INF 4300 – Support Vector Machine Classifiers (SVM)
Anne Solberg (anne@ifi.uio.no)
19.10.17

• Linear classifiers with maximum margin for two-class problems
• The kernel trick – from linear to a high-dimensional generalization
• Generation from 2 to M classes
• Practical issues
Curriculum

- Lecture foils are most important!
- The lectures are based on selected sections from Pattern Recognition, Third Edition, by Theodoridis and Koutroumbas:
  - 3.1-3.2, 3.7 (but 3.7.3 is a SVM-variant that we will skip)
  - 4.17
  - These sections use optimization theory described in Appendix C. We only include enough mathematics to state the optimization problem, and you are not required to understand how this optimization is solved.
  - Another useful note: Andrew Ng’s note http://cs229.stanford.edu/notes/cs229-notes3.pdf
Classification approaches

- Fit a parametric probability density function to the data and classify to the class that maximize the posterior probability.
- Knn-classification: use a non-parametric model.
- Other approaches to linear classification:
  - Logistic regression and Softmax (generalization to multiple classes) (INF 5860)
  - Feedforward neural net (INF 5860)
  - Support Vector Machine classification (today)
Linear algebra basics:
Inner product between two vectors.

- The inner product (or dot product) between two vectors (of length N) $a$ and $b$ or is given by
  \[
  \langle a, b \rangle = \sum_{i=1}^{N} a_i b_i = a^T b
  \]

- The angle between two vectors $A$ and $B$ is defined as:
  \[
  \cos \theta = \frac{\langle A, B \rangle}{\|A\|\|B\|}
  \]

- If the inner product of two vectors is zero, they are normal to each other.
From last week: Case 1: $\Sigma_j = \sigma^2 I$

- Now we get an equivalent formulation of the discriminant functions:

$$g_i(x) = w'_i x + w_{i0}$$

where $w_i = \frac{1}{\sigma^2} \mu_i$ and $w_{i0} = -\frac{1}{2\sigma^2} \mu'_i \mu_i + \ln P(\omega_i)$

- An equation for the decision boundary $g_i(x) = g_j(x)$ can be written as

$$w'(x - x_0) = 0$$

where $w = \mu_i - \mu_j$

and $x_0 = \frac{1}{2} (\mu_i - \mu_j) - \frac{\sigma^2}{\| \mu_i - \mu_j \|^2} \ln \frac{P(\omega_i)}{P(\omega_j)} (\mu_i - \mu_j)$

- $w = \mu_i - \mu_j$ is the vector between the mean values.

- This equation defines a hyperplane through the point $x_0$, and orthogonal to $w$. 
Gaussian model with $\Sigma=\sigma I$

Linear decision boundary

- We found that the discriminant function (when $\Sigma_j=\sigma^2 I$) that defines the border between class 1 and 2 in the feature space is a straight line.
- The discriminant function intersects the line connecting the two class means at the point $c=(\mu_1 - \mu_2)/2$ (if we do not consider prior probabilities).
- The discriminant function will also be normal to the line connecting the means.
Introduction to Support Vector Machine classifiers

• To understand Support Vector Machine (SVM) classifiers, we need to study the linear classification problem in detail.
• We will need to see how classification using this (the linear case on the previous slide) can be computed using inner products.
• We start with two linearly separable classes.
• Extension to two non-separable classes.
• Extension to M classes.
• The last step will be to use kernels to separate classes that cannot be separated in the input space.
A new view at linear classification using inner products

- We have two classes (+ and -) represented by the class means $c_+$ and $c_-$.  
- Let the feature vector be $x_i$, and let $y_i$ be the class of feature vector $i$.  
- If we have $m_+$ samples from class + and $m_-$ samples from class -, the class means are given by:
  
  $c_+ = \frac{1}{m_+} \sum_{i\{y_i=+\}} x_i$

  $c_- = \frac{1}{m_-} \sum_{i\{y_i=-\}} x_i$

- A new pattern $x$ should be classified to the class with the closest mean.
• Half way between the means lies the point $c=(c_++c_-)/2$.

We can compute the class of a new sample $x$ by checking whether the vector $x-c$ (connecting $x$ to $c$) encloses an angle smaller than $\pi/2$ (in terms of absolute value) with the vector $w=c_+-c_-$. This angle is given by the inner product between $w$ and $x-c$: $w^T(x-c)$.

• If a point $x$ is on the decision boundary hyperplane, then $w^Tx=0$.

• The angle between two vectors is computed by the inner product, which changes sign as the angle passes through $\pi/2$. 
Support Vector Machines
Two linear separable classes

- Let $x_i$, $i=1,...,N$ be all the $l$-dimensional feature vectors in a training set with $N$ samples.
- These belong to one of two classes, $\omega_1$ and $\omega_2$.
- We assume that the classes are **linearly separable**.
- This means that a hyperplane
  \[ g(x) = w^T x + w_0 = 0 \]
  correctly classifies all these training samples.
- $w = [w_1,...,w_l]$ is called a weight vector, and $w_0$ is the threshold.
Introduction to linear SVM

- Discriminant function:
  \[ g(x) = \mathbf{w}^T \mathbf{x} + w_0 \]

- Two-class problem, \( y_i \in \{-1, 1\} \)

- \( y_i = \begin{cases} 
  -1, & g(\mathbf{x}_i) < 0 \\
  1, & g(\mathbf{x}_i) > 0 
\end{cases} \)
Separable case: Many candidates

- Obviously we want the decision boundary to separate the classes..

- .. however, there can be many such hyperplanes.

- Which of these two candidates would you prefer? Why?
Distance to the decision boundary

- Since $w/||w||$ is a unit vector in the direction $w$,

$$B = x - z*\frac{w}{||w||}$$

- Because $B$ lies on the decision boundary,

$$w^T B + w_0 = 0$$

Solve this for $z$:

$$z = \frac{w^T x + w_0}{||w||} = \left(\frac{w}{||w||}\right)^T x + \frac{w_0}{||w||}$$

This is called the **margin** of the classifier

Distance from $x$ to the decision boundary
Hyperplanes and margins

• If both classes are equally probable, the **distance from the hyperplane to the closest points** in both classes should be equal. This is called the margin.

• The margin for «direction 1» is \(2z_1\), and for «direction 2» it is \(2z_2\).

• From previous slide; the distance from a point to the separating hyperplane is

\[
z = \frac{|g(x)|}{\|w\|}
\]

**Goal:** Find \(w\) and \(w_0\) maximizing the margin!

How would you write a program finding this? Not easy unless we state the objective function cleverly!
Towards a clever objective function

- We can scale $g(x)$ such that $g(x)$ will be equal to 1 or -1 at the closest points in the two classes. This is equivalent to:

1. Have a margin of $\frac{1}{||w||} + \frac{1}{||w||} = 2$

2. Require that
   
   $$g(x) = w^T x + w_0 \geq 1, \quad \forall x \in \omega_1$$
   $$g(x) = w^T x + w_0 \leq -1, \quad \forall x \in \omega_2$$

Remember our goal: Find $w$ and $w_0$ yielding the maximum margin.

Does not change the margin
Maximum-margin objective function

The hyperplane with maximum margin can be found by solving the optimization problem (w.r.t. $w$ and $w_0$):

\[
\begin{align*}
\text{minimize} & \quad J(w) = \frac{1}{2} \|w\|^2 \\
\text{subject to} & \quad y_i (w^T x_i + w_0) \geq 1, \quad i = 1,2,...,N
\end{align*}
\]

Note: We assume fully class-separable data!

Checkpoint: Do you understand the formulation?
How is this criterion related to maximizing the margin?

Note! We are somewhat done -- Matlab (or similar software) can solve this now.
But we seek more insight!
More on the optimization problem

Generalized Lagrangian function:

\[
\mathcal{L}(w, w_0, \lambda) = \frac{1}{2} w^T w - \sum_{i=1}^{N} \lambda_i [y_i (w^T x_i + w_0) - 1]
\]

We recommend, again, to read the note on Lagrangian multipliers (see *undervisningsplan*).

\[\begin{align*}
\frac{\partial}{\partial w} \mathcal{L}(w, w_0, \lambda) &= 0 \\
\frac{\partial}{\partial w_0} \mathcal{L}(w, w_0, \lambda) &= 0 \\
\lambda_i &\geq 0, \quad i = 1, 2, \ldots, N \\
\lambda_i [y_i (w^T x_i + w_0) - 1] &= 0, \quad i = 1, 2, \ldots, N \\
\sum_{i=1}^{N} \lambda_i y_i &= 0
\end{align*}\]

Either \( \lambda_i = 0 \) or \( g(x) = 1 \)

Karush-Kuhn-Tucker (KKT) conditions

[INF 4300 17]
Support vectors

- The feature vectors $x_i$ with a corresponding $\lambda_i > 0$ are called the support vectors for the problem.

- The classifier defined by this hyperplane is called a Support Vector Machine.

- Depending on $y_i$ (+1 or -1), the support vectors will thus lie on either of the two hyperplanes $w^T x + w_0 = \pm 1$

- The support vectors are the points in the training set that are closest to the decision hyperplane.

- The optimization has a unique solution, only one hyperplane satisfies the conditions.
Dual representation

- Plugging back into $L(w, w_0, \lambda)$ gives us

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

$$\sum_{i=1}^{N} \lambda_i y_i = 0$$

$$\max_{\lambda} \left( \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j} \lambda_i \lambda_j y_i y_j x_i^T x_j \right)$$

s.t. $$\sum_{i=1}^{N} \lambda_i y_i = 0$$

$$\lambda_i \geq 0 \forall i$$

Important (for later):
The samples come into play as inner products only!
The nonseparable case

- If the two classes are nonseparable, a hyperplane satisfying the conditions $w^T x - w_0 = \pm 1$ cannot be found.

- The feature vectors in the training set are now either:
  1. Vectors that fall outside the band and are correctly classified.
  2. Vectors that are inside the band and are correctly classified. They satisfy $0 \leq y_i (w^T x + w_0) < 1$
  3. Vectors that are misclassified – expressed as $y_i (w^T x + w_0) < 0$
• The three cases can be treated under a single type of constraints if we introduce slack variables $\xi_i$:

$$y_i[w^T x + w_0] \geq 1 - \xi_i$$

- The first category (outside, correct classified) have $\xi_i=0$
- The second category (inside, correct classified) have $0 \leq \xi_i \leq 1$
- The third category (inside, misclassified) have $\xi_i > 1$

• The optimization goal is now *to keep the margin as large as possible and the number of points with $\xi_i > 0$ as small as possible.*
Cost function – nonseparable case

• The cost function to minimize is now

\[
J(w, w_0, \xi) = \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} I(\xi_i)
\]

where \( I(\xi_i) = \begin{cases} 
1 & \xi_i > 0 \\
0 & \xi_i = 0
\end{cases} \)

and \( \xi \) is the vector of parameters \( \xi_i \).

• \( C \) is a parameter that controls how much misclassified training samples is weighted.

• We skip the mathematics and present the alternative dual formulation:

\[
\max_{\lambda} \left( \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j} \lambda_i \lambda_j y_i y_j x_i^T x_j \right)
\]

subject to \( \sum_{i=1}^{N} \lambda_i y_i = 0 \) and \( 0 \leq \lambda_i \leq C \ \forall i \)

• All points between the two hyperplanes \((\xi_i > 0)\) can be shown to have \( \lambda_i = C \).
Nonseparable vs. separable case

• Note that the slack variables $\xi_i$ does not enter the problem explicitly.
• The only difference between the linear separable and the non-separable case is that the Lagrange-multipliers are bounded by $C$.
• Training a SVM classifier consists of solving the optimization problem.
  – The problem is quite complex since it grows with the number of training pixels.
  – It is computationally heavy.
  – We will get back with hints of software libraries to use at the end of the lecture....
An example – the effect of C

- C is the misclassification cost.

- Selecting too high C will give a classifier that fits the training data perfect, but fails on different data set.

- The value of C should be selected using a separate validation set. Separate the training data into a part used for training, train with different values of C and select the value that gives best results on the validation data set. Then apply this to new data or the test data set. (explained later)
SVM: A geometric view

- SVMs can be related to the convex hull of the different classes. Consider a class that contains training samples \( X = \{x_1, \ldots, x_N\} \).
- The convex hull of the set of points in \( X \) is given by all convex combinations of the \( N \) elements in \( X \).

  - A region \( R \) is convex if and only if for any two points \( x_1, x_2 \) in \( R \), the whole line segment between \( x_1 \) and \( x_2 \) is inside the \( R \).
  - The convex hull of a region is the smallest convex region \( H \) which satisfies the conditions \( R \subseteq H \).
The convex hull for a class is the smallest convex set that contains all the points in the class (X).

Searching for the hyperplane with the highest margin is equivalent to searching for the two nearest points in the two convex sets.

- This can be proved, but we just take the result as an aid to get a better visual interpretation of the SVM hyperplane.
Reduced convex hull

- To get a useable interpretation for nonseparable classes, we need the reduced convex hull.
- The convex set can be expressed as:

\[ \text{conv}\{X\} = \{ y : y = \sum_{i=1}^{N} \lambda_i x_i : x_i \in X, \sum_{i=1}^{N} \lambda_i = 1, \ 0 \leq \lambda_i \leq 1 \} \]

- The **reduced convex hull** is:

\[ R\{X, \mu\} = \{ y : y = \sum_{i=1}^{N} \lambda_i x_i : x_i \in X, \sum_{i=1}^{N} \lambda_i = 1, \ 0 \leq \lambda_i \leq \mu \} \]

Here we add a restriction that \( \lambda_i \) must also be smaller than \( \mu \)

- \( \mu \) is a scalar between 0 and 1. \( \mu = 1 \) gives the regular convex hull.
Reduced convex hull - example

- Data set with overlapping classes.
- For small enough values of $\mu$, we can make the two reduced convex hulls non-overlapping.
- A very rough explanation of the non-separable SVM problem is that a value of $\mu$ that gives non-intersecting reduced convex hulls must be found.
- Given a value of $\mu$ that gives non-intersecting reduced convex hulls, the best hyperplane will bisect the line between the closest points in these two reduced convex hulls.
Relating $\mu$ and C

- Given a value of $\mu$ that gives non-intersecting reduced convex hulls, find the hyperplane by finding the closest two points in the two sets.
- Several values of $\mu$ can give nonintersecting reduced hulls.
- $\mu$ is related to $C$, the cost of misclassifying training regions (see page 101).
- A high $C$ will give regions that just barely give nonintersecting regions.
- The most robust considering a validation data set is probably a smaller value of $C$ (and $\mu$).
Checkpoint

• What does this criterion mean:

\[ J(w, w_0, \xi) = \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} I(\xi_i) \]

where

\[ I(\xi_i) = \begin{cases} 1 & \xi_i > 0 \\ 0 & \xi_i = 0 \end{cases} \]

and \( \xi \) is the vector of parameters \( \xi_i \).

• Which points are the support vectors in the linear case?
SVMs: The nonlinear case intro.

- The training samples are $l$-dimensional vectors; we have until now tried to find a linear separation in this $l$-dimensional feature space.

- This seems quite limiting.

- What if we increase the dimensionality (map our samples to a higher dimensional space) before applying our SVM?

- Perhaps we can find a better linear decision boundary in that space? Even if the feature vectors are not linearly separable in the input space, they might be (close to) separable in a higher dimensional space.
An example: from 2D to 3D

- Let \( \mathbf{x} \) be a 2D vector \( \mathbf{x} = [x_1, x_2] \).

- In the toy example on the right, the two classes cannot be linearly separated in the original 2D space.

- Consider now the transformation

\[
\mathbf{y} = \begin{bmatrix}
x_1^2 \\
\sqrt{2} x_1 x_2 \\
x_2^2
\end{bmatrix}
\]

- Now, the transformed points in this 3D space can be separated by a plane.

- The separating plane in 3D maps out an ellipse in the original 2D space.

Cf. next slide, note that 
\( y_i^T y_j = (x_i^T x_j)^2 \).
SVMs and kernels

- Note that in both the optimization problem and the evaluation function, \( g(x) \), the samples come into play as inner products only.

\[
\max_{\lambda} \left( \sum_{i=1}^{N} \lambda_i - \frac{1}{2} \sum_{i,j} \lambda_i \lambda_j y_i y_j x_i^T x_j \right)
\]

\[
\text{s.t. } 0 \leq \lambda_i \leq C \ \forall \ i
\]

\[
\sum_{i=1}^{N} \lambda_i y_i = 0
\]

- If we have a function evaluating inner products, \( K(x_i, x_j) \), we can ignore the samples themselves.

- Let’s say we have \( K(x_i, x_j) \) evaluating inner products in a higher dimensional space:

  -> no need to do the mapping of our samples explicitly!

\[
g(x) = w^T x + w_0
\]

\[
= \sum_{i=1}^{N} \lambda_i y_i x_i^T x + w_0
\]

Called «kernel»
Useful kernels for classification

- **Polynomial kernels**
  \[ K(x, z) = (x^T z - 1)^q, \quad q > 0 \]

- **Radial basis function kernels** (very commonly used!)
  \[ K(x, z) = \exp\left(-\frac{\|x - z\|^2}{\sigma^2}\right) \]
  Note the we need to set the \( \sigma \) parameter
  The «support» of each point is controlled by \( \sigma \).

- **Hyperbolic tangent kernels** (often with \( \beta=2 \) and \( \gamma=1 \))
  \[ K(x, z) = \tanh(\beta x^T z + \gamma) \]
  The kernel inputs need not be numeric, e.g. kernels for text strings are possible.
  The kernels give inner-product evaluations in the, possibly infinite-dimensional, transformed space.
The kernel formulation of the objective function

- Given the appropriate kernel (e.g. «radial» with width $\sigma$) and the cost of misclassification $C$, the optimization task is:

$$
\max_\lambda \left( \sum_i \lambda_i - \frac{1}{2} \sum_{i,j} \lambda_i \lambda_j y_i y_j K(x_i, x_j) \right)
$$

subject to $0 \leq \lambda_i \leq C, \ i = 1, \ldots, N$

$$
\sum_i \lambda_i y_i = 0
$$

- The resulting classifier is:

assign $x$ to class $\omega_1$ if $g(x) = \sum_{i=1}^{N} \lambda_i y_i K(x_i, x) + w_0 > 0$ and to class $\omega_2$ otherwise
Example of nonlinear decision boundary

- This illustrates how the nonlinear SVM might look in the original feature space
- RBF kernel used

Figure 4.23 in PR by Teodoridis et.al.
From 2 to M classes

• All we have discussed up until now involves only separating 2 classes. How do we extend the methods to M classes?

• Two common approaches:
  – One-against-all
    • For each class m, find the hyperplane that best discriminates this class from all other classes. Then classify a sample to the class having the highest output. (To use this, we need the VALUE of the inner product and not just the sign.)
  – Compare all sets of pairwise classifiers
    • Find a hyperplane for each pair of classes. This gives M(M-1)/2 pairwise classifiers. For a given sample, use a voting scheme for selecting the most-winning class.
How to use a SVM classifier

- Find a library with all the necessary SVM-functions 😊
  - For example LibSVM  http://www.csie.ntu.edu.tw/~cjlin/libsvm/
  - Or use the PRTools toolbox http://www.37steps.com/prtools/
- Read the introductory guides.
- Often a radial basis function kernel is a good starting point.
- Scale the data to the range [-1,1] (features with large values will not dominate).
- Find the optimal values of C and $\sigma$ by performing a grid search on selected values and using a validation data set.
- Train the classifier using the best value from the grid search.
- Test using a separate test set.
How to do a grid search

• Use n-fold cross validation (e.g. 10-fold cross-validation).
  – 10-fold: divide the training data into 10 subsets of equal size. Train on 9 subsets and test on the last subset. Repeat this procedure 10 times.
• Grid search: try pairs of \((C, \sigma)\). Select the pair that gets the best classification performance on average over all the n validation test subsets.
• Use the following values of C and \(\sigma\):
  • \(C = 2^{-5}, 2^{-3}, ..., 2^{15}\)
  • \(\sigma = 2^{-15}, 2^{-13}, ..., 2^{3}\)
Summary / Learning goals

• Understand enough of SVM classifiers to be able to use it for a classification application.
  – Understand the basic linear separable problem and what the meaning of the solution with the largest margin is.
  – Understand how SVMs work in the non-separable case using a cost for misclassification.
  – Accept the kernel trick: that the original feature vectors can be transformed into a higher dimensional space, and that linear SVM is applied in this space without explicitly doing the feature transform.
  – Know briefly how to extend from 2 to M classes.
  – Know which parameters (C, etc.) the user must specify and how to perform a grid search for these.
  – Be able to find a SVM library and use it correctly.