

# Семинары по линейным классификаторам

Евгений Соколов  
sokolov.evg@gmail.com

14 ноября 2014 г.

## 5 Ядра и их применение в машинном обучении

### §5.1 Восстановление нелинейных зависимостей линейными методами

Линейные методы классификации и регрессии являются хорошо изученными и обоснованными, однако предположение о линейной зависимости зачастую оказывается неверным в задачах машинного обучения. Оказывается, что линейные методы можно применять и для восстановления нелинейных зависимостей, если предварительно перейти к новым признакам.

Рассмотрим простой пример. На рис. 1 показана двумерная выборка с двумя классами, разделяющая поверхность для которой никак не может быть приближена гиперплоскостью. В то же время, если добавить третий признак  $x_3 = x_1^2 + x_2^2$ , то выборку можно будет идеально разделить гиперплоскостью вида  $x_3 = C$  (рис. 2). Такое пространство называется *спрямляющим*. В новом признаковом пространстве разделяющая поверхность является линейной, однако после ее проецирования на исходное пространства она окажется нелинейной.

Модель, в которой зависимость ищется как линейная комбинация нелинейных функций от выборки, называется *линейной моделью над базисными функциями* [1]. Например, для задачи регрессии она имеет вид

$$a(x; w) = \sum_{i=1}^m w_i \varphi_i(x),$$

где  $\varphi_i(x)$  — произвольные нелинейные функции от признаков (*базисные функции*). Проблема заключается в том, что на практике заранее нельзя сказать, какие именно базисные функции нужно взять, чтобы добиться линейной разделимости, поэтому приходится брать сразу большой набор таких функций (например, все мономы не больше определенной степени). В этом случае число признаков оказывается очень большим, из-за чего процесс обучения становится трудоемким как по времени, так и по памяти. Однако в некоторых случаях оказывается, что достаточно уметь быстро вычислять скалярные произведения объектов друг на друга.

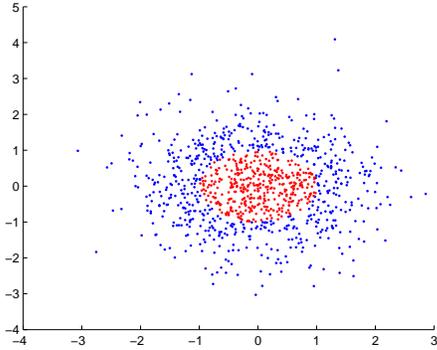


Рис. 1. Выборка с нелинейной разделяющей поверхностью. Разные классы обозначены разными цветами.

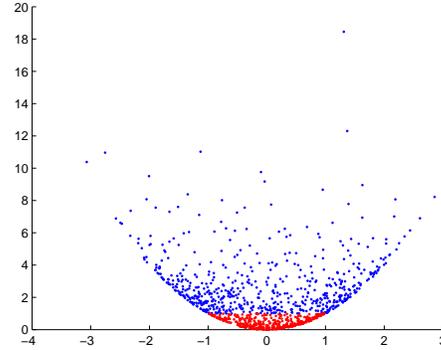


Рис. 2. Выборка после добавления третьего признака. Изображена проекция на первый и третий признаки.

## §5.2 Двойственное представление для линейной регрессии

Рассмотрим задачу построения линейной регрессии с квадратичной функцией потерь и квадратичным регуляризатором:

$$Q(w) = \frac{1}{2} \sum_{i=1}^{\ell} \left\{ \sum_{j=1}^m w_j \varphi_j(x_{ij}) - y_i \right\}^2 + \frac{\lambda}{2} \|w\|^2 = \frac{1}{2} \|\Phi w - y\|^2 + \frac{\lambda}{2} \|w\|^2 \rightarrow \min_w,$$

где  $\Phi$  — матрица, в которой  $i$ -я строка представлена вектором  $(\varphi_1(x_i), \dots, \varphi_m(x_i))$ . Дифференцируя функционал  $Q(w)$  и приравнявая его нулю, получаем

$$w = -\frac{1}{\lambda} \Phi^T (\Phi w - y).$$

Отсюда следует, что решение является линейной комбинацией строк матрицы  $\Phi$ :

$$w = \Phi^T a,$$

где за  $a$  мы обозначили вектор  $-\frac{1}{\lambda}(\Phi w - y)$ . Подставим это представление в функционал:

$$Q(a) = \frac{1}{2} \|\Phi \Phi^T a - y\|^2 + \frac{\lambda}{2} a^T \Phi \Phi^T a \rightarrow \min_a.$$

Заметим, что теперь функционал зависит не от самой матрицы признаков  $\Phi$ , а от ее произведения на саму себя  $\Phi \Phi^T$ . Это матрица скалярных произведений всех возможных пар объектов, называемая также *матрицей Грама*. Будем обозначать ее через

$$K = \Phi \Phi^T = (\langle \varphi(x_i), \varphi(x_j) \rangle)_{i,j=1}^{\ell} = (k(x_i, x_j))_{i,j=1}^{\ell},$$

где  $\varphi(x_i) = (\varphi_1(x_i), \dots, \varphi_m(x_i))$ , а  $k(x_i, x_j)$  — скалярное произведение объектов, называемое также *функцией ядра*.

Можно показать, что оптимальный вектор  $a$  имеет вид

$$a = (K + \lambda I)^{-1} y.$$

Функция регрессии при этом запишется как

$$y(x) = \langle w, \varphi(x) \rangle = w^T \varphi(x) = a^T \Phi \varphi(x) = k(x)^T (K + \lambda I)^{-1} y,$$

где  $k(x) = (k(x, x_1), \dots, k(x, x_\ell))$  — вектор скалярных произведений нового объекта  $x$  на объекты обучающей выборки.

Итак, нам удалось переписать функционал и модель так, что они зависят лишь от скалярных произведений объектов. В этом случае при росте размерности нового (спрямляющего) признакового пространства количество требуемой памяти остается константным и имеет порядок  $\ell^2$ . Далее мы покажем, что и вычисление скалярного произведения можно организовать так, что оно будет зависеть лишь от размерности исходного признакового пространства.

### §5.3 SVM и kernel trick

Переход к новому признаковому пространству можно применять и в задачах классификации:

$$a(x; w) = \text{sign}(\langle w, \varphi(x) \rangle + b).$$

Вспомним двойственную задачу метода опорных векторов:

$$\begin{cases} \sum_{i=1}^{\ell} \lambda_i - \frac{1}{2} \sum_{i,j=1}^{\ell} \lambda_i \lambda_j y_i y_j \langle x_i, x_j \rangle \rightarrow \max_{\lambda} \\ 0 \leq \lambda_i \leq C, \quad i = 1, \dots, \ell, \\ \sum_{i=1}^{\ell} \lambda_i y_i = 0. \end{cases}$$

После того, как она решена, новые объекты классифицируются с помощью алгоритма

$$a(x) = \text{sign} \left( \sum_{i=1}^{\ell} \lambda_i y_i \langle x_i, x \rangle + b \right).$$

Заметим, что как оптимизационная задача, так и итоговый классификатор зависят лишь от скалярных произведений объектов. Подставляя вместо скалярного произведения функцию ядра, мы будем настраивать классификатор в произвольном признаковом пространстве. Такая подмена получила в англоязычной литературе название *kernel trick*.

### §5.4 Операции в спрямляющем пространстве

*Ядром* мы будем называть функцию  $K(x, z)$ , представимую в виде скалярного произведения в некотором пространстве:  $K(x, z) = \langle \varphi(x), \varphi(z) \rangle$ , где  $\varphi : X \rightarrow H$  — отображение из исходного признакового пространства в некоторое *спрямляющее пространство*. Оказывается, ядро содержит в себе много информации о спрямляющем пространстве, и позволяет производить в нем различные операции, не зная самого отображения  $\varphi(x)$ .

**Задача 5.1.** Как вычислить норму вектора  $\varphi(x)$ , зная лишь ядро  $K(x, z)$ ?

**Решение.**

$$\|\varphi(x)\| = \sqrt{\|\varphi(x)\|^2} = \sqrt{\langle \varphi(x), \varphi(x) \rangle} = \sqrt{K(x, x)}.$$

■

**Задача 5.2.** Как вычислить расстояние между векторами  $\varphi(x)$  и  $\varphi(z)$ , зная лишь ядро  $K(x, z)$ ?

**Решение.**

$$\begin{aligned} \rho^2(\varphi(x), \varphi(z)) &= \|\varphi(x) - \varphi(z)\|^2 = \langle \varphi(x) - \varphi(z), \varphi(x) - \varphi(z) \rangle = \\ &= \langle \varphi(x), \varphi(x) \rangle - 2\langle \varphi(x), \varphi(z) \rangle + \langle \varphi(z), \varphi(z) \rangle = \\ &= K(x, x) - 2K(x, z) + K(z, z). \end{aligned}$$

■

Таким образом, ядра можно использовать и в метрических методах (например, kNN) — достаточно подставить в них в качестве функции расстояния величину  $K(x, x) - 2K(x, z) + K(z, z)$ .

**Задача 5.3.** Как изменить ядро, чтобы оно соответствовало скалярному произведению нормированных векторов в спрямляющем пространстве?

**Решение.** Определим новое отображение:

$$\hat{\varphi}(x) = \begin{cases} \frac{\varphi(x)}{\|\varphi(x)\|}, & x \neq 0; \\ 0, & x = 0. \end{cases}$$

Тогда нормированное ядро при  $x \neq 0, z \neq 0$  можно вычислять как

$$\begin{aligned} \hat{K}(x, z) &= \langle \hat{\varphi}(x), \hat{\varphi}(z) \rangle = \left\langle \frac{\varphi(x)}{\|\varphi(x)\|}, \frac{\varphi(z)}{\|\varphi(z)\|} \right\rangle = \\ &= \frac{\langle \varphi(x), \varphi(z) \rangle}{\|\varphi(x)\| \|\varphi(z)\|} = \frac{K(x, z)}{\sqrt{K(x, x)K(z, z)}}. \end{aligned}$$

Если же один из векторов  $x$  или  $z$  равен нулю, то ядро также будет равно нулю.

■

## §5.5 Построение ядер

Самый простой способ задать ядро — в явном виде построить отображение  $\varphi(x)$  в спрямляющее признаковое пространство. Тогда ядро определяется как скалярное произведение в этом пространстве:  $K(x, z) = \langle \varphi(x), \varphi(z) \rangle$ . При таком способе, однако, возникают проблемы с ростом вычислительной сложности, о которых уже было сказано выше.

Допустим, в качестве новых признаков мы хотим взять всевозможные произведения исходных признаков. Определим соответствующее отображение

$$\varphi(x) = (x_i x_j)_{i,j=1}^d \in \mathbb{R}^{d^2}$$

и найдем ядро:

$$\begin{aligned} K(x, z) &= \langle \varphi(x), \varphi(z) \rangle = \langle (x_i x_j)_{i,j=1}^d, (z_i z_j)_{i,j=1}^d \rangle = \\ &= \sum_{i,j=1}^d x_i x_j z_i z_j = \\ &= \sum_{i=1}^d x_i z_i \sum_{j=1}^d x_j z_j = \\ &= \langle x, z \rangle^2. \end{aligned}$$

Таким образом, ядро выражается через скалярное произведение в исходном пространстве, и для его вычисления необходимо порядка  $d$  операций (в то время как прямое вычисление ядра потребовало бы  $O(d^2)$  операций).

### 5.5.1 Неявное задание ядра

Пример с мономами показал, что можно определить ядро так, что оно не будет в явном виде использовать отображение объектов в новое признаковое пространство. Но как убедиться, что функция  $K(x, z)$  определяет скалярное произведение в некотором пространстве? Ответ на этот вопрос дает *теорема Мерсера*: функция  $K(x, z)$  является ядром тогда и только тогда, когда:

1. Она симметрична:  $K(x, z) = K(z, x)$ .
2. Она неотрицательно определена, то есть для любой конечной выборки  $(x_1, \dots, x_\ell)$  матрица  $K = (K(x_i, x_j))_{i,j=1}^\ell$  неотрицательно определена.

**Задача 5.4.** Покажите, что если  $K(x, z)$  — ядро, то оно симметрично и неотрицательно определено.

**Решение.** Функция  $K(x, z)$  — ядро, то есть она определяет скалярное произведение в некотором пространстве:  $K(x, z) = \langle \varphi(x), \varphi(z) \rangle$ . Симметричность этой функции вытекает из симметричности скалярного произведения.

Покажем неотрицательную определенность. Пусть  $(x_1, \dots, x_\ell)$  — выборка, а  $K = (K(x_i, x_j))_{i,j=1}^\ell$  — матрица ядра, соответствующая ей. Тогда для произвольного

вектора  $v$ :

$$\begin{aligned}
 \langle Kv, v \rangle &= \sum_{i,j=1}^{\ell} v_i v_j K(x_i, x_j) = \\
 &= \sum_{i,j=1}^{\ell} v_i v_j \langle \varphi(x_i), \varphi(x_j) \rangle = \\
 &= \sum_{i,j=1}^{\ell} \langle v_i \varphi(x_i), v_j \varphi(x_j) \rangle = \\
 &= \left\langle \sum_{i=1}^{\ell} v_i \varphi(x_i), \sum_{j=1}^{\ell} v_j \varphi(x_j) \right\rangle = \\
 &= \left\| \sum_{i=1}^{\ell} v_i \varphi(x_i) \right\|^2 \geq 0.
 \end{aligned}$$

Мы доказали неотрицательную определенность матрицы  $K$ , а значит и ядра  $K(x, z)$ . ■

Проверить условия теоремы Мерсера, однако, может быть достаточно трудно. Поэтому для построения ядер, как правило, пользуются несколькими базовыми ядрами и операциями над ними, сохраняющими симметричность и неотрицательную определенность.

**Теорема 5.1 ([2]).** Пусть  $K_1(x, z)$  и  $K_2(x, z)$  — ядра, заданные на множестве  $X$ ,  $f(x)$  — вещественная функция на  $X$ ,  $\varphi : X \rightarrow \mathbb{R}^N$  — векторная функция на  $X$ ,  $K_3$  — ядро, заданное на  $\mathbb{R}^N$ . Тогда следующие функции являются ядрами:

1.  $K(x, z) = K_1(x, z) + K_2(x, z)$ ,
2.  $K(x, z) = \alpha K_1(x, z)$ ,  $\alpha > 0$ ,
3.  $K(x, z) = K_1(x, z)K_2(x, z)$ ,
4.  $K(x, z) = f(x)f(z)$ ,
5.  $K(x, z) = K_3(\varphi(x), \varphi(z))$ .

**Теорема 5.2 ([3]).** Пусть  $K_1(x, z), K_2(x, z), \dots$  — последовательность ядер, причем предел

$$K(x, z) = \lim_{n \rightarrow \infty} K_n(x, z)$$

существует для всех  $x$  и  $z$ . Тогда  $K(x, z)$  — ядро.

**Задача 5.5.** Покажите, что произведение ядер является ядром (третий пункт теоремы 5.1).

**Решение.** Пусть ядро  $K_1$  соответствует отображению  $\varphi_1 : X \rightarrow \mathbb{R}^{d_1}$ , а ядро  $K_2$  — отображению  $\varphi_2 : X \rightarrow \mathbb{R}^{d_2}$ . Определим новое отображение, которое соответствует всевозможным произведениям признаков из первого и второго спрямляющих пространств:

$$\varphi_3(x) = \left( (\varphi_1(x))_i (\varphi_2(x))_j \right)_{i,j=1}^{d_1, d_2}.$$

Соответствующее этому спрямляющему пространству ядро примет вид

$$\begin{aligned} K_3(x, z) &= \langle \varphi_3(x), \varphi_3(z) \rangle = \\ &= \sum_{i=1}^{d_1} \sum_{j=1}^{d_2} (\varphi_3(x))_{ij} (\varphi_3(z))_{ij} = \\ &= \sum_{i=1}^{d_1} (\varphi_1(x))_i (\varphi_1(z))_i \sum_{j=1}^{d_2} (\varphi_2(x))_j (\varphi_2(z))_j = \\ &= K_1(x, z) K_2(x, z). \end{aligned}$$

Мы показали, что произведение двух ядер соответствует скалярному произведению в некотором спрямляющем пространстве, а значит является ядром. ■

Рассмотрим некоторые примеры построения ядер.

### 5.5.2 Полиномиальные ядра

**Задача 5.6.** Пусть  $p(x)$  — многочлен с положительными коэффициентами. Покажите, что  $K(x, z) = p(\langle x, z \rangle)$  — ядро.

**Решение.** Пусть многочлен имеет вид

$$p(x) = \sum_{i=0}^m a_i x^i.$$

Будем доказывать требуемое утверждение по шагам.

1.  $\langle x, z \rangle$  — ядро по определению ( $\varphi(x) = x$ );
2.  $\langle x, z \rangle^i$  — ядро как произведение ядер;
3.  $a_i \langle x, z \rangle^i$  — ядро как произведение положительной константы на ядро;
4. константный член  $a_0$  — ядро по пункту 4 теоремы 5.1, где  $f(x) = \sqrt{a_0}$ ;
5.  $\sum_{i=0}^m a_i \langle x, z \rangle^i$  — ядро как линейная комбинация ядер. ■

Аналогично можно показать, что  $p(K(x, z))$  — ядро. Рассмотрим частный случай полиномиального ядра:

$$K_m(x, z) = (\langle x, z \rangle + R)^m.$$

Распишем степень, воспользовавшись формулой бинома Ньютона:

$$K_m(x, z) = \sum_{i=0}^m C_m^i R^{m-i} \langle x, z \rangle^i.$$

Поскольку коэффициенты при скалярных произведениях  $C_m^i R^{m-i}$  положительны, то данное ядро действительно является ядром согласно последней задаче. Если расписать скалярные произведения, то можно убедиться, что оно соответствует переводу набора признаков во всевозможные мономы над признаками степени не больше  $m$ , причем моном степени  $i$  имеет вес  $\sqrt{C_m^i R^{m-i}}$ .

Заметим, что параметр  $R$  контролирует относительный вес при мономах больших степеней. Например, отношение веса при мономе степени  $m-1$  к весу при мономе первой степени равно

$$\sqrt{\frac{C_m^{m-1} R}{C_m^1 R^{m-1}}} = \sqrt{\frac{1}{R^{m-2}}},$$

то есть по мере увеличения  $R$  вес при мономах старших степеней будет становиться очень небольшим по сравнению с весом при остальных мономах. Можно сказать, что параметр  $R$  контролирует сложность модели.

### 5.5.3 Гауссовские ядра

**Задача 5.7.** *Покажите, что гауссовское ядро*

$$K(x, z) = \exp\left(-\frac{\|x - z\|^2}{2\sigma^2}\right)$$

*действительно является ядром.*

**Решение.** Покажем сначала, что функция  $\exp(\langle x, z \rangle)$  является ядром. Представим ее в виде предела последовательности:

$$\exp(\langle x, z \rangle) = \sum_{k=0}^{\infty} \frac{\langle x, z \rangle^k}{k!} = \lim_{n \rightarrow \infty} \sum_{k=0}^n \frac{\langle x, z \rangle^k}{k!}.$$

Каждый член предельной последовательности является многочленом с положительными коэффициентами, и поэтому является ядром. Предел существует во всех точках  $(x, z)$ , поскольку ряд Тейлора для функции  $e^x$  сходится на всей числовой прямой. Значит, по теореме 5.2 данная функция является ядром.

Аналогично можно доказать, что функция  $\exp(\langle x, z \rangle / \sigma^2)$  также является ядром. Выше мы показали, что ядро можно отнормировать, после чего оно останется ядром. Прделаем это с данным ядром:

$$\begin{aligned} \frac{\exp(\langle x, z \rangle / \sigma^2)}{\sqrt{\exp(\|x\|^2 / \sigma^2) \exp(\|z\|^2 / \sigma^2)}} &= \exp\left(\frac{\langle x, z \rangle}{\sigma^2} - \frac{\langle x, x \rangle}{2\sigma^2} - \frac{\langle z, z \rangle}{2\sigma^2}\right) \\ &= \exp\left(-\frac{\|x - z\|^2}{2\sigma^2}\right). \end{aligned}$$

Заметим, что можно построить гауссово ядро, используя любое другое ядро  $K(x, z)$ . В этом случае оно примет вид

$$\exp\left(-\frac{\|\varphi(x) - \varphi(z)\|^2}{2\sigma^2}\right) = \exp\left(-\frac{K(x, x) - 2K(x, z) + K(z, z)}{2\sigma^2}\right).$$

Здесь мы расписали расстояние между векторами  $\|\varphi(x) - \varphi(z)\|^2$  в спрямляющем пространстве через функцию ядра.

**Спрямляющее пространство.** Какому спрямляющему пространству соответствует гауссовское ядро? Оно является пределом последовательности полиномиальных ядер при стремлении степени ядра к бесконечности, что наталкивает на мысль, что и спрямляющее пространство будет бесконечномерным. Чтобы показать это формально, нам понадобится следующее утверждение.

**Утв. 5.3 ([4]).** Пусть  $x_1, \dots, x_\ell$  — различные точки пространства  $\mathbb{R}^d$ . Тогда матрица

$$G = \left[ \exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right) \right]_{i,j=1}^\ell$$

является невырожденной при  $\sigma > 0$ .

Вспомним также факт из линейной алгебры: матрица Грама системы точек  $x_1, \dots, x_\ell$  невырождена тогда и только тогда, когда эти точки линейно независимы. Поскольку матрица из утверждения 5.3 является матрицей Грама для точек  $x_1, \dots, x_\ell$  в спрямляющем пространстве гауссова ядра, то заключаем, что в данном пространстве существует сколь угодно много линейно независимых точек. Значит, данное пространство является бесконечномерным.

Можно показать это и менее формально. Распишем функцию ядра:

$$\begin{aligned} K(x, z) &= \exp\left(-\frac{\|x - z\|^2}{2\sigma^2}\right) = \exp\left(-\frac{\|x\|^2}{2\sigma^2}\right) \exp\left(-\frac{\|z\|^2}{2\sigma^2}\right) \exp\left(-\frac{\langle x, z \rangle}{\sigma^2}\right) = \\ &= \{\text{раскладываем экспоненту в ряд}\} = \\ &= \exp\left(-\frac{\|x\|^2}{2\sigma^2}\right) \exp\left(-\frac{\|z\|^2}{2\sigma^2}\right) \sum_{k=0}^{\infty} \frac{\langle x, z \rangle^k}{n! \sigma^{2k}}. \end{aligned}$$

Легко видеть, что для получения  $k$ -го слагаемого в спрямляющем пространстве должны быть все мономы степени  $k$  над исходными признаками. Поскольку всего в сумме бесконечное число слагаемых, то и размерность спрямляющего пространства должна быть бесконечной.

**Роль параметра  $\sigma$ .** Заметим, что параметр  $\sigma$  в разложении гауссова ядра в ряд Тейлора входит в коэффициент перед слагаемым  $\langle x, z \rangle^k$  как  $1/\sigma^{2k}$ . Его роль аналогична параметру  $m$  в полиномиальных ядрах. Маленькие значения  $\sigma$  соответствуют большим значениям  $m$ : чем меньше  $\sigma$ , тем больше вес при мономах большой степени, тем больше риск переобучения.

**Связь с kNN.** Если использовать гауссовское ядро (или, как его еще называют, RBF-ядро) в методе опорных векторов, то получится следующее решающее правило:

$$a(x) = \text{sign} \sum_{i=1}^{\ell} y_i \lambda_i \exp \left( -\frac{\|x - x_i\|^2}{2\sigma^2} \right).$$

Вспомним теперь, что решающее правило в методе  $k$  ближайших соседей выглядит как

$$a(x) = \arg \max_{y \in Y} \Gamma_y(x, X^\ell); \quad \Gamma_y(x, X^\ell) = \sum_{i=1}^{\ell} [y_x^{(i)} = y] w(i, x),$$

где  $w(i, x)$  — оценка важности  $i$ -го соседа для классификации объекта  $x$ , а  $y_x^{(i)}$  — метка  $i$ -го ближайшего соседа. Для случая двух классов  $\{+1, -1\}$  решающее правило можно записать как знак разности оценок за эти классы:

$$\begin{aligned} a(x) &= \text{sign} (\Gamma_{+1}(x, X^\ell) - \Gamma_{-1}(x, X^\ell)) = \\ &= \text{sign} \left( \sum_{i=1}^{\ell} [y_x^{(i)} = +1] w(i, x) - \sum_{i=1}^{\ell} [y_x^{(i)} = -1] w(i, x) \right) = \\ &= \text{sign} \sum_{i=1}^{\ell} ([y_x^{(i)} = +1] - [y_x^{(i)} = -1]) w(i, x) = \\ &= \text{sign} \sum_{i=1}^{\ell} y_x^{(i)} w(i, x). \end{aligned}$$

Заметим, что решающие правила метода опорных векторов с RBF-ядром и метода  $k$  ближайших соседей совпадут, если положить

$$w(i, x) = \lambda_{(i)} \exp \left( -\frac{\|x - x_{(i)}\|^2}{2\sigma^2} \right).$$

То есть SVM-RBF — это метод  $\ell$  ближайших соседей, использующий гауссово ядро в качестве функции расстояния, и настраивающий веса объектов путем максимизации отступов.

## Список литературы

- [1] *Bishop, C.M.* Pattern Recognition and Machine Learning. // Springer, 2006.
- [2] *Shawe-Taylor, J., Cristianini, N.* Kernel Methods for Pattern Analysis. // Cambridge University Press, 2004.
- [3] *Sholkopf, B.A., Smola, A.J.* Learning with kernels. // MIT Press, 2002.
- [4] *Micchelli, C.A.* Algebraic aspects of interpolation. // Proceedings of Symposia in Applied Mathematics, 36:81-102, 1986.