Support Vector Machines

www.cs.wisc.edu/~dpage

Goals for the lecture

you should understand the following concepts

- the margin
- slack variables
- the linear support vector machine
- nonlinear SVMs
- the kernel trick
- the primal and dual formulations of SVM learning
- support vectors
- the kernel matrix
- valid kernels
- polynomial kernel
- Gausian kernel
- string kernels
- support vector regression

Algorithm You Should Know

- SVM as constrained optimization
 - Fit training data and maximize margin
 - Primal and dual formulations
 - Kernel trick
 - Slack variables to allow imperfect fit
 - For now, assuming optimizer is black box
- Next lecture will look inside black box: sequential minimal optimization (SMO)



Burr Settles, UW CS PhD

Four key SVM ideas

- Maximize the margin don't choose just *any* separating hyperplane
- Penalize misclassified examples use soft constraints and slack variables
- Use optimization methods to find model linear programming quadratic programming

• Use kernels to represent nonlinear functions and handle complex instances (sequences, trees, graphs, etc.)







Some key vector concepts

the *dot product* between two vectors *w* and *x* is defined as:

$$\boldsymbol{w} \cdot \boldsymbol{x} = \boldsymbol{w}^{\mathsf{T}} \boldsymbol{x} = \sum_{i} w_{i} x_{i}$$

for example

$$\begin{bmatrix} 1 \\ 3 \\ -5 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -2 \\ -1 \end{bmatrix} = (1)(4) + (3)(-2) + (-5)(-1) = 3$$

the 2-norm (Euclidean length) of a vector *x* is defined as:

$$\left|\left|\boldsymbol{x}\right|\right|_{2} = \sqrt{\sum_{i} \left|\boldsymbol{x}_{i}\right|^{2}}$$

Linear separator learning revisited

suppose we encode our classes as $\{-1, +1\}$ and consider a linear classifier

$$h(\boldsymbol{x}) = \begin{cases} 1 \text{ if } \left(\sum_{i=1}^{n} w_i x_i\right) + b > 0\\ -1 \text{ otherwise} \end{cases}$$

an instance $\langle x, y \rangle$ will be classified correctly if

$$y(\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x} + \boldsymbol{b}) > 0$$



Large margin classification

- Given a training set that is linearly separable, there are infinitely many hyperplanes that could separate the positive/negative instances.
 - Which one should we choose?
- In SVM learning, we find the hyperplane that maximizes the margin.



Figure from Ben-Hur & Weston, Methods in Molecular Biology 2010

Large margin classification

- suppose we learn a hyperplane *h* given a training set *D*
- let x₊ denote the closest instance to the hyperplane among positive instances, and similarly for x₋ and negative instances
- the margin is given by

















But can double margin artificially

12 13





The hard-margin SVM

- given a training set $D = \{ \langle x^{(1)}, y^{(1)} \rangle, \dots, \langle x^{(m)}, y^{(m)} \rangle \}$
- we can frame the goal of maximizing the margin as a constrained optimization problem



and use standard algorithms to find an optimal solution to this problem

The soft-margin SVM

[Cortes & Vapnik, Machine Learning 1995]

- if the training instances are not linearly separable, the previous formulation will fail
- we can adjust our approach by using *slack variables* (denoted by ξ) to tolerate errors

minimize
$$w,b,\xi^{(1)}...\xi^{(m)}$$
 $\frac{1}{2} ||w||_2^2 + C \sum_{i=1}^m \xi^{(i)}$

subject to constraints:
$$y^{(i)}(w^{\mathsf{T}}x^{(i)} + b) \ge 1 - \xi^{(i)}$$

 $\xi^{(i)} \ge 0$

for i = 1, ..., m

• *C* determines the relative importance of maximizing margin vs. minimizing slack

The effect of *C* in a soft-margin SVM



Figure from Ben-Hur & Weston, *Methods in Molecular Biology* 2010















- What if a linear separator is not an appropriate decision boundary for a given task?
- For any (consistent) data set, there exists a mapping ϕ to a higher-dimensional space such that the data is linearly separable

$$\phi(\boldsymbol{x}) = \left(\phi_1(\boldsymbol{x}), \ \phi_2(\boldsymbol{x}), \ \dots, \ \phi_k(\boldsymbol{x})\right)$$

• Example: mapping to quadratic space

$$\boldsymbol{x} = \langle x_1, x_2 \rangle \quad \text{suppose } \boldsymbol{x} \text{ is represented by 2 features}$$
$$\phi(\boldsymbol{x}) = \left(x_1^2, \sqrt{2}x_1x_2, x_2^2, \sqrt{2}x_1, \sqrt{2}x_2, 1\right)$$

• now try to find a linear separator in this space

• for the linear case, our discriminant function was given by

$$h(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{w} \cdot \mathbf{x} + b > 0 \\ -1 & \text{otherwise} \end{cases}$$

• for the nonlinear case, it can be expressed as

$$h(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{w} \cdot \phi(\mathbf{x}) + b > 0 \\ -1 & \text{otherwise} \end{cases}$$

where w is a higher dimensional vector

SVMs with polynomial kernels



Figure from Ben-Hur & Weston, Methods in Molecular Biology 2010

The kernel trick

- explicitly computing this nonlinear mapping does not scale well
- a dot product between two higher-dimensional mappings can sometimes be implemented by a *kernel function*
- example: quadratic kernel

$$k(\mathbf{x}, \mathbf{z}) = (\mathbf{x} \cdot \mathbf{z} + 1)^{2}$$

= $(x_{1}z_{1} + x_{2}z_{2} + 1)^{2}$
= $x_{1}^{2}z_{1}^{2} + 2x_{1}x_{2}z_{1}z_{2} + x_{2}^{2}z_{2}^{2} + 2x_{1}z_{1} + 2x_{2}z_{2} + 1$
= $(x_{1}^{2}, \sqrt{2}x_{1}x_{2}, x_{2}^{2}, \sqrt{2}x_{1}, \sqrt{2}x_{2}, 1)$
 $(z_{1}^{2}, \sqrt{2}z_{1}z_{2}, z_{2}^{2}, \sqrt{2}z_{1}, \sqrt{2}z_{2}, 1)$
= $\phi(\mathbf{x}) \cdot \phi(\mathbf{z})$

The kernel trick

• thus we can use a kernel to compute the dot product without explicitly mapping the instances to a higher-dimensional space

$$k(\boldsymbol{x},\boldsymbol{z}) = (\boldsymbol{x}\cdot\boldsymbol{z}+1)^2 = \phi(\boldsymbol{x})\cdot\phi(\boldsymbol{z})$$

But why is the kernel trick helpful?

Using the kernel trick

- given a training set $D = \{ \langle x^{(1)}, y^{(1)} \rangle, \dots, \langle x^{(m)}, y^{(m)} \rangle \}$
- suppose the weight vector can be represented as a linear combination of the training instances

$$\boldsymbol{w} = \sum_{i=1}^{m} \alpha_i \boldsymbol{x}^{(i)}$$

• then we can represent a linear SVM as

$$\sum_{i=1}^m \alpha_i \mathbf{x}^{(i)} \bullet \mathbf{x} + b$$

and a nonlinear SVM as

$$\sum_{i=1}^{m} \alpha_{i} \phi(\mathbf{x}^{(i)}) \cdot \phi(\mathbf{x}) + b$$
$$= \sum_{i=1}^{m} \alpha_{i} k(\mathbf{x}^{(i)}, \mathbf{x}) + b$$

Can we represent a weight vector as a linear combination of training instances?

• consider perceptron learning, where each weight can be represented as

$$w_j = \sum_{i=1}^m \alpha_i x_j^{(i)}$$

• proof: each weight update has the form $w_i(t) = w_i(t-1) + \eta \delta_t^{(i)} y^{(i)} x_i^{(i)}$

 $\delta_{t}^{(i)}$

$$= \begin{cases} 1 \text{ if } \boldsymbol{x}^{(i)} \text{ misclassified in epoch } t \\ 0 \text{ otherwise} \end{cases}$$

$$w_j = \sum_t \sum_{i=1}^m \eta \delta_t^{(i)} y^{(i)} x_j^{(i)}$$

$$w_j = \sum_{i=1}^m \left(\sum_t \eta \delta_t^{(i)} y^{(i)}\right) x_j^{(i)}$$

$$w_j = \sum_{i=1}^m \alpha_i x_j^{(i)}$$

35

The primal and dual formulations of the hard-margin SVM

primal

r

minimize
$$\frac{1}{2} ||w||_2^2$$

subject to constraints: $y^{(i)}(w^T x^{(i)} + b) \ge 1$
for $i = 1, ..., m$

dual

$$\begin{array}{l} \underset{\alpha_{1},\ldots,\alpha_{m}}{\text{maximize}} \quad \sum_{i=1}^{m} \alpha_{i} - \frac{1}{2} \sum_{j=1}^{m} \sum_{k=1}^{m} \alpha_{j} \alpha_{k} y^{(j)} y^{(k)} \left(\boldsymbol{x}^{(j)} \boldsymbol{\cdot} \boldsymbol{x}^{(k)} \right) \\ \text{subject to constraints:} \quad \alpha_{i} \geq 0 \quad \text{ for } i = 1,\ldots, m \\ \sum_{i=1}^{m} \alpha_{i} y^{(i)} = 0 \end{array}$$

6

The *dual* formulation with a kernel (hard margin version)

primal

minimize
$$\frac{1}{2} ||w||_2^2$$

 w,b $\frac{1}{2} ||w||_2^2$
subject to constraints: $y^{(i)}(w^{\mathsf{T}}\phi(x^{(i)})+b) \ge 1$
for $i = 1,..., m$

dual

$$\begin{array}{l} \underset{\alpha_{1},\ldots,\alpha_{m}}{\text{maximize}} \quad \sum_{i=1}^{m} \alpha_{i} - \frac{1}{2} \sum_{j=1}^{m} \sum_{k=1}^{m} \alpha_{j} \alpha_{k} y^{(j)} y^{(k)} k\left(\boldsymbol{x}^{(j)}, \, \boldsymbol{x}^{(k)}\right) \\ \text{subject to constraints:} \quad \alpha_{i} \geq 0 \quad \text{ for } i = 1,\ldots, m \\ \sum_{i=1}^{m} \alpha_{i} y^{(i)} = 0 \end{array}$$

Support vectors

- the final solution is a sparse linear combination of the training instances
- those instances having $\alpha_i > 0$ are called *support vectors* they lie on the margin boundary
- the solution wouldn't change if all the instances with $\alpha_i = 0$ were deleted



The kernel matrix

• the kernel matrix (a.k.a. Gram matrix) represents pairwise similarities for instances in the training set

 it represents the information about the training set that is provided as input to the optimization process

Some common kernels

• polynomial of degree d

$$k(\boldsymbol{x},\boldsymbol{z}) = \left(\boldsymbol{x}\cdot\boldsymbol{z}\right)^d$$

• polynomial of degree up to d

$$k(\boldsymbol{x},\boldsymbol{z}) = (\boldsymbol{x}\cdot\boldsymbol{z}+1)^d$$

• radial basis function (RBF) (a.k.a. Gaussian)

$$k(\boldsymbol{x},\boldsymbol{z}) = \exp\left(-\gamma \left|\left|\boldsymbol{x}-\boldsymbol{z}\right|\right|^{2}\right)$$

The RBF kernel

- the feature mapping ϕ for the RBF kernel is infinite dimensional!
- recall that $k(x, z) = \phi(x) \bullet \phi(z)$

$$k(x,z) = \exp\left(-\frac{1}{2}||x-z||^2\right) \text{ for } \gamma = \frac{1}{2}$$

$$= \exp\left(-\frac{1}{2}||\boldsymbol{x}||^{2}\right)\exp\left(-\frac{1}{2}||\boldsymbol{z}||^{2}\right)\exp(\boldsymbol{x}\cdot\boldsymbol{z})$$

$$= \exp\left(-\frac{1}{2}||\boldsymbol{x}||^{2}\right)\exp\left(-\frac{1}{2}||\boldsymbol{z}||^{2}\right)\left(\sum_{n=0}^{\infty}\frac{(\boldsymbol{x}\cdot\boldsymbol{z})^{n}}{n!}\right)$$

from the Taylor series expansion of $exp(x \stackrel{4}{}^{1}z)$

The RBF kernel illustrated



Figures from openclassroom.stanford.edu (Andrew Ng)

What makes a valid kernel?

• k(x, z) is a valid kernel if there is some ϕ such that $k(x, z) = \phi(x) \cdot \phi(z)$

 this holds for a symmetric function k(x, z) if and only if the kernel matrix K is positive semidefinite for any training set (Mercer's theorem)

definition of positive semidefinite (p.s.d): $\forall v : v^{\top} K v \ge 0$

Support vector regression

- the SVM idea can also be applied in regression tasks
- an ϵ -insensitive error function specifies that a training instance is well explained if the model's prediction is within ϵ of $y^{(i)}$



Support vector regression

$$\begin{array}{c} \text{minimize} \\ w, b, \xi^{(1)} \dots \xi^{(m)}, \hat{\xi}^{(1)} \dots \hat{\xi}^{(m)} \end{array} & \frac{1}{2} \|w\|_{2}^{2} + C \sum_{i=1}^{m} \left(\xi^{(i)} + \hat{\xi}^{(i)}\right) \end{array}$$

subject to constraints: $(w^{\mathsf{T}}x^{(i)} + b) - y^{(i)} \le \varepsilon + \xi^{(i)}$ $y^{(i)} - \left(\boldsymbol{w}^{\mathsf{T}} \boldsymbol{x}^{(i)} + b \right) \leq \varepsilon + \hat{\xi}^{(i)}$ $\boldsymbol{\xi}^{(i)}, \boldsymbol{\hat{\xi}}^{(i)} \geq \boldsymbol{0}$ for i = 1, ..., m

> slack variables allow predictions for some training instances to be off by more than ϵ

Learning theory justification for maximizing the margin



Vapnik showed there is a connection between the margin and VC dimension

 $VC \le \frac{4R^2}{\operatorname{margin}_D(h)^2}$ constant dependent on training data

thus to minimize the VC dimension (and to improve the error bound) \rightarrow maximize the margin

The power of kernel functions

- kernels can be designed and used to represent complex data types such as
 - strings
 - trees
 - graphs
 - etc.
- let's consider a specific example









The protein classification task

Given: amino-acid sequence of a protein **Do**: predict the *family* to which it belongs



The *k*-spectrum feature map

• we can represent sequences by counts of all of their *k*-mers



- the dimension of $\phi(x) = |A|^k$ where |A| is the size of the alphabet
 - using 6-mers for protein sequences, $|20|^6 = 64$ million
 - almost all of the elements in φ(x) are 0 since a sequence of length *l* has at most *l*-*k*+1 *k*-mers

The *k*-spectrum kernel

• consider the *k*-spectrum kernel applied to *x* and *z* with k = 3

 $x = \mathbf{AKQDYYYYEI}$

 $z = \mathbf{AKQIAKQYEI}$

$$\phi(x) = (0, ..., 1, ..., 1, ..., 0)$$
AAA ..., AKQ ..., YEI ..., YYY
$$\phi(z) = (0, ..., 2, ..., 1, ..., 0)$$
AAA ..., AKQ ..., YEI ..., 0)
YYY

 $\phi(x) \bullet \phi(z) = 2 + 1 = 3$

(k, m)-mismatch feature map

- closely related protein sequences may have few exact matches, but many near matches
- the (*k*, *m*)-mismatch feature map uses the *k*-spectrum representation, but allows up to *m* mismatches

x = AKQ k = 3, m = 1 $\phi(x) = (0, ..., 1, ..., 1, ..., 1, ..., 0)$ AAA AAQ ... AKQ ... DKQ ... YYY

Using a trie to represent 3-mers

• example: representing all 3-mers of the sequence **QAAKKQAKKY**



Computing the kernels efficiently with tries [Leslie et al., NIPS 2002]

k-spectrum kernel

- for each sequence
 - build a trie representing its k-mers
- compute kernel $\phi(x) \bullet \phi(z)$ by traversing trie for x using k-mers from z
 - update kernel function when reaching a leaf

(k, m)-mismatch kernel

- for each sequence
 - build a trie representing its *k*-mers and also <u>k-mers with at most m</u> <u>mismatches</u>
- compute kernel $\phi(x) \bullet \phi(z)$ by traversing trie for x using k-mers from z
 - update kernel function when reaching a leaf

scales linearly with sequence length: $O(k^{m+1}|A|^m(|x|+|z|))$ 53

Kernel algebra

• given a valid kernel, we can make new valid kernels using a variety of operators

kernel composition	mapping composition
$k(\boldsymbol{x},\boldsymbol{v}) = k_a(\boldsymbol{x},\boldsymbol{v}) + k_b(\boldsymbol{x},\boldsymbol{v})$	$\phi(\boldsymbol{x}) = (\phi_a(\boldsymbol{x}), \phi_b(\boldsymbol{x}))$
$k(\boldsymbol{x}, \boldsymbol{v}) = \gamma \ k_a(\boldsymbol{x}, \boldsymbol{v}), \ \gamma > 0$	$\phi(\boldsymbol{x}) = \sqrt{\gamma} \ \phi_a(\boldsymbol{x})$
$k(\boldsymbol{x},\boldsymbol{v}) = k_a(\boldsymbol{x},\boldsymbol{v})k_b(\boldsymbol{x},\boldsymbol{v})$	$\phi_l(\boldsymbol{x}) = \phi_{ai}(\boldsymbol{x})\phi_{bj}(\boldsymbol{x})$
$k(\boldsymbol{x}, \boldsymbol{v}) = \boldsymbol{x}^{T} A \boldsymbol{v}, A \text{ is p.s.d.}$	$\phi(\mathbf{x}) = L^{T}\mathbf{x}$, where $A = LL^{T}$
$k(\boldsymbol{x}, \boldsymbol{v}) = f(\boldsymbol{x})f(\boldsymbol{v})k_a(\boldsymbol{x}, \boldsymbol{v})$	$\phi(\boldsymbol{x}) = f(\boldsymbol{x})\phi_a(\boldsymbol{x})$

Comments on SVMs

- we can find solutions that are globally optimal (maximize the margin)
 - because the learning task is framed as a convex optimization problem
 - no local minima, in contrast to multi-layer neural nets
- there are two formulations of the optimization: *primal* and *dual*
 - dual represents classifier decision in terms of support vectors
 - dual enables the use of kernel functions
- we can use a wide range of optimization methods to learn SVM
 - standard quadratic programming solvers
 - SMO [Platt, 1999]
 - linear programming solvers for some formulations
 - etc.

Comments on SVMs

- kernels provide a powerful way to
 - allow nonlinear decision boundaries
 - represent/compare complex objects such as strings and trees
 - incorporate domain knowledge into the learning task
- using the kernel trick, we can implicitly use high-dimensional mappings without explicitly computing them
- one SVM can represent only a binary classification task; multi-class problems handled using multiple SVMs and some encoding
 - one class vs. rest
 - ECOC
 - etc.
- empirically, SVMs have shown state-of-the art accuracy for many tasks
- the kernel idea can be extended to other tasks (anomaly detection, regression, etc.)