SVM (Support Vector Machine)

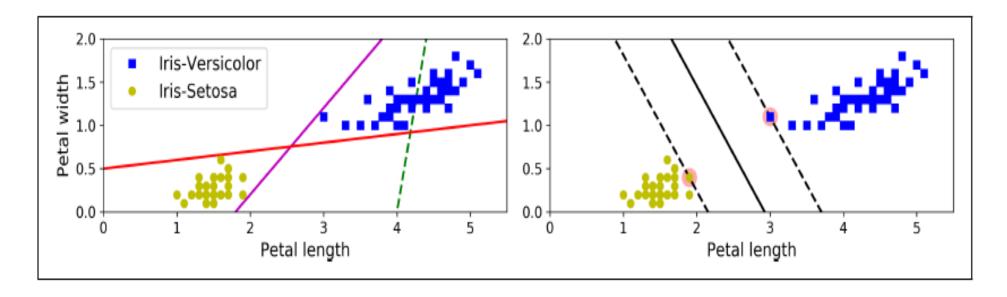
2021.8

Yongjin Jeong, KwangWoon University

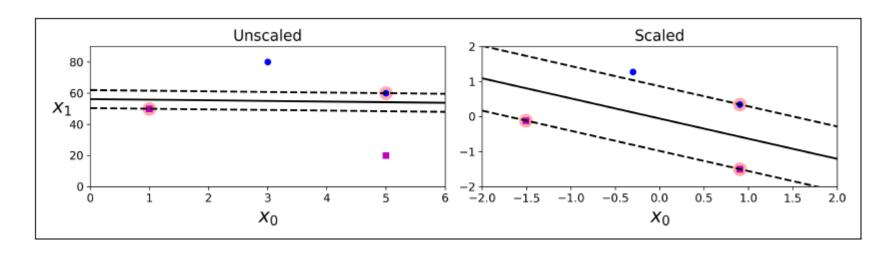
[참고] 본 자료에는 책이나 인터넷, 또는 외부 강의자료에서 인용하여 사용한 그림이나 수식들이 있으니 다른 용도로 사용하거나 외부로 유출을 금해 주시기 바랍니다.

- [1] Aurellian Geron, Hands-on Machine Learning with Scikit, Keras, and Tensorflow
- [2] https://www.robots.ox.ac.uk/~az/lectures (Prof. Zisserman's lecture slide)

Linear classification and SVM Classifier



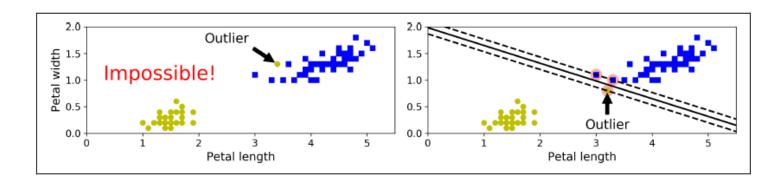
Sensitivity to feature scales



Before Scaling

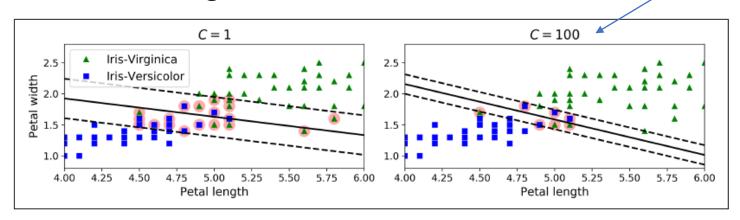
After Scaling

- Hard margin and Soft margin
 - Hard margin

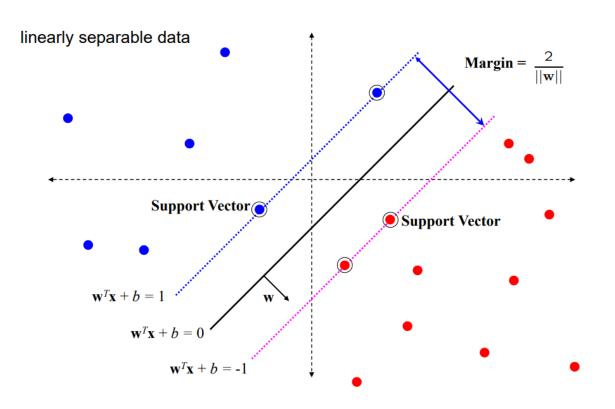


- Soft margin
 - Large margin and fewer margin violations

Overfitting 가능성



- Quadratic optimization problem subject to linear constraints
 - There is a unique minimum.



$$\overrightarrow{w} \bullet \overrightarrow{x_{+}} + b \ge \delta$$
 normalize $\overrightarrow{w} \bullet \overrightarrow{x_{+}} + b \ge 1$
 $\overrightarrow{w} \bullet \overrightarrow{x_{+}} + b < -\delta$ $\overrightarrow{w} \bullet \overrightarrow{x_{-}} + b \le -1$

SVM is formulated as an optimization:

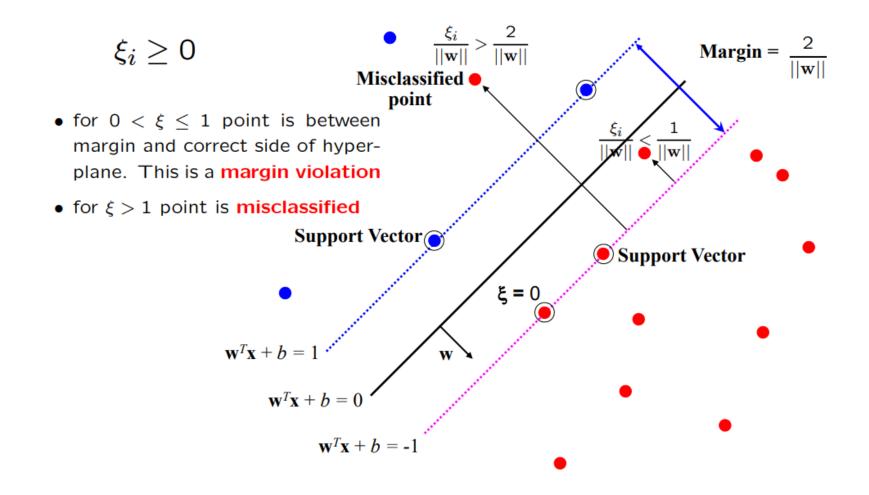
$$\max_{\mathbf{w}} \frac{2}{||\mathbf{w}||} \text{ subject to } \mathbf{w}^{\top} \mathbf{x}_i + b \overset{\geq}{\leq} 1 \quad \text{if } y_i = +1 \\ \leq -1 \quad \text{if } y_i = -1 \quad \text{for } i = 1 \dots N$$

Or equivalently

$$\min_{\mathbf{w}} ||\mathbf{w}||^2$$
 subject to $y_i \left(\mathbf{w}^{\top} \mathbf{x}_i + b \right) \geq 1$ for $i = 1 \dots N$

$$h_{\theta}(x) = \begin{cases} 1 & \text{if } \theta^T x >= 0 \\ 0 & \text{otherwise} \end{cases}$$

- Introduce Slack variables ('ksi')
 - amount of error (hinge loss) from the correct side of hyperplane



Soft margin

The optimization problem becomes

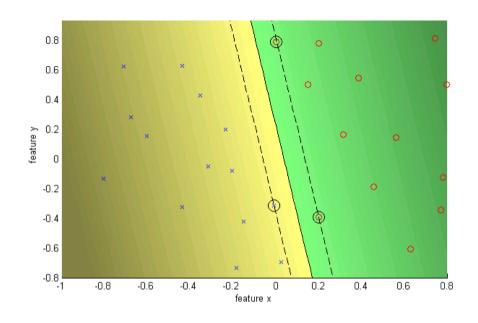
$$\min_{\mathbf{w} \in \mathbb{R}^d, \xi_i \in \mathbb{R}^+} ||\mathbf{w}||^2 + C \sum_{i=1}^{N} \xi_i$$

subject to

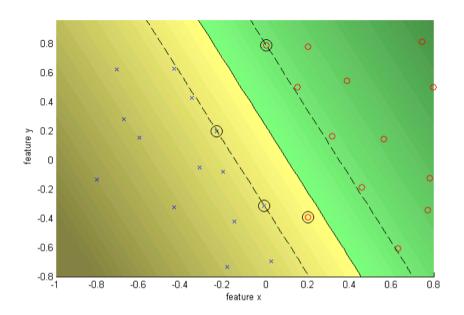
$$y_i\left(\mathbf{w}^{\top}\mathbf{x}_i + b\right) \geq 1 - \xi_i \text{ for } i = 1 \dots N$$

- \bullet Every constraint can be satisfied if ξ_i is sufficiently large
- C is a regularization parameter:
 - small C allows constraints to be easily ignored ightarrow large margin ightharpoonup soft margin
 - large C makes constraints hard to ignore \rightarrow narrow margin
 - $-C = \infty$ enforces all constraints: hard margin -> prone to overfitting
- ullet This is still a quadratic optimization problem and there is a unique minimum. Note, there is only one parameter, C.

Hard margin and Soft margin



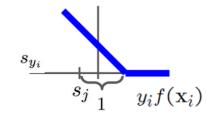
C = Infinity hard margin



C = 10 Soft margin

SVM Optimization

Constrained optimization problem



 The learning problem is now equivalent to the unconstrained optimization problem over w

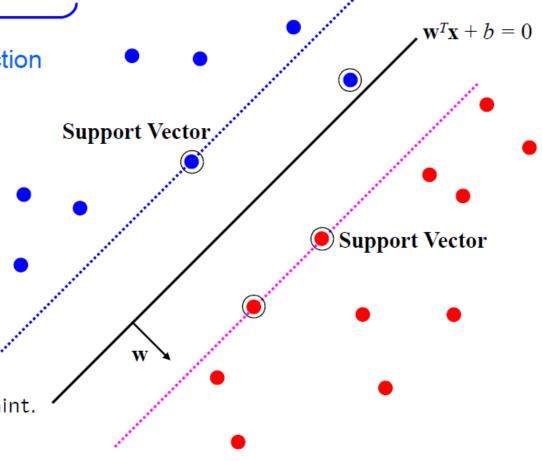
$$\min_{\mathbf{w} \in \mathbb{R}^d} ||\mathbf{w}||^2 + C \sum_{i}^{N} \max(\mathbf{0}, \mathbf{1} - y_i f(\mathbf{x}_i))$$
regularization loss function

Loss Function

 $\min_{\mathbf{w} \in \mathbb{R}^d} ||\mathbf{w}||^2 + C \sum_{i}^{N} \max(\mathbf{0}, \mathbf{1} - y_i f(\mathbf{x}_i))$ loss function

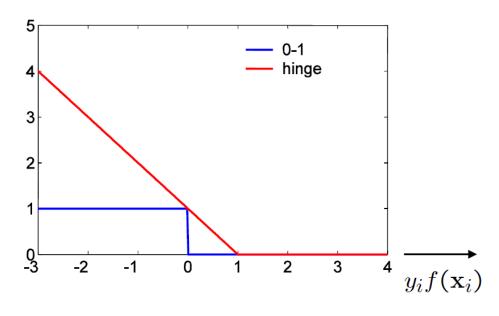
Points are in three categories:

- 1. $y_i f(x_i) > 1$ Point is outside margin. No contribution to loss
- 2. $y_i f(x_i) = 1$ Point is on margin. No contribution to loss. As in hard margin case.
- 3. $y_i f(x_i) < 1$ Point violates margin constraint. Contributes to loss



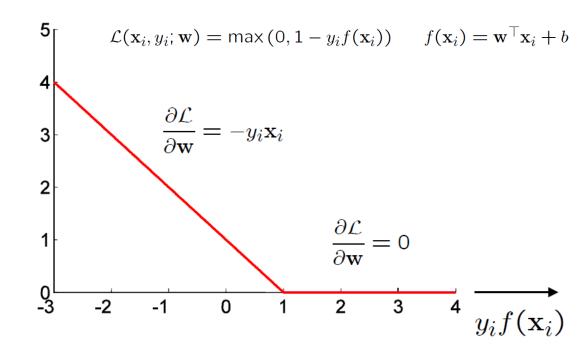
Hinge Loss

Hinge loss



- SVM uses "hinge" loss $\max(0, 1 y_i f(\mathbf{x}_i))$
- an approximation to the 0-1 loss

Sub-gradient for Hinge loss



Sub-gradient descent algorithm for SVM

$$C(\mathbf{w}) = \frac{1}{N} \sum_{i}^{N} \left(\frac{\lambda}{2} ||\mathbf{w}||^{2} + \mathcal{L}(\mathbf{x}_{i}, y_{i}; \mathbf{w}) \right)$$

The iterative update is

$$\mathbf{w}_{t+1} \leftarrow \mathbf{w}_{t} - \eta \nabla_{\mathbf{w}_{t}} \mathcal{C}(\mathbf{w}_{t})$$

$$\leftarrow \mathbf{w}_{t} - \eta \frac{1}{N} \sum_{i}^{N} (\lambda \mathbf{w}_{t} + \nabla_{\mathbf{w}} \mathcal{L}(\mathbf{x}_{i}, y_{i}; \mathbf{w}_{t}))$$

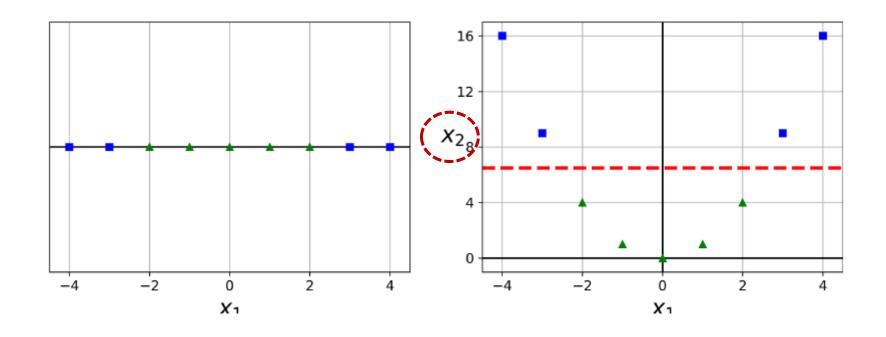
where η is the learning rate.

Then each iteration t involves cycling through the training data with the updates:

$$egin{array}{lll} \mathbf{w}_{t+1} &\leftarrow & \mathbf{w}_t - \eta(\lambda \mathbf{w}_t - y_i \mathbf{x}_i) & & ext{if } y_i f(\mathbf{x}_i) < 1 \ &\leftarrow & \mathbf{w}_t - \eta \lambda \mathbf{w}_t & & ext{otherwise} \end{array}$$

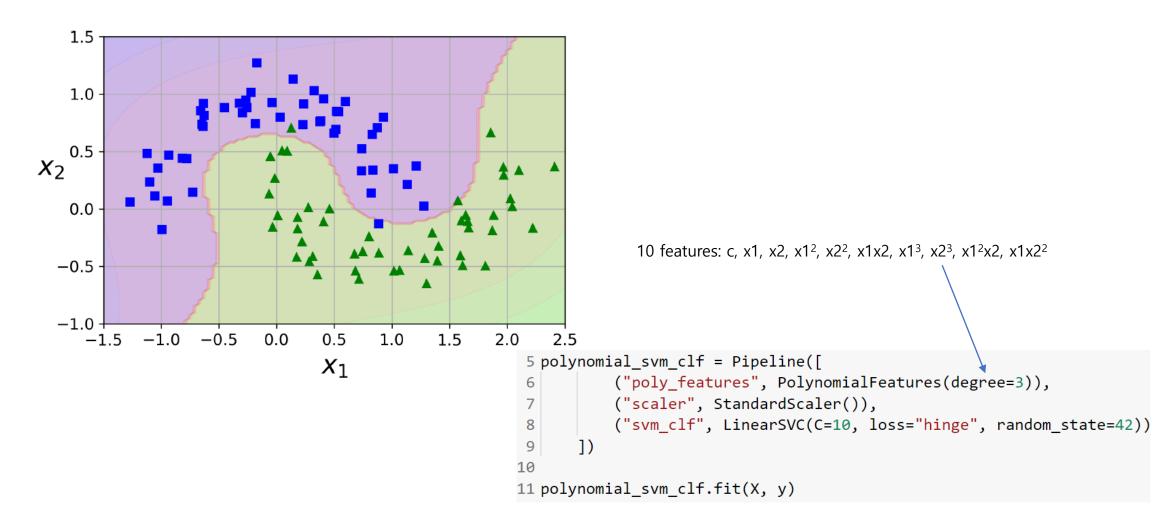
Nonlinear SVM Classifier

- Adding features to make a dataset linearly separable
 - Add a second feature $x_2 = (x_1)^2$



Nonlinear SVM Classifier

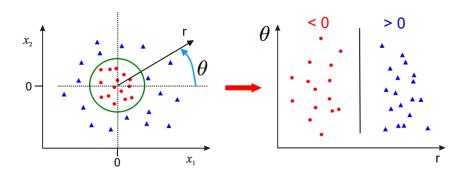
Linear SVM classifier using polynomial features



Nonlinear SVM Classifier

General (linearly) non-separable data

Use polar coordinates



- Data is linearly separable in polar coordinates
- · Acts non-linearly in original space

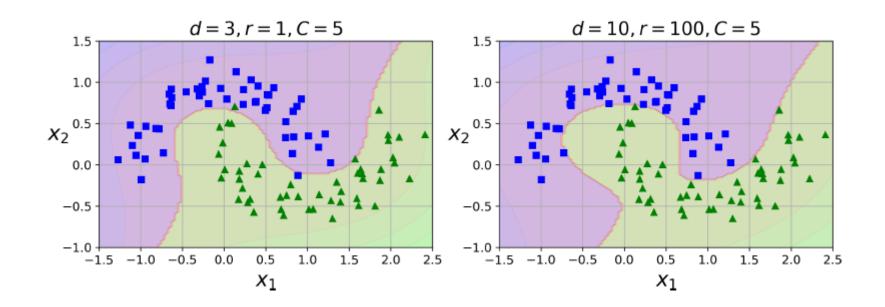
$$\Phi: \left(\begin{array}{c} x_1 \\ x_2 \end{array}\right) \to \left(\begin{array}{c} r \\ \theta \end{array}\right) \quad \mathbb{R}^2 \to \mathbb{R}^2$$

Map data to higher dimension

Non-linear Classification - SVM Kernels

SVM classifiers with a polynomial kernel

$$\mathbf{K}(\mathsf{a},\mathsf{b}) = (a \times b + r)^d$$
- a, b: 서로 다른 데이터
- r: polynomial의 coefficient를 결정
- d: polynomial의 차수

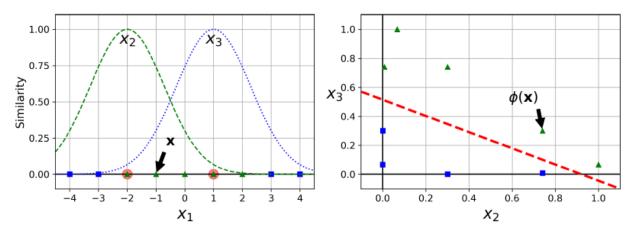


SVM Kernels

- SVM with Similarity features
 - Use a similarity function that measures how much each instance resembles a particular landmark.
 - define the similarity function: **Gaussian Radial Basis Function** (*RBF*)

$$\phi_{\gamma}(\mathbf{x}, \ell) = \exp(-\gamma ||\mathbf{x} - \ell||^2)$$

original feature: $x_1 = -1$



Take two landmarks at $x_1 = -2$, $x_1 = 1$ then, new features are:

$$x_2 = \exp(-0.3 \times 1^2) \approx 0.74$$

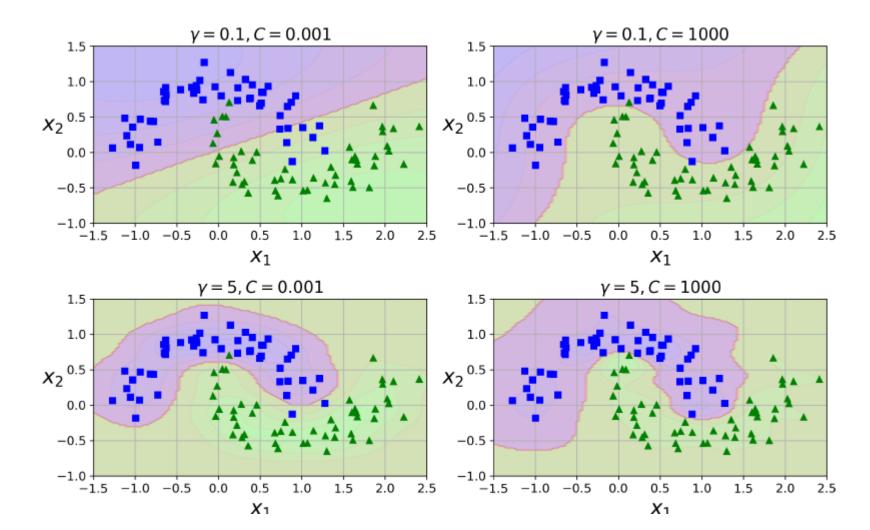
$$x_3 = \exp(-0.3 \times 2^2) \approx 0.30$$

now, linearly separable.

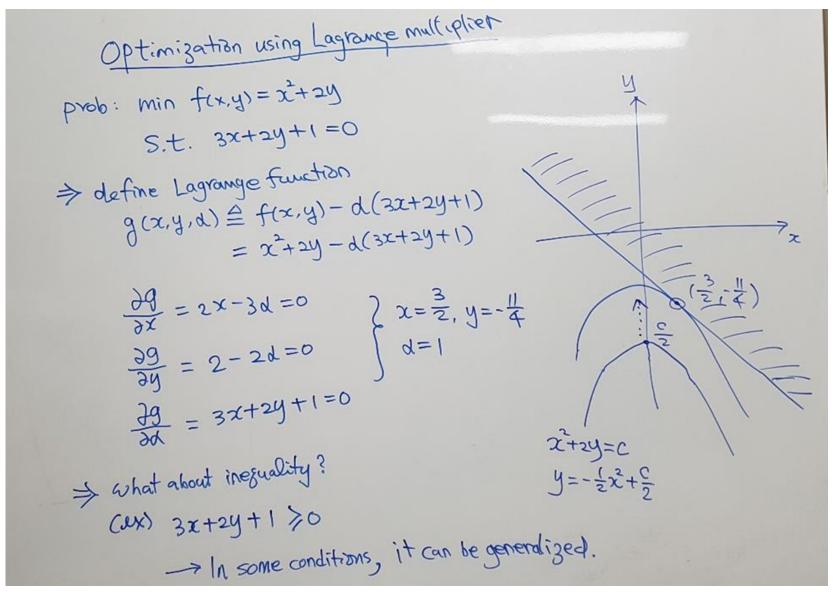
Create landmarks at the location of each instance, then (assuming drop of the original features)
 m instances, n features -> m instances, m features (large features!)

SVM Kernels

Gaussian RBF Kernel



Optimization – Lagrangian multiplier



Optimization – SVM Hard margin

ti=(+1 (9;=1)
SVM.
SVM. Hand margin SVM problem
min = w.m (= min +wt)
Subject to (tiluTx; +b)>1, for i=1,2-m
\Rightarrow Generalized Lograngian $L(w,b,d) \triangleq \frac{1}{2} \omega^T w - \sum_{i=1}^{m} d_i (t_i(\omega^T x_i + b) - 1)$
(Luckily, sum problem meats the generalization
$ \sqrt{\frac{1}{2}}d(\omega,b,d) = W - \sum_{i=1}^{m} d_i t_{i} x_{i} $ $ \frac{\partial}{\partial b}d(\omega,b,d) = -\sum_{i=1}^{m} d_i t_{i} $
$\Rightarrow \widehat{\omega} = \sum_{i=1}^{m} \widehat{\alpha}_{i} t_{i} x_{i}, \sum_{i=1}^{m} \widehat{\alpha}_{i} t_{i} = 0$

⇒ Generalized dayrange function is $\mathcal{L}(\widehat{w}, b, \lambda) = \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} didjtitj X_{i}^{T}X_{j} - \sum_{i=1}^{m} di$ with λ_{i} 7.0 for $i=1,2,\cdots m$ Now, the goal is to find the vector \widehat{d} that minimizes this function, with $\widehat{d}i$ 7.0.

for all instances.

Primal and Dual formulations

N is number of training points, and d is dimension of feature vector ${f x}$.

Primal problem: for $\mathbf{w} \in \mathbb{R}^d$

$$\min_{\mathbf{w} \in \mathbb{R}^d} ||\mathbf{w}||^2 + C \sum_{i}^{N} \max \left(0, 1 - y_i f(\mathbf{x}_i)\right)$$

Dual problem: for $\alpha \in \mathbb{R}^N$ (stated without proof):

$$\max_{\alpha_i \geq 0} \sum_i \alpha_i - \frac{1}{2} \sum_{jk} \alpha_j \alpha_k y_j y_k (\mathbf{x}_j^\top \mathbf{x}_k) \text{ subject to } 0 \leq \alpha_i \leq C \text{ for } \forall i, \text{ and } \sum_i \alpha_i y_i = 0$$

- ullet Need to learn d parameters for primal, and N for dual
- If N << d then more efficient to solve for α than ${\bf w}$
- Dual form only involves $(\mathbf{x}_j^{\mathsf{T}}\mathbf{x}_k)$.

Primal and Dual in transformed Feature space

Primal Classifier in transformed feature space

Classifier, with $\mathbf{w} \in \mathbb{R}^D$:

$$f(\mathbf{x}) = \mathbf{w}^{\top} \mathbf{\Phi}(\mathbf{x}) + b$$

Learning, for $\mathbf{w} \in \mathbb{R}^D$

$$\min_{\mathbf{w} \in \mathbb{R}^D} ||\mathbf{w}||^2 + C \sum_{i=1}^{N} \max(0, 1 - y_i f(\mathbf{x}_i))$$

- Simply map x to $\Phi(x)$ where data is separable
- ullet Solve for ${f w}$ in high dimensional space ${\mathbb R}^D$
- If D >> d then there are many more parameters to learn for w. Can this be avoided?

Dual Classifier in transformed feature space

Classifier:

$$f(\mathbf{x}) = \sum_{i}^{N} \underline{\alpha_{i} y_{i} \mathbf{x}_{i}^{\top} \mathbf{x}} + b \quad \longleftarrow \quad \text{wx + b}$$

$$\to f(\mathbf{x}) = \sum_{i}^{N} \alpha_{i} y_{i} \Phi(\mathbf{x}_{i})^{\top} \Phi(\mathbf{x}) + b$$

Learning:

$$\max_{\alpha_i \ge 0} \sum_i \alpha_i - \frac{1}{2} \sum_{jk} \alpha_j \alpha_k y_j y_k \mathbf{x}_j^{\top} \mathbf{x}_k$$

$$\rightarrow \max_{\alpha_i \ge 0} \sum_i \alpha_i - \frac{1}{2} \sum_{jk} \alpha_j \alpha_k y_j y_k \mathbf{\Phi}(\mathbf{x}_j)^{\top} \mathbf{\Phi}(\mathbf{x}_k)$$

subject to

$$0 \le \alpha_i \le C$$
 for $\forall i$, and $\sum_i \alpha_i y_i = 0$

SVM Kernels

Dual Classifier in transformed feature space

- Note, that $\Phi(\mathbf{x})$ only occurs in pairs $\Phi(\mathbf{x}_i)^{\top}\Phi(\mathbf{x}_i)$
- ullet Once the scalar products are computed, only the N dimensional vector $oldsymbol{lpha}$ needs to be learnt; it is not necessary to learn in the D dimensional space, as it is for the primal
- Write $k(\mathbf{x}_j, \mathbf{x}_i) = \Phi(\mathbf{x}_j)^\top \Phi(\mathbf{x}_i)$. This is known as a Kernel

Classifier:

$$f(\mathbf{x}) = \sum_{i}^{N} \alpha_{i} y_{i} k(\mathbf{x}_{i}, \mathbf{x}) + b$$

Learning:

$$\max_{\alpha_i \ge 0} \sum_i \alpha_i - \frac{1}{2} \sum_{jk} \alpha_j \alpha_k y_j y_k \, k(\mathbf{x}_j, \mathbf{x}_k)$$

subject to

$$0 \le \alpha_i \le C$$
 for $\forall i$, and $\sum_i \alpha_i y_i = 0$

Special transformations

$$\Phi: \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \begin{pmatrix} x_1^2 \\ x_2^2 \\ \sqrt{2}x_1x_2 \end{pmatrix} \quad \mathbb{R}^2 \to \mathbb{R}^3$$

$$\Phi(\mathbf{x})^\top \Phi(\mathbf{z}) = \begin{pmatrix} x_1^2, x_2^2, \sqrt{2}x_1x_2 \end{pmatrix} \begin{pmatrix} z_1^2 \\ z_2^2 \\ \sqrt{2}z_1z_2 \end{pmatrix}$$

$$= x_1^2 z_1^2 + x_2^2 z_2^2 + 2x_1x_2z_1z_2$$

$$= (x_1 z_1 + x_2 z_2)^2$$

$$= (\mathbf{x}^\top \mathbf{z})^2$$

Kernel Trick

- ullet Classifier can be learnt and applied without explicitly computing $\Phi(x)$
- All that is required is the kernel $k(\mathbf{x}, \mathbf{z}) = (\mathbf{x}^{\top} \mathbf{z})^2$
- Complexity of learning depends on N (typically it is $O(N^3)$) not on D

Common SVM Kernels

Mercer's Theorem

According to *Mercer's theorem*, if a function $K(\mathbf{a}, \mathbf{b})$ respects a few mathematical conditions called *Mercer's conditions* (K must be continuous, symmetric in its arguments so $K(\mathbf{a}, \mathbf{b}) = K(\mathbf{b}, \mathbf{a})$, etc.), then there exists a function ϕ that maps \mathbf{a} and \mathbf{b} into another space (possibly with much higher dimensions) such that $K(\mathbf{a}, \mathbf{b}) = \phi(\mathbf{a})^T \phi(\mathbf{b})$. So you can use K as a kernel since you know ϕ exists, even if you don't know what ϕ is. In the case of the Gaussian RBF kernel, it can be shown that ϕ actually maps each training instance to an infinite-dimensional space, so it's a good thing you don't need to actually perform the mapping!

Linear:
$$K(\mathbf{a}, \mathbf{b}) = \mathbf{a}^T \mathbf{b}$$

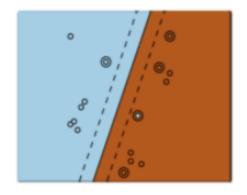
Polynomial:
$$K(\mathbf{a}, \mathbf{b}) = (\gamma \mathbf{a}^T \mathbf{b} + r)^d$$

Gaussian RBF:
$$K(\mathbf{a}, \mathbf{b}) = \exp(-\gamma ||\mathbf{a} - \mathbf{b}||^2)$$

Sigmoid:
$$K(\mathbf{a}, \mathbf{b}) = \tanh \left(\gamma \mathbf{a}^T \mathbf{b} + r \right)$$

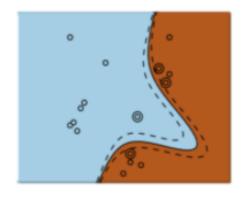
Common SVM Kernels

Linear Kernel



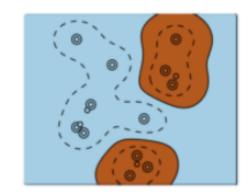
C hyperparameter

Polynomial Kernel



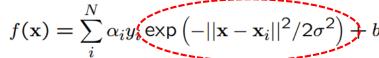
C plus gamma, degree and coefficient hyperparameters

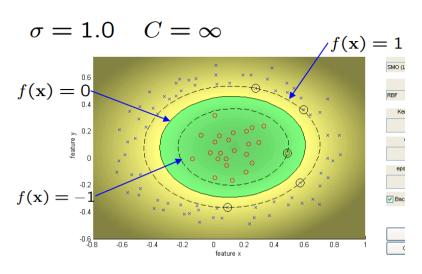
RBF Kernel



C plus gamma hyperparameter

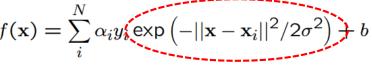
RBF Kernel SVM Example



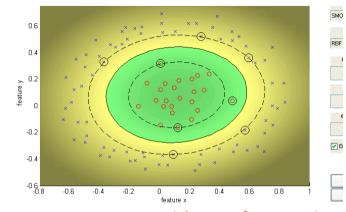


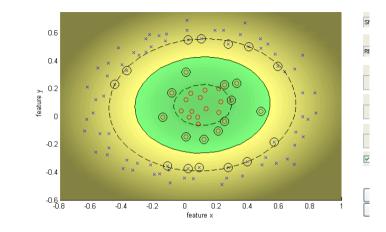
 $\sigma = 1.0$ $C = \infty$

$$\sigma = 1.0$$
 $C = 100$



$$\sigma = 1.0$$
 $C = 10$

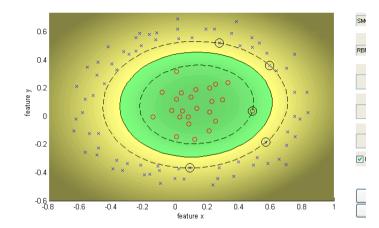


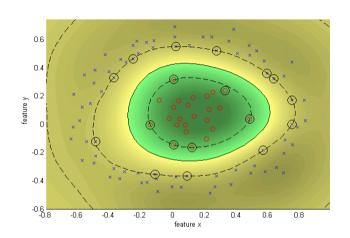


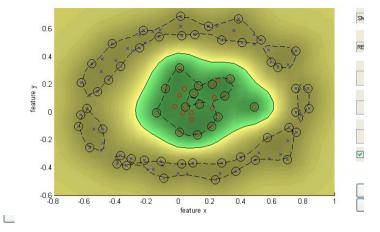
Decrease C -> wider (soft) margin

$$\sigma = 0.25$$
 $C = \infty$

 $\sigma = 0.1$ $C = \infty$



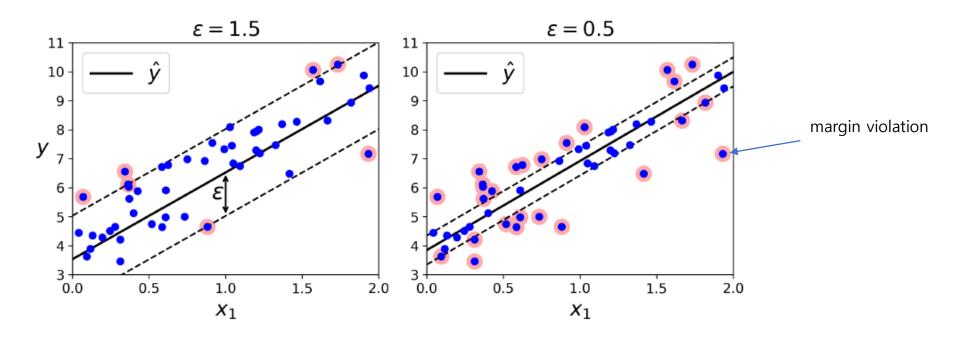




Decrease sigma (increase gamma) -> move towards nearest neighbor classifier

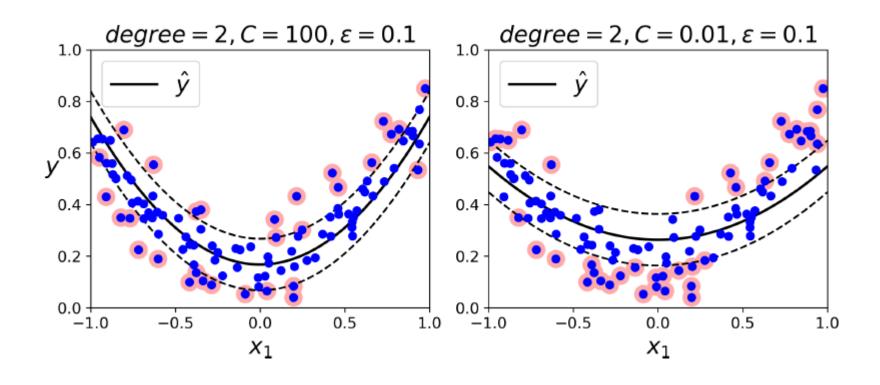
SVM Regression

- · It also supports linear and nonlinear regression.
- Reverse the object:
 - instead of trying to fit the largest possible street between two classes while limiting margin violations,
 - SVM Regression tries to **fit as many instances as possible** *on* **the street** while limiting margin violations (i.e., instances *off* the street).
 - The width of the street is controlled by a hyper-parameter ϵ .



SVM Regression

• SVM regression using 2nd degree polynomial kernel



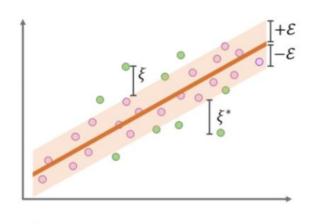
SVM Regression

- Loss function: ε-insensitive loss:
 - Ignores errors that are within ε distance by treating them as zero
 - Measured based on the distance between observed value y and the ε boundary

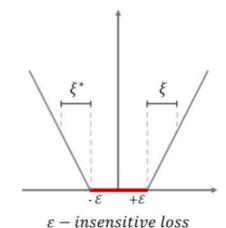
$$L_{\varepsilon} = \begin{cases} 0 & \text{if } |y - f(x)| \le \varepsilon \\ |y - f(x)| - \varepsilon & \text{otherwise} \end{cases}$$

$$L_{SVR} = \min rac{1}{2} {\|w\|}^2 + C {\sum_{i=1}^n} \left({{\xi _i} + {\xi _i^*}}
ight)$$

$$s.t. \quad (w^T x_i + b) - y_i \le \epsilon + \xi_i$$
 $y_i - (w^T x_i + b) \le \epsilon + \xi_i^*$ $\xi_i, \xi_i^* \ge 0$

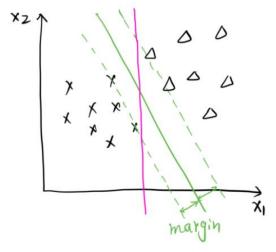


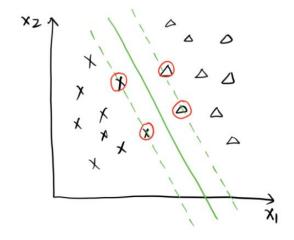
: Support Vector

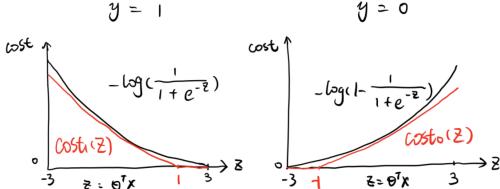


Linear SVM

- Concept
- support vectors
- Loss function
- Hypothesis





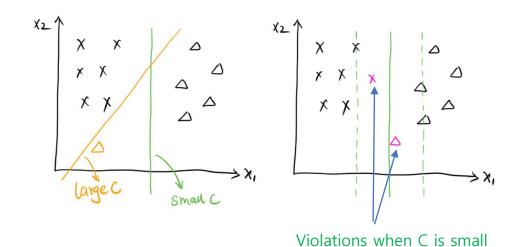


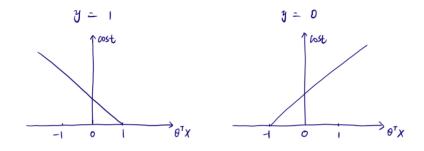
$$h_{\theta}(x) = \begin{cases} 1 & \text{if } \theta^T x >= 0 \\ 0 & \text{otherwise} \end{cases}$$

SVM cost function

$$J(\theta) = C[\sum_{i=1}^{m} y^{(i)} Cost_1(\theta^T(x^{(i)}) + (1 - y^{(i)}) Cost_0(\theta^T(x^{(i)})] + \frac{1}{2} \sum_{j=1}^{n} \theta_j^2$$

 $m = number of samples, \quad n = number of features$

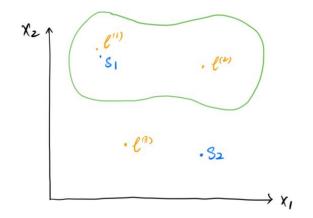


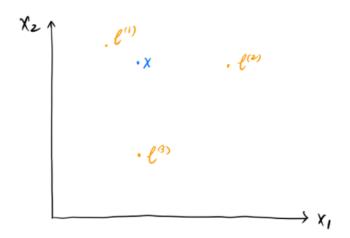


$$Cost(h_{\theta}(x), y) = \begin{cases} max(0, 1 - \theta^{T}x) & \text{if } y = 1\\ max(0, 1 + \theta^{T}x) & \text{if } y = 0 \end{cases}$$

Non-linear (rbf) SVM

- Hypothesis and cost function are almost the same (x -> f)
- Define landmarks to see how close x is to them (similarity) kernel function
- Gaussian kernel (RBF: radial basis function) basically the same (use γ to represent $1/2\sigma^2$)
- Now we have new features (f1,f2,f3) instead of x1 and x2.
- Prediction: $\theta^T f = \theta 0 + \theta 1 f 1 + \theta 2 f 2 + \theta 3 f 3$





$$f1 = Similarity(x, l^{(1)}) \text{ or } k(x, l^{(1)})$$

$$f2 = Similarity(x, 1^{(2)}) \text{ or } k(x, 1^{(2)})$$

$$f3 = Similarity(x, 1^{(3)}) \text{ or } k(x, 1^{(3)})$$

$$f_1 = Similarity(x, l^{(1)}) = exp(\frac{||x - l^{(1)}||^2}{2\sigma^2})$$

$$f_2 = Similarity(x, l^{(2)}) = exp(\frac{||x - l^{(2)}||^2}{2\sigma^2})$$

$$f_3 = Similarity(x, l^{(3)}) = exp(\frac{||x - l^{(3)}||^2}{2\sigma^2})$$

Non-linear (rbf) SVM

Given
$$(x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), \dots, (x^{(m)}, y^{(m)})$$

Choose $l^{(1)} = x^{(1)}, l^{(2)} = x^{(2)}, \dots, l^{(m)} = x^{(m)}$
 $m = number \ of \ samples$

Hypothesis:
$$h_{\theta}(x) = \begin{cases} 1 & \text{if } \theta^T f >= 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\theta^T f = \theta_0 f_0 + \theta_1 f_1 + \dots + \theta_m f_m$$

Given the i^{th} sample $x^{(i)}$:

$$f_1^{(i)} = k(x^{(i)}, l^{(1)})$$

$$f_2^{(i)} = k(x^{(i)}, l^{(2)})$$

$$\dots$$

$$f_i^{(i)} = k(x^{(i)}, l^{(i)})$$

$$\dots$$

$$f_m^{(i)} = k(x^{(i)}, l^{(m)})$$
where $x^{(i)} = l^{(i)}, f_i^{(i)} = 1$

Regularized Cost Function:

$$J(\theta) = C[\sum_{i=1}^{m} [y^{(i)}Cost_1(\theta^T(f^{(i)}) + (1 - y^{(i)})Cost_0(\theta^T(f^{(i)})] + \frac{1}{2}\sum_{j=1}^{m} \theta_j^2$$