ECE 302: Chapter 06 Extra: Classification

Fall 2018

Prof Stanley Chan

School of Electrical and Computer Engineering
Purdue University

Purdue University
Classification — A Primer
Terminologies

Definition (Likelihood, Prior, Posterior)
Let \( X \in \mathbb{R}^d \) be a random variable. Let \( Y \in \{1, 2\} \) be the class. The likelihood of \( X \) given \( Y \)
is

\[
f_{X|Y}(x|i) = \frac{1}{\sqrt{(2\pi)^d |\Sigma_i|}} \exp \left\{ -\frac{1}{2} (x - \mu_i)^T \Sigma_i^{-1} (x - \mu_i) \right\}. \tag{1}
\]

The prior of \( Y \) is \( f_Y(i) = \pi_i \).

The posterior of \( Y \) given \( X \) is

\[
f_{Y|X}(i|x) = \frac{f_{X|Y}(x|i)f_Y(i)}{f_X(x)} \propto \frac{1}{\sqrt{(2\pi)^d |\Sigma_i|}} \exp \left\{ -\frac{1}{2} (x - \mu_i)^T \Sigma_i^{-1} (x - \mu_i) \right\} \cdot \pi_i. \tag{2}
\]
Definition (MAP Decision)
The maximum-a-posterior decision is

\[ f_{Y|x}(1|x) \geq_{C_2} c_{1} f_{Y|x}(2|x). \]  \hspace{1cm} (3)

Why this?
MAP Decision

Theorem (MAP rule)

For multidimensional Gaussian, the decision is simplified to

\[
g_1(x) \gtrless_{C_2}^{C_1} g_2(x),
\]

where

\[
g_1(x) = \frac{1}{2}(x - \mu_1)^T \Sigma_1^{-1}(x - \mu_1) + \frac{1}{2} \log |\Sigma_1| - \log \pi_1,
\]

\[
g_2(x) = \frac{1}{2}(x - \mu_2)^T \Sigma_2^{-1}(x - \mu_2) + \frac{1}{2} \log |\Sigma_2| - \log \pi_2.
\]

Why Care?
Simplified Case

What if $\Sigma_i = \sigma^2 I$?

**Corollary (Simplified Case)**

If $\Sigma_i = \sigma^2 I$, the MAP decision is reduced to

$$g_1(x) \preceq_{\frac{C_1}{C_2}} g_2(x),$$

where

$$g_1(x) = \left( \frac{\mu_1}{\sigma^2} \right)^T x - \left( \frac{\|\mu_1\|^2}{2\sigma^2} + \log \pi_1 \right)$$

$$g_2(x) = \left( \frac{\mu_2}{\sigma^2} \right)^T x - \left( \frac{\|\mu_2\|^2}{2\sigma^2} + \log \pi_2 \right).$$
Simplifying the rules

Just need to check this:

\[ g_1(x) - g_2(x) \geq_{\frac{C_1}{C_2}} 0. \]

and what is \( g_1(x) - g_2(x) \)?

**Corollary**

\[ g_1(x) - g_2(x) = w^T (x - x_0), \geq_0 \]  \hspace{1cm} (8)

where

\[ w = \frac{\mu_1 - \mu_2}{\sigma^2} \]

\[ x_0 = \frac{\mu_1 + \mu_2}{2} + \sigma^2 \left( \log \frac{\pi_1}{\pi_2} \right) \frac{\mu_1 - \mu_2}{\|\mu_1 - \mu_2\|^2}. \]  \hspace{1cm} (9)
Geometry!

\[ w^T(x - x_0) < 0 \quad \text{and} \quad w^T(x - x_0) > 0 \]
Adversarial Attack — A Primer
Adversarial Attack

$z_0$ is the original correct input. Assume $\mathbf{w}^T(z_0 - x_0) > 0$.

**Definition**

Adversarial attack is a perturbation of $z_0$ such that

$$\minimize_{\mathbf{z}} \|\mathbf{z} - \mathbf{z}_0\|^2, \quad \text{subject to} \quad \mathbf{w}^T(\mathbf{z} - \mathbf{x}_0) \leq 0. \quad (10)$$

**Why works?**
Geometry of Attack

$Z_0 + \eta w$
Minimum Perturbation Distance

\[ \lambda^* = \frac{w^T(x_0 + w_0)}{\|w\|_2} \]
Example
ECE 302: Chapter 06: Limit Theorem

Fall 2018
Prof Stanley Chan

School of Electrical and Computer Engineering
Purdue University

Purdue
1. Introduction
Statistics is for BIG data
Let $X_1, \ldots, X_N$ be a sequence of i.i.d. random variables.
For example,

- $X_n$ is a state (+1 or -1) of a magnet
- $X_n$ is the energy state of a molecule
- $X_n$ is the instantaneous frequency of the current
- $X_n$ is the rating of a movie

You are usually not interested in these individual $X_n$'s.

Let $M_N$ be the **sample mean**:

$$ M_N = \frac{1}{N} \sum_{n=1}^{N} X_n. $$

- You care about $M_N$ because you want to get the macro-perspective of the system.
- You care about $M_N$ when $N$ is very large, i.e., $N \rightarrow \infty$. 
As $N \to \infty$:

Two questions to ask:

- Where does $M_N$ converge to? **Law of Large Number**.
- What is the distribution of $M_N$? **Central Limit Theorem**.