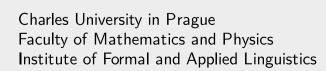


Soft-margin SVM, SMO

Milan Straka

■ November 14, 2022







Support Vector Machines



In order to solve the constrained problem of

$$rg\min_{oldsymbol{w},b}rac{1}{2}\|oldsymbol{w}\|^2 \ ext{ given that } \ t_iy(oldsymbol{x}_i)\geq 1,$$

we write the Lagrangian with multipliers $oldsymbol{a}=(a_1,\ldots,a_N)$ as

$$\mathcal{L} = rac{1}{2} \|oldsymbol{w}\|^2 - \sum_i a_i ig(t_i y(oldsymbol{x}_i) - 1ig).$$

Setting the derivatives with respect to $oldsymbol{w}$ and b to zero, we get

$$egin{aligned} oldsymbol{w} &= \sum_i a_i t_i arphi(oldsymbol{x}_i), \ 0 &= \sum_i a_i t_i. \end{aligned}$$

Support Vector Machines



Substituting these to the Lagrangian, we want to maximize

$$\mathcal{L} = \sum_i a_i - rac{1}{2} \sum_i \sum_j a_i a_j t_i t_j K(oldsymbol{x}_i, oldsymbol{x}_j)$$

with respect to a_i subject to the constraints $a_i \geq 0$ and $\sum_i a_i t_i = 0$, using the kernel $K(\boldsymbol{x}, \boldsymbol{z}) = \varphi(\boldsymbol{x})^T \varphi(\boldsymbol{z})$.

The solution will fulfill the KKT conditions, meaning that

$$a_i \geq 0, \qquad t_i y(oldsymbol{x}_i) - 1 \geq 0, \qquad a_i ig(t_i y(oldsymbol{x}_i) - 1ig) = 0.$$

Therefore, either a point \boldsymbol{x}_i is on a boundary, or $a_i=0$. Given that the prediction for \boldsymbol{x} is $y(\boldsymbol{x})=\sum_i a_i t_i K(\boldsymbol{x},\boldsymbol{x}_i)+b$, we only need to keep the training points \boldsymbol{x}_i that are on the boundary, the so-called **support vectors**. Therefore, even though SVM is a nonparametric model, it needs to store only a subset of the training data.

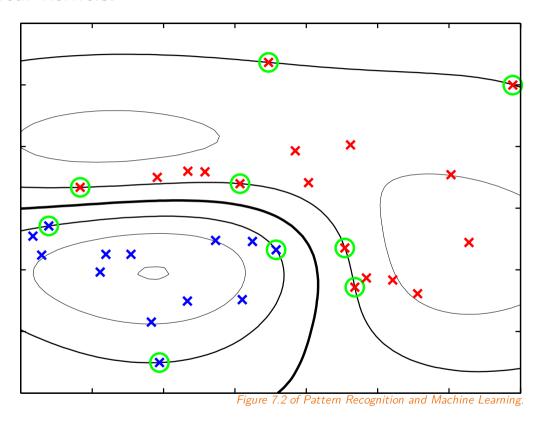
Hinge

Support Vector Machines



The dual formulation allows us to use nonlinear kernels.

Figure 7.2 Example of synthetic data from two classes in two dimensions showing contours of constant $y(\mathbf{x})$ obtained from a support vector machine having a Gaussian kernel function. Also shown are the decision boundary, the margin boundaries, and the support vectors.



Support Vector Machines for Non-linearly Separable Data



5/28

Until now, we assumed the data to be linearly separable – the hard-margin SVM variant. We now relax this condition to arrive at soft-margin SVM. The idea is to allow points to be in the margin or even on the *wrong side* of the decision boundary. We introduce slack variables $\xi_i \geq 0$, one for each training instance, defined as

$$\xi_i = egin{cases} \xi_i \geq 0, & ext{one for each training instance, defined as} \ | ar{c}_i = egin{cases} \frac{1}{2} & ext{cases} & ext{one for each training instance, defined as} \ | ar{c}_i = egin{cases} \frac{1}{2} & ext{one for points fulfilling } t_i y(oldsymbol{x}_i) \geq 1, \ |t_i - y(oldsymbol{x}_i)| & ext{otherwise.} \end{cases}$$

Therefore, $\xi_i=0$ signifies a point outside of margin, $0<\xi_i<1$ denotes a point inside the margin, $\xi_i=1$ is a point on the decision boundary, and $\xi_i>1$ indicates the point is on the opposite side of the separating hyperplane.

Therefore, we want to optimize

$$rg\min_{oldsymbol{w},b} C \sum
olimits_i \xi_i + rac{1}{2} \|oldsymbol{w}\|^2 ext{ given that } t_i y(oldsymbol{x}_i) \geq 1 - \xi_i ext{ and } \xi_i \geq 0.$$

SMO

Figure 7.3 of Pattern Recognition and Machine

Support Vector Machines for Non-linearly Separable Data



To solve the soft-margin variant, we again create a Lagrangian, this time with two sets of multipliers ${m a}=(a_1,\ldots,a_N)$ and ${m \mu}=(\mu_1,\ldots,\mu_N)$:

$$\mathcal{L} = rac{1}{2} \|oldsymbol{w}\|^2 + C \sum_i \xi_i - \sum_i a_i ig(t_i y(oldsymbol{x}_i) - 1 + \xi_iig) - \sum_i \mu_i \xi_i.$$

Solving for the critical points and substituting for w, b, and ξ (obtaining an additional constraint $\mu_i = C - a_i$ compared to the previous case), we obtain the Lagrangian in the form

$$\mathcal{L} = \sum_i a_i - rac{1}{2} \sum_i \sum_j a_i a_j t_i t_j K(oldsymbol{x}_i, oldsymbol{x}_j),$$

which is identical to the previous case, but the constraints are a bit different:

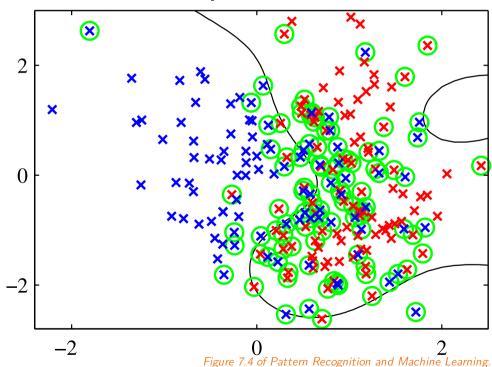
$$orall i: C \geq a_i \geq 0 \ \ ext{and} \ \ \sum_i a_i t_i = 0.$$

Support Vector Machines for Non-linearly Separable Data



Using the KKT conditions, we can see that the support vectors (examples with $a_i > 0$) are the ones with $t_i y(\mathbf{x}_i) = 1 - \xi_i$, i.e., the examples on the margin boundary, inside the margin, and on the opposite side of the decision boundary.





SGD-like Formulation of Soft-Margin SVM



Note that the slack variables can be written as in the slack variables if
$$t$$
. So we can refermulate the soft margin SVM objective using the **bings** loss.

so we can reformulate the soft-margin SVM objective using the hinge loss

$$\mathcal{L}_{ ext{hinge}}(t,y) \stackrel{ ext{ iny def}}{=} \max(0,1-ty)$$

to

$$rg\min_{oldsymbol{w},b} C \sum_i \mathcal{L}_{ ext{hinge}}ig(t_i,y(oldsymbol{x}_i)ig) + rac{1}{2}\|oldsymbol{w}\|^2.$$

Such formulation is analogous to a regularized loss, where C is an *inverse* regularization strength, so $C=\infty$ implies no regularization, and C=0 ignores the data entirely.

Hinge

Comparison of Linear and Logistic Regression and SVM



For $y(\boldsymbol{x};\boldsymbol{w},b)\stackrel{\text{def}}{=} \boldsymbol{\varphi}(\boldsymbol{x})^T\boldsymbol{w}+b$, we have seen the following losses:

Model	Objective	Per-Instance Loss
Linear Regression	$\left rg\min_{oldsymbol{w},b} \sum_i \mathcal{L}_{ ext{MSE}}ig(t_i,y(oldsymbol{x}_i)ig) + rac{1}{2}\lambda oldsymbol{w} ^2 ight.$	$\mathcal{L}_{ ext{MSE}}(t,y) = rac{1}{2}(t-y)^2$
Logistic regression	$rg\min_{m{w},b} \sum_i \mathcal{L}_{ ext{o-NLL}}ig(t_i,y(m{x}_i)ig) + rac{1}{2}\lambda m{w} ^2$	$\mathcal{L}_{ ext{o-NLL}}(t,y) = -\log igg(rac{\sigma(y)^t \cdot}{\cdot ig(1 - \sigma(y)ig)^{1-t}}igg)$
Softmax regression	$lpha \min_{oldsymbol{W},oldsymbol{b}} \sum_i \mathcal{L}_{ ext{s-NLL}}ig(t_i,oldsymbol{y}(oldsymbol{x}_i)ig) + rac{1}{2}\lambda oldsymbol{w} ^2$	$\mathcal{L}_{ ext{s-NLL}}(t,oldsymbol{y}) = -\log \operatorname{softmax}(oldsymbol{y})_t$
SVM	$lpha \min_{m{w},b} C \sum_i \mathcal{L}_{ ext{hinge}}ig(t_i,y(m{x}_i)ig) + rac{1}{2} m{w} ^2$	$\mathcal{L}_{ ext{hinge}}(t,y) = \max(0,1-ty)$

Note that $\mathcal{L}_{ ext{MSE}}(t,y) \propto -\log \left(\mathcal{N}(t;\mu=y,\sigma^2= ext{const})
ight)$ and $\mathcal{L}_{ ext{o-NLL}}(t,y) = \mathcal{L}_{ ext{s-NLL}}(t,[y,0])$.

SMO

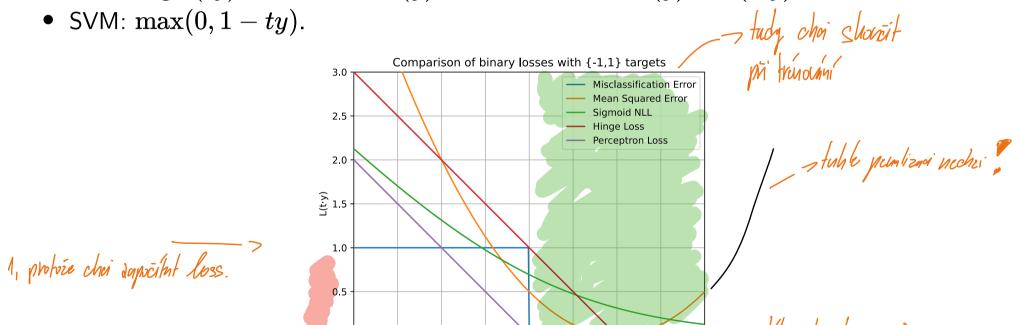
Hinge

Binary Classification Loss Functions Comparison



To compare various functions for binary classification, we need to formulate them all in the same settings, with $t \in \{-1, 1\}$.

- MSE: $\frac{1}{2}(ty-1)^2$, because it is $(y-1)^2$ for t=1, $(y+1)^2=(-y-1)^2$ for t=-1,
- LR: $-\log \sigma(ty)$, because it is $\sigma(y)$ for t=1 and $1-\sigma(y)=\sigma(-y)$ for t=-1,



NPFL129. Lecture 7

Refresh

Soft-margin SVM

-2.0

Hinge

-1.0

-1.5

SMO

Primal vs Dual

0.5

1.0

MultiSVM

SVR

Demos

10/28



To solve the dual formulation of a SVM, usually the Sequential Minimal Optimization (SMO; John Platt, 1998) algorithm is used.

Before we introduce it, we start with the coordinate descent optimization algorithm.

Consider solving an unconstrained optimization problem

$$rg\min_{m{w}} L(w_1, w_2, \ldots, w_D).$$

Instead of the usual SGD approach, we could optimize the weights one by one, using the following algorithm:

- loop until convergence
 - \circ for i in $\{1, 2, \ldots, D\}$:
 - $lacksquare w_i \leftarrow rg\min_{w_i} L(w_1, w_2, \dots, w_D)$

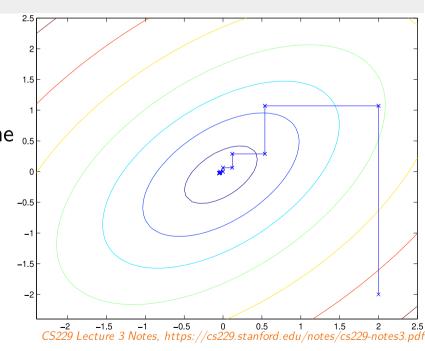


- loop until convergence
 - \circ for i in $\{1, 2, \ldots, D\}$:
 - $lacksquare w_i \leftarrow rg\min_{w_i} L(w_1, w_2, \dots, w_D)$

If the inner $arg \min$ can be performed efficiently, the coordinate descent can be fairly efficient.

Note that we might want to choose w_i in a different order, for example by trying to choose w_i providing the observed largest decrease of L.

The Kernel linear regression dual formulation with single-example batches was in fact trained by a coordinate descent – updating a single β_i corresponds to updating weights for a single example.





In soft-margin SVM, we try to maximize

$$\mathcal{L} = \sum
olimits_i a_i - rac{1}{2} \sum
olimits_i \sum
olimits_j a_i a_j t_i t_j K(oldsymbol{x}_i, oldsymbol{x}_j).$$

with respect to a_i , such that

$$orall i:C\geq a_i\geq 0 \ \ ext{and} \ \ \sum_i a_it_i=0.$$

The third KKT conditions of the solution, namely $a_i(t_iy(\boldsymbol{x}_i)+\xi_i-1)=0$ and $\mu_i\xi_i=0$, can be reformulated as the following equivalent implications (while assuming the rest of the KKT conditions, so $a_i\geq 0$, $t_iy(\boldsymbol{x}_i)\geq 1-\xi_i$, $\mu_i\geq 0$, $\xi_i\geq 0$):

$$egin{aligned} a_i > 0 \Rightarrow t_i y(m{x}_i) \leq 1, & ext{because } t_i y(m{x}_i) + \xi_i - 1 = 0 \Leftrightarrow t_i y(m{x}_i) \leq 1, \ a_i < C \Rightarrow t_i y(m{x}_i) \geq 1, & ext{because } \mu_i > 0 \Leftrightarrow a_i < C & ext{and } \xi_i = 0 \Leftrightarrow t_i y(m{x}_i) \geq 1. \end{aligned}$$

Note that when $0 < a_i < C$, we get $t_i y(\boldsymbol{x}_i) = 1$ by combining both the implications.



At its core, the SMO algorithm is just a coordinate descent.

It tries to find a_i maximizing \mathcal{L} while fulfilling the KKT conditions – once found, an optimum has been reached, given that for soft-margin SVM the KKT conditions are sufficient conditions for optimality (for soft-margin SVM, the loss is convex and the inequality constraints are not only convex but even affine).

However, note that because of the $\sum_i a_i t_i = 0$ constraint, we cannot optimize just one a_i , because a single a_i is determined from the others. Therefore, in each step, we pick two a_i, a_j coefficients and try to maximize the loss while fulfilling the constraints.

- ullet loop until convergence (until $orall \, i: a_i < C \Rightarrow t_i y(m{x}_i) \geq 1$ and $a_i > 0 \Rightarrow t_i y(m{x}_i) \leq 1$)
 - \circ for i in $\{1,2,\ldots,N\}$:
 - lacksquare choose j
 eq i in $\{1, 2, \dots, N\}$
 - $\blacksquare \ a_i, a_j \leftarrow rg \max_{a_i, a_j} \mathcal{L}(a_1, a_2, \dots, a_N)$, while respecting the constraints:
 - $lacksquare 0 \leq a_i \leq C$, $0 \leq a_i \leq C$, $\sum_i a_i t_i = 0$



The SMO is an efficient algorithm because we can compute the update to a_i, a_j efficiently, given that there exists a closed-form solution.

Assume that we are updating a_i and a_j . Then using the condition $\sum_k a_k t_k = 0$ we can write $a_i t_i = -\sum_{k \neq i} a_k t_k$. Given that $t_i^2 = 1$ and denoting $\zeta = -\sum_{k \neq i, k \neq j} a_k t_k$, we get

$$a_i = t_i(\zeta - a_j t_j).$$

Maximizing $\mathcal{L}(a)$ with respect to a_i and a_j then amounts to maximizing a quadratic function of a_i , which has an analytical solution.

Note that the real SMO algorithm employs several heuristics for choosing a_i, a_j such that the \mathcal{L} can be maximized the most.



Input: Dataset $(X \in \mathbb{R}^{N \times D}, t \in \{-1, 1\}^N)$, kernel K, regularization parameter C, tolerance tol, $max_passes_without_as_changing$ value

- Initialize $\boldsymbol{a} \leftarrow \boldsymbol{0}$, $b \leftarrow 0$, $passes \leftarrow 0$
- while $passes < max_passes_without_as_changing$ (or we run out of patience):
 - \circ $changed_as \leftarrow 0$
 - \circ for i in $1, 2, \ldots, N$:
 - $lacksquare E_i \leftarrow y(oldsymbol{x}_i) t_i$
 - lacksquare if $(a_i < C-tol)$ and $t_i E_i < -tol)$ or $(a_i > tol)$ and $t_i E_i > tol)$:
 - choose $j \neq i$ randomly
 - try updating a_i , a_j to maximize $\mathcal{L}(a_1, a_2, \ldots, a_N)$ such that $0 \leq a_k \leq C$ and $\sum_i a_i t_i = 0$; if successful, set b to fulfill the KKT conditions and set $changed_as \leftarrow changed_as + 1$
 - $\circ \ passes \leftarrow 0 \ ext{if} \ changed_as \ ext{else} \ passes + 1$

Demos



We already know that $a_i = t_i (\zeta - a_j t_j)$.

To find a_j maximizing \mathcal{L} , we use the formula for locating a vertex of a parabola

$$a_j^{ ext{new}} \leftarrow a_j - rac{\partial \mathcal{L}/\partial a_j}{\partial^2 \mathcal{L}/\partial a_i^2},$$

which is in fact one Newton-Raphson iteration step.

Denoting $E_i \stackrel{ ext{ iny def}}{=} y(oldsymbol{x}_i) - t_j$, we can compute the first derivative as

$$rac{\partial \mathcal{L}}{\partial a_i} = t_j (E_i - E_j),$$

and the second derivative as

$$egin{split} rac{\partial^2 \mathcal{L}}{\partial a_i^2} &= 2K(oldsymbol{x}_i,oldsymbol{x}_j) - K(oldsymbol{x}_i,oldsymbol{x}_i) - K(oldsymbol{x}_j,oldsymbol{x}_j) = -ig\|arphi(oldsymbol{x}_i) - arphi(oldsymbol{x}_j)ig\|^2 \leq 0. \end{split}$$



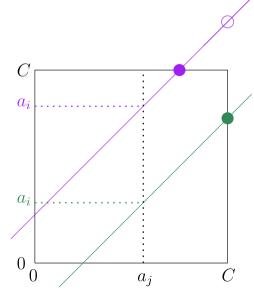
If the second derivative is strictly negative, we know that the vertex is really a maximum, in which case we get

$$a_j^{ ext{new}} \leftarrow a_j - t_j rac{E_i - E_j}{2K(oldsymbol{x}_i, oldsymbol{x}_j) - K(oldsymbol{x}_i, oldsymbol{x}_i) - K(oldsymbol{x}_i, oldsymbol{x}_j)}.$$

However, our maximization is constrained – it must hold that $0 \le a_i \le C$ and $0 \le a_j \le C$.

Recalling that $a_i = -t_i t_j a_j + \mathrm{const}$, we can plot the dependence of a_i and a_j . If for example $-t_i t_j = 1$ and $a_j^{\mathrm{new}} > C$, we need to find the "right-most" solution fulfilling both $a_i \leq C$ and $a_j \leq C$. Such a solution is either:

- ullet when a_i^{new} is clipped to C, as in the green case in the example,
- ullet when $a_j^{
 m new}$ is clipped so that $a_i^{
 m new}=C$ (the purple case in the example), in which case $a_i^{
 m new}=a_j+(C-a_i)$.



SMO

Demos



If we consider both $t_it_j=\pm 1$ and $a_j^{\rm new}<0$, $a_j^{\rm new}>C$, we get that the value maximizing the Lagrangian is $a_j^{\rm new}$ clipped to range [L,H], where

$$egin{aligned} t_i &= t_j \Rightarrow L = \max(0, a_i + a_j - C), H = \min(C, a_i + a_j) \ t_i &\neq t_j \Rightarrow L = \max(0, a_j - a_i), H = \min(C, C + a_j - a_i). \end{aligned}$$

After obtaining a_j^{new} we can compute a_i^{new} . Remembering that $a_i = -t_i t_j a_j + \text{const}$, we can compute it efficiently as

$$a_i^{ ext{new}} \leftarrow a_i - t_i t_j ig(a_j^{ ext{new}} - a_j ig).$$



20/28

To arrive at the bias update, we consider the KKT condition that for $0 < a_j^{\text{new}} < C$, it must hold that $1 = t_j y(\boldsymbol{x}_j) = t_j \left[\left(\sum_l a_l^{\text{new}} t_l K(\boldsymbol{x}_j, \boldsymbol{x}_l) \right) + b^{\text{new}} \right]$. Combining it with the fact that $\left(\sum_l a_l t_l K(\boldsymbol{x}_j, \boldsymbol{x}_l) \right) + b = E_j + t_j$, we obtain

$$b_i^{ ext{new}} = b - E_j - t_i(a_i^{ ext{new}} - a_i)K(oldsymbol{x}_i, oldsymbol{x}_j) - t_j(a_j^{ ext{new}} - a_j)K(oldsymbol{x}_j, oldsymbol{x}_j).$$

Analogously for $0 < a_i^{
m new} < C$ we get

$$b_i^{ ext{new}} = b - E_i - t_i(a_i^{ ext{new}} - a_i)K(oldsymbol{x}_i, oldsymbol{x}_i) - t_j(a_i^{ ext{new}} - a_j)K(oldsymbol{x}_j, oldsymbol{x}_i).$$

Finally, if $a_j^{\rm new}, a_i^{\rm new} \in \{0,C\}$ and $L \neq H$, it can be shown that all values between $b_i^{\rm new}$ and $b_j^{\rm new}$ fulfill the KKT conditions. We therefore arrive at the following update for the bias:

$$b^{ ext{new}} = egin{cases} b_i^{ ext{new}} & ext{if} \ 0 < a_i^{ ext{new}} < C, \ b_j^{ ext{new}} & ext{if} \ 0 < a_j^{ ext{new}} < C, \ (b_i^{ ext{new}} + b_j^{ ext{new}})/2 & ext{otherwise.} \end{cases}$$



Input: Dataset $(X \in \mathbb{R}^{N \times D}, t \in \{-1, 1\}^N)$, kernel K, regularization parameter C, tolerance tol, $max_passes_without_as_changing$ value

- Try updating a_i , a_j and b to fulfill the KKT conditions:
 - \circ Find a_j maximizing \mathcal{L} , in which we express a_i using a_j .
 - Such \mathcal{L} is a quadratic function of a_j .
 - If the second derivative of \mathcal{L} is not negative, stop.
 - \circ Clip a_j so that $0 \le a_i \le C$ and $0 \le a_j \le C$.
 - If we did not make enough progress (the new a_j is very similar), revert the value of a_j and stop.
 - \circ Compute corresponding a_i .
 - \circ Compute b appropriate for the updated a_i , a_j .

Primal versus Dual Formulation



Assume we have a dataset with N training examples, each with D features. Also assume the used feature map φ generates F features.

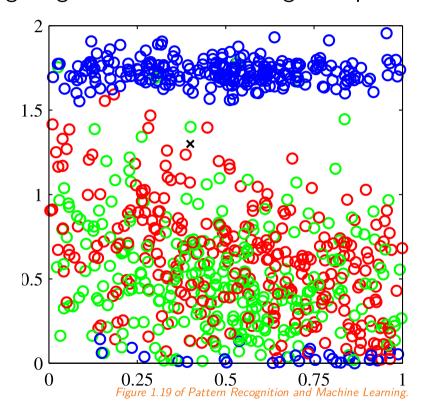
Property	Primal Formulation	Dual Formulation
Parameters	$oxed{F}$	N
Model size	$oldsymbol{F}$	$s \cdot D$ for s support vectors
Usual training time	$\Theta(e \cdot N \cdot F)$ for e epochs	between $\Omega(ND)$ and $\mathcal{O}(N^2D)$
Inference time	$\Theta(F)$	$\Theta(s\cdot D)$ for s support vectors

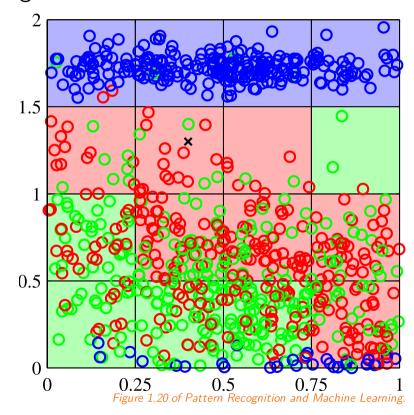
Hinge

SVM With RBF



The SVM algorithm with RBF kernel implements a better variant of the k-NN algorithm, weighting "evidence" of training data points according to their distance.





Multiclass SVM



There are two general approaches for building a K-class classifier by combining several binary classifiers:

- **one-versus-rest** scheme: K binary classifiers are constructed, the $i^{
 m th}$ separating instances of class i from all others; during prediction, the one with the highest probability is chosen the binary classifiers need to return calibrated probabilities (not SVM)
- **one-versus-one** scheme: $\binom{K}{2}$ binary classifiers are constructed, one for each (i,j) pair of class indices; during prediction, the class with the majority of votes wins (used by SVM)

However, voting suffers from serious difficulties, because when the binary classifiers are trained independently, usually large regions in the feature space receive tied votes (and such regions are then ambiguous).

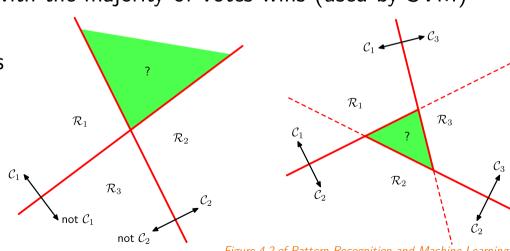


Figure 4.2 of Pattern Recognition and Machine Learning.

NPFL129. Lecture 7

Refresh

Soft-margin SVM

SMO

Hinge

Primal vs Dual

MultiSVM

SVR

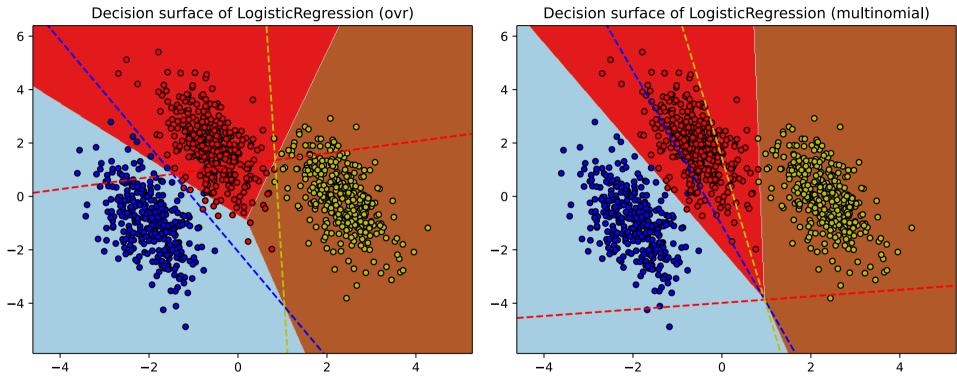
Demos

24/28

One-Versus-Rest Compared to Softmax Classification



25/28



https://scikit-learn.org/stable/auto_examples/linear_model/plot_logistic_multinomial.html https://scikit-learn.org/stable/auto_examples/linear_model/plot_logistic_multinomial.html

NPFL129, Lecture 7 Refresh Soft-margin SVM Hinge SMO Primal vs Dual MultiSVM

SVM For Regression



The idea of SVM for regression is to use an ε -insensitive error function

$$\mathcal{L}_{arepsilon}ig(t,y(oldsymbol{x})ig) = \maxig(0,|y(oldsymbol{x})-t|-arepsilonig).$$

The primary formulation of the loss is then

$$C\sum_{i}\mathcal{L}_{arepsilon}ig(t_{i},y(oldsymbol{x}_{i})ig)+rac{1}{2}\|oldsymbol{w}\|^{2}.$$

In the dual formulation, we require every training example to be within ε of its target, but introduce two slack variables $\boldsymbol{\xi}^-$, $\boldsymbol{\xi}^+$ to allow

$$C\sum(\xi_i^-+\xi_i^+)+rac{1}{2}\|oldsymbol{w}\|^2$$

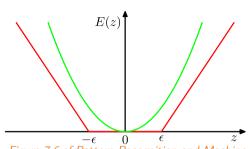
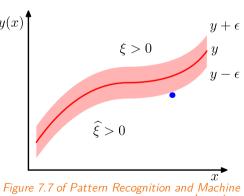


Figure 7.6 of Pattern Recognition and Machine



while requiring for every example $t_i - \varepsilon - \xi_i^- \le y(\boldsymbol{x}_i) \le t_i + \varepsilon + \xi_i^+$ for $\xi_i^- \ge 0, \xi_i^+ \ge 0$.

SMO

outliers. We therefore minimize the loss

SVM For Regression



The Lagrangian after substituting for $oldsymbol{w}$, b, $oldsymbol{\xi}^-$ and $oldsymbol{\xi}^+$ is

$$\mathcal{L} = \sum_i (a_i^+ - a_i^-) t_i - arepsilon \sum_i (a_i^+ + a_i^-) - rac{1}{2} \sum_i \sum_i (a_i^+ - a_i^-) (a_j^+ - a_j^-) K(m{x}_i, m{x}_j)$$

subject to

$$0 \leq a_i^+, a_i^- \leq C, \ \sum_i (a_i^+ - a_i^-) = 0.$$

The prediction is then given by

$$y(oldsymbol{z}) = \sum_i (a_i^+ - a_i^-) K(oldsymbol{z}, oldsymbol{x}_i) + b.$$

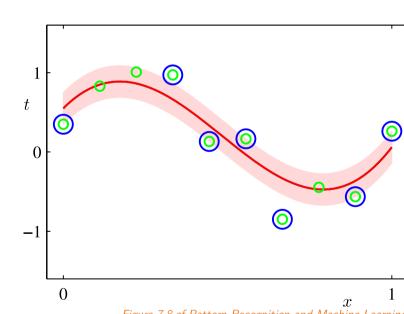


Figure 7.8 of Pattern Recognition and Machine Learning.





SVM Demos

https://cs.stanford.edu/~karpathy/svmjs/demo/

MLP Demos

- https://cs.stanford.edu/~karpathy/svmjs/demo/demonn.html
- https://playground.tensorflow.org

NPFL129, Lecture 7 Ref

Hinge