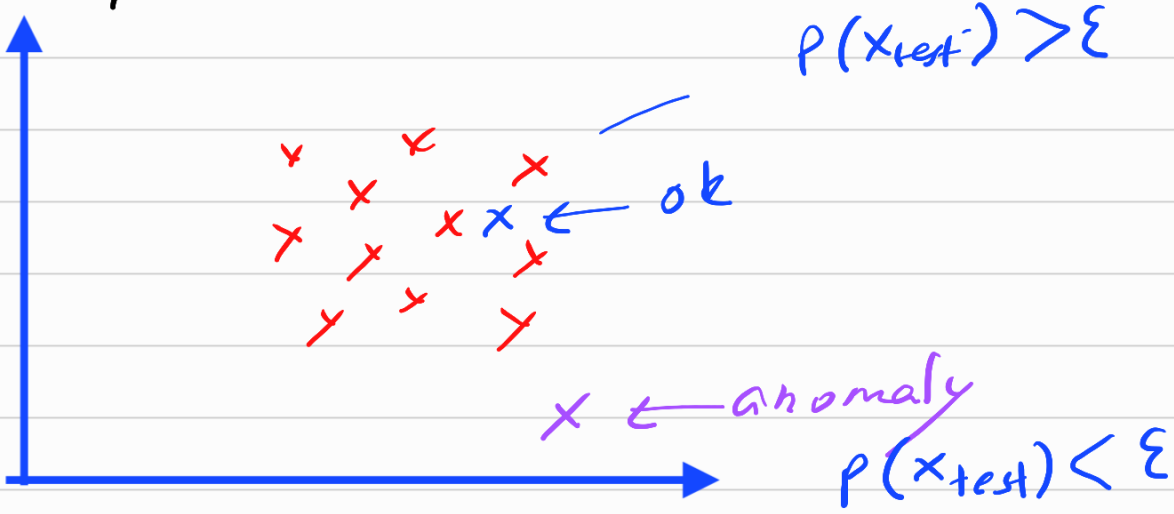
Anomaly Detection;



Density estimation;

↳ Probability of x being seen in dataset.

eg:-

Fraud detection

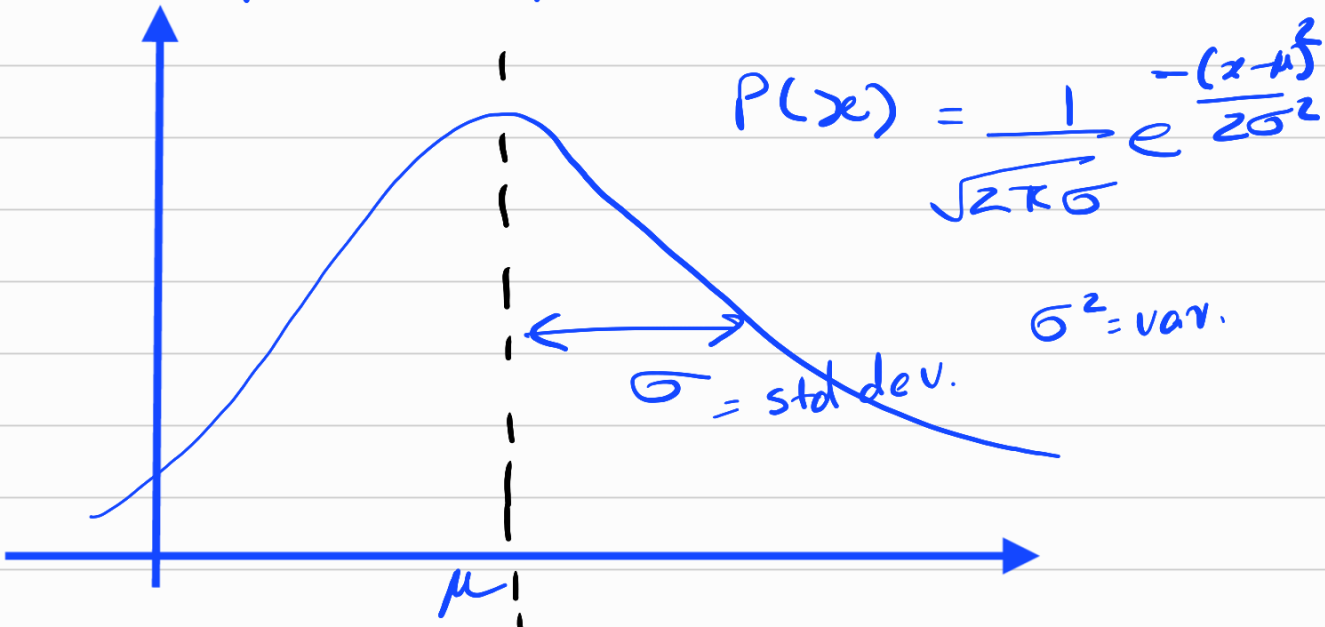
normal features of user

how often login ?

transactions ?

typing speed ?

Gaussian / Normal / Bell Distribution



Parameter estimation

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x^{(i)} \qquad \sigma^2 = \frac{1}{m}\sum_{i=1}^{m}\left(x^{(i)} - \mu\right)^2$$

maximum likelihood estimates for μ, σ

$$\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

$$p(x) = p(x_1) \cdot p(x_2) \cdot p(x_3) \cdots p(x_n)$$

$$; \mu_1, \sigma_1^2 \quad \cdots \quad \mu_n, \sigma_n^2$$

eg:- x_1 = high temp = 1/10

x_2 = high vibration = 1/40

$$p(x_1, x_2) = p(x_1) \cdot p(x_2) = \frac{1}{200}$$

Algorithm:

① choose n features x_i

② Fit parameters

$$\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)} \qquad \sigma_j^2 = \frac{1}{m}\sum_{i=1}^{m}(x_j^{(i)} - \mu_j)^2$$

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x^{(i)} \xrightarrow{\text{vectorized}} \mu = \begin{matrix}\mu_1 \\ \mu_2 \\ \vdots \\ \mu_n\end{matrix}$$

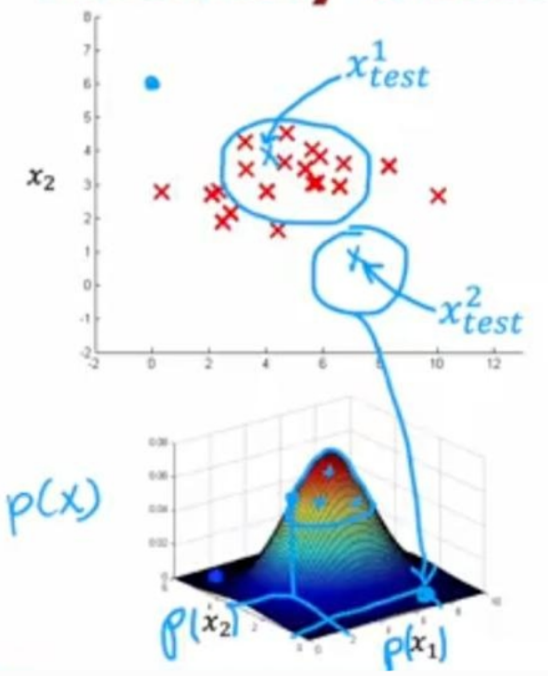
③ Given new example x,

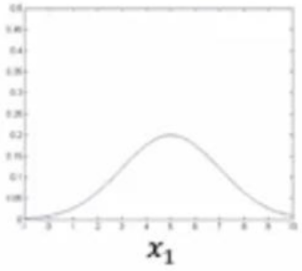
$$p(x) = \prod_{j=1}^{n} \frac{1}{\sqrt{2\pi}\sigma_j} \exp\left(-\frac{(x_j - \mu_j)^2}{2\sigma_j^2}\right)$$

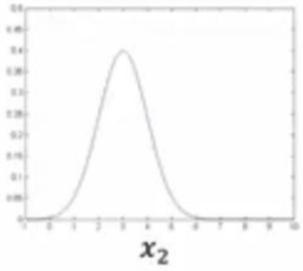
if $p(x) < \varepsilon \longrightarrow$ anomaly

if an anomaly $\longrightarrow$ unusually large
unusually small
— multiplication $< \varepsilon$

Anomaly detection example







$\mu_1 = 5,\ \sigma_1 = 2$

$p(x_1; \mu_1, \sigma_1^2)$

$\mu_2 = 3,\ \sigma_2 = 1$

$p(x_2; \mu_2, \sigma_2^2)$

$\varepsilon = 0.02$

$p\left(x^{(1)}_{test}\right) = 0.0426 \longrightarrow$ "ok"

$p\left(x^{(2)}_{test}\right) = 0.0021 \longrightarrow$ anomaly

Real-Number evaluation;

normal ex:- $y = 0$

include some anomalies $y = 1$

↳ tune ε tune x_j

alt. → No test set

$$y = \begin{cases} 1 & \text{if } p(x) < \varepsilon \text{ (anomaly)} \\ 0 & \text{if } p(x) \geq \varepsilon \text{ (normal)} \end{cases}$$

alternatives;

true positive, negative

false — precision / recall

F1-score

Anomaly

small no. of positive examples

many types. So hard to learn from positive examples (new anomalies)

Fraud detection

↳ unseen ones

Supervised

Large number of positive & negative

enough positive example

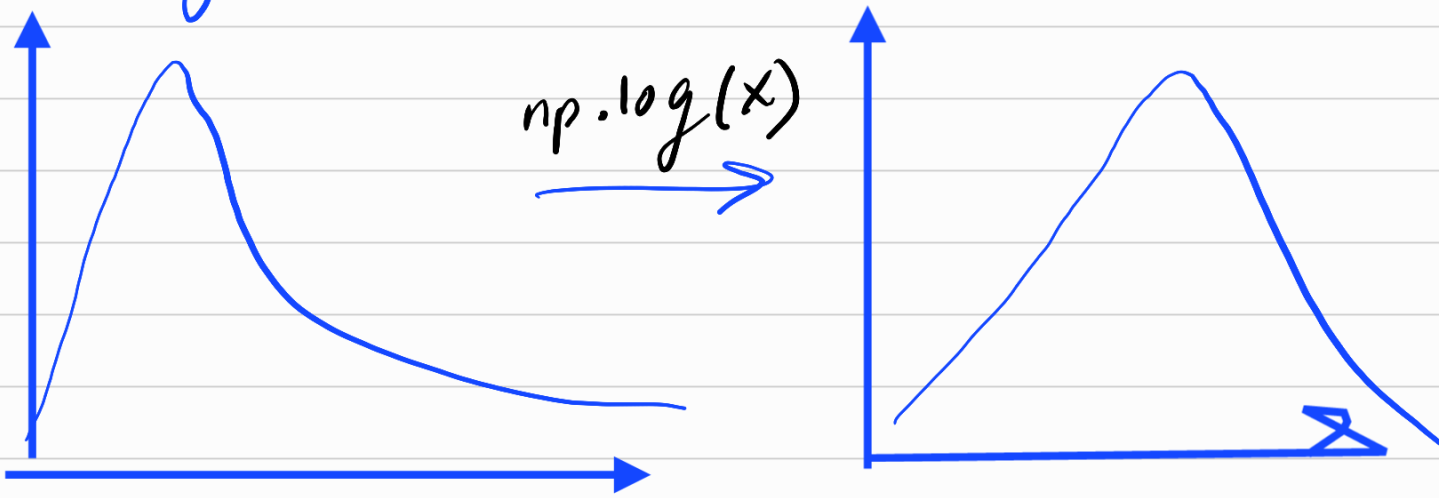
→ future ones similar

Email Spam class.

previously seen

Choosing features;

Non gussian;



$x_1 \leftarrow \log(x_1)$

$x_2 \leftarrow \log(x_2+1)$ $\quad \log(x_2+c)$

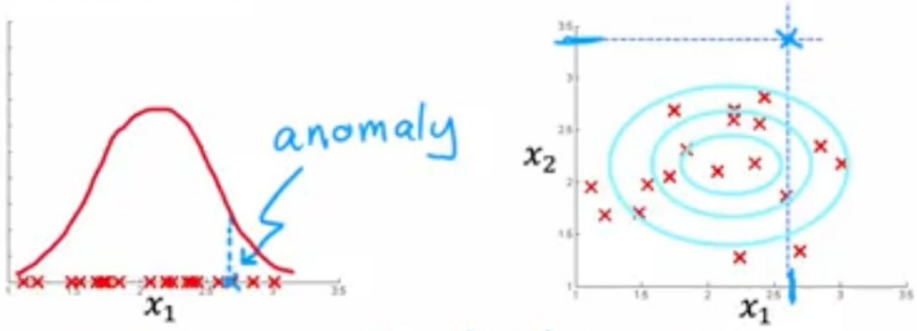
$x_3 = \sqrt{x_3} = x_3$

$x_4 \leftarrow x_4^{1/3}$

Error analysis for anomaly detection

Want $p(x) \geq \varepsilon$ large for normal examples x.
$p(x) < \varepsilon$ small for anomalous examples x.

Most common problem:
$p(x)$ is comparable for normal and anomalous examples.
($p(x)$ is large for both)



X_1 num transactions X_2 typing speed

Features ⟶ Unusually large or small values in the event

ex:- CPU load ↑ } anomaly
network traffic ↓

↓

x_3 = CPU load or $\leftarrow^2$
Network traffic