.t. $a_{n} \geq 0$, $n = 1, ..., N$, $\sum_{n=1}^{N} a_{n} t_{n} = 0$ (5-2-4)

➤由于 (5-2-4) 存在不等式约束,需要验证最优解是否满足KKT (Karush-Kuhn-Tucker) 条件,才可以确定对偶问题是否等价于原问题

- 拉格朗日对偶性
 - > 不失一般性,设存在不等式约束的优化问题

 \triangleright 定义 $\theta_P(w) = \max_{\alpha,\beta; \alpha_i \geq 0} L(w,\alpha,\beta)$, 只有当满足约束条件,才有最大值

$$\theta_P(w) = \begin{cases} f(w), \text{ 若 } w \text{ 满足约束条件} \\ +\infty, \text{ 否则} \end{cases}$$

● 拉格朗日对偶性

 \triangleright 原问题 $\min_{w} f(w)$ 转化为 p^*

$$p^* = \min_{w} \theta_P(w) = \min_{w} \max_{\alpha,\beta ; \alpha_i \geq 0} L(w,\alpha,\beta)$$

▶直接求解较困难,进而转向求解其对偶问题 d*

$$\theta_D(\alpha, \beta) = \min_{w} L(w, \alpha, \beta)$$

$$d^* = \max_{\alpha, \beta; \alpha_i \ge 0} \theta_D(\alpha, \beta) = \max_{\alpha, \beta; \alpha_i \ge 0} \min_{w} L(w, \alpha, \beta)$$

- 拉格朗日对偶性
 - ▶ p*和 d* 存在如下关系

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$
取最大值时的解
$$= f(w^*) + \sum_{i=1}^k \alpha^* g_i(w^*) + \sum_{i=1}^l \beta_i^* h_i(w^*) \le f(w^*) = p^*$$

$$g_i(w) \le 0$$

$$h_i(w) = 0$$

$$p^* = \min_w \theta_P(w) = f(w^*)$$

〉在无其他条件约束下, $d^* \le p^*$,两个对偶问题是不一定等价的,那满足什么条件可以使原问题与对偶问题等价,即 $d^* = p^*$ 呢?

● 拉格朗日对偶性

 \triangleright 若使 $d^* = p^*$,则应将下式中的不等号取等号:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

$$= f(w^*) + \sum_{i=1}^k \alpha_i^* g_i(w^*) + \sum_{i=1}^l \beta_i^* h_i(w^*) \le f(w^*) = p^*$$
等号成立

$$h_i(w) = 0$$
,
此部分已知为 0

 * 当 $\alpha_i^* g_i(w^*) = 0$ 时,此时取等号

》所以,当同时满足 $\frac{\partial}{\partial w_i} L(w^*, \alpha^*, \beta^*) = 0$ 和 $\alpha_i^* g_i(w^*) = 0$ 时,原问题与对偶问题等价。 这两个条件和之前已知的约束条件共同组成了KKT条件

(详细推导过程见附录)

● KKT (Karush-Kuhn-Tucker) 条件

$$\frac{\partial}{\partial w_i}L(w^*,\alpha^*,\beta^*)=0,i=1,...,n$$
 $\alpha_i^*g_i(w^*)=0,i=1,...,k$ $g_i(w^*)\leq 0,i=1,...,k$

KKT互补松弛条件

如果 w^* , α^* , β^* 满足上述的KKT条件, 那么它们就是原问题和对偶问题的解。

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

>KKT互补松弛条件分析:

补充条件隐含如果 $\alpha^* > 0$,那么 $g_i(w^*) = 0$,即w处于可行域的边界上,是起作用的 (Active)约束,而位于可行域内部的点都是不起作用的约束,其 $\alpha^* = 0$ 。

● 求解分类超平面

➤回归到SVM求解问题,已知对偶问题:

$$\max_{a} \sum_{n=1}^{N} a_{n} - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_{n} a_{m} t_{n} t_{m} x_{n}^{T} x_{m} \quad \text{s.t.} \quad a_{n} \geq 0, \ n = 1, ..., N, \ \sum_{n=1}^{N} a_{n} t_{n} = 0$$
 (5-2-4)

如果原问题和对偶问题等价,必须满足KKT条件:

$$a_n \ge 0$$
, $t_n y(x_n) - 1 \ge 0$, $a_n \{t_n y(x_n) - 1\} = 0$ (互补松弛条件) (5-2-5)

曲
$$\frac{\partial L(w,b,a)}{\partial w} = w - \sum_{n=1}^{N} a_n t_n x_n = 0$$
和 $\frac{\partial L(w,b,a)}{\partial b} = \sum_{n=1}^{N} a_n t_n = 0$,可以得到超平面为:

$$y(x) = \sum_{n=1}^{N} a_n t_n x_n^T x + b, b = \frac{1}{N_S} \sum_{n \in S} (t_n - \sum_{m \in S} a_m t_m x_n^T x_m)$$
 (5-2-6)

● KKT条件分析

分类超平面
$$y(x) = \sum_{n=1}^{N} a_n t_n x_n^T x + b$$

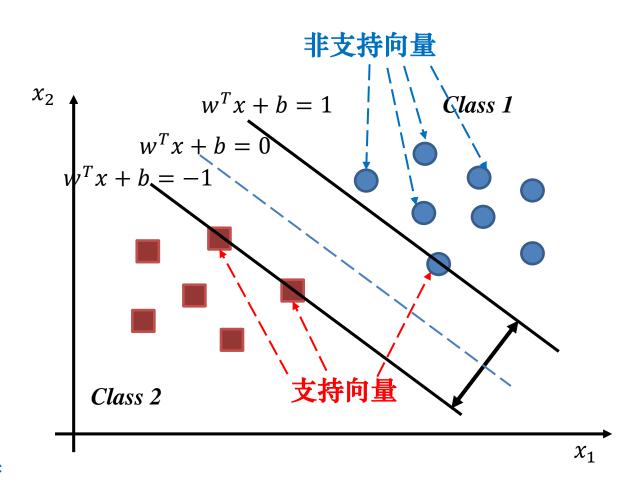
互补松弛条件 $a_n\{t_ny(x_n)-1\}=0$

 \triangleright 支持向量: $t_n(w^Tx+b)=1$, $a_n>0$

非支持向量: $t_n(w^Tx + b) > 1, a_n = 0$



只有<mark>支持向量</mark>决定分类超平面,非支持 向量与其无关



线性支持向量机的求解示例

●示例

- ightharpoonup 已知正样本点为 $x_1 = (3,3)^T$, $x_2 = (4,3)^T$, 负样本点
- 为 $x_3 = (1,1)^T$,求线性可分支持向量机。
- ▶解:由公式(5-2-4),得到对偶问题为:

$$\min_{a} \frac{1}{2} (18a_1^2 + 25a_2^2 + 2a_3^2 + 42a_1a_2 - 12a_1a_3 - 14a_2a_3) - a_1 - a_2 - a_3$$
s.t. $a_1 + a_2 - a_3 = 0, \ a_i \ge 0, i = 1, 2, 3$

 $a_3 = a_1 + a_2$ 带入对偶问题优化目标函数,记为 $s(a_1, a_2) = 4a_1^2 + \frac{13}{2}a_2^2 + 10a_1a_2 - 2a_1 - 2a_2$

可知 $s(a_1, a_2)$ 在 $(\frac{3}{2}, -1)^T$ 取极值,但此时 $a_2 = -1$ 不满足 $a_2 \ge 0$,则最小值只能在约束边界上取得。

——本例参考自 李航 《统计学习方法》 7.2节

线性支持向量机的求解举例

●举例

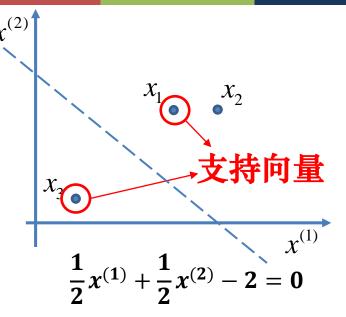
则有,当 $a_1 = 0$ 时,最小值 $s(0, \frac{2}{13}) = -\frac{2}{13}$,当 $a_2 = 0$ 时,最小值 $s(\frac{1}{4}, 0) = -\frac{1}{4}$,于是 $s(a_1, a_2)$ 在 $a_1 = \frac{1}{4}$, $a_2 = 0$ 时取最小值,则 $a_3 = \frac{1}{4}$

- ightharpoonup 基于KKT条件,可知在 $a_n > 0$ 时为支持向量,所以 a_1 和 a_3 ,所对应的实例点 x_1 和 x_3 是支持向量。
- > 由公式 (5-2-3) 可求

$$w = \sum_{n=1}^{N} a_n t_n x_n = \frac{1}{4} \times 1 \times (3,3)^T + 0 + \frac{1}{4} \times (-1) \times (1,1)^T = (\frac{1}{2}, \frac{1}{2})$$

$$b = \frac{1}{N_S} \sum_{n \in S} (t_n - \sum_{m \in S} a_m t_m x_n^T x_m)$$
 ,则有 $b = -2$

> 则分类超平面为: $\frac{1}{2}x^{(1)} + \frac{1}{2}x^{(2)} - 2 = 0$

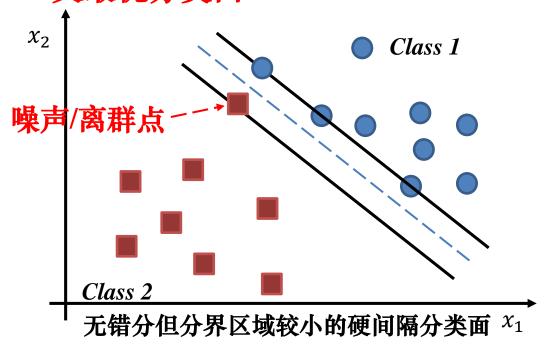


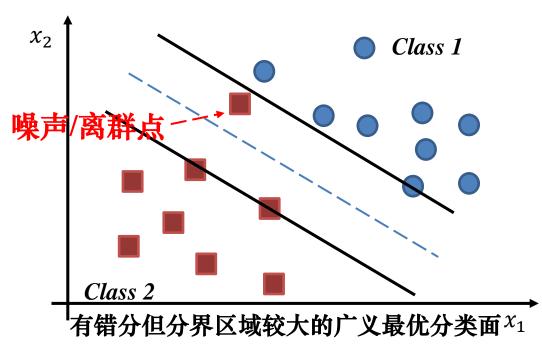
5.3 软间隔

- 什么是软间隔
- 软间隔的求解

硬间隔的局限

- 硬间隔难以处理噪声和离群点
 - ▶ 由于样本中不可避免地存在噪声和离群点,可能导致硬间隔求解的最优分类面泛 化性能差。
 - ▶对于分布有交集的数据,需要有一定范围内的"错分",又有较大分界区域的广 义最优分类面。





什么是软间隔

- 引入松弛变量处理噪声和离群点
 - > 引入松弛变量 $\xi_n \ge 0$

$$\xi_n = 0$$
 最大间隔边界

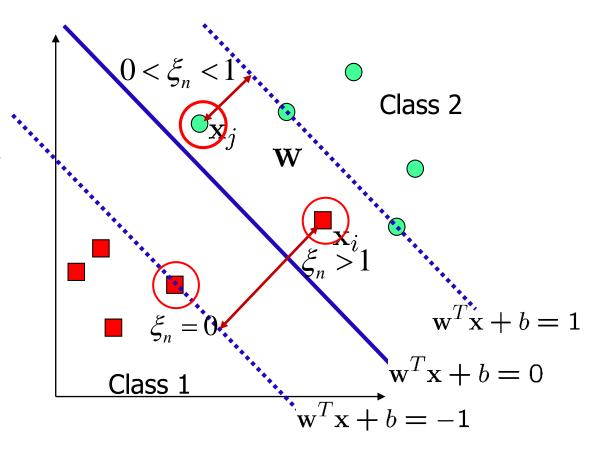
$$|\xi_n| = |t_n - y(x_n)|$$
 $\Rightarrow 0 < \xi_n \le 1$ 最大间隔内部 且未被错分

$$\xi_n > 1$$

被错分

原有不等式约束修改为

$$t_n y(x_n) \ge 1$$
 \Rightarrow $t_n y(x_n) \ge 1 - \xi_n$



> 这种处理方式也被视为是从硬间隔 (Hard Margin) 向软间隔 (Soft Margin) 的转变。

什么是软间隔

● 基于软间隔的优化问题

惩罚系数: 反映对离群点容忍度 松弛变量

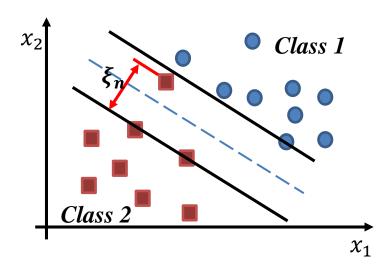
软间隔

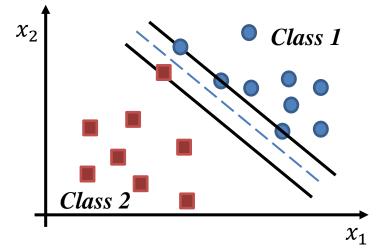
$$\min_{w,b} \frac{1}{2} ||w||^2 + C \sum_{n=1}^{N} \xi_n$$
s.t. $t_n(w^T x_n + b) \ge 1 - \xi_n, n = 1, ..., N$
 $\xi_n \ge 0$

硬间隔

$$\min_{w,b} \frac{1}{2} ||w||^2$$
s.t. $t_n(w^T x_n + b) \ge 1, n = 1,..., N$

软间隔虽然存在少量错分,但带来更大的间隔,具有 更好的泛化性能





● 利用拉格朗日乘子法进行软间隔求解

》 优化目标:
$$\min_{w,b} \frac{1}{2} ||w||^2 + C \sum_{n=1}^{N} \xi_n$$
 $s.t. t_n(w^T x_n + b) \ge 1 - \xi_n \xi_n \ge 0, n = 1, ..., N$

相比硬间隔添加了松弛变量 和对应的惩罚系数

松弛变量引入约束条件

>拉格朗日函数:

业格朗日图数:
$$L(w,b,\xi,a,\mu) = \frac{1}{2} ||w||^2 + C \sum_{n=1}^N \xi_n - \sum_{n=1}^N a_n \{t_n y(x_n) - 1 + \xi_n\} + \sum_{n=1}^N \mu_n \xi_n$$
 由于 $\xi_n \geq 0$,松弛变量添加为拉格朗日函数的一项, $\mu_n \geq 0$ 是对应的拉格朗日乘子

光化w,b,{
$$\xi_n$$
}: $\frac{\partial L}{\partial w} = 0 \Rightarrow w = \sum_{n=1}^{N} a_n t_n x_n$ $\frac{\partial L}{\partial b} = 0 \Rightarrow \sum_{n=1}^{N} a_n t_n = 0$ $\frac{\partial L}{\partial \xi_n} = 0 \Rightarrow a_n = C - \mu_n$

日乘子

松弛变量作为一个变量求对应偏 导,偏导为0,此时有 $a_n + \mu_n = C$

- 利用拉格朗日乘子法进行软间隔求解
 - > 带入拉格朗日函数,得到对偶问题:

$$\max_{a} \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m x_n^T x_m$$

$$s. t. 0 \le a_n \le C, n = 1, 2, \dots, N$$

$$\sum_{n=1}^{N} a_n t_n = 0$$

>KKT条件:

$$a_n \geq 0$$
, $\mu_n \geq 0$, $\xi_n \geq 0$

$$t_n y(x_n) - 1 + \xi_n \ge 0$$

互补松弛条件:
$$a_n\{t_ny(x_n)-1+\xi_n\}=0$$

$$\mu_n \xi_n = 0$$

与硬间隔对偶问题相比,只有约束 条件不同,硬间隔中要求 $a_n \ge 0$

约束 $t_n(w^Tx_n+b) \geq 1-\xi_n$ 的互补松弛条件 约束 $\xi_n \geq 0$ 的互补松弛条件

● KKT互补松弛条件分析

 $a_n = 0$ 样本 x_n 不受约束,与分类超平面无关,是非支持向量

$$a_n\{t_n y(x_n) - 1 + \xi_n\} = 0$$

$$\mu_n \xi_n = 0$$

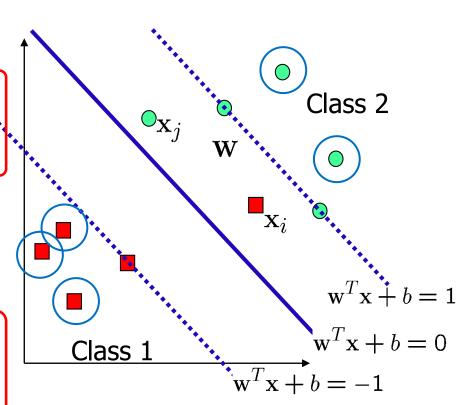


$$a_n \ge 0$$

$$a_n > 0$$

$$t_n y(x_n) - 1 + \xi_n = 0$$
 样本 x_n 是支持向量

$$\mu_n \xi_n = 0$$



● KKT互补松弛条件分析

 $a_n > 0$ $t_n y(x_n) - 1 + \xi_n = 0$ $\mu_n \xi_n = 0$

$$0 < a_n \le C,$$

$$a_n + \mu_n = C$$

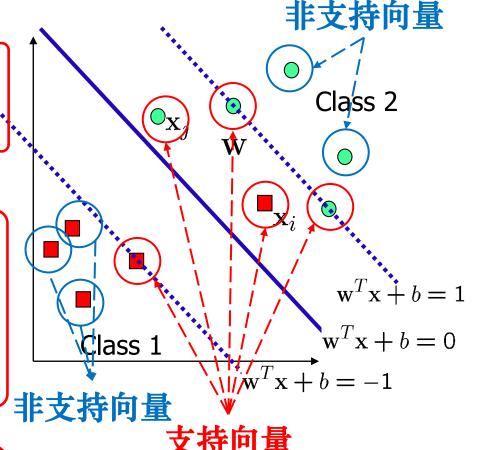
 $a_n < C, \mu_n > 0$

 $\xi_n = 0$ 样本 x_n 在最大分隔边界上

$$a_n = C, \mu_n = 0, \mu_n$$
不再约束 ξ_n

 $\xi_n \le 1$ 样本 x_n 在最大分隔内且被未错分

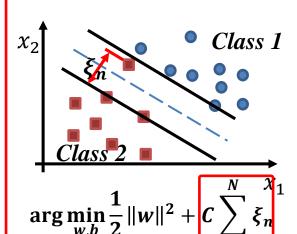
 $\xi_n > 1$ 样本 x_n 被错分



软间隔支持向量机的最终超平面也仅与支持向量有关

总结

●总结



s.t. $t_n(w^Tx_n+b) \ge 1-\xi_n$,

 $n=1,\ldots,N,\xi_n\geq 0$

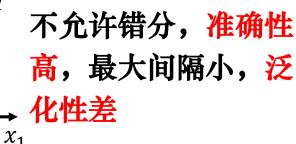
软间隔

允许对噪声/离群点有一 定错分,最大间隔更大, 泛化性更好

求解时有超参惩罚系数, 求解比硬间隔复杂

软间隔是权衡泛化性和准确性的综合选择



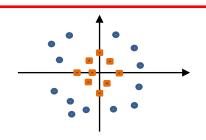


$$rg \min_{w,b} rac{1}{2} \|w\|^2$$

s.t. $t_n (w^T x_n + b) \ge 1$, $n = 1, \dots, N$

求解过程较简单

▶思考新问题:介绍了使用硬间隔SVM和软间隔SVM求解 线性分类问题,SVM是否可以解决非线性问题?

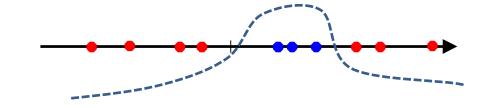


5.4 非线性支持向量机

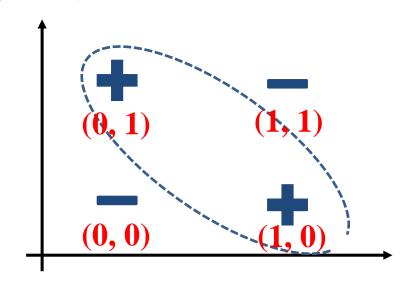
- 非线性支持向量机原理
- 核函数原理

非线性支持向量机原理

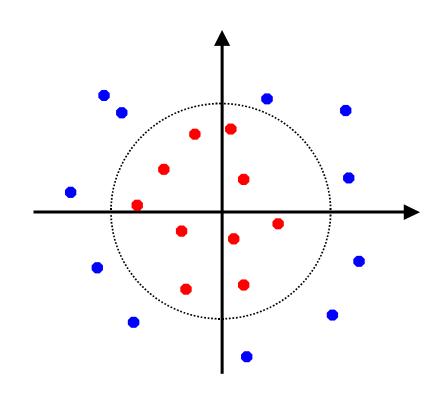
- 支持向量机如何解决非线性问题
 - (1) 一维线性不可分问题



(3) 异或问题



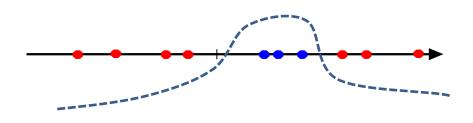
(2) 二维线性不可分问题



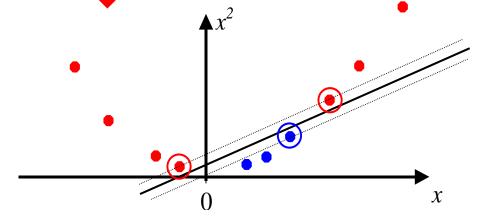
非线性支持向量机原理

● 非线性SVM的基本思想

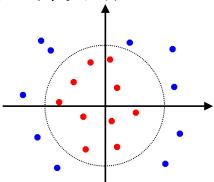
(1)一维线性不可分问题



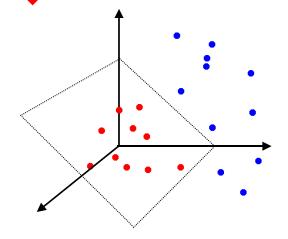
 $\Phi: x \to \phi(x)$ 升至二维空间实现线性可分



(2) 二维线性不可分问题



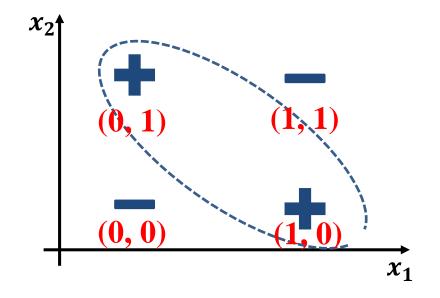
 $\Phi: x \to \phi(x)$ 升至三维空间实现线性可分



非线性支持向量机原理

● 非线性SVM的基本思想

(3) 异或问题



$$\Phi: x \to \phi(x)$$

$$\boldsymbol{\phi}(x) = (x_1, x_2, x_1 x_2)$$

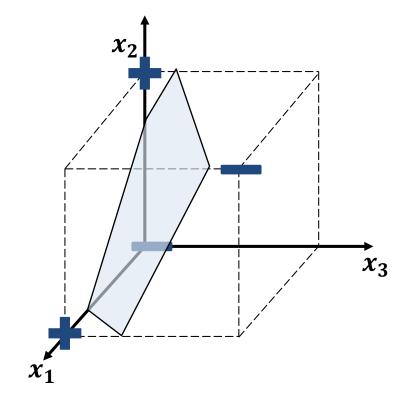


$$(0,0) \rightarrow (0,0,0)$$

$$(1,1) \rightarrow (1,1,1)$$

$$(0,1) \rightarrow (0,1,0)$$

$$(1,0) \rightarrow (1,0,0)$$



非线性支持向量机原理

●高维映射引发维度灾难

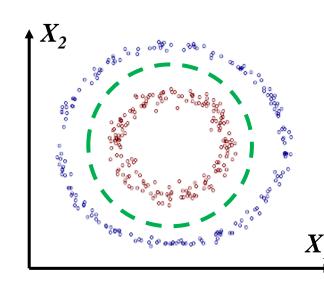
__ ___

$$a_1X_1 + a_2X_1^2 + a_3X_2 + a_4X_2^2 + a_5X_1X_2 + a_6 = 0$$

一种映射:

$$oldsymbol{Z}_1=oldsymbol{X}_1$$
 ; $oldsymbol{Z}_2=oldsymbol{X}_1^2$; $oldsymbol{Z}_3=oldsymbol{X}_2$; $oldsymbol{Z}_4=oldsymbol{X}_2^2$; $oldsymbol{Z}_5=oldsymbol{X}_1oldsymbol{X}_2$

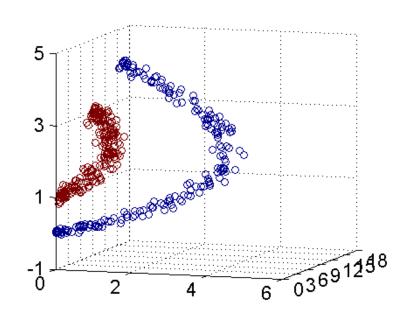
另一种映射:



$$a_1 X_1^2 + a_2 (X_2 - c)^2 + a_3 = 0$$

$$Z_1 = X_1^2; Z_2 = X_2^2; Z_3 = X_2$$

$$\phi: \mathbb{R}^2 o \mathbb{R}^3$$



非线性支持向量机原理

●高维映射引发维度灾难

原始样本分布:
$$a_1X_1 + a_2X_1^2 + a_3X_2 + a_4X_2^2 + a_5X_1X_2 + a_6 = 0$$

$$\sum_{i=1}^5 a_iZ_i + a_6 = 0 \quad \phi: \mathbb{R}^2 \to \mathbb{R}^5$$

原始样本增到三维:

$$a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_1^2X_2 + a_5X_1^2X_3 + a_6X_2^2X_1 + a_7X_2^2X_3 + a_8X_3^2X_1 + a_9X_3^2X_2 + a_{10}X_1X_2X_3 + a_{11}X_1^2 + a_{12}X_2^2 + a_{13}X_3^2 + a_{14}X_1X_2 + a_{15}X_2X_3 + a_{16}X_1X_3 + a_{17}X_1 + a_{18}X_2 + a_{19}X_3 + a_{20} = 0$$

非线性SVM是如何解决高维映射引发的维度灾难?

核函数原理

▶非线性支持向量机

 \rightarrow 设样本集 $\{x_n,t_n\}$,样本 x_n 映射后的向量为 $\phi(x_n)$,分类超平面为 $y(x)=w^T\phi(x)+b$

$$\rightarrow$$
 优化目标为: $\min_{w,b} \frac{1}{2} ||w||^2$

s. t.
$$t_n(w^T\phi(x_n) + b) \ge 1$$
, $n = 1, 2, ..., N$.

> 对偶问题为:

$$\max_{a} \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m \phi(x_n)^{\mathrm{T}} \phi(x_m)$$

$$s.t.\sum_{n=1}^{\infty}a_nt_n=0, \quad a_n\geq 0, \quad i=1,2,...,N$$

$$s.t.\sum_{n=1}^{N}a_{n}t_{n}=0, \quad a_{n}\geq 0, \quad i=1,2,...,N.$$

$$> 分类超平面为: \ y(x)=w^{T}\phi(x)+b=\sum_{n=1}^{N}a_{n}t_{n}\phi(x_{n})^{T}\phi(x)+b$$

分类超平面包含高维映射的内积

核函数原理

● 非线性支持向量机

> 分类超平面为:

$$y(x) = w^{T}\phi(x) + b = \sum_{n=1}^{N} a_{n}t_{n}\phi(x_{n})^{T}\phi(x) + b$$

构造如下函数:

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

此时,分类超平面表示为:

$$y(x) = w^{T}\phi(x) + b = \sum_{n=1}^{N} a_{n}t_{n}k(x, x_{n}) + b$$

这里 $k(x,x_n)$ 就是核函数,至此,在处理高维的非线性问题时,利用核函数直接在原来的低维空间中进行计算不需要显式地写出映射后的结果,避免了先映射到高维空间中然后再根据内积的公式进行计算

核函数原理

●常见核函数

> 根据问题和数据的不同,选择不同的核函数。一些常用的核函数有:

线性核: $k(x_1, x_2) = x_1^T x_2$

多项式核: $k(x_1, x_2) = (\langle x_1, x_2 \rangle + R)^d$

高斯核: $k(x_1, x_2) = \exp\left\{-\frac{\|x_1 - x_2\|^2}{2\sigma^2}\right\}$

Sigmoid核: $k(x_1, x_2) = \tanh(\beta_0 x_1^T x_2 + \beta_1)$

如何判断一个函数是否可以作为核函数?



Mercer定理:

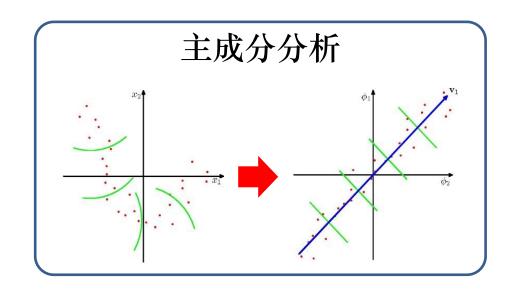
 $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ 上的映射k是一个有效核函数(也称Mercer核函数),当且仅当对于训练样本其相应的核函数矩阵是对称半正定的,即对于任何平方可积函数 g(x)有

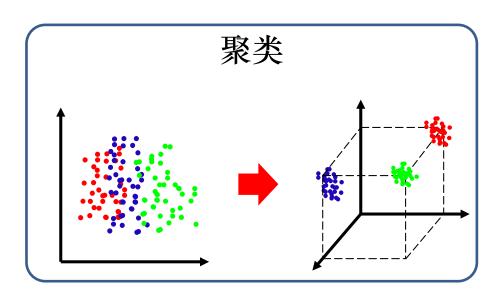
$$\iint k(x,y)g(x)g(y)dxdy \geq 0$$

核技巧

• 核技巧的应用

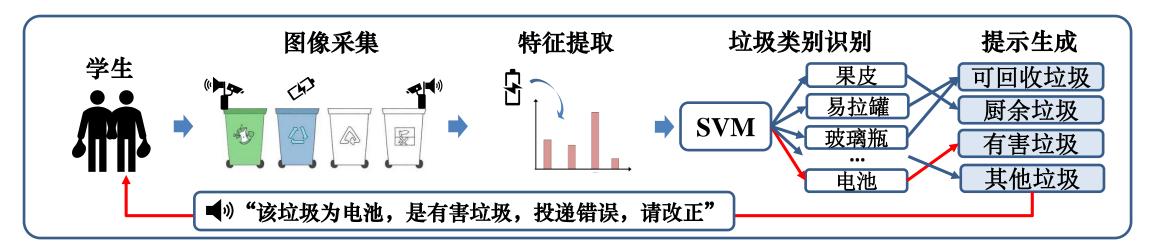
在SVM解决非线问题中,在不显式定义高维映射φ(x)的情况下,这种通过设计核函数来隐式地在特征空间进行计算的技巧称为核技巧。这种核技巧不仅应用于非线性支持向量机中,之后课程中的主成分分析和聚类方法也使用核技巧来解决非线性问题中的维度灾难。





支持向量机应用

- 使用SVM实现自动垃圾分类
 - ➤ 应用背景: 我国自2019年起在多个城市强制实施垃圾分类,垃圾分类已成为城市管理的重要组成部分。但在实际生活中,许多居民和游客仍然难以正确分类垃圾,不仅影响资源的回收利用,还增加了垃圾处理难度。某高校学生通过在垃圾桶上安装摄像头,实现在同学们投放垃圾时给予提醒。由于只获取了少量的垃圾样本,所以采用在样本受限条件下依旧性能较好的SVM来构建一个垃圾类别提示系统
 - > 垃圾类别提示系统



支持向量机应用

• 使用SVM实现自动垃圾分类

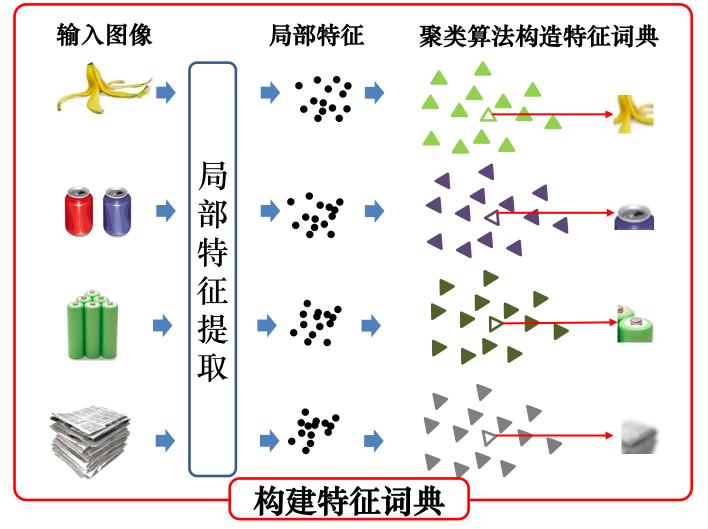
> 特征提取算法选择:

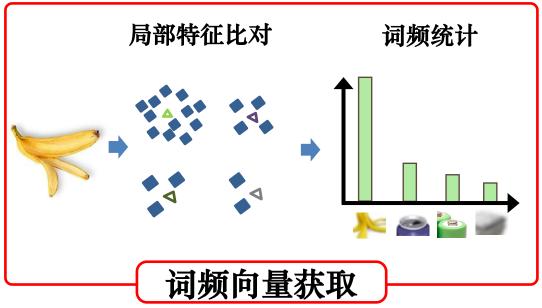
Bag of Words (BOW) 是一种经典的特征提取方法,通过统计数据中各类特征(例如图像中的局部特征)的出现频率,将图像转换为特征向量。由于垃圾图像表现出类间差异大、类内差异小的特点,使用BOW可有效捕捉同类垃圾的特征,并将其转化为可用于分类的词频向量。此外,BOW方法受垃圾图像中的位置、大小和旋转等因素影响较小,提取的垃圾图像特征更加鲁棒。

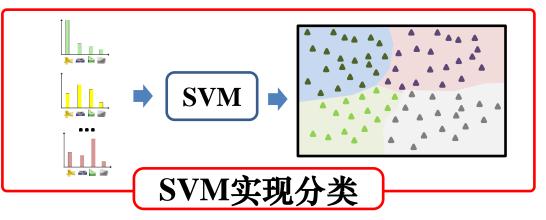
Scale-Invariant Feature Transform (SIFT): SIFT通过在高斯差分空间检测关键点,并利用梯度方向 直方图对关键点进行方向归一化,所提取的局部特征具有尺度和旋转不变性,适合提取多角度、多尺度的垃圾图像。同时SIFT对噪声具有较强的抗干扰能力,适合复杂环境条件下的垃圾图像特征提取。

支持向量机应用

● 使用SVM实现自动垃圾分类







5.5 序列最小优化算法

- 什么是序列最小优化算法?
- 序列最小优化算法

什么是序列最小优化算法?

支持向量机的学习问题可以形式化为求解具有全局最优解的凸二次规划问题。许多方法可以用于求解这一问题,但当训练样本容量很大时,这些算法往往效率较低,以致无法使用。

【1999年J. C. Platt提出】

- 序列最小优化算法(Sequential Minimal Optimization, SMO)
 - 户启发式算法
 - ➤ 先前可用的SVM使用复杂的训练方法。SMO算法较好地避免了这一问题,用于解决支持向量机训练目标函数优化问题(凸二次规划问题)的算法

什么是序列最小优化算法?

- 序列最小优化算法(Sequential Minimal Optimization, SMO)
 - ▶基本假设:如果所有变量的解都满足优化问题的KKT条件,那么优化问题的解 就得到了,因为KKT条件是该最优化问题有解的充要条件。
 - ▶基本思想:不断地将原二次规划问题分解为只有两个变量的二次规划问题,并对子问题进行解析求解,直到所有变量都满足KKT条件为止。因为子问题解析解存在,所以每次计算子问题都很快,虽然子问题次数很多,但是总体上还是高效的。

● SMO算法解凸二次规划问题

▶优化目标:

$$\min_{a} \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_{n} a_{m} t_{n} t_{m} k(x_{m}, x_{n}) - \sum_{n=1}^{N} a_{n}$$
s. t. $0 \le a_{n} \le C, n = 1, 2, \dots, N,$ $\sum_{n=1}^{N} a_{n} t_{n} = 0$

 \triangleright SMO是解决支持向量机优化问题的<mark>迭代算法</mark>。由于目标函数为凸函数,一般的优化算法都通过梯度方法一次优化一个变量求解二次规划问题的最大值,但由于限制条件 $\sum_{n=1}^{N}a_nt_n=0$,当某个 a_i 从 a_i^{old} 更新至 a_i^{new} 时等式约束不成立,上述限制条件被打破。为了满足约束条件,SMO采用一次更新两个变量的方法。

● SMO算法解凸二次规划问题

产在每个迭代步骤中,算法首先选取两个待更新的向量 a_1 和 a_2 ,分别计算它们的误差项,并求解出 a_1^{new} , a_2^{new} 。最后再根据SVM的定义计算偏移量b。对于误差项而言,可以根据 a_1^{new} , a_2^{new} , b的增量进行调整,无需每次重新计算。

SMO算法流程:

步骤1:随机数初始化向量权重 a_i ,计算偏移量b

步骤2:初始化误差项 E_i

步骤3: 选取两个向量 a_1 和 a_2 作为待更新向量

步骤4: 求解 a_1^{new}, a_2^{new}

步骤5: 利用求解的 a_1^{new} , a_2^{new} 更新 E_i 和b

步骤6: 重复步骤3-5, 直至达到终止条件

选择变量的启发式方法

两个变量二次规划的解析方法

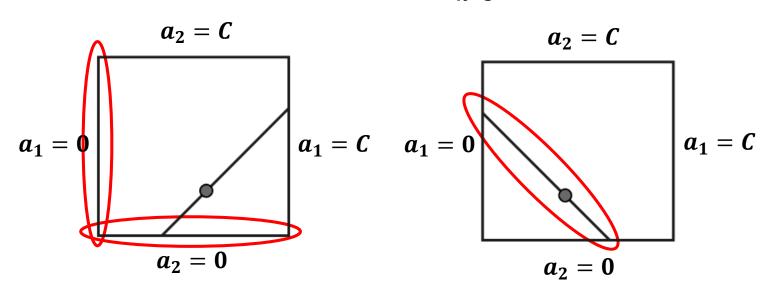
- 步骤4. 两个变量二次规划的解析方法
 - ightharpoonup不失一般性,对两个变量 a_1 和 a_2 进行更新,固定其他变量 $a_i(i=3,4,\cdots,N)$,原最优化问题可以表示为:

$$\begin{aligned} & \min_{a_1,a_2} W(a_1,a_2) = \frac{1}{2} K_{11} a_1^2 + \frac{1}{2} K_{22} a_2^2 + t_1 t_2 K_{12} a_1 a_2 - (a_1 + a_2) \\ & + t_1 a_1 \sum_{n=3}^{N} t_n a_n K_{n1} + t_2 a_2 \sum_{n=3}^{N} t_n a_n K_{n2} + const \end{aligned}$$
 s. t.
$$a_1 t_1 + a_2 t_2 = -\sum_{n=3}^{N} a_n t_n = \zeta, \quad 0 \le a_i \le C, i = 1, 2$$

其中核函数 $K_{mn}=K(x_m,x_n),m,n=1,2,\cdots,N,\zeta$ 是常数,上式中省略了不含 a_1 和 a_2 的常数项。

- 两个变量二次规划的解析方法
 - \rightarrow 两个变量 (a_1,a_2) 的约束条件可用二维空间的图形表示

$$a_1t_1 + a_2t_2 = -\sum_{n=3}^{N} a_nt_n = \zeta, \quad 0 \le a_i \le C, i = 1, 2$$



目标函数在一条平行于对 角线的线段上取得最优解, 两个变量的最优化问题转 化为单变量最优化问题。

$$t_1 \neq t_2 \Longrightarrow a_1 - a_2 = k$$

$$t_1 = t_2 \Longrightarrow a_1 + a_2 = k$$

- 两个变量二次规划的解析方法
 - 》考虑变量为 a_2 的最优化问题,假设问题的初始可行解为 a_1^{old} , a_2^{old} ,最优解为 a_1^{new} , a_2^{new} ,并且在沿着约束方向未经<u>剪</u>辑(未考虑不等式约束 $0 \le a_n \le C$, n = 1, 2)时 a_2 的最优解为 $a_2^{new,unc}$ 。
 - \triangleright 由于 a_2^{new} 需要满足不等式约束,所以其取值范围须满足 $L \le a_n^{new} \le H$,其中,L与H是 a_2^{new} 所在的对角线段端点的界。

如果
$$t_1 \neq t_2$$
,则 $L = \max(\mathbf{0}, a_2^{old} - a_1^{old})$, $H = \min(C, C + a_2^{old} - a_1^{old})$ 如果 $t_1 = t_2$,则 $L = \max(\mathbf{0}, a_2^{old} + a_1^{old} - C)$, $H = \min(C, a_2^{old} + a_1^{old})$

● 两个变量二次规划的解析方法

- ightharpoonup记 $g(x) = \sum_{n=1}^{N} a_n y_n K(x_n, x) + b$,描述输入变量 x_n 的预测值; 令 $E_n = g(x_n) y_n = (\sum_{m=1}^{N} a_m y_m K(x_m, x_n) + b) y_n$, n = 1, 2 即n = 1, 2时, E_n 为函数g(x)对输入 x_n 的预测值与真实输出 y_n 之差。
- > 那么未经剪辑的 a_2 的解 $a_2^{new,unc} = a_2^{old} + \frac{y_2(E_1-E_2)}{\eta}$, 其中 $\eta = K_{11} + K_{22} - 2K_{12} = \| \phi(x_1) - \phi(x_2) \|^2$ 。
- ightarrow 经剪辑后 a_2 的解是 $a_2^{new} = egin{cases} H, & a_2^{new,unc} > H \ a_2^{new,unc}, & L \leq a_2^{new,unc} \leq H \ L, & a_2^{new,unc} < L \end{cases}$
- \Rightarrow 由 a_2^{new} 求得 $a_1^{new} = a_1^{old} + y_1 y_2 (a_2^{old} a_2^{new})$

- 步骤3. 变量的选择方法
 - >(1)第一个变量 a_1 的选择: 外层循环

外层循环在训练样本中选取违反KKT条件最严重的样本点,并将其对应的变量作为第一个变量。检验是否满足KKT条件:

$$a_i = 0 \Leftrightarrow y_i g(x_i) \ge 1$$
 $0 < a_i < C \Leftrightarrow y_i g(x_i) = 1$
 $a_i = C \Leftrightarrow y_i g(x_i) \le 1$

外循环首先遍历满足条件 $0 < a_i < C$ 的样本点,就是在边界上的支持向量点,如果都满足KKT条件,再遍历整个训练集,从整个数据集中选取违反KKT条件最严重的点。

●变量的选择方法

 \triangleright (2)第二个变量 a_2 的选择:内层循环 假设在外层循环已经找到第一个变量 a_1 ,那么内层循环要找到第二个变量 a_2 ,希望使 a_2 有足够大的变化。

$$a_2^{new} = egin{cases} H, & a_2^{new,unc} > H \ a_2^{new,unc}, & L \leq a_2^{new,unc} \leq H \ L, & a_2^{new,unc} < L \end{cases} \qquad a_2^{new,unc} = a_2^{old} + rac{y_2(E_1 - E_2)}{\eta}$$

 a_2^{new} 是依赖于的 $|E_1-E_2|$ 的,简单做法是选择 a_2 使 $|E_1-E_2|$ 最大: a_1 已定, E_1 确定,如果 E_1 为正,选择最小的 E_i 作为 E_2 ;如果 E_1 为负,选择最大的 E_i 作为 E_2 。

●变量的选择方法

 \triangleright (2)第二个变量 a_2 的选择:内层循环

如果通过 $|E_1 - E_2|$ 最大化的方法无法使目标函数有足够的变化,那就遍历间隔边界上的支持向量点,依次将其对应的乘子作为 a_2 ,直到目标函数有足够的下降。

如果间隔边界上的支持向量仍未使得目标函数有足够的下降,那么遍历整个数据集,如果数据集还未使得目标函数有足够的下降,则更换 a_1 ,重新找到新的 a_1 进行优化。

- \bullet 步骤5. 更新b和差值 E_i
 - 》在每次完成两个变量的优化后,都要重新计算偏移量b。当 $0 < a_1^{new}, a_2^{new} < C$ 时,由KKT条件 $0 < a_i < C \Leftrightarrow y_i g(x_i) = 1$ 可计算:

$$b_1^{new} = -E_1 - y_1 K_{11} (a_1^{new} - a_1^{old}) - y_2 K_{21} (a_2^{new} - a_2^{old}) + b^{old}$$

$$b_2^{new} = -E_2 - y_1 K_{12} (a_1^{new} - a_1^{old}) - y_2 K_{22} (a_2^{new} - a_2^{old}) + b^{old}$$

ightharpoonup如果 a_1^{new} , a_2^{new} 同时满足条件 $0 < a_i^{new} < C$, i = 1, 2, 那么 $b_1^{new} = b_2^{new}$ 。如果 a_1^{new} , a_2^{new} 是0或者C,那么 b_1^{new} , b_2^{new} 以及他们之间的数都是符合KKT条件的阈值,这时取它们的中点作为 b^{new} ,之后更新 E_i 。

$$E_i = \sum_{S} y_j a_j K(x_i, x_j) + b^{new} - y_i$$

●SMO算法

输入: 训练数据集 $T = \{(x_1, y_1), (x_2, y_2), \cdots (x_N, y_N)\}$, 其中 $x_i \in X = R^n$, $y_i \in Y = \{-1, +1\}$, $i = 1, 2, \cdots, N$, 精度 ϵ ;

输出: 近似解â。

- (1) 取初值 $a^{(0)} = 0$, 令 k = 0;
- (2) 选取优化变量 a_1^k, a_2^k ,解析求解两个变量的最优化问题,求得最优解 a_1^{k+1}, a_2^{k+1} ,更新a为 a^{k+1} 。
- (3) 若在精度 ϵ 范围内满足停止条件 $\sum_{i=1}^{N}a_{i}y_{i}=0$, $0 \leq a_{i} \leq C$, $i=1,2,\cdots,N$,其中 $g(x_{i})=\sum_{j=1}^{N}a_{j}y_{j}K(x_{j},x_{i})$

$$+b , y_i g(x_i) = \begin{cases} \geq 1, & \{x_i | a_i = 0\} \\ = 1, & \{x_i | 0 < a_i < C\}, \text{ 则转至 (4) , 否则令}k = k+1, 转至 (2) ; \\ \leq 1, & \{x_i | a_i = C\} \end{cases}$$

(4)
$$\Re \hat{a} = a^{(k+1)}$$
.

● 对偶问题和KKT条件

> 为了不失一般性,设存在不等式约束的函数极值问题,优化目标为:

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

求取拉格朗日函数:

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

定义 $\theta_P(w) = \max_{\alpha,\beta; \alpha_i \geq 0} L(w,\alpha,\beta)$, 当违背约束条件时, $g_i(w) > 0$, $h_i(w) \neq 0$, $L(w,\alpha,\beta)$ 的最大值为无穷大

● 对偶问题和KKT条件

当满足约束条件时,有 $g_i(w) \le 0$, $h_i(w) = 0$,此时 $L(w, \alpha, \beta)$ 有最大值,即f(w),则有:

$$\theta_P(w) = \begin{cases} f(w), \text{如果w 满足约束条件} \\ +\infty, \text{否则} \end{cases}$$

则原问题 minf(w) 为一个求极小极大值问题:

$$\min_{w} \theta_{P}(w) = \min_{w} \max_{\alpha,\beta; \alpha_{i} \geq 0} L(w, \alpha, \beta)$$

这里 $\min_{w} \theta_{P}(w)$ 记为 p^*

 \triangleright 直接求解困难,进而转向另一个问题: $\theta_D(\alpha, \beta) = \min_{w} L(w, \alpha, \beta)$

● 对偶问题和KKT条件

这里,先固定 α , β ,求拉格朗日函数关于w的最小值,再求 $\theta_D(\alpha,\beta)$ 最大值,则有:

$$\max_{\alpha,\beta; \alpha_i \geq 0} \theta_D(\alpha,\beta) = \max_{\alpha,\beta; \alpha_i \geq 0} \min_{w} L(w,\alpha,\beta)$$

此问题就是原问题的对偶问题,记为 d^*

 \rightarrow 对比 p^* 和 d^* ,存在如下的关系:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*)$$

这里 α^* , β^* 是 $\theta_D(\alpha, \beta)$ 取最大时的 α, β 的取值,同时, θ_D 是关于w的求最小的拉格朗日函数,则有:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*)$$

● 对偶问题和KKT条件

显然, $\min L(w, \alpha^*, \beta^*)$ 一定小于等于w取任意值的 $L(w, \alpha^*, \beta^*)$, 则有:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

这里, w取 w^* , 即 $L(w,\alpha^*,\beta^*)$ 取最小值时的w值,则有:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

$$= f(w^*) + \sum_{i=1}^k \alpha_i^* g_i(w^*) + \sum_{i=1}^l \beta_i^* h_i(w^*)$$

由于 $g_i(w) \leq 0, h_i(w) = 0$,则有:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta_l^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

$$= f(w^*) + \sum_{i=1}^k \alpha_i^* g_i(w^*) + \sum_{i=1}^k \beta_i^* h_i(w^*) \le f(w^*)$$

● 对偶问题和KKT条件

之前已知:

$$p^* = \min_{w} \theta_P(w) = f(w^*)$$

则有:

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

$$= f(w^*) + \sum_{i=1}^k \alpha_i^* g_i(w^*) + \sum_{i=1}^l \beta_i^* h_i(w^*) \le f(w^*) = p^*$$

此时可知, $d^* \le p^*$,原问题与对偶问题是不等价,只有当上式中的两个 \le 均取等号时,原问题与对偶问题才等价。

● 对偶问题和KKT条件

$$d^* = \max \theta_D(\alpha, \beta) = \theta_D(\alpha^*, \beta^*) = \min L(w, \alpha^*, \beta^*) \le L(w^*, \alpha^*, \beta^*)$$

$$= f(w^*) + \sum_{i=1}^k \alpha_i^* g_i(w^*) + \sum_{i=1}^l \beta_i^* h_i(w^*) \le f(w^*) = p^*$$

当 $w = w^*$ 时,即 $\frac{\partial}{\partial w_i} L(w^*, \alpha^*, \beta^*) = 0$ 时,第一个 \leq 取等号,

由于 $h_j(w) = 0$, 当 $\alpha_i^* g_i(w^*) = 0$ 时,第二个 \leq 取等号。

即满足 $\frac{\partial}{\partial w_i}L(w^*,\alpha^*,\beta^*)=0$ 和 $\alpha_i^*g_i(w^*)=0$ 时, $d^*=p^*$

ightharpoonup所以,当同时满足 $\frac{\partial}{\partial w_i}L(w^*,\alpha^*,\beta^*)=0$ 和 $\alpha_i^*g_i(w^*)=0$ 时,原问题与对偶问题等价。

线性支持向量机模型推导

● KKT (Karush-Kuhn-Tucker) 条件

$$rac{\partial}{\partial w_i}L(w^*, lpha^*, eta^*) = 0, i = 1, ..., n$$
 $lpha_i^*g_i(w^*) = 0, i = 1, ..., k$ $g_i(w^*) \leq 0, i = 1, ..., k$

KKT互补松弛条件

如果 w^* , α^* , β^* 满足上述的KKT条件, 那么它们就是原问题和对偶问题的解。

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

>KKT互补松弛条件分析:

补充条件隐含如果 $\alpha^* > 0$,那么 $g_i(w^*) = 0$,即w处于可行域的边界上,是起作用的 (Active)约束,而位于可行域内部的点都是不起作用的约束,其 $\alpha^* = 0$ 。