Support Vector Machines Machine Learning

Torsten Möller

- Chapter 7 + Appendix E of "Pattern Recognition and Machine Learning" by Bishop
- Chapter 12 of "The Elements of Statistical Learning" by Hastie, Tibshirani, Friedman

Outline

Maximum Margin Criterion

Math

Maximizing the Margin

Non-Separable Data

Linear Classification

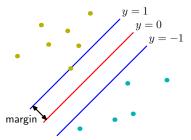
- Consider a two class classification problem
- Use a linear model

$$y(\boldsymbol{x}) = \boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}) + b$$

followed by a threshold function

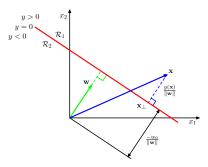
- For now, let's assume training data are linearly separable
 - Recall that the perceptron would converge to a perfect classifier for such data
 - But there are many such perfect classifiers

Max Margin



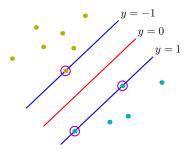
- We can define the margin of a classifier as the minimum distance to any example
- In support vector machines the decision boundary which maximizes the margin is chosen

Marginal Geometry



- Recall from Ch. 4
- Projection of $m{x}$ in $m{w}$ dir. is $\frac{m{w}^Tm{x}}{||m{w}||}$
- y(x) = 0 when $w^T x = -b$, or $\frac{w^T x}{||w||} = \frac{-b}{||w||}$
- So $\frac{w^Tx}{||w||} \frac{-b}{||w||} = \frac{y(x)}{||w||}$ is signed distance to decision boundary

Support Vectors



- Assuming data are separated by the hyperplane, distance to decision boundary is $\frac{t_n y(x_n)}{||x_n||}$
- The maximum margin criterion chooses w, b by:

$$\arg\max_{\boldsymbol{w},b} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$

Points with this min value are known as support vectors @Möller/Mori

• This optimization problem is complex:

$$\arg\max_{\boldsymbol{w},b} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$

- Note that rescaling $w \to \kappa w$ and $b \to \kappa b$ does not change distance $\frac{t_n y(x_n)}{||w||}$ (many equiv. answers)
- So for x_* closest to surface, can set:

$$t_*(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_*) + b) = 1$$

• All other points are at least this far away:

$$\forall n$$
 , $t_n(oldsymbol{w}^Toldsymbol{\phi}(oldsymbol{x}_n)+b)\geq 1$

$$\arg\max_{\boldsymbol{w},b} \frac{1}{||\boldsymbol{w}||} = \arg\min_{\boldsymbol{w},b} \frac{1}{2} ||\boldsymbol{w}||^2$$

• This optimization problem is complex:

$$\arg\max_{\boldsymbol{w},b} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$

- Note that rescaling $w \to \kappa w$ and $b \to \kappa b$ does not change distance $\frac{t_n y(x_n)}{||w||}$ (many equiv. answers)
- So for x_* closest to surface, can set:

$$t_*(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_*) + b) = 1$$

• All other points are at least this far away:

$$\forall n$$
 , $t_n(oldsymbol{w}^Toldsymbol{\phi}(oldsymbol{x}_n)+b)\geq 1$

$$\arg\max_{\boldsymbol{w},b}\frac{1}{||\boldsymbol{w}||}=\arg\min_{\boldsymbol{w},b}\frac{1}{2}||\boldsymbol{w}||^2$$

Canonical Representation

• This optimization problem is complex:

$$\arg\max_{\boldsymbol{w},b} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$

- Note that rescaling $w \to \kappa w$ and $b \to \kappa b$ does not change distance $\frac{t_n y(x_n)}{||w||}$ (many equiv. answers)
- So for x_* closest to surface, can set:

$$t_*(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_*) + b) = 1$$

• All other points are at least this far away:

$$\forall n \text{ , } t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b) \geq 1$$

$$\arg\max_{\boldsymbol{w},b} \frac{1}{||\boldsymbol{w}||} = \arg\min_{\boldsymbol{w},b} \frac{1}{2}||\boldsymbol{w}||^2$$

Canonical Representation

• This optimization problem is complex:

$$\arg\max_{\boldsymbol{w},b} \left\{ \frac{1}{||\boldsymbol{w}||} \min_{n} [t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b)] \right\}$$

- Note that rescaling $w \to \kappa w$ and $b \to \kappa b$ does not change distance $\frac{t_n y(x_n)}{||w||}$ (many equiv. answers)
- So for x_* closest to surface, can set:

$$t_*(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_*) + b) = 1$$

All other points are at least this far away:

$$\forall n \text{ , } t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b) \geq 1$$

$$\arg\max_{oldsymbol{w},b} rac{1}{||oldsymbol{w}||} = \arg\min_{oldsymbol{w},b} rac{1}{2}||oldsymbol{w}||^2$$

Canonical Representation

• So the optimization problem is now a constrained optimization problem:

$$\arg\min_{{\bm w},b}\frac{1}{2}||{\bm w}||^2$$
 $s.t.$ $\forall n$, $t_n({\bm w}^T{\bm \phi}({\bm x}_n)+b)\geq 1$

 To solve this, we need to take a detour into Lagrange multipliers

13

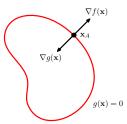
Outline

Maximum Margin Criterion

Math

Maximizing the Margin

Non-Separable Data

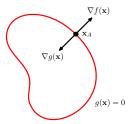


$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$
 s.t.
$$g(\boldsymbol{x}) = 0$$

- Points on q(x) = 0 must have $\nabla q(x)$ normal to surface
- A stationary point must have no change in f in the direction
 - So there must be some λ such that $\nabla f(x) + \lambda \nabla g(x) = 0$

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

- Stationary points of $L(x, \lambda)$ have
- So are stationary points Möller/Moristrained problem!

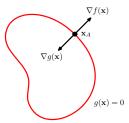


$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$
 s.t.
$$g(\boldsymbol{x}) = 0$$

- Points on $q(\mathbf{x}) = 0$ must have $\nabla q(\mathbf{x})$ normal to surface
- A stationary point must have no change in f in the direction • So there must be some λ such that $\nabla f(x) + \lambda \nabla g(x) = 0$

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

- Stationary points of $L(x, \lambda)$ have
- So are stationary points Möller/Moristrained problem!

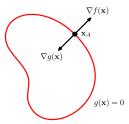


$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$
 s.t.
$$g(\boldsymbol{x}) = 0$$

- Points on $q(\mathbf{x}) = 0$ must have $\nabla q(\mathbf{x})$ normal to surface
- A stationary point must have no change in f in the direction of the surface, so $\nabla f(x)$ must also be in this same direction
 - So there must be some λ such that $\nabla f(x) + \lambda \nabla g(x) = 0$

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

- Stationary points of $L(x, \lambda)$ have
- So are stationary points Moller/Moristrained problem!

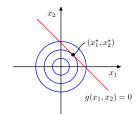


$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$
 s.t.
$$g(\boldsymbol{x}) = 0$$

- Points on $q(\mathbf{x}) = 0$ must have $\nabla q(\mathbf{x})$ normal to surface
- A stationary point must have no change in f in the direction of the surface, so $\nabla f(x)$ must also be in this same direction
 - So there must be some λ such that $\nabla f(x) + \lambda \nabla g(x) = 0$
- Define Lagrangian:

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

- Stationary points of $L(x, \lambda)$ have $\nabla_{\boldsymbol{x}} L(\boldsymbol{x}, \lambda) = \nabla f(\boldsymbol{x}) + \lambda \nabla g(\boldsymbol{x}) = 0$ and $\nabla_{\lambda}L(\boldsymbol{x},\lambda)=q(\boldsymbol{x})=0$
- So are stationary points of the destrained problem!



Consider the problem

$$\max_{x} f(x_1, x_2) = 1 - x_1^2 - x_2^2$$
s.t.
$$g(x_1, x_2) = x_1 + x_2 - 1 = 0$$

Lagrangian:

$$L(\mathbf{x}, \lambda) = 1 - x_1^2 - x_2^2 + \lambda(x_1 + x_2 - 1)$$

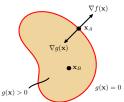
Stationary points require:

$$\partial L/\partial x_1 = -2x_1 + \lambda = 0$$

 $\partial L/\partial x_2 = -2x_2 + \lambda = 0$
 $\partial L/\partial \lambda = x_1 + x_2 - 1 = 0$

• So stationary point is $(x_1^*, x_2^*) = (\frac{1}{2}, \frac{1}{2}), \lambda = 1$ @Möller/Mori

Lagrange Multipliers - Inequality Constraints



Consider the problem:

$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$
s.t. $g(\boldsymbol{x}) \ge 0$

 Optimization over a region – solutions either at stationary points (gradients 0) in region or on boundary

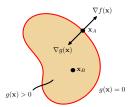
$$L(x,\lambda) = f(x) + \lambda g(x)$$

- Solutions have either:
 - $\nabla f(x) = 0$ and $\lambda = 0$ (in region), or

Math

- $\nabla f(x) = -\lambda \nabla g(x)$ and $\lambda > 0$ (on boundary, > for maximizing f).
- For both, $\lambda g(x) = 0$
- Solutions have $g(x) \ge 0, \lambda \ge 0, \lambda g(x) = 0$

Lagrange Multipliers - Inequality Constraints



Consider the problem:

$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$

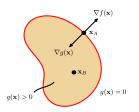
$$s.t. \qquad g(\boldsymbol{x}) \ge 0$$

 Optimization over a region – solutions either at stationary points (gradients 0) in region or on boundary

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

- Solutions have either:
 - $\nabla f(x) = 0$ and $\lambda = 0$ (in region), or
 - $\nabla f(x) = -\lambda \nabla g(x)$ and $\lambda > 0$ (on boundary, > for maximizing f).
 - For both, $\lambda g(x) = 0$
- Solutions have $g(\boldsymbol{x}) \geq 0, \lambda \geq 0, \lambda g(\boldsymbol{x}) = 0$

Lagrange Multipliers - Inequality Constraints



Consider the problem:

$$\max_{\boldsymbol{x}} f(\boldsymbol{x})$$

$$s.t.$$
 $g(\mathbf{x}) \geq 0$

 Exactly how does the Lagrangian relate to the optimization problem in this case?

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

It turns out that the solution to optimization problem is:

$$\max_{\boldsymbol{x}} \min_{\lambda \geq 0} L(\boldsymbol{x}, \lambda)$$

Max-min

Lagrangian

$$L(\boldsymbol{x}, \lambda) = f(\boldsymbol{x}) + \lambda g(\boldsymbol{x})$$

• Consider the following:

$$\min_{\lambda \geq 0} L(\boldsymbol{x}, \lambda)$$

- If the constraint $g(x) \ge 0$ is not satisfied, g(x) < 0
 - Hence, λ can be made ∞ , and $\min_{\lambda \geq 0} L(\boldsymbol{x}, \lambda) = -\infty$
- Otherwise, $\min_{\lambda \geq 0} L(x, \lambda) = f(x)$, (with $\lambda = 0$)
- Hence,

$$\min_{\lambda \geq 0} L(\boldsymbol{x}, \lambda) = \left\{ \begin{array}{ll} -\infty & \text{constraint not satisfied} \\ f(\boldsymbol{x}) & \text{otherwise} \end{array} \right.$$

23

Min-max (Dual form)

So the solution to optimization problem is:

$$L_P(\boldsymbol{x}) = \max_{\boldsymbol{x}} \min_{\lambda \ge 0} L(\boldsymbol{x}, \lambda)$$

which is called the primal problem

 The dual problem is when one switches the order of the max and min:

$$L_D(\lambda) = \min_{\lambda \ge 0} \max_{\boldsymbol{x}} L(\boldsymbol{x}, \lambda)$$

- These are not the same, but it is always the case the dual is a bound for the primal (in the SVM case with minimization, $L_D(\lambda) \leq L_P(\boldsymbol{x})$
- Slater's theorem gives conditions for these two problems to be equivalent, with $L_D(\lambda) = L_P(x)$.
- Slater's theorem applies for the SVM optimization problem, and solving the dual leads to kernelization and can be easier than solving the primal

24

Outline

Maximum Margin Criterion

Math

Maximizing the Margin

Non-Separable Data

 So the optimization problem is now a constrained optimization problem:

$$rg\min_{m{w},b}rac{||m{w}||^2}{2} \ s.t. \qquad orall n$$
 , $t_n(m{w}^Tm{\phi}(m{x}_n)+b)\geq 1$

• For this problem, the Lagrangian (with N multipliers a_n) is:

$$L(\boldsymbol{w}, b, \boldsymbol{a}) = \frac{||\boldsymbol{w}||^2}{2} - \sum_{n=1}^{N} a_n \left\{ t_n(\boldsymbol{w}^T \boldsymbol{\phi}(\boldsymbol{x}_n) + b) - 1 \right\}$$

• We can find the derivatives of L wrt w, b and set to 0:

$$oldsymbol{w} = \sum_{n=1}^{N} a_n t_n oldsymbol{\phi}(oldsymbol{x}_n)$$
 $0 = \sum_{n=1}^{N} a_n t_n$

Dual Formulation

 Plugging those equations into L removes w and b results in a version of L where ∇w,bL = 0:

$$\tilde{L}(\boldsymbol{a}) = \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m \boldsymbol{\phi}(\boldsymbol{x}_n)^T \boldsymbol{\phi}(\boldsymbol{x}_m)$$

this new \tilde{L} is the dual representation of the problem (maximize with constraints)

- Note that it is kernelized
- It is quadratic, convex in a
- ullet Bounded above since $oldsymbol{K}$ positive semi-definite
- Optimal a can be found
 - With large datasets, descent strategies employed

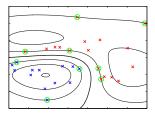
From a to a Classifier

- We found a optimizing something else
- This is related to classifier by

$$egin{array}{lll} oldsymbol{w} &=& \sum_{n=1}^N a_n t_n oldsymbol{\phi}(oldsymbol{x}_n) \ &=& oldsymbol{w}^T oldsymbol{\phi}(oldsymbol{x}) + b = \sum_{n=1}^N a_n t_n k(oldsymbol{x}, oldsymbol{x}_n) + b \end{array}$$

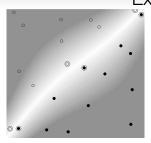
- Recall $a_n\{t_ny(x_n)-1\}=0$ condition from Lagrange
 - Either $a_n = 0$ or x_n is a support vector
- a will be sparse many zeros
 - Don't need to store x_n for which $a_n = 0$
- Another formula for finding b

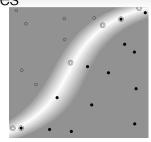
28



- SVM trained using Gaussian kernel
- Support vectors circled
- Note non-linear decision boundary in x space

Maximizing the Margin





- From Burges, A Tutorial on Support Vector Machines for Pattern Recognition (1998)
- SVM trained using cubic polynomial kernel $k(x_1, x_2) = (x_1^T x_2 + 1)^3$
- Left is linearly separable
 - Note decision boundary is almost linear, even using cubic polynomial kernel
- Right is not linearly separable
 - But is separable using polynomial kernel @Möller/Mori

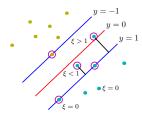
Outline

Maximum Margin Criterion

Math

Maximizing the Margin

Non-Separable Data



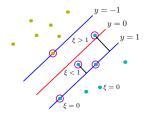
- For most problems, data will not be linearly separable (even in feature space φ)
- · Can relax the constraints from

$$t_n y(\boldsymbol{x}_n) \geq 1$$
 to $t_n y(\boldsymbol{x}_n) \geq 1 - \xi_n$

- The $\xi_n > 0$ are called slack variables
 - $\xi_n = 0$, satisfy original problem, so x_n is on margin or correct side of margin
 - $0 < \xi_n < 1$, inside margin, but still correctly classifed
 - $\xi_n > 1$, mis-classified

32

Loss Function For Non-separable Data



 Non-zero slack variables are bad, penalize while maximizing the margin:

$$\min C \sum_{n=1}^{N} \xi_n + \frac{1}{2} ||\boldsymbol{w}||^2$$

- Constant C>0 controls importance of large margin versus incorrect (non-zero slack)
 - Set using cross-validation
- Optimization is same quadratic, different constraints, convex

SVM Loss Function

• The SVM for the separable case solved the problem:

$$\arg\min_{\pmb{w}} \frac{1}{2} ||\pmb{w}||^2$$

$$s.t. \qquad \forall n \text{ , } t_n y_n \geq 1$$

Can write this as:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{\infty}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where $E_{\infty}(z) = 0$ if $z \geq 0$, ∞ otherwise

Non-separable case relaxes this to be:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{SV}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where
$$E_{SV}(t_ny_n-1)=[1-y_nt_n]_+$$
 hinge loss • $[u]_+=u$ if $u\geq 0$, 0 otherwise

©MöllerMori

SVM Loss Function

• The SVM for the separable case solved the problem:

$$\arg\min_{\pmb{w}} \frac{1}{2} ||\pmb{w}||^2$$

$$s.t. \qquad \forall n \text{ , } t_n y_n \geq 1$$

Can write this as:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{\infty}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where $E_{\infty}(z) = 0$ if $z \ge 0$, ∞ otherwise

Non-separable case relaxes this to be:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{SV}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where
$$E_{SV}(t_ny_n-1)=[1-y_nt_n]_+$$
 hinge loss • $[u]_+=u$ if $u\geq 0$, 0 otherwise

©Möller/Mori

SVM Loss Function

• The SVM for the separable case solved the problem:

$$\arg\min_{\pmb{w}} \frac{1}{2} ||\pmb{w}||^2$$

$$s.t. \qquad \forall n \text{ , } t_n y_n \geq 1$$

Can write this as:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{\infty}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where $E_{\infty}(z) = 0$ if $z \geq 0$, ∞ otherwise

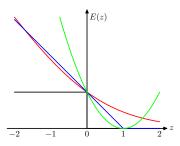
Non-separable case relaxes this to be:

$$\arg\min_{\boldsymbol{w}} \sum_{n=1}^{N} E_{SV}(t_n y_n - 1) + \lambda ||\boldsymbol{w}||^2$$

where $E_{SV}(t_n y_n - 1) = [1 - y_n t_n]_+$ hinge loss

• $[u]_+ = u$ if $u \ge 0$, 0 otherwise $u \ge 0$ otherwise

Loss Functions



- Linear classifiers, compare loss function used for learning
 - Black is misclassification error
 - Simple linear classifier, squared error: $(y_n t_n)^2$
 - Logistic regression, cross-entropy error: $t_n \ln y_n$
 - SVM, hinge loss: $\xi_n = [1 y_n t_n]_+$

Non-Separable Data

Conclusion

- Readings: Ch. 7 up to and including Ch. 7.1.2
- Maximum margin criterion for deciding on decision boundary
 - Linearly separable data
- Relax with slack variables for non-separable case
- Global optimization is possible in both cases
 - Convex problem (no local optima)
 - Descent methods converge to global optimum
- Kernelized