Principles of Machine Learning

Bayes Classifier



Kevin Moon (kevin.moon@usu.edu)
STAT/CS 5810/6655



Outline



- Multivariate Gaussian distribution
- 2. Probabilistic setting for classification
- 3. Bayes classifier
- 4. Plug-in Methods
 - 1. Linear Discriminant Analysis
 - 2. Logistic Regression
 - 3. Naïve Bayes

Multivariate Gaussian Distribution



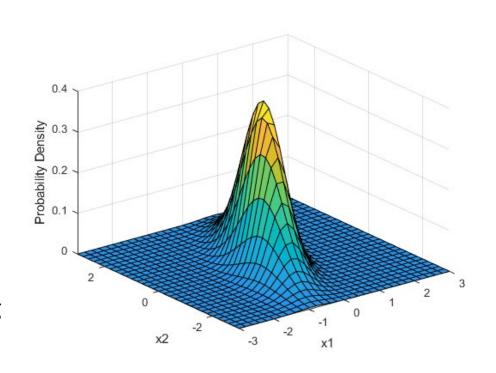
• We say $X \in \mathbb{R}^d$ has a (multivariate) Gaussian distribution if its joint pdf is

$$\phi(x; \mu, \Sigma) := (2\pi)^{-d/2} |\Sigma|^{-1/2} \exp\left(-\frac{1}{2}(x - \mu)^T \Sigma^{-1}(x - \mu)\right)$$

where $\boldsymbol{\mu} \in \mathbb{R}^d$ and Σ is symmetric and positive definite.

- Notation: $X \sim \mathcal{N}(\boldsymbol{\mu}, \Sigma)$
- \bullet $E[X] = \mu$
- $E[(\boldsymbol{X} \boldsymbol{\mu})(\boldsymbol{X} \boldsymbol{\mu})^T] = \Sigma$
- Level sets of a MVG are

• Many uses in machine learning





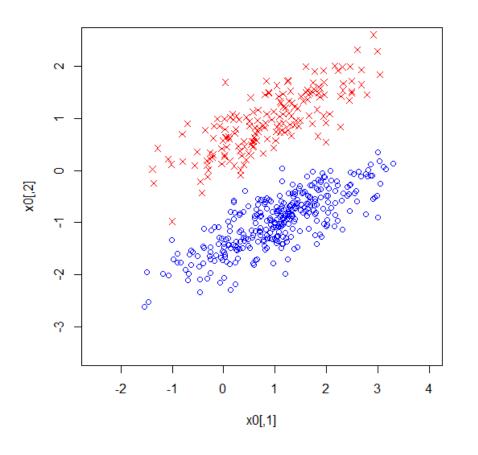
- We are interested in classification (part of supervised learning)
- Feature vector $X \in \mathbb{R}^d$
- Label $Y \in \{1, ..., M\}$
- Assume (X, Y) are jointly distributed (d + 1) dimensional)
- Two ways to think about the joint distribution:
 - 1. $P_{XY} \leftrightarrow (P_{X|Y}, P_Y)$
 - 2. $P_{XY} \leftrightarrow (P_X, P_{Y|X})$



- Two ways to think about the joint distribution
- Binary classification: $Y \in \{0,1\}$
- Notation:
 - Prior class distribution
 - $\pi := \Pr(Y = 1)$
 - Class-conditional distributions
 - $p_0(\mathbf{x}) \coloneqq p_{\mathbf{X}|\mathbf{Y}=0}(\mathbf{x}|0)$
 - $p_1(\mathbf{x}) \coloneqq p_{\mathbf{X}|\mathbf{Y}=1}(\mathbf{x}|1)$
 - Marginal distribution of X
 - $p(x) \coloneqq P_X(x)$
 - Posterior class distribution
 - $\eta(x) \coloneqq P_{Y|X=x}(1|x)$
- First way: $P_{XY} \leftrightarrow (\pi, p_0(x), p_1(x))$
- Second way: $P_{XY} \leftrightarrow (p(x), \eta(x))$
- The two representations are equivalent, but one may be more useful than the other depending on the context



- Example: $\pi=1/3$, p_{γ} are bivariate Gaussians
- $P_{XY} \leftrightarrow (\pi, p_0(x), p_1(x))$

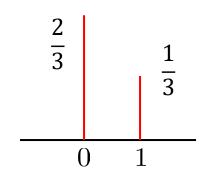


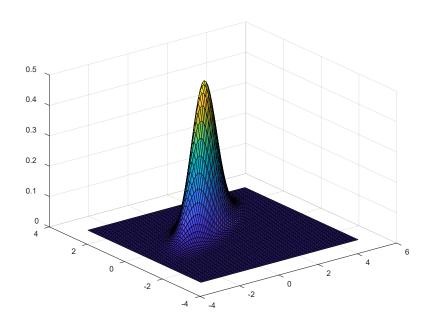
```
N = 500
p = 1/3
y = rbinom(N,1,p)
mu0 = c(1,-1)
mu1 = c(1,1)
Sigma = matrix(c(.9,.4,.4,.3),2,2)
N1 = sum(y)
N0 = N-N1
x0 = mvrnorm(N0, mu0, Sigma)
x1 = mvrnorm(N1,mu1,Sigma)
plot(x0,col='blue',xlim=c(-2.5,4),ylim=c(-3.5,2.5))
points(x1,col='red',pch=4)
```

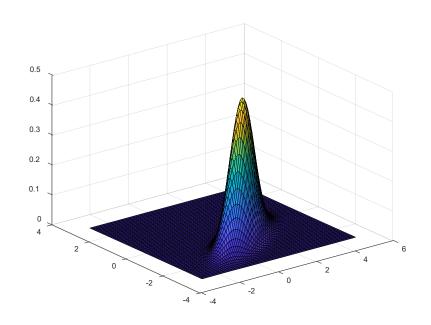


• Example: $\pi=1/3$, p_y are bivariate Gaussians

•
$$P_{XY} \leftrightarrow (\pi, p_0(\mathbf{x}), p_1(\mathbf{x}))$$







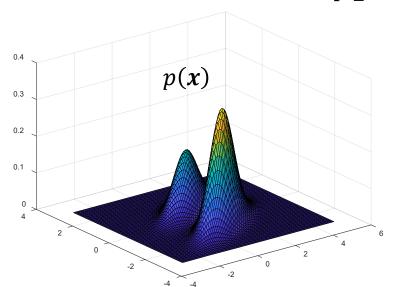


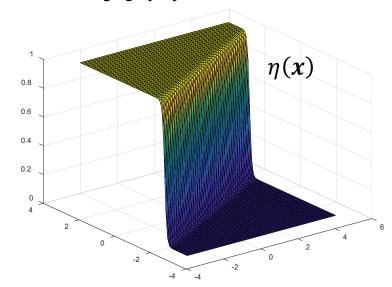
- Example: $\pi=1/3$, p_y are bivariate Gaussians
- $P_{XY} \leftrightarrow (p(x), \eta(x))$
- Law of total probability:

$$p(x) = \pi p_1(x) + (1 - \pi)p_0(x)$$

• Bayes rule:

$$\eta(\mathbf{x}) = \frac{\pi p_1(\mathbf{x})}{\pi p_1(\mathbf{x}) + (1 - \pi)p_0(\mathbf{x})}$$





Multiclass Classification



- Feature vector $X \in \mathbb{R}^d$
- Label $Y \in \{1, ..., M\}$
- Assume (X,Y) are jointly distributed (d+1) dimensional)
- Notation:
 - $\pi_k \coloneqq \Pr(Y = k)$
 - $p_k(\mathbf{x}) \coloneqq p_{\mathbf{X}|Y=k}(\mathbf{x}|k)$
 - $p(\mathbf{x}) = \sum_{k=1}^{M} \pi_k p_k(\mathbf{x})$
 - $\eta_k(\mathbf{x}) \coloneqq P_{Y|\mathbf{X}=\mathbf{x}}(k|\mathbf{x})$
- Equivalent representations
 - $P_{XY} \leftrightarrow (\pi_1, \dots, \pi_M, p_1(\mathbf{x}), \dots, p_M(\mathbf{x}))$
 - $P_{XY} \leftrightarrow (p(x), \eta_1(x), ..., \eta_M(x))$

Bayes Classifier



- A *classifier* is a function $f: \mathbb{R}^d \to \{1, ..., M\}$
- Given a joint distribution P_{XY} of (X,Y), what is the best possible classifier?
 - Depends on how you measure performance
- Most common classification performance measure is the probability of error, or *risk*

$$R(f) \coloneqq P_{XY}(f(X) \neq Y)$$

• I.e., the probability of the event

$$\{(x,y)\in\mathbb{R}^d\times\{1,\ldots,M\}\big|f(x)\neq y\}$$

- The Bayes risk is the smallest risk of any classifier, and is denoted R^{st}
- If $R(f) = R^*$, f is called a Bayes classifier

Bayes Classifier



• **Theorem:** The classifier

$$f^*(\mathbf{x}) = \arg \max_{k=1,...,M} \eta_k(\mathbf{x})$$
$$= \arg \max_{k=1,...,M} \pi_k p_k(\mathbf{x})$$

is a Bayes classifier.

Bayes Classifier: Proof



• **Theorem:** The classifier

$$f^*(\mathbf{x}) = \arg \max_{k=1,...,M} \eta_k(\mathbf{x})$$
$$= \arg \max_{k=1,...,M} \pi_k p_k(\mathbf{x})$$

is a Bayes classifier.

Bayes Classifier: Proof



For convenience, assume $X \mid Y = k$ has a continuous distribution for each k. Let f denote an arbitrary classifier. Denote the decision regions

$$\Gamma_k(f) = \{ \boldsymbol{x} \mid f(\boldsymbol{x}) = k \}$$

Then

$$1 - R(f) = P_{\boldsymbol{X}Y}(f(\boldsymbol{X}) = Y)$$

$$= \sum_{k=1}^{M} P_{Y}(Y = k) \cdot P_{\boldsymbol{X}|Y=k}(f(\boldsymbol{X}) = k)$$

$$= \sum_{k=1}^{M} \pi_{k} \cdot \int_{\Gamma_{k}(f)} p_{k}(\boldsymbol{x}) d\boldsymbol{x}$$

$$= \int_{\mathbb{R}^{d}} (\sum_{k=1}^{M} \pi_{k} p_{k}(\boldsymbol{x}) \mathbf{1}_{\{\boldsymbol{x} \in \Gamma_{k}(f)\}}) d\boldsymbol{x}$$

where $\mathbf{1}_A$ denotes the indicator function on event A.

Bayes Classifier: Proof (cont.)



Notice that $\Gamma_1(f), \ldots \Gamma_K(f)$ from a partition of \mathbb{R}^d , i.e., every $\boldsymbol{x} \in \mathbb{R}^d$ belongs to one and only one $\Gamma_k(f)$. Thus, to maximize 1 - R(f), we should choose $\Gamma_k(f)$ such that

$$\boldsymbol{x} \in \Gamma_k(f) \iff \pi_k p_k(\boldsymbol{x}) \text{ is maximal.}$$

So a Bayes classifier is

$$f^*(\boldsymbol{x}) = \arg\max_k \pi_k p_k(\boldsymbol{x}).$$

Now note that $\sum_{l=1}^{M} \pi_l p_l(\boldsymbol{x})$ is independent of k. The proof is completed by observing

$$\eta_k(oldsymbol{x}) = rac{\pi_k p_k(oldsymbol{x})}{\sum\limits_{l=1}^{M} \pi_l p_l(oldsymbol{x})}$$

which follows by Bayes' rule.

The Bayes Risk



Binary case: a corollary of the theorem is that

$$R^* = \int \min(\eta(\mathbf{x}), 1 - \eta(\mathbf{x})) p(\mathbf{x}) d\mathbf{x}$$
$$= \int \min(\pi p_1(\mathbf{x}), (1 - \pi) p_0(\mathbf{x})) d\mathbf{x}$$

Multi-class case

$$R^* = 1 - \int \max_{k} (\eta_k(\mathbf{x})) p(\mathbf{x}) d\mathbf{x}$$
$$= 1 - \int \max_{k} (\pi_k p_k(\mathbf{x})) d\mathbf{x}$$

Plug-in Classifiers

LDA, naïve Bayes, logistic regression

Plug-in classifiers



- In most machine learning problems, P_{XY} is unknown
 - Therefore, so is the Bayes classifier
- One approach: estimate the quantities from training data and plug the estimates in the formula to get a classifier
- Linear discriminant analysis (LDA) and naïve Bayes have the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\pi}_{k} \, \hat{p}_{k}(\mathbf{x})$$

Logistic regression has the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\eta}_{k}(\mathbf{x})$$

Linear Discriminant Analysis



• Training data

$$(\boldsymbol{x}_1,y_1),\ldots,(\boldsymbol{x}_n,y_n)\stackrel{iid}{\sim} P_{\boldsymbol{X}Y}.$$

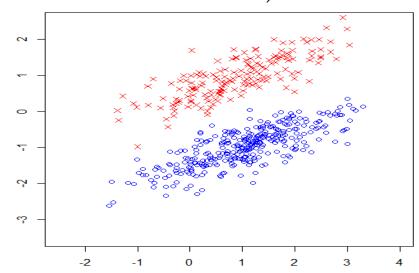
• LDA assumption:

$$X \mid Y = k \sim \mathcal{N}(\boldsymbol{\mu}_k, \Sigma), \quad k = 1, \dots, M$$

for some unknown μ_1, \ldots, μ_M and Σ . Equivalently

$$p_k(\mathbf{x}) = (2\pi)^{-d/2} |\Sigma|^{-1/2} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_k)^T \Sigma^{-1}(\mathbf{x} - \boldsymbol{\mu}_k)\right)$$

• LDA is the plug-in rule based on this model. We use training data to estimate μ_1, \ldots, μ_M and Σ .



LDA Estimates



 LDA is the classifier obtained by plugging the following into the Bayes classifier formula:

•
$$\hat{\pi}_k = \frac{n_k}{n}$$
, $n_k = |\{i: y_i = k\}|$

•
$$\widehat{\boldsymbol{\mu}}_k = \frac{1}{n_k} \sum_{i:y_i=k} \boldsymbol{x}_i$$

•
$$\widehat{\Sigma} = \frac{1}{n} \sum_{i=1}^{n} (\mathbf{x}_i - \widehat{\boldsymbol{\mu}}_{y_i}) (\mathbf{x}_i - \widehat{\boldsymbol{\mu}}_{y_i})^T$$

- $\widehat{\mu}_k$ is the sample mean for each class
- $\widehat{\Sigma}$ is the pooled sample covariance
- These estimates are all *maximum likelihood estimates*

LDA is a linear classifier



• Binary setting, $Y \in \{0,1\}$. A classifier f is called linear if it has the form

$$f(\boldsymbol{x}) = \begin{cases} 1 & \text{if } \boldsymbol{w}^T \boldsymbol{x} + b \ge 0 \\ 0 & \text{if } \boldsymbol{w}^T \boldsymbol{x} + b < 0 \end{cases}$$

for some $\mathbf{w} \in \mathbb{R}^d$ and $b \in \mathbb{R}$. (The case $\mathbf{w}^T \mathbf{x} + b = 0$ can be labeled arbitrarily.)

LDA is a linear classifier



• Binary setting, $Y \in \{0,1\}$. A classifier f is called *linear* if it has the form

$$f(\boldsymbol{x}) = \begin{cases} 1 & \text{if } \boldsymbol{w}^T \boldsymbol{x} + b \ge 0 \\ 0 & \text{if } \boldsymbol{w}^T \boldsymbol{x} + b < 0 \end{cases}$$

for some $\mathbf{w} \in \mathbb{R}^d$ and $b \in \mathbb{R}$. (The case $\mathbf{w}^T \mathbf{x} + b = 0$ can be labeled

poitrarily.)
$$f(x) = \begin{cases} 1 & \hat{\pi}_i \hat{p}_i(x) = \hat{\pi}_o \hat{p}_o(x) \\ 0 & \text{otherwise} \end{cases}$$

=
$$\begin{cases} 0 & \text{otherwise} \end{cases}$$

= $\begin{cases} 1 & \text{log } \hat{\pi}_1 + \text{log } \hat{p}_1(x) \geq \text{log } \hat{\pi}_0 + \text{log } \hat{p}_0(x) \end{cases}$
ow

Need to show
$$log \hat{\pi}_1 + log \hat{p}_1(x) - log \hat{\pi}_0 - log \hat{p}_0(x) = u^T x + b$$

LDA is a linear classifier

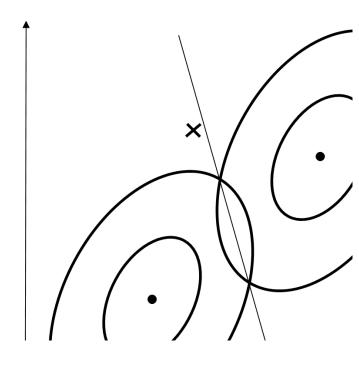


Mahalanobis Distance



- Which mean is closer to the test point?
 - Figure assumes $\pi_0 = \pi_1$
- The LDA classifier assigns x to the class with the nearest "centroid" $\hat{\mu}_0$ or $\hat{\mu}_1$ where distance is the Mahalanobis distance:

$$d_M(\mathbf{x}, \widehat{\boldsymbol{\mu}}) \coloneqq \sqrt{(\mathbf{x} - \widehat{\boldsymbol{\mu}})^T \widehat{\Sigma}^{-1} (\mathbf{x} - \widehat{\boldsymbol{\mu}})}$$



Group Exercise



- 1. Is LDA generative or discriminative?
- 2. Is LDA parametric or nonparametric?
- 3. What do the decision regions look like for the multiclass case?
- 4. Interpret LDA in the case where Σ is assumed to be a multiple of the identity $\sigma^2 I$
- Describe the decision boundary in the two-class case when the covariance matrices are not assumed to be the same but are estimated separately
- 6. What are some drawbacks of LDA?

Naïve Bayes

Review: Plug-in classifiers



- In most machine learning problems, P_{XY} is unknown
 - Therefore, so is the Bayes classifier
- One approach: estimate the quantities from training data and plug the estimates in the formula to get a classifier
- Linear discriminant analysis (LDA) and naïve Bayes have the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\pi}_{k} \, \hat{p}_{k}(\mathbf{x})$$

Logistic regression has the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\eta}_{k}(\mathbf{x})$$

Naïve Bayes Assumption



Training data

$$(X_1, Y_1), ..., (X_n, Y_n) \sim P_{XY}.$$

Notation:

$$X = \begin{bmatrix} X^{(1)} \\ \vdots \\ X^{(d)} \end{bmatrix}$$

- Naïve Bayes assumption: given Y, the components $X^{(1)}, \dots, X^{(d)}$ are independent
- Naïve Bayes is a plug-in method. It could be generative or discriminative and parametric or nonparametric depending on how the distribution of $X^{(j)}|Y=k$ is modeled.

Naïve Bayes



- Main use: Features with finite range
- Assume the possible outcomes of $X^{(j)}$ are z_1, \ldots, z_L .
- Example: Document Classification
- Suppose we wish to classify documents into categories like "business," "politics," "sports," etc. A simple yet popular feature representation is the <u>bag-of-words</u> representation. A document is represented as a vector

$$oldsymbol{X} = egin{bmatrix} X^{(1)} \ dots \ X^{(d)} \end{bmatrix}$$

where d is the number of words in the vocabulary, and

$$X^{(j)} = \begin{cases} 1 & \text{if } j^{th} \text{ word occurs in document} \\ 0 & \text{otherwise.} \end{cases}$$

• In this example, L = 2

Naïve Bayes Classifier



• Let $p_k(x)$ be the pmf of X|Y=k. By the Naïve Bayes assumption

$$p_k(\mathbf{x}) = \prod_{j=1}^d p_k^{(j)} (x^{(j)})$$

where $p_k^{(j)}(x^{(j)})$ is the marginal pmf of $X^{(j)}|Y=k$.

• Let $(x_1, y_1), ..., (x_n, y_n)$ be the training data and let

$$\hat{\pi}_k = \frac{n_k}{n}$$
, $n_k = |\{i: y_i = k\}|$

$$\hat{p}_k^{(j)} = \text{estimate of } p_k^{(j)}$$

• Then the Naïve Bayes classifier is

$$\hat{f}(x) = \arg\max_{k} \hat{\pi}_{k} \prod_{j=1}^{n} \hat{p}_{k}^{(j)} (x^{(j)})$$

Naïve Bayes Classifier



- How should we estimate $p_k^{(j)}$?
- Denote

$$n_k = |\{i: y_i = k\}|$$
 $n_{kl}^{(j)} = \left| \{i: y_i = k \text{ AND } x_i^{(j)} = z_l \} \right|$

• Then the natural (and maximum likelihood) estimate of

$$p_k^{(j)}(z_l) = \Pr\{X^{(j)} = z_l | Y = k\}$$

is

$$\hat{p}_k^{(j)}(z_l) = \frac{n_{kl}^{(j)}}{n_k}$$

Logistic Regression

Review: Plug-in classifiers



- In most machine learning problems, P_{XY} is unknown
 - Therefore, so is the Bayes classifier
- One approach: estimate the quantities from training data and plug the estimates in the formula to get a classifier
- Linear discriminant analysis (LDA) and naïve Bayes have the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\pi}_{k} \, \hat{p}_{k}(\mathbf{x})$$

Logistic regression has the form

$$f(\mathbf{x}) = \arg\max_{k} \hat{\eta}_{k}(\mathbf{x})$$

Logistic Regression

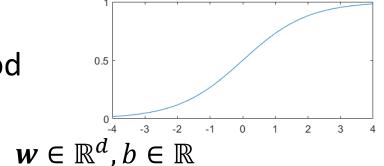


• For binary classification with labels $Y \in \{0,1\}$, the Bayes classifier can be written as

$$f^*(\mathbf{x}) = \begin{cases} 1 & \text{if } \eta(\mathbf{x}) \ge \frac{1}{2} \\ 0 & \text{otherwise} \end{cases}$$

- Recall $\eta(x) := \Pr(Y = 1 | X = x)$
- Logistic Regression is a plug-in method
 - Assume

$$\eta(\mathbf{x}) = \frac{1}{1 + \exp(-(\mathbf{w}^T \mathbf{x} + b))},$$



Determine an estimate

$$\hat{\theta} = \begin{bmatrix} \hat{b} \\ \hat{w} \end{bmatrix}$$
 of $\theta = \begin{bmatrix} b \\ w \end{bmatrix} \in \mathbb{R}^{d+1}$

Plug the below estimate into the formula for the Bayes classifier 3.

$$\hat{\eta}(x) = \frac{1}{1 + \exp\left(-\left(\hat{w}^T x + \hat{b}\right)\right)}$$

Logistic Regression is a linear classifier



$$\hat{f}(x) = 1 \iff \hat{\eta}(x) \ge \frac{1}{2}$$

$$\Leftrightarrow \frac{1}{1 + \exp\left(-(\hat{w}^T x + \hat{b})\right)} \ge \frac{1}{2}$$

$$\Leftrightarrow 1 \ge \exp\left(-(\hat{w}^T x + \hat{b})\right)$$

$$\Leftrightarrow \hat{w}^T x + \hat{b} \ge 0$$

Why Logistic Regression?



- More than a classifier—it predicts the probability of each class
 - Gives a little bit of interpretability
- Slightly more flexible than LDA
- Widely used in health sciences and other applications

Visualizing the Posterior



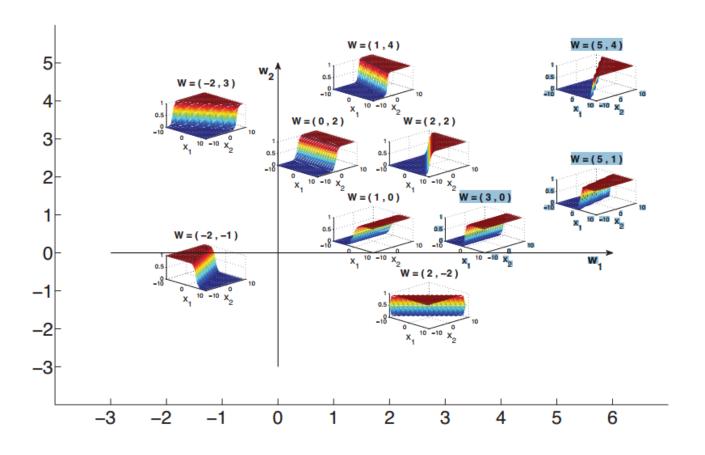


Figure 8.1 Plots of $\operatorname{sigm}(w_1x_1 + w_2x_2)$. Here $\mathbf{w} = (w_1, w_2)$ defines the normal to the decision boundary. Points to the right of this have $\operatorname{sigm}(\mathbf{w}^T\mathbf{x}) > 0.5$, and points to the left have $\operatorname{sigm}(\mathbf{w}^T\mathbf{x}) < 0.5$. Based on Figure 39.3 of (MacKay 2003). Figure generated by sigmoidplot2D.

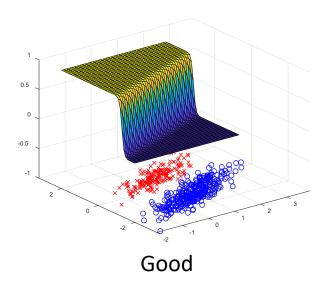
Figure from Murphy, p. 246

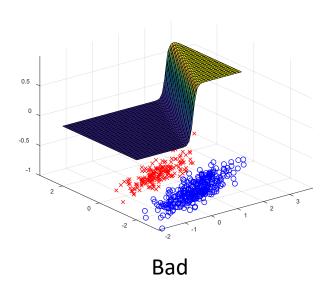
Implementing Logistic Regression



• How do you estimate
$$\theta = \begin{bmatrix} b \\ w \end{bmatrix}$$
?

- $\min_{\boldsymbol{\theta}} \sum_{i} (y_i \eta(\boldsymbol{x}_i; \boldsymbol{\theta}))^2$?
 - Not convex
- \min_{θ} training error?
 - Not convex nor differentiable
- Maximum likelihood





Maximum likelihood estimation (MLE)



- Let $p(y|x;\theta)$ denote the conditional pmf of y given x
 - It is also a function of $oldsymbol{ heta}$
- Observe

$$p(y|\mathbf{x};\boldsymbol{\theta}) = \begin{cases} 1 - \eta(\mathbf{x};\boldsymbol{\theta}) & y = 0 \\ \eta(\mathbf{x};\boldsymbol{\theta}) & y = 1 \end{cases}$$
$$= \eta(\mathbf{x};\boldsymbol{\theta})^y (1 - \eta(\mathbf{x};\boldsymbol{\theta}))^{1-y}$$

• The *likelihood* of $\boldsymbol{\theta}$ is defined to be

$$L(\boldsymbol{\theta}) := \prod_{i=1}^{n} p(y_i|\boldsymbol{x}_i;\boldsymbol{\theta})$$
$$= \prod_{i=1}^{n} \eta(\boldsymbol{x}_i;\boldsymbol{\theta})^{y_i} (1 - \eta(\boldsymbol{x}_i;\boldsymbol{\theta}))^{1-y_i}$$

• Choose $\boldsymbol{\theta}$ that maximizes $L(\boldsymbol{\theta})$

Log likelihood



Notation

$$\widetilde{\boldsymbol{x}}_{i} = \begin{bmatrix} 1, x_{i}^{(1)}, \dots, x_{i}^{(d)} \end{bmatrix}^{T}$$

$$\boldsymbol{\theta} = \begin{bmatrix} b, w^{(1)}, \dots, w^{(d)} \end{bmatrix}^{T}$$

• The log-likelihood of $oldsymbol{ heta}$ is

$$\ell(\boldsymbol{\theta}) := \log L(\boldsymbol{\theta})$$

$$= \sum_{i=1}^{n} \left[y_i \log \left(\frac{1}{1 + e^{-\boldsymbol{\theta}^T \widetilde{\boldsymbol{x}}_i}} \right) + (1 - y_i) \log \left(\frac{e^{-\boldsymbol{\theta}^T \widetilde{\boldsymbol{x}}_i}}{1 + e^{-\boldsymbol{\theta}^T \widetilde{\boldsymbol{x}}_i}} \right) \right]$$

- Take the derivative wrt $oldsymbol{ heta}$ and set to zero
 - No closed form solution
 - Need other tools to solve this (optimization theory)

Further reading



- Murphy, Machine Learning: A Probabilistic Perspective
- ISL Sections 2.2 and 4.4
- ESL Sections 2.4 and 4.3