

Support Vector Machines

- Optimally defined decision surface
- Typically nonlinear in the input space
- Linear in a higher dimensional space
- Implicitly defined by a kernel function

Acknowledgments: These slides combine and modify ones provided by Andrew Moore (CMU), Jerry Zhu (Wisconsin), Glenn Fung (Wisconsin), and Olvi Mangasarian (Wisconsin)

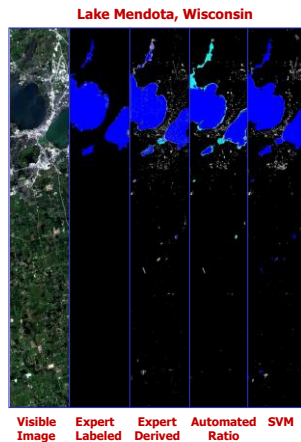
What are Support Vector Machines Used For?

- Classification
- Regression and data-fitting
- Supervised and unsupervised learning

Lake Mendota, Madison, WI

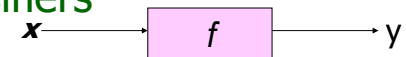
- Identify areas of land cover (land, ice, water, snow) in a scene
- Two methods:
 - Scientist manually-derived
 - Support Vector Machine (SVM)

Classifier	Expert Derived	SVM
cloud	45.7%	58.5%
ice	60.1%	80.4%
land	93.6%	94.0%
snow	63.5%	71.6%
water	84.2%	89.1%
unclassified	45.7%	



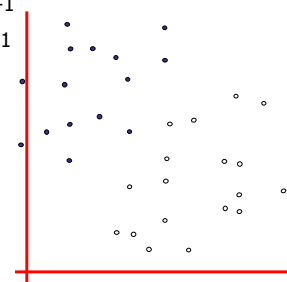
Courtesy of Steve Chien of NASA/JPL

Linear Classifiers



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



How would you classify this data?

Linear Classifiers (aka Linear Discriminant Functions)

- Definition

A function that is a linear combination of the components of the input (column vector) \mathbf{x}

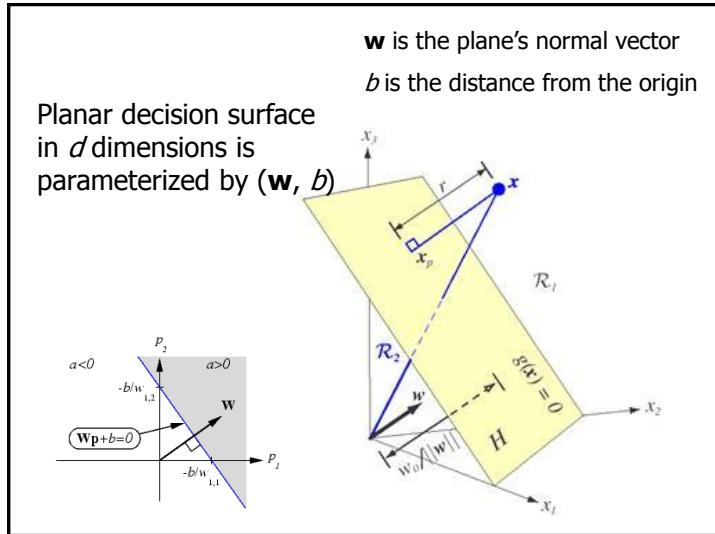
$$f(\mathbf{x}) = \sum_{j=1}^m w_{ij} x_j + b = \mathbf{w}^T \mathbf{x} + b$$

where \mathbf{w} is the weight (column vector) and b is the bias

- A **2-class classifier** then uses the rule:

Decide class c_1 if $f(\mathbf{x}) \geq 0$ and class c_2 if $f(\mathbf{x}) < 0$

\Leftrightarrow Decide c_1 if $\mathbf{w}^T \mathbf{x} \geq -b$ and c_2 otherwise

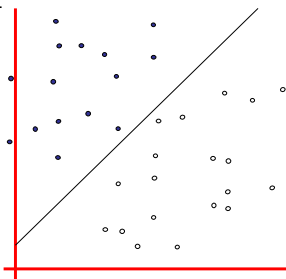


Linear Classifiers



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



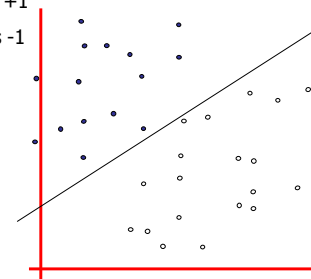
How would you classify this data?

Linear Classifiers



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



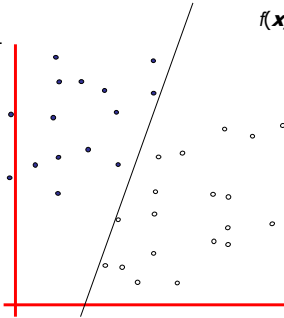
How would you classify this data?

Linear Classifiers



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



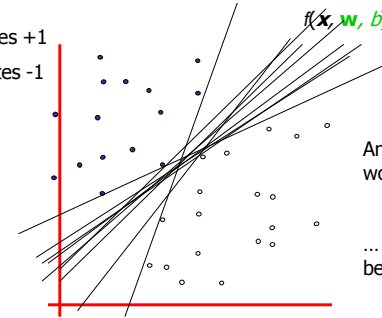
How would you classify this data?

Linear Classifiers



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



Any of these would be fine ...

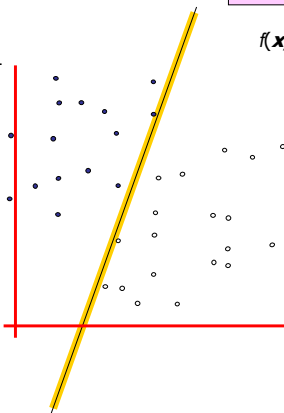
... but which is best?

Classifier Margin



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1



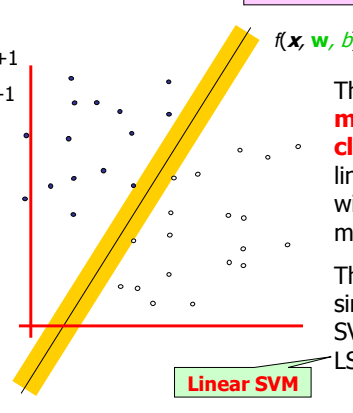
Define the **margin** of a linear classifier as the width that the boundary could be increased by before hitting a data point

Maximum Margin



$$f(\mathbf{x}, \mathbf{w}, b) = \text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$$

- denotes +1
- denotes -1

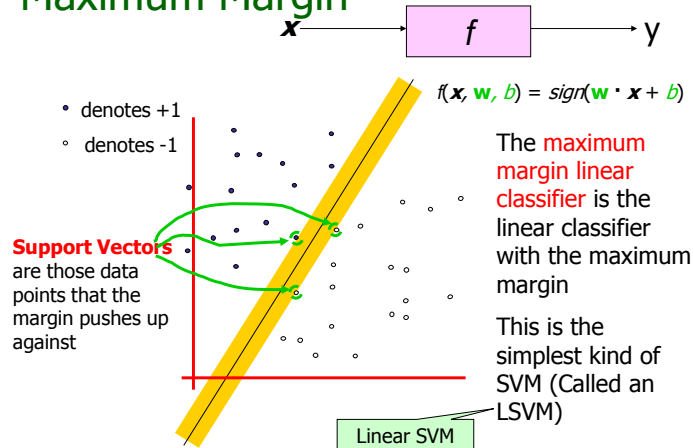


The **maximum margin linear classifier** is the linear classifier with the maximum margin!

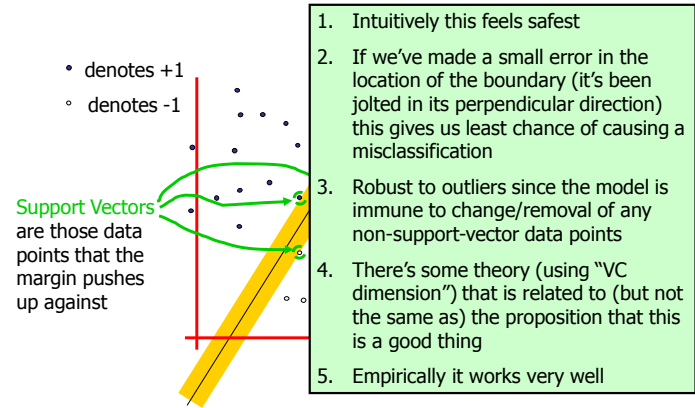
This is the simplest kind of SVM (Called an LSVM)

Linear SVM

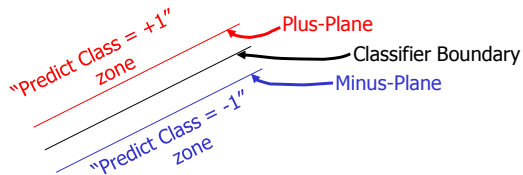
Maximum Margin



Why Maximum Margin?

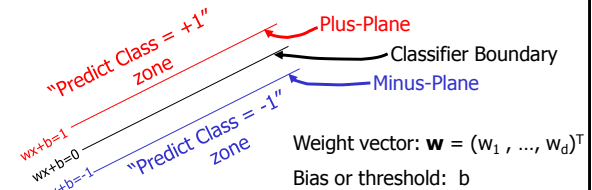


Specifying a Line and Margin



- How do we represent this mathematically?
- ... in d input dimensions?
- An example $\mathbf{x} = (x_1, \dots, x_d)^T$

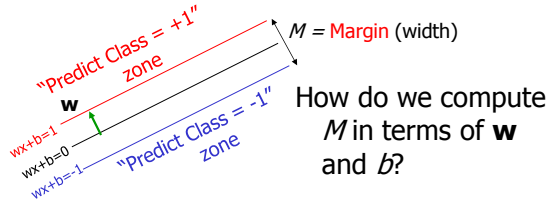
Specifying a Line and Margin



- Plus-plane = $\mathbf{w}^T \cdot \mathbf{x} + b = +1$
 - Minus-plane = $\mathbf{w}^T \cdot \mathbf{x} + b = -1$
- The dot product $\mathbf{w}^T \cdot \mathbf{x} = \sum w_i x_i$ is a scalar: \mathbf{x} 's projection onto \mathbf{w}

Classify as $+1$ if $\mathbf{w}^T \cdot \mathbf{x} + b \geq 1$
 -1 if $\mathbf{w}^T \cdot \mathbf{x} + b \leq -1$
 ? if $-1 < \mathbf{w}^T \cdot \mathbf{x} + b < 1$

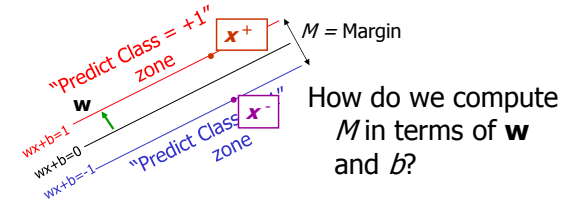
Computing the Margin



- Plus-plane = $\mathbf{w} \mathbf{x} + b = +1$
 - Minus-plane = $\mathbf{w} \mathbf{x} + b = -1$
- Note: From now on, transpose symbol on \mathbf{w} implied

Claim: The vector \mathbf{w} is perpendicular to the Plus-Plane

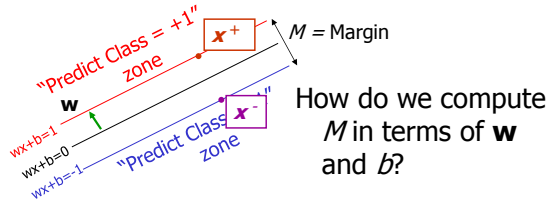
Computing the Margin



- Plus-plane = $\mathbf{w} \mathbf{x} + b = +1$
- Minus-plane = $\mathbf{w} \mathbf{x} + b = -1$
- The vector \mathbf{w} is perpendicular to the Plus Plane
- Let \mathbf{x}^- be any point on the minus plane
- Let \mathbf{x}^+ be the closest plus-plane-point to \mathbf{x}^-

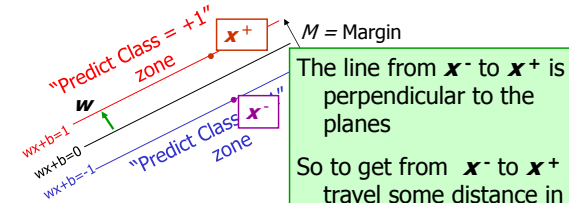
Any location in \mathbb{R}^n ; not necessarily a data point

Computing the Margin



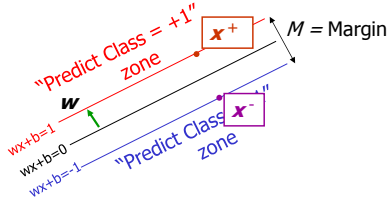
- Plus-plane = $\mathbf{w} \mathbf{x} + b = +1$
- Minus-plane = $\mathbf{w} \mathbf{x} + b = -1$
- The vector \mathbf{w} is perpendicular to the Plus Plane
- Let \mathbf{x}^- be any point on the minus plane
- Let \mathbf{x}^+ be the closest plus-plane-point to \mathbf{x}^-
- **Claim:** $\mathbf{x}^+ = \mathbf{x}^- + \lambda \mathbf{w}$ for some value of λ . **Why?**

Computing the Margin



- Plus-plane = $\mathbf{w} \mathbf{x} + b = +1$
- Minus-plane = $\mathbf{w} \mathbf{x} + b = -1$
- The vector \mathbf{w} is perpendicular to the Plus Plane
- Let \mathbf{x}^- be any point on the minus plane
- Let \mathbf{x}^+ be the closest plus-plane-point to \mathbf{x}^-
- **Claim:** $\mathbf{x}^+ = \mathbf{x}^- + \lambda \mathbf{w}$ for some value of λ . **Why?**

Computing the Margin

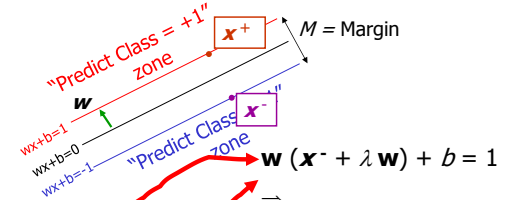


What we know:

- $\mathbf{w} \mathbf{x}^+ + b = +1$
- $\mathbf{w} \mathbf{x}^- + b = -1$
- $\mathbf{x}^+ = \mathbf{x}^- + \lambda \mathbf{w}$
- $\|\mathbf{x}^+ - \mathbf{x}^-\| = M$

It's now easy to get M in terms of \mathbf{w} and b

Computing the Margin



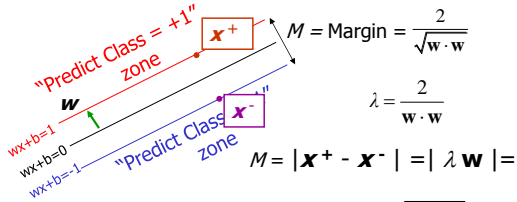
What we know:

- $\mathbf{w} \mathbf{x}^+ + b = +1$ $\mathbf{w} \mathbf{x}^- + b + \lambda \mathbf{w} \mathbf{w} = 1$
- $\mathbf{w} \mathbf{x}^- + b = -1$ \Rightarrow
- $\mathbf{x}^+ = \mathbf{x}^- + \lambda \mathbf{w}$ $-1 + \lambda \mathbf{w} \mathbf{w} = 1$
- $\|\mathbf{x}^+ - \mathbf{x}^-\| = M$

It's now easy to get M in terms of \mathbf{w} and b

$$\Rightarrow \lambda = \frac{2}{\mathbf{w}^T \mathbf{w}}$$

Computing the Margin



What we know:

- $\mathbf{w} \mathbf{x}^+ + b = +1$
- $\mathbf{w} \mathbf{x}^- + b = -1$
- $\mathbf{x}^+ = \mathbf{x}^- + \lambda \mathbf{w}$
- $\|\mathbf{x}^+ - \mathbf{x}^-\| = M$

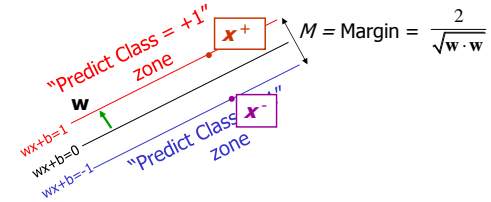
$$M = \|\mathbf{x}^+ - \mathbf{x}^-\| = \|\lambda \mathbf{w}\| = \lambda \|\mathbf{w}\| = \lambda \sqrt{\mathbf{w} \cdot \mathbf{w}}$$

$$\lambda = \frac{2}{\mathbf{w} \cdot \mathbf{w}}$$

$$M = \frac{2\sqrt{\mathbf{w} \cdot \mathbf{w}}}{\mathbf{w} \cdot \mathbf{w}} = \frac{2}{\sqrt{\mathbf{w} \cdot \mathbf{w}}}$$

$$= \frac{2}{\|\mathbf{w}\|} = M, \text{ margin size}$$

Learning the Maximum Margin Classifier



Given a guess of \mathbf{w} and b we can

1. Compute whether all data points in the correct half-planes
2. Compute the width of the margin

So now we just need to write a program to search the space of \mathbf{w} 's and b 's to find the widest margin that matches all the data points. *How?*

SVM as Constrained Optimization

- Unknowns: \mathbf{w} , b
- Objective function: maximize the margin
 $M=2/||\mathbf{w}'||$
- Equivalent to **minimizing** $||\mathbf{w}'||$ or $||\mathbf{w}'||^2 = \mathbf{w}'^T \mathbf{w}'$

- Assume N training points (x_k, y_k) , $y_k = 1$ or -1
- Subject to each training point on the correct side (the constraint), i.e.,
subject to $y_k(\mathbf{w}'^T x_k + b) \geq 1$ for all k

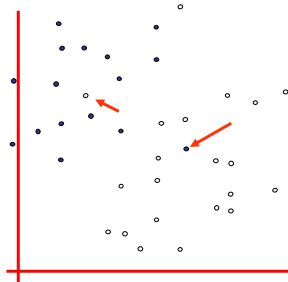
This is a **Quadratic optimization problem**, which can be solved efficiently

SVMs: More than Two Classes

- SVMs can only handle two-class problems
- N -class problem: Split the task into N **binary** tasks and learn N SVMs:
 - Class 1 vs. the rest (classes 2 — N)
 - Class 2 vs. the rest (classes 1, 3 — N)
 - ...
 - Class N vs. the rest
- Finally, pick the class that puts the point farthest into the positive region

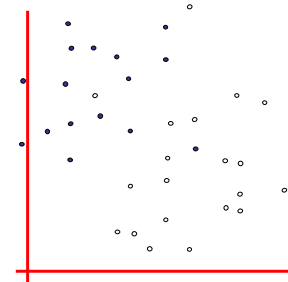
SVM: Non Linearly-Separable Data

- What if the data are **not** linearly separable?



SVM: Non Linearly-Separable Data

- Two solutions:
 - Allow a few points on the wrong side (**slack variables**)
 - Map data to a higher dimensional space, and do linear classification there (**kernel trick**)

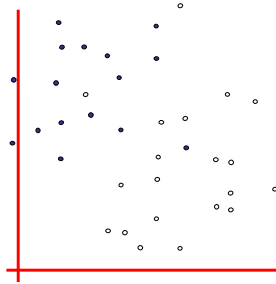


Non Linearly-Separable Data

- Approach 1: Allow a few points on the wrong side (**slack variables**)

What should we do?

- denotes +1
- denotes -1



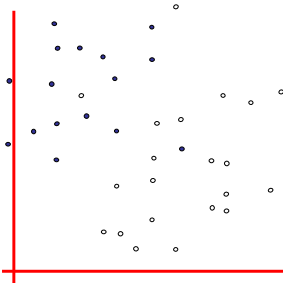
What should we do?

Idea 1:

Find minimum $\|w\|^2$ while minimizing number of training set errors

Problem: Two things to minimize makes for an ill-defined optimization

- denotes +1
- denotes -1



What should we do?

Idea 1.1:

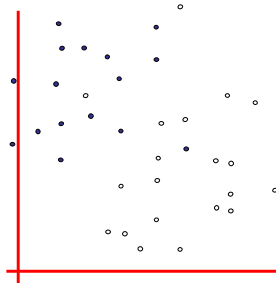
Minimize

$\|w\|^2 + C(\# \text{ train errors})$

Tradeoff parameter

There's a serious practical problem with this approach

- denotes +1
- denotes -1



What should we do?

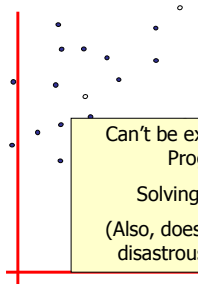
Idea 1.1:

Minimize

$$\|\mathbf{w}\|^2 + C(\# \text{ train errors})$$

Tradeoff parameter

- denotes +1
- denotes -1



Can't be expressed as a Quadratic Programming problem.
Solving it may be too slow.
(Also, doesn't distinguish between disastrous errors and near misses)

serious practical with this

So... any other ideas?

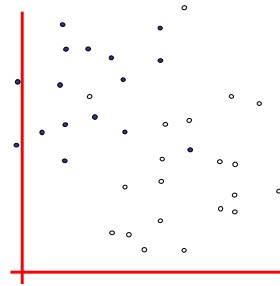
What should we do?

Idea 2.0:

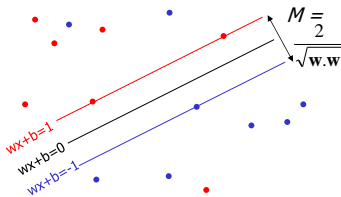
Minimize

$$\|\mathbf{w}\|^2 + C(\text{distance of "error points" to their correct place})$$

- denotes +1
- denotes -1



Learning Maximum Margin with Noise

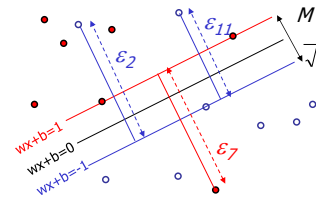


- Given guess of \mathbf{w} , b , we can
1. Compute sum of distances of points to their correct zones
 2. Compute the margin width
- Assume N examples, each (\mathbf{x}_k, y_k) where $y_k = +/- 1$

What should our quadratic optimization criterion be?

How many constraints will we have?
What should they be?

Learning Maximum Margin with Noise



"slack variables"

- Given guess of \mathbf{w} , b we can
1. Compute sum of distances of points to their correct zones
 2. Compute the margin width
- Assume N examples, each (\mathbf{x}_k, y_k) where $y_k = +/- 1$

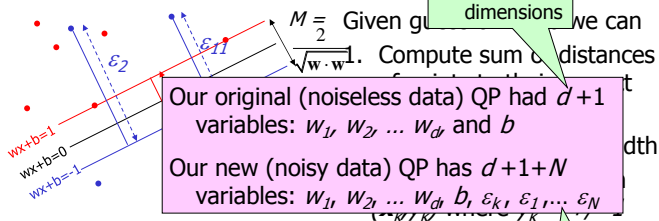
What should our quadratic optimization criterion be?

How many constraints will we have? N
What should they be?

$$\text{Minimize } \frac{1}{2} \mathbf{w} \cdot \mathbf{w} + C \sum_{k=1}^N \varepsilon_k$$

$$y_k(\mathbf{w}^T \mathbf{x}_k + b) \geq 1 - \varepsilon_k \text{ for all } k$$

Learning Maximum Margin with Noise



What should our quadratic optimization criterion be?

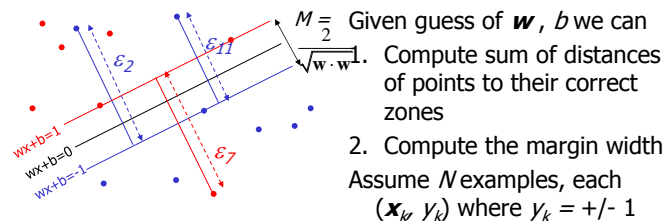
$$\text{Minimize } \frac{1}{2} \mathbf{w} \cdot \mathbf{w} + C \sum_{k=1}^N \varepsilon_k$$

How many constraints will we have? N

What should they be?

$$\begin{aligned} \mathbf{w} \cdot \mathbf{x}_k + b &\geq 1 - \varepsilon_k \text{ if } y_k = +1 \\ \mathbf{w} \cdot \mathbf{x}_k + b &\leq -1 + \varepsilon_k \text{ if } y_k = -1 \end{aligned}$$

Learning Maximum Margin with Noise



What should our quadratic optimization criterion be?

$$\text{Minimize } \frac{1}{2} \mathbf{w} \cdot \mathbf{w} + C \sum_{k=1}^N \varepsilon_k$$

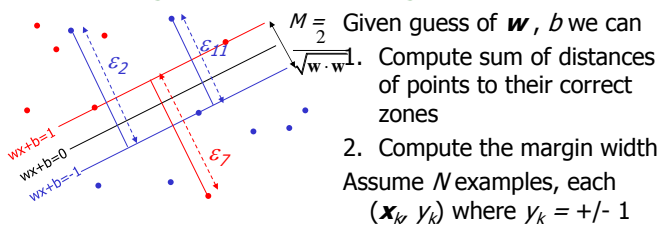
How many constraints will we have? N

What should they be?

$$\begin{aligned} \mathbf{w} \cdot \mathbf{x}_k + b &\geq 1 - \varepsilon_k \text{ if } y_k = +1 \\ \mathbf{w} \cdot \mathbf{x}_k + b &\leq -1 + \varepsilon_k \text{ if } y_k = -1 \end{aligned}$$

There's a bug in this QP. Can you spot it?

Learning Maximum Margin with Noise



What should our quadratic optimization criterion be?

$$\text{Minimize } \frac{1}{2} \mathbf{w} \cdot \mathbf{w} + C \sum_{k=1}^N \varepsilon_k$$

How many constraints will we have? $2N$

What should they be?

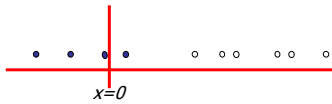
$$\begin{aligned} \mathbf{w} \cdot \mathbf{x}_k + b &\geq +1 - \varepsilon_k \text{ if } y_k = +1 \\ \mathbf{w} \cdot \mathbf{x}_k + b &\leq -1 + \varepsilon_k \text{ if } y_k = -1 \\ \varepsilon_k &\geq 0 \text{ for all } k \end{aligned}$$

Non Linearly-Separable Data

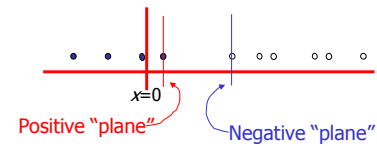
- Approach 2: Map data to a higher dimensional space, and do linear classification there (**kernel trick**)

Suppose we're in 1 Dimension

What would SVMs do with this data?

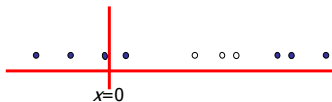


Suppose we're in 1 Dimension



Harder 1D Dataset: Not Linearly-Separable

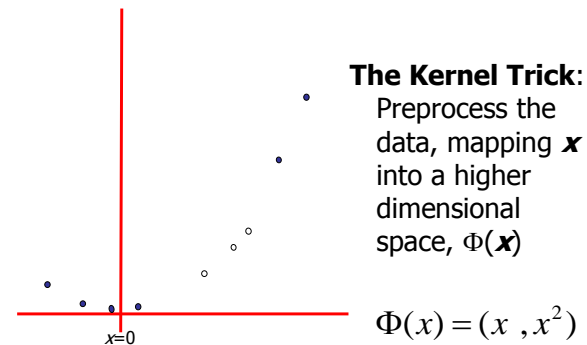
What can be done about this?



Harder 1D Dataset

The Kernel Trick:

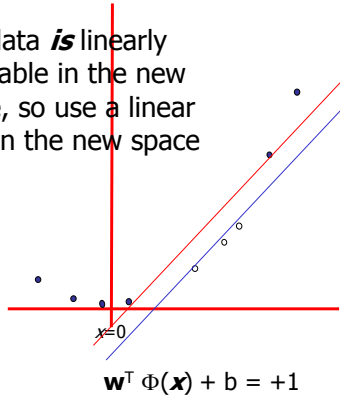
Preprocess the data, mapping \mathbf{x} into a higher dimensional space, $\Phi(\mathbf{x})$



Here, Φ maps data from 1D to 2D

Harder 1D Dataset

The data *is* linearly separable in the new space, so use a linear SVM in the new space



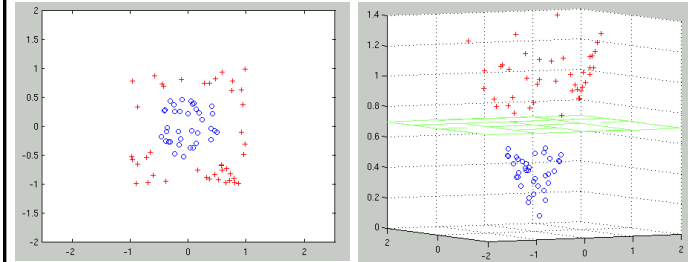
The Kernel Trick:
Preprocess the data, mapping \mathbf{x} into a higher dimensional space, $\Phi(\mathbf{x})$

$$\Phi(x) = (x, x^2)$$

$$\mathbf{w}^T \Phi(\mathbf{x}) + b = +1$$

Another Example

$$(x_1, x_2) \Rightarrow (x_1, x_2, \sqrt{x_1^2 + x_2^2})$$



- Project examples into some higher dimensional space where the data *is* linearly separable, defined by $\mathbf{z} = \Phi(\mathbf{x})$
- Can formulate optimization problem so that objective function depends *only* on dot products of the form $\Phi(\mathbf{x}_i)^T \cdot \Phi(\mathbf{x}_j)$ where \mathbf{x}_i and \mathbf{x}_j are two data points
- Example:

$$\Phi(x) = (x_1^2, \sqrt{2}x_1x_2, x_2^2)$$

$$\text{Define } K(\mathbf{x}_i, \mathbf{x}_j) = \Phi(\mathbf{x}_i)^T \cdot \Phi(\mathbf{x}_j) = (\mathbf{x}_i \cdot \mathbf{x}_j)^2$$

- Claim: Can compute kernel function K *without* explicitly computing $\Phi(\mathbf{x})$ or \mathbf{w}
- Dimensionality of \mathbf{z} space is generally *much larger* than the dimensionality of input space \mathbf{x}

What's Special about a Kernel?

- Say data is 2D: $\mathbf{s} = (s_1, s_2)$
- We decide to use a particular mapping into 6D space:

$$\Phi(\mathbf{s}) = (s_1^2, s_2^2, \sqrt{2} s_1 s_2, s_1, s_2, 1)$$
- Let another point be $\mathbf{t} = (t_1, t_2)$
- Then,

$$\Phi(\mathbf{s})^T \cdot \Phi(\mathbf{t}) = s_1^2 t_1^2 + s_2^2 t_2^2 + 2s_1 s_2 t_1 t_2 + s_1 t_1 + s_2 t_2 + 1$$
- Let the **kernel** be $K(\mathbf{s}, \mathbf{t}) = (\mathbf{s}^T \cdot \mathbf{t} + 1)^2 = (s_1 t_1 + s_2 t_2 + 1)^2$
- $K(\mathbf{s}, \mathbf{t}) = \Phi(\mathbf{s})^T \cdot \Phi(\mathbf{t})$
- **We save computation** by using K

Some Commonly Used Kernels

- **Linear** kernel: $K(\mathbf{x}_i, \mathbf{x}_j) = \mathbf{x}_i^T \mathbf{x}_j$
- **Quadratic** kernel: $K(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i^T \mathbf{x}_j + 1)^2$
- **Polynomial** kernel: $K(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i^T \mathbf{x}_j + 1)^d$
- **Radial Basis Function** kernel:

$$K(\mathbf{x}_i, \mathbf{x}_j) = \exp(- \|\mathbf{x}_i - \mathbf{x}_j\|^2 / \sigma^2)$$
- Many other kernels
- Hacking with SVMs: create various kernels, hope their space Φ is meaningful, plug them into SVM, pick one with good classification accuracy
- Kernel can be combined with slack variables

Example Application: The Federalist Papers Dispute

- Written in 1787-1788 by Alexander **Hamilton**, John Jay, and James **Madison** to persuade the citizens of New York to ratify the U.S. Constitution
- Papers consisted of short essays, 900 to 3500 words in length
- Authorship of **12** of those papers have been in dispute (**Madison** or **Hamilton**); these papers are referred to as the **disputed Federalist papers**

Description of the Data

- For every paper:
 - Machine readable text was created using a scanner
 - Computed relative frequencies of **70** words that Mosteller-Wallace identified as good candidates for author-attribution studies
 - Each document is represented as a vector containing the **70** real numbers corresponding to the **70** word frequencies
- The dataset consists of **118** papers:
 - **50** Madison papers
 - **56** Hamilton papers
 - **12** disputed papers

Function Words Based on Relative Frequencies

1	<i>a</i>	15	<i>do</i>	29	<i>is</i>	43	<i>or</i>	57	<i>this</i>
2	<i>all</i>	16	<i>down</i>	30	<i>it</i>	44	<i>our</i>	58	<i>to</i>
3	<i>also</i>	17	<i>even</i>	31	<i>its</i>	45	<i>shall</i>	59	<i>up</i>
4	<i>an</i>	18	<i>every</i>	32	<i>may</i>	46	<i>should</i>	60	<i>upon</i>
5	<i>and</i>	19	<i>for</i>	33	<i>more</i>	47	<i>so</i>	61	<i>was</i>
6	<i>any</i>	20	<i>from</i>	34	<i>must</i>	48	<i>some</i>	62	<i>were</i>
7	<i>are</i>	21	<i>had</i>	35	<i>my</i>	49	<i>such</i>	63	<i>what</i>
8	<i>as</i>	22	<i>has</i>	36	<i>no</i>	50	<i>than</i>	64	<i>when</i>
9	<i>at</i>	23	<i>have</i>	37	<i>not</i>	51	<i>that</i>	65	<i>which</i>
10	<i>be</i>	24	<i>her</i>	38	<i>now</i>	52	<i>the</i>	66	<i>who</i>
11	<i>been</i>	25	<i>his</i>	39	<i>of</i>	53	<i>their</i>	67	<i>will</i>
12	<i>but</i>	26	<i>if</i>	40	<i>on</i>	54	<i>then</i>	68	<i>with</i>
13	<i>by</i>	27	<i>in</i>	41	<i>one</i>	55	<i>there</i>	69	<i>would</i>
14	<i>can</i>	28	<i>into</i>	42	<i>only</i>	56	<i>things</i>	70	<i>your</i>

Feature Selection for Classifying the Disputed Federalist Papers

- Apply the SVM Successive Linearization Algorithm for feature selection to:
 - Train on the 106 Federalist papers with known authors
 - Find a classification hyperplane that uses as few words as possible
- Use the hyperplane to classify the 12 disputed papers

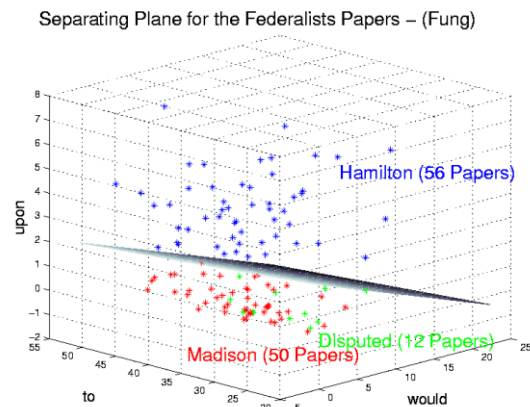
Hyperplane Classifier Using 3 Words

- A hyperplane depending on three words was found:

$$0.537to + 24.663upon + 2.953would = 66.616$$

- All disputed papers ended up on the Madison side of the plane

Results: 3D Plot of Hyperplane



SVM Applet

<http://svm.dcs.rhbnc.ac.uk/pagesnew/GPat.shtml>

Summary

- Learning linear functions
 - Pick separating plane that maximizes margin
 - Separating plane defined in terms of support vectors only
- Learning non-linear functions
 - Project examples into higher dimensional space
 - Use kernel functions for efficiency
- Generally avoids overfitting problem
- Global optimization method; no local optima
- Can be expensive to apply, especially for multi-class problems