EECS 545: Machine Learning

Lecture 6. Classification 3

Honglak Lee 1/31/2020





Announcements

- HW1 due by today, 23:55
- HW2 due by Feb/11, 23:55
- Google <u>calendar</u> for the class schedule
 - Subscribe it!

Outline

- Probabilistic generative models
 - Gaussian discriminant analysis (already covered)
 - Naive Bayes
- Discriminant functions
 - Fisher's linear discriminant
 - Perceptron learning algorithm

Recap: Learning the Classifier

- Goal: Learn the distributions $p(C_k \mid \mathbf{x})$.
- (a) Discriminative models: Directly model $p(C_k|\mathbf{x})$ and learn parameters from the training set.
 - Logistic regression
 - Softmax regression
 - (b) Generative models: Learn class densities $p(\mathbf{x} | C_k)$ and priors $p(C_k)$
 - Gaussian Discriminant Analysis
 - Naive Bayes

Recap: Learning the Classifier

- Goal: Learn the distributions $p(C_k \mid \mathbf{x})$.
- (a) Discriminative models: Directly model $p(C_k|\mathbf{x})$ and learn parameters from the training set.
 - Logistic regression
 - Softmax regression
 - (b) Generative models: Learn class densities $p(x|C_k)$ and priors $p(C_k)$
 - Gaussian Discriminant Analysis
 - Naive Bayes

- Prior distribution:
 - $-p(C_k)$: Constant (e.g., Bernoulli)
- Likelihood
 - Naive Bayes assumption: $P(\mathbf{x} | C_k)$ is factorized (Each coordinate of \mathbf{x} is conditionally independent of other coordinates given the class label)

$$P(x_1, ..., x_M | C_k) = P(x_1 | C_k) \cdots P(x_M | C_k) = \prod_{i=1}^M P(x_i | C_k)$$

Classification: use Bayes rule

(binary)
$$P(C_1|\mathbf{x}) = \frac{P(C_1,\mathbf{x})}{P(\mathbf{x})} = \frac{P(C_1,\mathbf{x})}{P(C_1,\mathbf{x}) + P(C_2,\mathbf{x})}$$

 When classifying, we can simply take the MAP (Maximum a Posteriori) estimation:

$$\arg\max_{k} P(C_k|\mathbf{x}) = \arg\max_{k} P(C_k,\mathbf{x})$$

 When classifying, we can simply take the MAP (Maximum a Posteriori) estimation:

$$\arg \max_{k} P(C_k | \mathbf{x}) = \arg \max_{k} P(C_k, \mathbf{x})$$
$$= \arg \max_{k} P(C_k) P(\mathbf{x} | C_k)$$

 When classifying, we can simply take the MAP (Maximum a Posteriori) estimation:

$$\arg\max_k P(C_k|\mathbf{x}) = \arg\max_k P(C_k,\mathbf{x})$$

$$= \arg\max_k P(C_k)P(\mathbf{x}|C_k)$$
 Naive Bayes assumption
$$= \arg\max_k P(C_k)\prod_{j=1}^M P(x_j|C_k)$$

Example: Spam mail classification

- Label: y=1 (spam), y=0 (non-spam)
- Features:
 - $-x_i$: j-th word in the mail, where M is the vocabulary size.
 - Multinomial variable (M-dimensional binary vector with only one coordinate with 1)
- Naive Bayes Assumption:
 - Given a class label y, each word in a mail is a independent multinomial variable.

Model

```
P(\text{spam}) = Bernoulli(\phi)
P(\text{word}|\text{spam}) = Multinomial(\mu_1^s, \dots, \mu_M^s)
P(\text{word}|\text{nonspam}) = Multinomial(\mu_1^{ns}, \dots, \mu_M^{ns})
```

Goal

: Find ϕ , μ^{s} , μ^{ns} that best fits the data $\{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

Model

```
P(\text{spam}) = Bernoulli(\phi)
P(\text{word}|\text{spam}) = Multinomial(\mu_1^s, \dots, \mu_M^s)
P(\text{word}|\text{nonspam}) = Multinomial(\mu_1^{ns}, \dots, \mu_M^{ns})
```

Goal

: Find ϕ , μ^{s} , μ^{ns} that best fits the data $\{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

Likelihood

$$\prod_{i=1}^{N} P(\mathbf{x}^{(i)}, y^{(i)})$$

Model

$$P(\text{spam}) = Bernoulli(\phi)$$

$$P(\text{word}|\text{spam}) = Multinomial(\mu_1^s, \dots, \mu_M^s)$$

$$P(\text{word}|\text{nonspam}) = Multinomial(\mu_1^{ns}, \dots, \mu_M^{ns})$$

Goal

: Find ϕ , μ^{s} , μ^{ns} that best fits the data $\{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

Likelihood

$$\begin{split} &\prod_{i=1}^{N} P(\mathbf{x}^{(i)}, y^{(i)}) \\ &= \prod_{i=1}^{N} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)}) \\ &= \left[\left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)}) \right) \right] \left(\prod_{i:y^{(i)}=0} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)}) \right) \\ &\text{Spam} & \text{Non-spam} \end{split}$$

Likelihood - spam

$$\left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})
ight) \qquad \qquad x_k^{(i)}$$
 i-th mail $x_k^{(i)}$ k-th word

Naive Bayes assumption:

$$P(\operatorname{spam}) = Bernoulli(\phi)$$

$$P(\operatorname{word}|\operatorname{spam}) = Multinomial(\mu_1^s, \dots, \mu_M^s)$$

$$P(x^{(i)}|y^{(i)} = 1) = \prod_{k=1}^{len(x^{(i)})} P(x_k^{(i)}|y^{(i)} = 1)$$

$$= \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} (\mu_j^s)^{I(x_k^{(i)} = "j" \operatorname{th} \operatorname{word})}$$

$$P(y^{(i)} = 1) = \phi$$

$$\left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right)$$

$$= \left(\prod_{i:y^{(i)}=1}^{N} \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} (\mu_j^s)^{I\left(x_k^{(i)}="j"\text{th word}\right)} \phi\right)$$

$$\begin{pmatrix}
\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)}) \\
= \left(\prod_{i:y^{(i)}=1}^{N} \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} (\mu_{j}^{s})^{I(x_{k}^{(i)}="j"\text{th word})} \phi \right) \\
= \left(\prod_{i:y^{(i)}=1}^{N} \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} (\mu_{j}^{s})^{I(x_{k}^{(i)}="j"\text{th word})} \right) \left(\prod_{i:y^{(i)}=1}^{N} \phi \right)$$

$$\begin{split} &\left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right) \\ &= \left(\prod_{i:y^{(i)}=1}^{N} \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} \left(\mu_{j}^{s}\right)^{I\left(x_{k}^{(i)}="j"\text{th word}\right)} \phi\right) \\ &= \left(\prod_{i:y^{(i)}=1}^{N} \prod_{k=1}^{len(x^{(i)})} \prod_{j=1}^{M} \left(\mu_{j}^{s}\right)^{I\left(x_{k}^{(i)}="j"\text{th word}\right)}\right) \left(\prod_{i:y^{(i)}=1}^{N} \phi\right) \\ &= \left(\prod_{j=1}^{M} \left(\mu_{j}^{s}\right)^{\sum_{i:y^{(i)}=1}^{N} \sum_{k=1}^{len(x^{(i)})} I\left(x_{k}^{(i)}="j"\text{th word}\right)}\right) \left(\prod_{i:y^{(i)}=1}^{N} \phi\right) \end{split}$$

$$\begin{split} &\left(\prod_{i:y^{(i)}=1}P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right)\\ &=\left(\prod_{i:y^{(i)}=1}^{N}\prod_{k=1}^{len(x^{(i)})}\prod_{j=1}^{M}\left(\mu_{j}^{s}\right)^{I\left(x_{k}^{(i)}="j"\text{th word}\right)}\phi\right)\\ &=\left(\prod_{i:y^{(i)}=1}^{N}\prod_{k=1}^{len(x^{(i)})}\prod_{j=1}^{M}\left(\mu_{j}^{s}\right)^{I\left(x_{k}^{(i)}="j"\text{th word}\right)}\right)\left(\prod_{i:y^{(i)}=1}^{N}\phi\right)\\ &=\left(\prod_{j=1}^{M}\left(\mu_{j}^{s}\right)^{\sum_{i:y^{(i)}=1}^{N}\sum_{k=1}^{len(x^{(i)})}I\left(x_{k}^{(i)}="j"\text{th word}\right)\right)\left(\prod_{i:y^{(i)}=1}^{N}\phi\right)\\ &=\left(\prod_{j=1}^{M}\left(\mu_{j}^{s}\right)^{N_{j}^{spam}}\right)\phi^{N^{spam}} \end{split}$$

Putting together:

$$\prod_{i=1}^{N} P(\mathbf{x}^{(i)}, y^{(i)}) \\
= \left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)}) P(y^{(i)}) \right) \left(\prod_{i:y^{(i)}=0} P(\mathbf{x}^{(i)}|y^{(i)}) P(y^{(i)}) \right)$$

Putting together:

$$\prod_{i=1}^{N} P(\mathbf{x}^{(i)}, y^{(i)})$$

$$= \left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right) \left(\prod_{i:y^{(i)}=0} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right)$$

$$= \left(\phi^{N^{spam}} \prod_{word j} (\mu_{j}^{s})^{N_{j}^{spam}}\right) \left((1-\phi)^{N^{nonspam}} \prod_{word j} (\mu_{j}^{ns})^{N_{j}^{nonspam}}\right)$$

Putting together:

$$\prod_{i=1}^{N} P(\mathbf{x}^{(i)}, y^{(i)})$$

$$= \left(\prod_{i:y^{(i)}=1} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right) \left(\prod_{i:y^{(i)}=0} P(\mathbf{x}^{(i)}|y^{(i)})P(y^{(i)})\right)$$

$$= \left(\phi^{N^{spam}} \prod_{word j} (\mu_j^s)^{N_j^{spam}}\right) \left((1-\phi)^{N^{nonspam}} \prod_{word j} (\mu_j^{ns})^{N_j^{nonspam}}\right)$$

Log-likelihood

$$\log P(\mathcal{D})$$

$$= \log \prod_{i=1}^{N} P(x^{(i)}, y^{(i)})$$

$$= N^{spam} \log \phi + \sum_{word j} N_{j}^{spam} \log \mu_{j}^{s} + N^{nonspam} \log (1 - \phi) + \sum_{word j} N_{j}^{nonspam} \log \mu_{j}^{ns}$$

Log-likelihood

$$\begin{split} & \log P(\mathcal{D}) \\ &= & \log \prod_{i=1}^{N} P(x^{(i)}, y^{(i)}) \\ &= & N^{spam} \log \phi + \sum_{word j} N_{j}^{spam} \log \mu_{j}^{s} + N^{nonspam} \log (1 - \phi) + \sum_{word j} N_{j}^{nonspam} \log \mu_{j}^{ns} \end{split}$$

- Maximum-likelihood
 - Take the derivative of log-likelihood w.r.t. the parameters, and set it to zero.

• From
$$\frac{\partial l}{\partial \phi} = \frac{1}{\phi} N^{spam} - \frac{1}{1-\phi} N^{nonspam} = 0$$

- We get $\phi = \frac{N^{spam}}{N^{spam} + N^{nonspam}}$

• Make the parameters μ independent:

$$\sum_{word \, j=1}^{M} N_{j}^{spam} \log \mu_{j}^{s} = \sum_{word \, j=1}^{M-1} N_{j}^{spam} \log \mu_{j}^{s} + N_{M}^{spam} \log (1 - \sum_{j=1}^{M-1} \mu_{j}^{s})$$

$$\frac{\partial}{\partial \mu_{j}^{s}} \left(\sum_{word \, j=1}^{M} N_{j}^{spam} \log \mu_{j}^{s} \right) = \frac{N_{j}^{spam}}{\mu_{j}^{s}} - \frac{N_{M}^{spam}}{1 - \sum_{j=1}^{M-1} \mu_{j}^{s}} = 0$$

$$\begin{array}{ll} \bullet & \text{From} & \frac{\partial l}{\partial \phi} = \frac{1}{\phi} N^{spam} - \frac{1}{1-\phi} N^{nonspam} = 0 \\ & - \text{We get} & \phi = \frac{N^{spam}}{N^{spam} + N^{nonspam}} \end{array}$$

We finally get

• Make the parameters μ independent:

$$\begin{split} \sum_{word\,j=1}^{M} N_{j}^{spam} \log \mu_{j}^{s} &= \sum_{word\,j=1}^{M-1} N_{j}^{spam} \log \mu_{j}^{s} + N_{M}^{spam} \log (1 - \sum_{j=1}^{M-1} \mu_{j}^{s}) \\ \frac{\partial}{\partial \mu_{j}^{s}} \left(\sum_{word\,j=1}^{M} N_{j}^{spam} \log \mu_{j}^{s} \right) &= \frac{N_{j}^{spam}}{\mu_{j}^{s}} - \frac{N_{M}^{spam}}{1 - \sum_{j=1}^{M-1} \mu_{j}^{s}} = 0 \\ \frac{N_{j}^{spam}}{\mu_{j}^{s}} &= constant, \, \forall j \end{split}$$
 We finally get
$$\mu_{j}^{s} = \frac{N_{j}^{spam}}{\sum_{i} N_{i}^{spam}} \end{split}$$

• Summary:

$$\begin{split} P(spam) &= \phi = \frac{N^{spam}}{N^{spam} + N^{nonspam}} \\ P(word = j | spam) &= \mu_j^s = \frac{N_j^{spam}}{\sum_j N_j^{spam}} \\ P(word = j | non - spam) &= \mu_j^{ns} = \frac{N_j^{nonspam}}{\sum_j N_j^{nonspam}} \end{split}$$

Recall:

 N^{spam} : total # examples for spam $N^{nonspam}$: total # examples for non-spam

 N_j^{spam} : total # word j from the entire spam emails $N_i^{nonspam}$: total # word j from the entire nonspam emails

Laplace smoothing

- Maximum likelihood is problematic when a specific word count is 0
 - Leads to probability of 0!
- Solution: Put "imaginary" counts for each word
 - prevent zero probability estimates (overfitting)!
 - E.g.: Adding "1" as imaginary count for each word

$$\begin{split} P(spam) &= \phi = \frac{N^{spam}}{N^{spam} + N^{nonspam}} \\ P(word = j | spam) &= \mu_j^s = \frac{N_j^{spam} + 1}{\sum_j N_j^{spam} + M} \\ P(word = j | non - spam) &= \mu_j^{ns} = \frac{N_j^{nonspam} + 1}{\sum_j N_j^{nonspam} + M} \end{split}$$

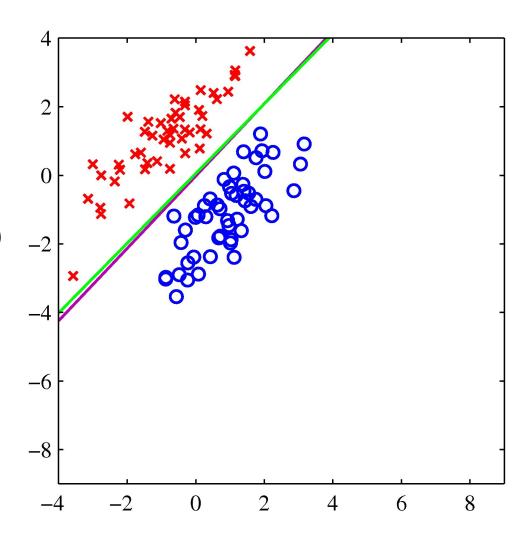
Discriminant functions

Linear Discriminant functions: Discriminating two classes

 Specify a weight vector w and a bias w0

$$h(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + w_0$$

- Assign x to C₁ if
 h(x) ≥ 0 and to C₀
 otherwise.
- Q: How to pick w?



Linear Discriminant functions: Discriminating K>2 classes

• Instead each class C_k gets its own function

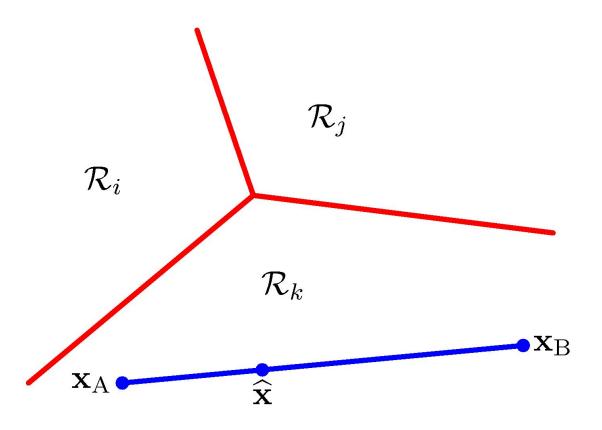
$$h_k(\mathbf{x}) = \mathbf{w}_k^T \mathbf{x} + w_{k,0}$$

– Assign **x** to C_k if

$$h_k(\mathbf{x}) > h_j(\mathbf{x}) \text{ for all } j \neq k$$

• The decision regions are convex polyhedra.

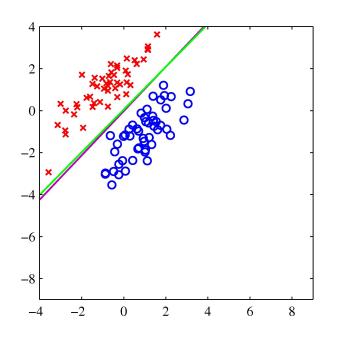
Decision Regions

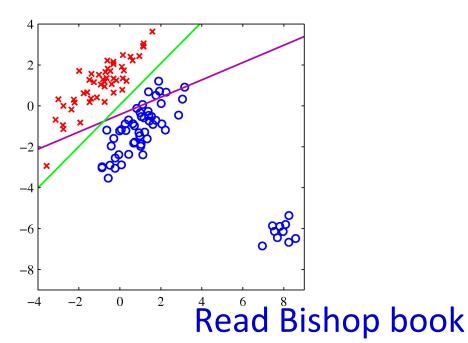


 Decision regions are convex, with piecewise linear boundaries.

How do we set the weights w?

- How about w that minimizes squared error?
 - Label y versus linear prediction h(w).
 - Least squares is too sensitive to outliers. (why?)





Learning linear discriminant functions (this lecture)

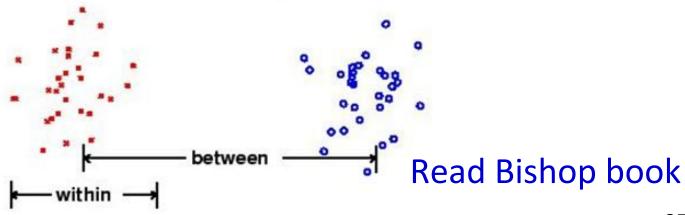
- Fisher's linear discriminant
- Perceptron learning algorithm

Fisher's Linear Discriminant

Use w to project x to one dimension.

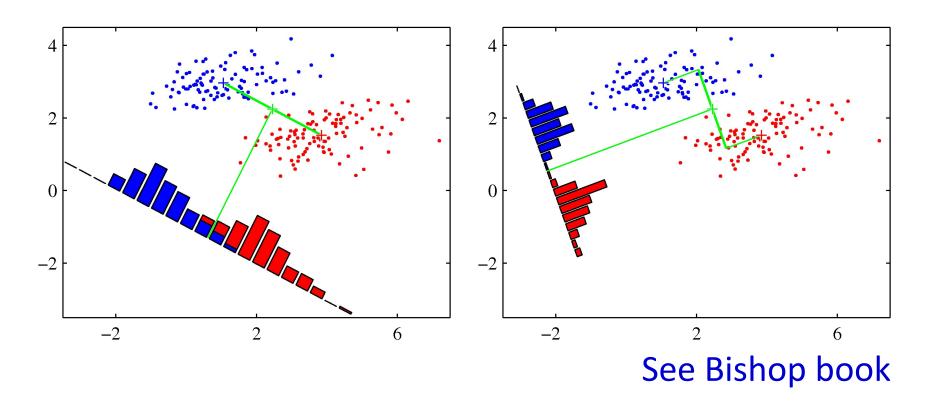
if
$$\mathbf{w}^T \mathbf{x} \geq -w_0$$
 then C_1 else C_0

- Select w that best <u>separates</u> the classes.
- By "separating", the algorithm simultaneously
 - maximizes between-class variances
 - minimizes within-class variances



Fisher's Linear Discriminant

- Maximizing separation alone doesn't work.
 - Minimizing class variance is a big help.



Objective function

We want to maximize the "distance between classes"

$$\underline{m_2}-m_1\equiv \mathbf{w}^T(\mathbf{m}_2-\mathbf{m}_1)$$
 where $\mathbf{m}_k=\frac{1}{N_k}\sum_{n\in C_k}\mathbf{x}_n$ cted mean

Projected mean

Objective function

We want to maximize the "distance between classes"

$$\underline{m_2} - m_1 \equiv \mathbf{w}^T (\underline{\mathbf{m}}_2 - \underline{\mathbf{m}}_1) \qquad \text{where } \underline{\mathbf{m}}_k = \frac{1}{N_k} \sum_{n \in C_k} \mathbf{x}_n$$
 Projected mean

While minimizing the "distance within each class"

$$s_1^2 + s_2^2 \equiv \sum_{n \in C_1} (\mathbf{w}^T \mathbf{x}_n - m_1)^2 + \sum_{n \in C_2} (\mathbf{w}^T \mathbf{x}_n - m_2)^2$$

Objective function

We want to maximize the "distance between classes"

$$\underline{m}_2-m_1\equiv \mathbf{w}^T(\underline{\mathbf{m}}_2-\mathbf{m}_1) \qquad ext{where } \mathbf{m}_k=rac{1}{N_k}\sum_{n\in C_k}\mathbf{x}_n$$
 Projected mean

While minimizing the "distance within each class"

$$s_1^2 + s_2^2 \equiv \sum_{n \in C_1} (\mathbf{w}^T \mathbf{x}_n - m_1)^2 + \sum_{n \in C_2} (\mathbf{w}^T \mathbf{x}_n - m_2)^2$$

• Objective function:
$$J(\mathbf{w}) = \frac{(m_2 - m_1)^2}{s_1^2 + s_2^2}$$

Derivation of objective

- Numerator: $m_2 m_1 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1)$:
 - $||m_2 m_1||^2 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1) (\mathbf{m}_2 \mathbf{m}_1)^T \mathbf{w}$

Derivation of objective

- Numerator: $m_2 m_1 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1)$:
 - $||m_2 m_1||^2 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1) (\mathbf{m}_2 \mathbf{m}_1)^T \mathbf{w}$
- Denominator:
 - $s_k^2 = \sum_{n \in C_k} (\mathbf{w}^T \mathbf{x}_n m_k)^2$ $= \sum_{n \in C_k} \mathbf{w}^T (\mathbf{x}_n \mathbf{m}_k) (\mathbf{x}_n \mathbf{m}_k)^T \mathbf{w}$
 - $s_1^2 + s_2^2 = \mathbf{w}^T \left[\sum_{k=1,2} \sum_{n \in C_k} (\mathbf{x}_n \mathbf{m}_k) (\mathbf{x}_n \mathbf{m}_k)^T \right] \mathbf{w}$

Derivation of objective

- Numerator: $m_2 m_1 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1)$:
 - $||m_2 m_1||^2 = \mathbf{w}^T (\mathbf{m}_2 \mathbf{m}_1) (\mathbf{m}_2 \mathbf{m}_1)^T \mathbf{w}$
- Denominator:
 - $S_k^2 = \sum_{n \in C_k} (\mathbf{w}^T \mathbf{x}_n m_k)^2$ $= \sum_{n \in C_k} \mathbf{w}^T (\mathbf{x}_n \mathbf{m}_k) (\mathbf{x}_n \mathbf{m}_k)^T \mathbf{w}$
 - $s_1^2 + s_2^2 = \mathbf{w}^T \left[\sum_{k=1,2} \sum_{n \in C_k} (\mathbf{x}_n \mathbf{m}_k) (\mathbf{x}_n \mathbf{m}_k)^T \right] \mathbf{w}$
- After definition of terms, we get

$$J(w) = \frac{\mathbf{w}^T S_B \mathbf{w}}{\mathbf{w}^T S_W \mathbf{w}}$$

• Solution: $\mathbf{w} \propto S_W^{-1}(\mathbf{m}_2 - \mathbf{m}_1)$

The Perceptron

A "generalized linear function"

$$h(\mathbf{x}) = f(\mathbf{w}^T \phi(\mathbf{x}))$$

Where

$$f(a) = \begin{cases} +1, & a \ge 0 \\ -1, & a < 0 \end{cases}$$

- Uses target code: y=+1 for C_1 , y=-1 for C_2 .
- Means we always want:

$$\mathbf{w}^T \phi(\mathbf{x}_n) y_n > 0$$

The Perceptron Criterion

Only count errors from misclassified points:

$$E_P(\mathbf{w}) = -\sum_{\mathbf{x}_n \in \mathcal{M}} \mathbf{w}^T \phi(\mathbf{x}) y_n$$

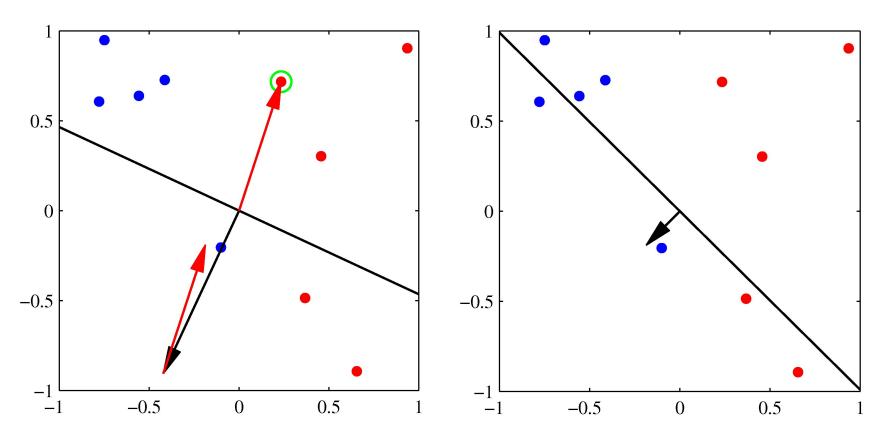
- where M are the misclassified points.
- Stochastic gradient descent:
 - Update the weight vector according to the misclassified points:

$$\mathbf{w}^{(\tau+1)} = \mathbf{w}^{(\tau)} - \eta \nabla E_P(\mathbf{w}) = \mathbf{w}^{(\tau)} + \eta \phi(\mathbf{x}) y_n$$

Note: update only for misclassified examples

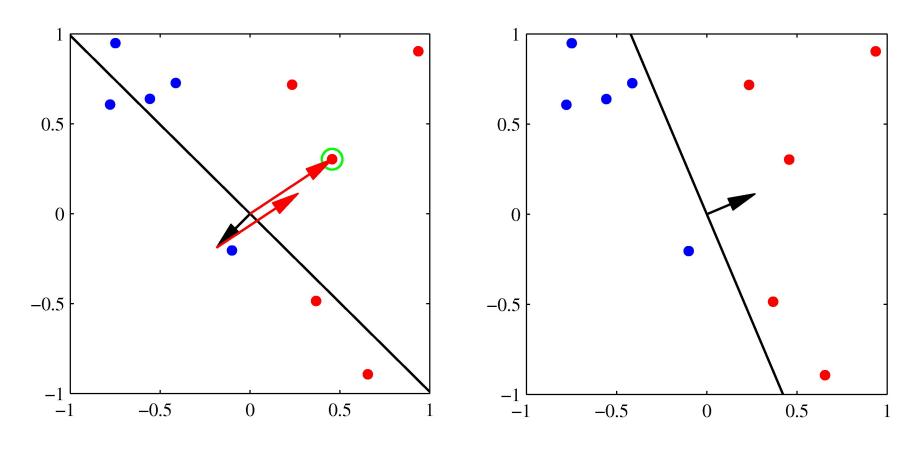
Perceptron Learning (1)

• If \mathbf{x}_n is misclassified, add $\phi(\mathbf{x}_n)$ into w.



Perceptron Learning (2)

• If \mathbf{x}_n is misclassified, add $\phi(\mathbf{x}_n)$ into w.



Perceptron Learning

- Perceptron Convergence Theorem:
 - If there exists an exact solution (i.e., if the training data is linearly separable)
 - then the learning algorithm will find it in a finite number of steps.
- Limitations of perceptron learning:
 - The convergence can be very slow.
 - If dataset is not linearly separable, it won't converge.
 - Does not generalize well to K>2 classes.

Next class

Kernel methods