Методы машинного обучения. Метод опорных векторов

Bоронцов Константин Вячеславович www.MachineLearning.ru/wiki?title=User:Vokov вопросы к лектору: k.vorontsov@iai.msu.ru

материалы курса: github.com/MSU-ML-COURSE/ML-COURSE-25-26 орг.вопросы по курсу: ml.cmc@mail.ru

ВМК МГУ • 14 октября 2025

Содержание

- 1 Метод опорных векторов SVM
 - Принцип оптимальной разделяющей гиперплоскости
 - Двойственная задача
 - Понятие опорного вектора
- Обобщения линейного SVM
 - Ядра и спрямляющие пространства
 - SVM как двухслойная нейронная сеть
 - SVM-регрессия
- - Подбор коэффициента регуляризации
 - Регуляризаторы для отбора признаков
 - Метод релевантных векторов RVM

Дано:

Обучающая выборка $X^{\ell} = (x_i, y_i)_{i=1}^{\ell}, x_i \in \mathbb{R}^n, y_i \in \{-1, +1\}$

Найти:

Параметры $w \in \mathbb{R}^n$, $w_0 \in \mathbb{R}$ линейной модели классификации $a(x; w, w_0) = \operatorname{sign}(\langle x, w \rangle - w_0).$

Критерий — минимум эмпирического риска:

$$\sum_{i=1}^{\ell} [a(x_i; w, w_0) \neq y_i] = \sum_{i=1}^{\ell} [M_i(w, w_0) < 0] \rightarrow \min_{w, w_0}.$$

где $M_i(w, w_0) = (\langle x_i, w \rangle - w_0) y_i - o\tau c\tau y\pi \text{ (margin) объекта } x_i,$

В. Н. Вапник, А. Я. Лернер. Узнавание образов при помощи обобщенных портретов 1963

C. Cortes, V. Vapnik. Support vector networks. 1995.

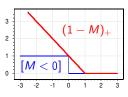
Аппроксимация и регуляризация эмпирического риска

Эмпирический риск — это кусочно-постоянная функция. Заменим его оценкой сверху, непрерывной по параметрам:

$$Q(w, w_0) = \sum_{i=1}^{\ell} \left[M_i(w, w_0) < 0 \right] \leqslant$$

$$\leqslant \sum_{i=1}^{\ell} \left(1 - M_i(w, w_0) \right)_+ + \frac{1}{2C} ||w||^2 \rightarrow \min_{w, w_0}.$$

- Аппроксимация штрафует объекты за приближение к границе классов, увеличивая зазор между классами
- Регуляризация штрафует неустойчивые решения в случае мультиколлинеарности



C. Cortes, V. Vapnik. Support vector networks. 1995.

В. Н. Вапник, А. Я. Лернер. Узнавание образов при помощи обобщенных портретов. 1963.

Оптимальная разделяющая гиперплоскость

Линейный классификатор: $a(x,w) = \operatorname{sign} \left(\langle w,x \rangle - w_0 \right)$

Пусть выборка $X^\ell = (x_i, y_i)_{i=1}^\ell$ линейно разделима:

$$\exists w, w_0: M_i(w, w_0) = y_i(\langle w, x_i \rangle - w_0) > 0, \quad i = 1, \ldots, \ell$$

Нормировка: $\min_{i=1,\ldots,\ell} M_i(w,w_0) = 1$

Разделяющая полоса (разделяющая гиперплоскость посередине):

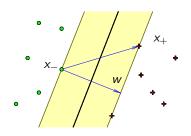
$$\{x: -1 \leqslant \langle w, x \rangle - w_0 \leqslant 1\}$$

$$\exists x_+: \langle w, x_+ \rangle - w_0 = +1$$

$$\exists x_{-}: \quad \langle w, x_{-} \rangle - w_{0} = -1$$

Ширина полосы:

$$\frac{\langle x_{+} - x_{-}, w \rangle}{\|w\|} = \frac{2}{\|w\|} \to \max$$



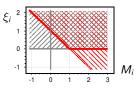
Обоснование кусочно-линейной функции потерь

Линейно разделимая выборка

$$\begin{cases} \frac{1}{2} \|w\|^2 \to \min_{w,w_0}; \\ M_i(w,w_0) \geqslant 1, \quad i = 1,\ldots,\ell. \end{cases}$$

Переход к линейно неразделимой выборке (эвристика)

$$\begin{cases} \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{\ell} \xi_i \to \min_{w, w_0, \xi}; \\ \xi_i \geqslant 1 - M_i(w, w_0), \quad i = 1, \dots, \ell; \\ \xi_i \geqslant 0, \quad i = 1, \dots, \ell. \end{cases}$$



Эквивалентная задача безусловной минимизации:

$$C\sum_{i=1}^{\ell} (1 - M_i(w, w_0))_+ + \frac{1}{2} ||w||^2 \rightarrow \min_{w, w_0}.$$

Напоминание. Условия Каруша-Куна-Таккера (ККТ)

Задача математического программирования:

$$\begin{cases} f(x) \to \min_{x}; \\ g_{i}(x) \leqslant 0, \quad i = 1, \dots, m; \\ h_{j}(x) = 0, \quad j = 1, \dots, k. \end{cases}$$

Необходимые условия. Если x — точка локального минимума, то существуют множители $\mu_i,\ i=1,\ldots,m,\ \lambda_j,\ j=1,\ldots,k$:

$$\begin{cases} \frac{\partial \mathscr{L}}{\partial x} = 0, & \mathscr{L}(x; \mu, \lambda) = f(x) + \sum_{i=1}^m \mu_i g_i(x) + \sum_{j=1}^k \lambda_j h_j(x); \\ g_i(x) \leqslant 0; & h_j(x) = 0; \text{ (исходные ограничения)} \\ \mu_i \geqslant 0; & \text{ (двойственные ограничения)} \\ \mu_i g_i(x) = 0; & \text{ (условие дополняющей нежёсткости)} \end{cases}$$

го вектора

Применение условий ККТ к задаче SVM

Функция Лагранжа: $\mathscr{L}(w,w_0,\xi;\lambda,\eta)=$

$$= \frac{1}{2} ||w||^2 - \sum_{i=1}^{\ell} \lambda_i (M_i(w, w_0) - 1) - \sum_{i=1}^{\ell} \xi_i (\lambda_i + \eta_i - C),$$

 λ_i — переменные, двойственные к ограничениям $M_i\geqslant 1-\xi_i$; η_i — переменные, двойственные к ограничениям $\xi_i\geqslant 0$.

$$\begin{cases} \frac{\partial \mathcal{L}}{\partial w} = 0, & \frac{\partial \mathcal{L}}{\partial w_0} = 0, & \frac{\partial \mathcal{L}}{\partial \xi} = 0; \\ \xi_i \geqslant 0, & \lambda_i \geqslant 0, & \eta_i \geqslant 0, & i = 1, \dots, \ell; \\ \lambda_i = 0 \text{ либо } M_i(w, w_0) = 1 - \xi_i, & i = 1, \dots, \ell; \\ \eta_i = 0 \text{ либо } \xi_i = 0, & i = 1, \dots, \ell; \end{cases}$$

Необходимые условия седловой точки функции Лагранжа

Функция Лагранжа: $\mathscr{L}(w,w_0,\xi;\lambda,\eta)=$

$$= \frac{1}{2} \|w\|^2 - \sum_{i=1}^{\ell} \lambda_i (M_i(w, w_0) - 1) - \sum_{i=1}^{\ell} \xi_i (\lambda_i + \eta_i - C),$$

Необходимые условия седловой точки функции Лагранжа:

$$\frac{\partial \mathcal{L}}{\partial w} = w - \sum_{i=1}^{\ell} \lambda_i y_i x_i = 0 \quad \Longrightarrow \quad w = \sum_{i=1}^{\ell} \lambda_i y_i x_i;$$

$$\frac{\partial \mathcal{L}}{\partial w_0} = -\sum_{i=1}^{\ell} \lambda_i y_i = 0 \quad \Longrightarrow \quad \sum_{i=1}^{\ell} \lambda_i y_i = 0;$$

$$\frac{\partial \mathcal{L}}{\partial \varepsilon_i} = -\lambda_i - \eta_i + C = 0 \quad \Longrightarrow \quad \eta_i + \lambda_i = C, \quad i = 1, \dots, \ell.$$

Понятие опорного вектора и типизация объектов

Система условий ККТ:

$$\begin{cases} w = \sum_{i=1}^{\ell} \lambda_i y_i x_i; & \sum_{i=1}^{\ell} \lambda_i y_i = 0; \quad M_i(w, w_0) \geqslant 1 - \xi_i; \\ \xi_i \geqslant 0, \quad \lambda_i \geqslant 0, \quad \eta_i \geqslant 0, \quad \eta_i + \lambda_i = C; \\ \lambda_i = 0 \quad \text{либо} \quad M_i(w, w_0) = 1 - \xi_i; \\ \eta_i = 0 \quad \text{либо} \quad \xi_i = 0; \end{cases}$$

Определение. Объект x_i называется *опорным*, если $\lambda_i \neq 0$.

Типизация объектов x_i , $i = 1, \ldots, \ell$:

- 1. $\lambda_i = 0$; $\eta_i = C$; $\xi_i = 0$; $M_i \geqslant 1$ периферийный.
- $0 < \lambda_i < C; \; 0 < \eta_i < C; \; \xi_i = 0; \; M_i = 1$ опорный-граничный
- 3. $\lambda_i = C$; $\eta_i = 0$; $\xi_i > 0$; $M_i < 1$ опорный-нарушитель

Двойственная задача

$$\begin{cases} -\mathcal{L}(\lambda) = -\sum_{i=1}^{\ell} \lambda_i + \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j y_i y_j \langle \mathbf{x}_i, \mathbf{x}_j \rangle & \to & \min_{\lambda}; \\ \sum_{i=1}^{\ell} \lambda_i y_i = 0; & 0 \leqslant \lambda_i \leqslant C, \quad i = 1, \dots, \ell \end{cases}$$

Решение прямой задачи выражается через решение двойственной:

$$egin{cases} w = \sum\limits_{i=1}^\ell \lambda_i y_i x_i; \ w_0 = \langle w, x_i
angle - y_i, \quad$$
 для любого i : $\lambda_i > 0, \; M_i = 1.$

Линейный классификатор с признаками $f_i(x) = \langle x, x_i \rangle$:

$$a(x) = \operatorname{sign} \Big(\sum_{i=1}^{\ell} \lambda_i y_i \langle x, x_i \rangle - w_0 \Big).$$

S.Fine, K.Scheinberg. INCAS: An incremental active set method for SVM. 2002. J.Platt. Fast training support vector machines using sequential minimal optimization. 1999.

Двойственная задача. Нелинейное обобщение с ядром K

$$\begin{cases} -\mathscr{L}(\lambda) = -\sum_{i=1}^{\ell} \lambda_i + \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j y_i y_j \mathcal{K}(\mathbf{x}_i, \mathbf{x}_j) \rightarrow \min_{\lambda} \\ \sum_{i=1}^{\ell} \lambda_i y_i = 0; \qquad 0 \leqslant \lambda_i \leqslant C, \quad i = 1, \dots, \ell \end{cases}$$

Решение прямой задачи выражается через решение двойственной:

$$egin{cases} w = \sum\limits_{i=1}^\ell \lambda_i y_i x_i; \ w_0 = \langle w, x_i
angle - y_i, \quad$$
 для любого i : $\lambda_i > 0, \; M_i = 1.$

Линейный классификатор с признаками $f_i(x) = K(x, x_i)$:

$$a(x) = \operatorname{sign}\left(\sum_{i=1}^{\ell} \lambda_i y_i K(x, x_i) - w_0\right).$$

S.Fine, K.Scheinberg. INCAS: An incremental active set method for SVM. 2002. J. Platt. Fast training support vector machines using sequential minimal optimization. 1999.

Нелинейное обобщение SVM

Идея: заменить $\langle x, x' \rangle$ нелинейной функцией K(x, x').

Переход к спрямляющему пространству, как правило, более высокой размерности: $\psi \colon X o H$.

Определение

Функция $K: X \times X \to \mathbb{R}$ — ядро, если $K(x, x') = \langle \psi(x), \psi(x') \rangle$ при некотором $\psi \colon X \to H$, где H — гильбертово пространство.

Теорема

Функция K(x, x') является ядром тогда и только тогда, когда она симметрична: K(x, x') = K(x', x); и неотрицательно определена:

$$\int_X \int_X K(x,x')g(x)g(x')dxdx'\geqslant 0$$
 для любой $g\colon X o \mathbb{R}$.

Конструктивные методы синтеза ядер

- ② константа K(x, x') = 1 -ядро;
- ullet произведение ядер $K(x,x') = K_1(x,x')K_2(x,x')$ ядро;
- lacktriangledown $\forall \psi: X
 ightarrow \mathbb{R}$ произведение $K(x,x') = \psi(x)\psi(x')$ ядро;
- ullet $\forall arphi: X {
 ightarrow} X$ если K_0 ядро, то $K(x,x') = K_0(arphi(x),arphi(x'))$ ядро;
- $m{\circ}$ если $s\colon X imes X o \mathbb{R}$ симметричная интегрируемая функция, то $K(x,x')=\int_X s(x,z)s(x',z)\,dz$ ядро;
- lacktriangledown если K_0 ядро и функция $f: \mathbb{R} \to \mathbb{R}$ представима в виде сходящегося степенного ряда с неотрицательными коэффициентами, то $K(x,x')=f\left(K_0(x,x')\right)$ ядро;

Пример: спрямляющее пространство для квадратичного ядра

Пусть
$$X=\mathbb{R}^2$$
, $K(u,v)=\langle u,v\rangle^2$, где $u=(u_1,u_2)$, $v=(v_1,v_2)$.

Задача: найти пространство H и преобразование $\psi\colon X\to H$, при которых $K(x,x')=\langle \psi(x),\psi(x')\rangle_H$.

Разложим квадрат скалярного произведения:

$$K(u,v) = \langle u,v \rangle^2 = \langle (u_1,u_2), (v_1,v_2) \rangle^2 =$$

$$= (u_1v_1 + u_2v_2)^2 = u_1^2v_1^2 + u_2^2v_2^2 + 2u_1v_1u_2v_2 =$$

$$= \langle (u_1^2, u_2^2, \sqrt{2}u_1u_2), (v_1^2, v_2^2, \sqrt{2}v_1v_2) \rangle.$$

Таким образом,

$$H = \mathbb{R}^3, \quad \psi \colon (u_1, u_2) \mapsto (u_1^2, u_2^2, \sqrt{2}u_1u_2),$$

Линейной поверхности в пространстве H соответствует квадратичная поверхность в исходном пространстве X.

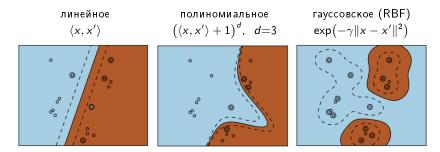
Примеры ядер

- ullet квадратичное ядро, $\dim H = rac{1}{2}n(n+1)$ $K(x,x') = \langle x,x'
 angle^2$
- $oldsymbol{0}$ полиномиальное с мономами степени d, $\dim H = C_{n+d-1}^d$ $K(x,x') = \langle x,x'
 angle^d$
- ullet полиномиальное с мономами всех степеней от 0 до d $\mathcal{K}(x,x')=\left(\langle x,x'
 angle+1
 ight)^d$
- $oldsymbol{oldsymbol{eta}}$ нейросеть с сигмоидными функциями активации $\mathcal{K}(x,x')= ext{th}ig(k_1\langle x,x'
 angle-k_0ig),\;\;k_0,k_1\geqslant 0$
- ullet сеть радиальных базисных функций (RBF ядро) $\mathcal{K}(x,x') = \exp(-\gamma \|x-x'\|^2)$

Классификация с различными ядрами

Гиперплоскость в спрямляющем пространстве соответствует нелинейной разделяющей поверхности в исходном.

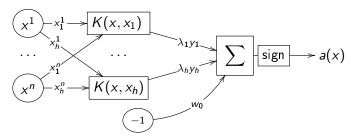
Примеры с различными ядрами K(x,x')



SVM: двухслойная нейросеть и метрический классификатор

Перенумеруем объекты так, чтобы x_1, \ldots, x_h были опорными.

$$a(x) = \operatorname{sign}\left(\sum_{i=1}^{h} \lambda_i y_i K(x, x_i) - w_0\right).$$



Первый слой вместо скалярных произведений вычисляет ядра Веса первого слоя — это сами опорные объекты Метрический классификатор, если K — функция близости

Преимущества и недостатки SVM

Преимущества SVM перед двухслойными нейронными сетями:

- задача выпуклого квадратичного программирования имеет единственное решение
- число нейронов скрытого слоя определяется автоматически — это число опорных векторов

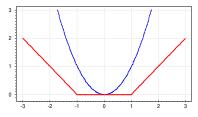
Недостатки классического SVM:

- шумовые объекты (выбросы) являются опорными
- ullet нет общих подходов к оптимизации K(x,x') под задачу
- на больших данных SVM обучается медленнее SG
- нет «встроенного» отбора признаков
- ullet приходится подбирать константу C

SVM-регрессия

Модель регрессии:
$$a(x,w)=\langle x,w\rangle-w_0,\ w\in\mathbb{R}^n,\ w_0\in\mathbb{R}$$

Функции потерь:
$$\mathscr{L}(\varepsilon) = \varepsilon^2$$
, $\mathscr{L}(\varepsilon) = (|\varepsilon| - \delta)_+$, $\varepsilon = a - y$



Постановка задачи:

$$\sum_{i=1}^{\ell} (|\langle w, x_i \rangle - w_0 - y_i| - \delta)_+ + \frac{1}{2C} ||w||^2 \to \min_{w, w_0}$$

Задача решается путём замены переменных и сведения к задаче квадратичного программирования

SVM-регрессия

Замена переменных:

$$\xi_i^+ = (\langle w, x_i \rangle - w_0 - y_i - \delta)_+$$

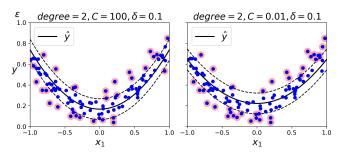
$$\xi_i^- = (-\langle w, x_i \rangle + w_0 + y_i - \delta)_+$$

Постановка задачи SVM-регрессии:
$$\begin{cases} \frac{1}{2}\|w\|^2 + C \sum_{i=1}^{\ell} (\xi_i^+ + \xi_i^-) \to \min_{w,w_0,\xi^+,\xi^-} \\ y_i - \delta - \xi_i^- \leqslant \langle w, x_i \rangle - w_0 \leqslant y_i + \delta + \xi_i^+, \quad i = 1,\dots,\ell \\ \xi_i^- \geqslant 0, \quad \xi_i^+ \geqslant 0, \quad i = 1,\dots,\ell \end{cases}$$

- выпуклая задача квадратичного программирования
- следовательно, решение единственное
- решение разреженное выражается через опорные векторы
- ullet возможна замена $\langle x, x_i \rangle$ ядром $K(x, x_i)$

SVM-регрессия. Пример 1

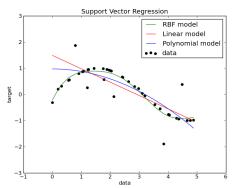
SVM-регрессия с полиномиальным ядром степени 2:



- Выделены опорные векторы
- ullet Результат слабо зависит от константы C

SVM-регрессия. Пример 2

Сравнение SVM-регрессии с гауссовским (RBF) ядром, линейной и полиномиальной регрессией:



• Удачный выбор ядра имеет значение!

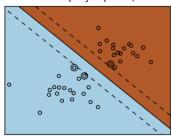
http://scikit-learn.org/0.5/auto_examples/svm/plot_svm_regression.html

Влияние константы C на решение SVM

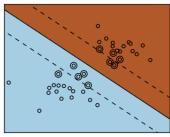
SVM — аппроксимация и регуляризация эмпирического риска:

$$\sum_{i=1}^{\ell} (1 - M_i(w, w_0))_+ + \frac{1}{2C} ||w||^2 \rightarrow \min_{w, w_0}.$$

большой *С* слабая регуляризация



малый *С* сильная регуляризация



1-norm SVM (LASSO SVM)

Аппроксимация эмпирического риска с L_1 -регуляризацией:

$$\sum_{i=1}^{\ell} (1 - M_i(w, w_0))_+ + \mu \sum_{j=1}^{n} |w_j| \rightarrow \min_{w, w_0}.$$

Почему L_1 -регуляризатор приводит $\check{\kappa}$ отбору признаков?

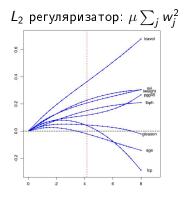
Замена переменных: $u_j=\frac{1}{2}\big(|w_j|+w_j\big),\ v_j=\frac{1}{2}\big(|w_j|-w_j\big).$ Тогда $w_j=u_j-v_j$ и $|w_j|=u_j+v_j$;

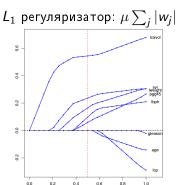
$$\begin{cases} \sum_{i=1}^{\ell} (1 - M_i(u - v, w_0))_+ + \mu \sum_{j=1}^{n} (u_j + v_j) \to \min_{u, v} \\ u_j \geqslant 0, \quad v_j \geqslant 0, \quad j = 1, \dots, n; \end{cases}$$

чем больше μ , тем больше индексов j таких, что $u_j = v_j = 0$, но тогда $w_i = 0$, значит, признак не учитывается.

Сравнение L_2 и L_1 регуляризации

Зависимость весов w_j от коэффициента $\frac{1}{\mu}$





Задача из UCI: prostate cancer (диагностика рака)

T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning. 2001.

Негладкие регуляризаторы для отбора и группировки признаков

Общий вид регуляризаторов (μ — параметр селективности):

$$\sum_{i=1}^{\ell} \left(1 - M_i(w, w_0)\right)_+ + \sum_{j=1}^{n} R_{\mu}(w_j) \ o \ \min_{w} .$$

Регуляризаторы с эффектами отбора и группировки признаков:

LASSO (
$$L_1$$
): $R_{\mu}(w) = \mu |w|$

Elastic Net:
$$R_{\mu}(w) = \mu |w| + \tau w^2$$

Support Feature Machine (SFM):

$$R_{\mu}(w) = egin{cases} 2\mu |w|, & |w| \leqslant \mu; \ \mu^2 + w^2, & |w| \geqslant \mu; \end{cases}$$

Relevance Feature Machine (RFM):

$$R_{\mu}(w) = \ln(\mu w^2 + 1)$$





Метод релевантных векторов RVM (Relevance Vector Machine)

Положим, как и в SVM, при некоторых $\lambda_i\geqslant 0$

$$w = \sum_{i=1}^{\ell} \lambda_i y_i x_i,$$

причём опорным векторам x_i соответствуют $\lambda_i \neq 0$.

Проблема: Какие из коэффициентов λ_i лучше обнулить?

Идея: пусть регуляризатор зависит не от w, а от λ_i .

Пусть λ_i независимые, гауссовские, с дисперсиями α_i :

$$p(\lambda) = \frac{1}{(2\pi)^{\ell/2} \sqrt{\alpha_1 \cdots \alpha_\ell}} \exp\left(-\sum_{i=1}^{\ell} \frac{\lambda_i^2}{2\alpha_i}\right);$$

$$\sum_{i=1}^{\ell} \left(1 - M_i(w(\lambda), w_0)\right)_+ + \frac{1}{2} \sum_{i=1}^{\ell} \left(\ln \alpha_i + \frac{\lambda_i^2}{\alpha_i}\right) \to \min_{\lambda, \alpha}.$$

Преимущества и недостатки RVM

Преимущества:

- Опорных векторов, как правило, меньше (более «разреженное» решение).
- 🕀 Шумовые выбросы уже не входят в число опорных.
- \oplus Не надо искать параметр регуляризации (вместо этого α_i оптимизируются в процессе обучения).
- ⊕ Аналогично SVM, можно использовать ядра.

Недостатки:

⊖ Не всегда есть преимущество по качеству классификации.

M. E. Tipping. The relevance vector machine. 2000.

C. M. Bishop, M. E. Tipping. Variational relevance vector machine. 2000

Резюме по линейным классификаторам

- SVM лучший метод линейной классификации
- SVM легко обобщается и на задачи регрессии
- С помощью *ядер* (kernel trick) SVM изящно обобщается для нелинейной классификации и нелинейной регрессии
- Регуляризация увеличивает зазор, устраняет мультиколлинеарность и уменьшает переобучение
- Аппроксимация пороговой функции потерь $\mathscr{L}(M)$ также увеличивает зазор и повышает надёжность классификации
- Негладкость функции потерь приводит к отбору объектов
- Негладкость регуляризатора приводит к отбору признаков

В. Н. Вапник, А. Я. Лернер. Узнавание образов при помощи обобщенных портретов. 1963.

C. Cortes, V. Vapnik. Support vector networks. 1995.