



Linear Regression

m: Number of training examples

x⁽ⁱ⁾: "input" variable / featurey⁽ⁱ⁾: "output" variable / target variable

h(x)

$$h_{\theta}(x) = \theta_0 + \theta_1 x$$

θ_i's : parametersminimize $\frac{1}{m} \sum_{i=1}^m (h_{\theta}(x^{(i)}) - y^{(i)})^2$

cost function

$$\theta_0, \theta_1 \Rightarrow J(\theta_0, \theta_1) = \frac{1}{m} \sum_{i=1}^m (h_{\theta}(x^{(i)}) - y^{(i)})^2$$

(x, y) ← One training example

(x⁽ⁱ⁾, y⁽ⁱ⁾) i-th training example

Training Set

Learning Algorithm

hypothesis

squared error function



X → h → Y

surf(X, Y, Z)
 [X Y] = meshgrid(X, Y)
 Z = X.^Y

Hypothesis: $h_{\theta}(x) = \theta_0 + \theta_1 x$ Parameter: θ_0, θ_1 Cost function: $J(\theta_0, \theta_1) = \frac{1}{m} \sum_{i=1}^m (h_{\theta}(x^{(i)}) - y^{(i)})^2$ Goal: minimize $J(\theta_0, \theta_1)$

[Gradient descent algorithm]

learning rate

$$\theta_j := \theta_j - \alpha \frac{\partial}{\partial \theta_j} J(\theta_0, \theta_1)$$

 $\theta_0 := \theta_0 - \alpha \frac{\partial}{\partial \theta_0} J(\theta_0, \theta_1)$ $\theta_1 := \theta_1 - \alpha \frac{\partial}{\partial \theta_1} J(\theta_0, \theta_1)$

↓ D

J(θ_1)J(θ_0)θ₁θ₀J(θ_1)θ₁J(θ_0)θ₀J(θ_1)θ₁J(θ_0)θ₀

[Feature Scaling]

Idea: Make sure features are on a similar scale

$$\text{E.g. } x_1 = \text{size (0~2000 feet)}$$

$$x_2 = \text{number of bedrooms (1~5)}$$

\Rightarrow

$$\begin{aligned} x_1 &= \frac{\text{size}}{2000} & \theta_2 & \text{converge faster} \\ x_2 &= \frac{\text{number of rooms}}{5} & \theta_1 & \end{aligned}$$

$$\text{ratio} = 2000 : 5$$

Very long time to find global minimum

[Mean normalization]

Replace x_i with $x_i - \mu_i$ to make features have approximately zero mean (Do not apply to $\theta_0 = 1$)

$$\text{E.g. } x_1 = \frac{\text{size}-100}{2000} \quad x_2 = \frac{\text{bedrooms}-2}{5} \quad \begin{cases} -0.5 \leq x_1 \leq 0.5 \\ -0.5 \leq x_2 \leq 0.5 \end{cases}$$

$$x_1 \leftarrow \frac{x_1 - \mu_1}{s_1} \quad s_1 \leftarrow \text{range of the value (max-min)}$$

[Polynomial Regression] Sigmoid function $\text{Quadratic function}$ Cubic function

[Normal Equation]

Method to solve for θ analytically

$$\begin{aligned} X &= \begin{bmatrix} 1 & x_1^{(1)} & x_2^{(1)} & \dots & x_n^{(1)} \\ 1 & x_1^{(2)} & x_2^{(2)} & \dots & x_n^{(2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_1^{(m)} & x_2^{(m)} & \dots & x_n^{(m)} \end{bmatrix} & y &= \begin{bmatrix} y^{(1)} \\ \vdots \\ y^{(m)} \end{bmatrix} \\ \text{design matrix} & m \times (n+1) & n \text{ features} & \end{aligned}$$

[Gradient Descent vs Normal Equation]

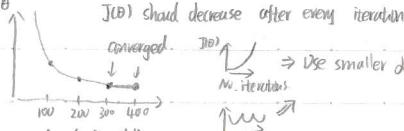
Need to choose α	No need to choose α
Need many iterations	Don't need to iterate
Work well even if n is large	Need to compute $(X^T X)^{-1}$ $O(n^3)$ slow if n is very large

$\dots n=1000$

Get every feature into approximately a $-1 \leq x_i \leq 1$ range

[Making sure gradient descent is working correctly]

min J(θ)



J(θ) should decrease after every iteration
converged \rightarrow use smaller α
No. of iterations

$$\begin{aligned} h_{\theta}(x) &= \theta_0 + \theta_1 x_1 + \theta_2 x_2 + \theta_3 x_3 \\ &= \theta_0 + \theta_1 x_1 + \theta_2 x_1^2 + \theta_3 x_1^3 \end{aligned}$$

Minimize the cost function

$$\theta = (X^T X)^{-1} X^T y$$

Feature scaling not necessarily

- What if $X^T X$ is non-invertible? (singular / degenerate)
 ① Redundant features $x_1 = (1, 28)^T x_2$
 ② Too many features ($m \leq n$). Delete some feature.
 Regularization $\lambda \theta$

[Vectorization]

$$h_{\theta}(x) = \sum_{j=0}^n \theta_j x_j = \theta^T x$$

Unvectorized implementation
for $j=1:n+1$

$$\text{sum} = \text{sum} + \theta(j) \cdot x(j)$$

Vectorized implementation
sum = theta^T * x

[Optimization algorithms]

- Conjugate gradient Adv: no need to manually pick α
- BFGS Faster than gradient descent
- LBFGS Disadv: More complex

[Advanced optimization functions]

- fminunc()
- function minimization
- unconstrained

Binary Classification

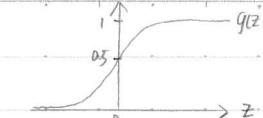
new example
 x : Use linear regression to change new hypothesis in straight line fit the data from the original one.

{ Sigmoid function
Logistic function

[Logistic Regression] 罗吉斯回归

$$0 \leq h_{\theta}(x) \leq 1 \quad h_{\theta}(x) = g(\theta^T x)$$

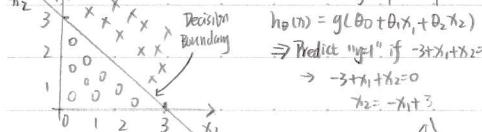
$$g(z) = \frac{1}{1+e^{-z}} = \frac{1}{1+e^{-\theta^T z}}$$



$h_{\theta}(x) = \text{estimated probability that } y=1 \text{ on input } x \Rightarrow h_{\theta}(x) = p(y=1 | x; \theta)$
 $\text{If } x = [1 \ x_1] = [1 \ \text{tumor size}] \Rightarrow h_{\theta}(x)=0.7$
 "probability that $y=1$, given x , parameterized by θ "
 Tell the patient that 70% chance of tumor being bad

[Decision Boundary]

决策边界 ← Is a property of hypothesis, not a property of data set



[Cost function]

$$\text{cost}(h_{\theta}(x), y) = \begin{cases} -\log(h_{\theta}(x)) & \text{if } y=1 \\ -\log(1-h_{\theta}(x)) & \text{if } y=0 \end{cases}$$

$$\text{cost} = 0 \text{ if } y=1, h_{\theta}(x)=1$$

But as $h_{\theta}(x) \rightarrow 0$. If $h_{\theta}(x)=0$, predict $P(y=1 | x; \theta)=0$ but $y=1$, penalize learning algorithm by a very large cost

$$\text{Cost}(h_{\theta}(x), y) = -y \log(h_{\theta}(x)) - (1-y) \log(1-h_{\theta}(x))$$

$$J(\theta) = \frac{1}{m} \sum_{i=1}^m \text{Cost}(h_{\theta}(x^{(i)}), y^{(i)})$$

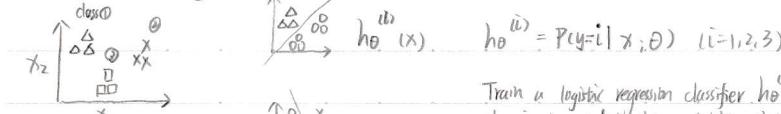
$$\text{Cost}(h_{\theta}(x), y) = \begin{cases} -\log(h_{\theta}(x)) & \text{if } y=1 \\ -\log(1-h_{\theta}(x)) & \text{if } y=0 \end{cases}$$

$$\min_{\theta} J(\theta) \Rightarrow h_{\theta}(x) = \frac{1}{1+e^{-\theta^T x}} \quad (P(y=1 | x; \theta))$$

$$\theta_j := \theta_j - \alpha \sum_{i=1}^m (h_{\theta}(x^{(i)}) - y^{(i)}) x_j^{(i)}$$

$$\hookrightarrow h_{\theta}(x) = \frac{1}{1+e^{-\theta^T x}}$$

[Multiclass classification]



One-vs-all
(One-vs-Reset)

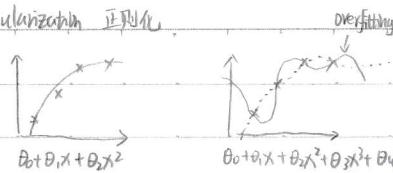


Train a logistic regression classifier $h_{\theta}^{(i)}(x)$ for each class i to predict the probability that $y=i$

On a new input x to make a prediction, pick the class i that maximizes $\max_i h_{\theta}^{(i)}(x)$

$$\theta_0 + \theta_1 x_1 + \theta_2 x_2 + \theta_3 x_1^2 + \theta_4 x_2^2$$

Regularization 正则化



suppose we penalize and make θ_3, θ_4 really small.

$$\min_{\theta} \frac{1}{2m} \sum_{i=1}^m (\hat{y}_i - y_i)^2 + 1000\theta_3^2 + 1000\theta_4^2 \quad \left\{ \begin{array}{l} \theta_3 \approx 0 \\ \theta_4 \approx 0 \end{array} \right.$$

[Regularity]

Small values for parameters $\theta_0, \theta_1, \dots, \theta_n$

- "Simpler" hypothesis
- Less prone to overfitting

$$J(\theta) = \frac{1}{2m} \sum_{i=1}^m (\hat{y}_i - y_i)^2 + \lambda \cdot \sum_{j=1}^n \theta_j^2 \quad \begin{matrix} \text{regularization parameter} \\ \uparrow \\ \text{Trade off between the cost & penalty of large } \theta \end{matrix}$$

$$\lambda \cdot (\theta_0^2 + \theta_1^2 + \theta_2^2 + \theta_3^2 + \dots + \theta_n^2)$$

! 求偏导时只有 θ_j^2 用得到
其它全为常数

[Regularized Linear Regression]

$$\frac{\partial}{\partial \theta} \left(\frac{1}{2m} \cdot \lambda \cdot \theta_j^2 \right) = \frac{\lambda}{m} \theta_j$$

$$\text{Repeat: } \theta_0 := \theta_0 - \lambda \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_0^{(i)}$$

$$\theta_j := \theta_j - \lambda \left[\frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_j^{(i)} + \frac{\lambda}{m} \theta_j \right] \Rightarrow \theta_j := \theta_j (1 - \lambda \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_j^{(i)}) - \lambda \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_j^{(i)}$$

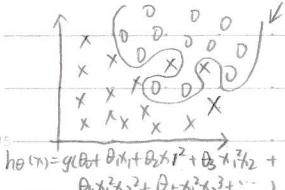
Normal equation $X \in \mathbb{R}^{m \times (n+1)}$

$$\theta = (X^T X + \lambda \underbrace{I}_{(n+1) \times (n+1)})^{-1} X^T y$$

正则化可以解决奇异数
但不能解决的情况

[Regularized Logistic regression]

overfitting



$$J(\theta) = - \frac{1}{m} \sum_{i=1}^m [y_i \log(\hat{y}_i) + (1-y_i) \log(1-\hat{y}_i)] + \frac{\lambda}{2m} \sum_{j=1}^n \theta_j^2$$

$$\theta_0 := \theta_0 - \lambda \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_0^{(i)}$$

$$\theta_j := \theta_j - \lambda \left[\frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_j^{(i)} + \frac{\lambda}{m} \theta_j \right] \quad \hat{y}_i = \frac{1}{1+e^{-\theta^T x}}$$

Advanced optimization

function [JVal, gradient] = costFunction(theta)

$$J(\theta) = - \frac{1}{m} \sum_{i=1}^m [y_i \log(\hat{y}_i) + (1-y_i) \log(1-\hat{y}_i)] + \frac{\lambda}{2m} \sum_{j=1}^n \theta_j^2$$

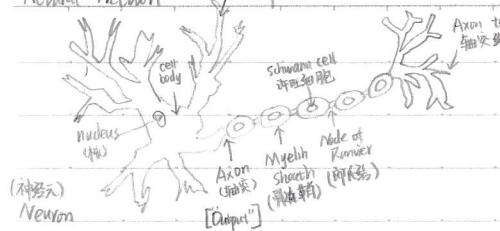
$$\theta_0 \text{ gradient}(1) = \frac{\partial J(\theta)}{\partial \theta_0} = \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_0^{(i)}$$

$$\theta_1 \text{ gradient}(2) = \frac{\partial J(\theta)}{\partial \theta_1} = \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_1^{(i)} + \frac{\lambda}{m} \theta_1$$

$$\theta_2 \text{ gradient}(3) = \frac{\partial J(\theta)}{\partial \theta_2} = \frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i) \cdot x_2^{(i)} + \frac{\lambda}{m} \theta_2$$

Dendrite (树突)

Natural Network



Neuron model: Logistic unit

$$h_\theta(x) = \frac{1}{1+e^{-\theta^T x}}$$

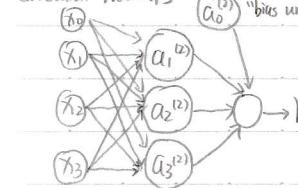
$$g(z) = \frac{1}{1+e^{-z}}$$

$$\begin{bmatrix} \theta_0 \\ \theta_1 \\ \theta_2 \\ \theta_3 \end{bmatrix} \leftarrow \begin{bmatrix} \theta_0 \\ \theta_1 \\ \theta_2 \\ \theta_3 \end{bmatrix} \quad \text{bias unit}$$

E.g. $a^{(2)} :=$ the activation of the first unit in layer 2

"Activation" means the value that is computed by and is output by a specific

[Natural Network]



Layer 1 Layer 2 Layer 3

Input Layer "Hidden" Layer Output Layer

$a_i^{(j)}$: "activation" of unit i in layer j

$\theta^{(j)}$: matrix of weights controlling function mapping from layer j to layer $j+1$

$$\begin{cases} a_0^{(2)} = g(\theta_{00}^{(1)} x_0 + \theta_{10}^{(1)} x_1 + \theta_{20}^{(1)} x_2 + \theta_{30}^{(1)} x_3) \\ a_1^{(2)} = g(\theta_{01}^{(1)} x_0 + \theta_{11}^{(1)} x_1 + \theta_{21}^{(1)} x_2 + \theta_{31}^{(1)} x_3) \\ a_2^{(2)} = g(\theta_{02}^{(1)} x_0 + \theta_{12}^{(1)} x_1 + \theta_{22}^{(1)} x_2 + \theta_{32}^{(1)} x_3) \end{cases} \quad \theta^{(1)} \in \mathbb{R}^{3 \times 4}$$

$$\begin{cases} h_\theta(x) = a_0^{(3)} = g(\theta_{00}^{(2)} a_0^{(2)} + \theta_{10}^{(2)} a_1^{(2)} + \theta_{20}^{(2)} a_2^{(2)} + \theta_{30}^{(2)} a_3^{(2)}) \end{cases} \quad \theta^{(2)} \in \mathbb{R}^{4 \times 1}$$

Assume $x = a^{(0)}$

$$\begin{cases} z^1 = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \\ z^2 = \begin{bmatrix} z_1^{(2)} \\ z_2^{(2)} \\ z_3^{(2)} \end{bmatrix} = \begin{bmatrix} \theta_{00}^{(1)} x_0 + \theta_{10}^{(1)} x_1 + \theta_{20}^{(1)} x_2 + \theta_{30}^{(1)} x_3 \\ \theta_{01}^{(1)} x_0 + \theta_{11}^{(1)} x_1 + \theta_{21}^{(1)} x_2 + \theta_{31}^{(1)} x_3 \\ \theta_{02}^{(1)} x_0 + \theta_{12}^{(1)} x_1 + \theta_{22}^{(1)} x_2 + \theta_{32}^{(1)} x_3 \end{bmatrix} \\ z^3 = \begin{bmatrix} z^{(3)} \end{bmatrix} = \begin{bmatrix} \theta_{00}^{(2)} z_0^{(2)} + \theta_{10}^{(2)} z_1^{(2)} + \theta_{20}^{(2)} z_2^{(2)} + \theta_{30}^{(2)} z_3^{(2)} \end{bmatrix} \end{cases} \quad z^{(2)} = \theta^{(1)} x = \theta^{(1)} a^{(1)}$$

$$a^{(2)} = g(z^{(2)})$$

Became we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...

$$h_\theta(x) \rightarrow \begin{cases} z^{(3)} = \theta^{(2)} a^{(2)} \\ h_\theta(x) = a^{(3)} = g(z^{(3)}) \end{cases}$$

Forward propagation: Vectorized Implementation

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

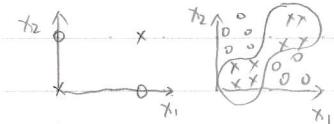
$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

$$\begin{cases} a^{(0)} \\ a^{(1)} \end{cases} \xrightarrow{\text{Add}} \begin{cases} a^{(2)} \\ a^{(3)} \end{cases} \quad \text{Because we start with the activation of the input units and then we sort of forward-propagate that to the hidden layer and compute the activations...}$$

Non-linear classification example: XOR / NOR

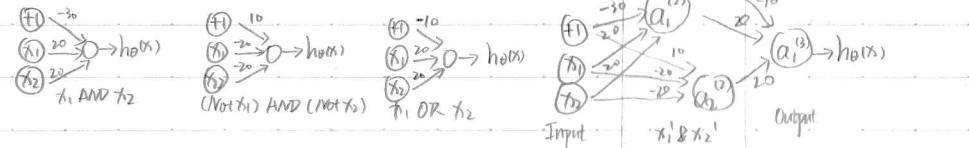
x_1, x_2 are binary ($0, 1$)



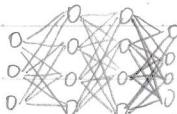
[OR function]

$x_1 \cdot x_2$	$h_{\theta}(x)$
0 0	$g(1) = 0$
0 1	$g(1) = 1$
1 0	$g(1) = 1$
1 1	$g(2) = 1$

[Together]



[Multiple output units: One vs all]



Training set: $(x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), \dots, (x^{(m)}, y^{(m)})$

$y^{(i)}$ one of $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

K output units

$$h_{\theta}(x) = \mathbb{R}^K$$

$$S_L = K$$

L : total no. of layers in network ($L=4$)

S_L : no. of units (not counting bias unit) in layer L

$$\begin{cases} S_1 = 3 \\ S_2 = 4 \\ S_3 = 4 \\ S_4 = 4 \end{cases}$$

[Cost function]

$$h_{\theta}(x) \in \mathbb{R}^K \quad (h_{\theta}(x))_i = i^{\text{th}} \text{ output}$$

$$J(\theta) = -\frac{1}{m} \left[\sum_{k=1}^m \sum_{i=1}^K y_k^{(i)} \log(h_{\theta}(x^{(k)}))_k + (1-y_k^{(i)}) \log(1-h_{\theta}(x^{(k)}))_k \right] - \frac{1}{2m} \sum_{l=1}^{L-1} \sum_{i=1}^{S_l} \sum_{j=1}^{S_{l+1}} (\theta_{ji}^{(l)})^2$$

[Gradient computation]

Given one training example. (x, y) :

Forward propagation

$$\begin{aligned} a^{(1)} &= x \\ z^{(2)} &= \theta^{(1)} a^{(1)} \\ a^{(2)} &= g(z^{(2)}) \quad (\text{add } a_0^{(2)}) \\ z^{(3)} &= \theta^{(2)} a^{(2)} \\ a^{(3)} &= g(z^{(3)}) \quad (\text{add } a_0^{(3)}) \\ z^{(4)} &= \theta^{(3)} a^{(3)} \\ a^{(4)} &= h_{\theta}(x) = g(z^{(4)}) \end{aligned}$$

[Backpropagation Algorithm]

$\delta_j^{(l)} = \text{"error" of node } j \text{ in layer } l$

$$\delta_j^{(4)} = a_j^{(4)} - y_j \quad (\text{vectorized})$$

$$\begin{aligned} \delta_j^{(3)} &= (\theta^{(3)})^T \delta^{(4)} \cdot g'(z^{(3)}) \rightarrow a^{(3)} \cdot (1-a^{(3)}) \\ \delta_j^{(2)} &= (\theta^{(2)})^T \delta^{(3)} \cdot g'(z^{(2)}) \end{aligned}$$

$$\frac{\partial}{\partial \theta_{ij}^{(l)}} J(\theta) = a_j^{(l)} \delta_i^{(l+1)} \quad (\text{ignoring } a_0)$$

[Backpropagation Algorithm]

Training Set: $\{(x^{(1)}, y^{(1)}), \dots, (x^{(m)}, y^{(m)})\}$

Set $\Delta_{ij}^{(l)} = 0$ (for all i, j)

For $l=1$ to m

Set $a^{(1)} = x^{(1)}$

Perform forward propagation to compute $a^{(l)}$ for $l=2, 3, \dots, L$

Using $y^{(l)}$, compute $\delta^{(l)} = a^{(l)} - y^{(l)}$

Compute $\delta^{(l-1)}, \delta^{(l-2)}, \dots, \delta^{(1)}$

$$\Delta_{ij}^{(l)} = \delta_{ij}^{(l)} + \alpha^{(l)} \delta_i^{(l+1)}$$

$$\begin{cases} D_{ij}^{(1)} := \frac{1}{m} \Delta_{ij}^{(1)} + \lambda \theta_{ij}^{(1)} & j \neq 0 \\ D_{ij}^{(1)} := \frac{1}{m} \Delta_{ij}^{(1)} & j = 0 \end{cases}$$

$$\frac{\partial}{\partial \theta_{ij}^{(l)}} J(\theta) = D_{ij}^{(l)}$$

$X(i, :)$ - size,

$D_{ij}^{(l)}$ - $2 \times m \times n$

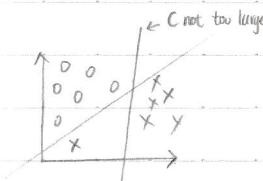
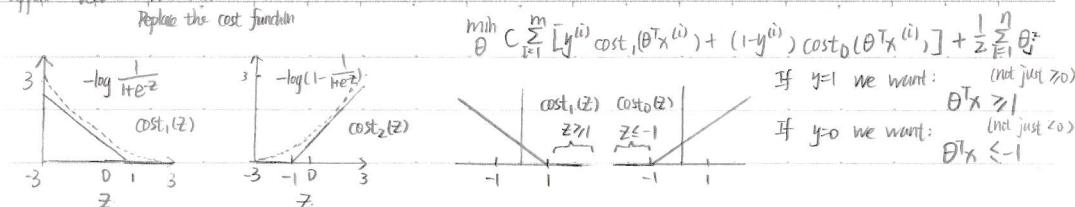
$D_{ij}^{(l)}$ - 1×1

$D_{ij}^{(l)}$ - 1×1

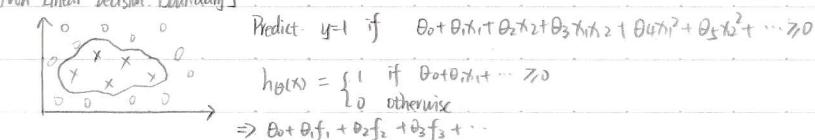
$D_{ij}^{(l)}$ - 1×1

Support Vector Machine

Replace the cost function



[Non-Linear Decision Boundary]



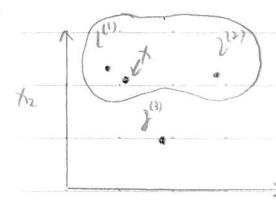
[Kernel]

Given x , compute new feature depending on proximity to landmarks $L^{(1)}, L^{(2)}, L^{(3)}$

$$\begin{array}{c} x_2 \uparrow \\ \cdot \quad L^{(1)} \quad L^{(2)} \quad \cdot \\ \cdot \quad L^{(3)} \quad \cdot \\ x_1 \end{array} \quad \begin{array}{l} \text{Given } x: f_1 = \text{similarity}(x, L^{(1)}) = \exp\left(1 - \frac{\|x - L^{(1)}\|^2}{2\sigma^2}\right) \\ f_2 = \text{similarity}(x, L^{(2)}) = \exp\left(1 - \frac{\|x - L^{(2)}\|^2}{2\sigma^2}\right) \\ \vdots \\ f_3 = \text{similarity}(x, L^{(3)}) = \exp\left(1 - \frac{\|x - L^{(3)}\|^2}{2\sigma^2}\right) \end{array}$$

Kernel function (Gaussian Kernels)

$$f_1 = \text{similarity}(x, L^{(1)}) = \exp\left(-\frac{\|x - L^{(1)}\|^2}{2\sigma^2}\right) = \exp\left(\frac{-\|x - L^{(1)}\|^2}{2\sigma^2}\right) \quad \begin{cases} \text{If } x \approx L^{(1)} \rightarrow f_1 \approx \exp\left(-\frac{0^2}{2\sigma^2}\right) \approx 1 \\ \text{If } x \text{ far from } L^{(1)} \rightarrow f_1 \approx \exp\left(-\frac{(\text{large number})^2}{2\sigma^2}\right) \approx 0 \end{cases}$$

Predict "1" when $\theta_0 + \theta_1 f_1 + \theta_2 f_2 + \theta_3 f_3 \geq 0$ Assume $\theta_0 = -0.5, \theta_1 = 1, \theta_2 = 1, \theta_3 = 0$

$$x: \theta_0 + \theta_1 x_1 + \theta_2 x_2 + \theta_3 x_3 = -0.5 + 1 = 0.5 \geq 0$$

附近的最近，成为"1"

[SVM with Kernels]

Hypothesis: Given x_i , compute features $f_i \in \mathbb{R}^{m+1}$

Predict " $y=1$ " if $\theta^T f \geq 0$

Training

$$\min_{\theta} C \sum_{i=1}^m y^{(i)} \text{cost}_1(\theta^T f^{(i)}) + (1-y^{(i)}) \text{cost}_0(\theta^T f^{(i)}) + \frac{1}{2} \sum_{j=1}^n \theta_j^2$$

↓
↓
n,m

$C \leftarrow \frac{1}{n}$ Large C : Low bias, high variance

Small C : Higher bias, low variance

σ^2 Large σ^2 : Features f_i , very more smoothly

Higher bias, lower variance

Small σ^2 : Features f_i very less smoothly

Low bias, higher variance

Use software package (e.g. liblinear, libsvm) to solve for parameters θ .

Need to specify:

Choice of parameter C

Choice of kernel (similarity function). * No kernel ("linear kernel") → Predict " $y=1$ " if $\theta^T x \geq 0$

Gaussian kernel:

$$f_i = \exp\left(-\frac{\|x - x^{(i)}\|^2}{2\sigma^2}\right), \text{ where } L^{(i)} = x^{(i)} \text{ Need to choose } \sigma^2. * \text{ Do perform feature scaling}$$

If function $f = \text{kernel}(x_1, x_2)$

No.

Date

10001

10001

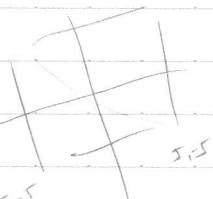
120

0

10

11

55



(55) 111 + 5 + 1

Campus

GES (GCD(2))

1208

No.

32 nm → 17686.8

ALU[8]

size

5316 × CA16

838 × 20210

10001 1011 283

0001

S: 00000001

R: 00000000

D 00000001

112

1113

00011111

01100011

01111100

7 C.

0

00000000, 010100112 - 110010102

01010011

00000000

→ 01010011

xor 10100100

→ 11110101

xor 0100

00100101, 10

101001100

101001100000

10100110000000

X 111110111110 mod 100011011

xor 1000011011

→ 01110000011110

x 1000011011

→ D110110101110

100011011

→ 010101110110

100011011

→ 000100011010

100011011

→ 0000000001

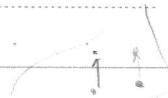
11B

KOKUYO

No.

Date

data



$$0x80 = 1000,0000$$

$$0x1B = 0001,1101$$

polynomial basis

$$p=1 \quad q=1$$

$$p = P^q \cdot q^{(1)} \cdot \dots \cdot q^{(n-1)} \\ p = 0000,0011$$

$$\begin{aligned} gf(2^6) &= 10110100 \\ gf(2^4) &= 00000010 \\ gf(2^2) &= 00000001 \\ g &= 11111111 \end{aligned}$$

$$\frac{d}{dx} \frac{u}{\partial x}$$

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 \\ &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 \end{aligned}$$

Campus

Lambda

 φ

Delta

125%

No.

Date

Galois Field I

$$gf(p^n) = (0, 1, 2, \dots, p-1) \cup$$

$$(p, p+1, p+2, \dots, p(p-1)) \cup$$

$$(p^2, p^2+1, p^2+2, \dots, p^2(p-1)) \cup$$

$$(p^{n-1}, p^{n-1}+1, p^{n-1}+2, \dots, p^{n-1}(p-1))$$

$$gf(5) = (0, 1, 2, 3, 4)$$

$$gf(2^3) = (0, 1, 2, 2+1, 2^2, 2^2+1, 2^2+2, 2^2+2+1) \\ = (0, 1, 2, 3, 4, 5, 6, 7)$$

$$84 = 2^6 + 2^4 + 2^2 = 01010100$$

$$13 = 2^3 + 2^2 + 2^0 = 00001101$$

$$101100011$$

$$01010100$$

$$\times 00001101$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

$$00000000$$

$$01010100$$

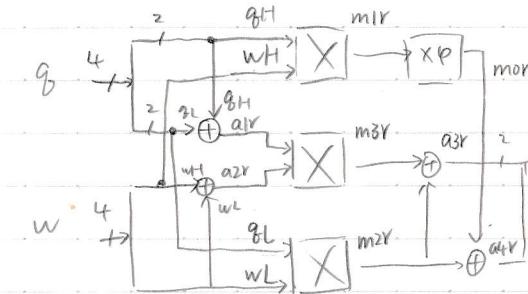
$$00000000$$

$$01010100$$

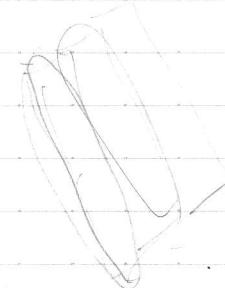
$$00000000$$

$$(gh+gL)(wH+wL)$$

$$ghwH + gwL + gwLH + gwLW$$



max(a[1..7])



KOKUYO

No.

Date

$$\begin{array}{c} a \\ \diagup \quad \diagdown \\ b \quad c \end{array}$$

$$\delta_0 = a - b$$

$$\delta_1 = c - d$$

$$\begin{array}{c} a \\ \diagup \quad \diagdown \\ b \quad d \end{array}$$

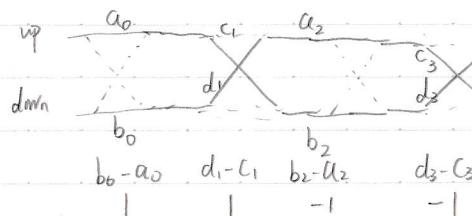
$$R_0$$

Date

$$\begin{array}{ccccccc} \downarrow & l & 0 & 1 & 1 & \downarrow & l \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ \downarrow & 2 & 2 & 2 & 2 & \downarrow & 0 \\ 2 & 3 & 3 & 3 & 3 & 2 & 1 \\ \downarrow & 4 & 4 & 4 & 4 & 4 & 1 \\ 3 & 4 & 4 & 4 & 4 & 4 & 1 \\ \downarrow & & & & & & 1 \\ 4 & & & & & & 1 \end{array}$$

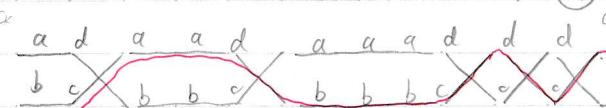
Dir

$$\begin{array}{cccc} & -1 & -1 & 1 \\ & -1 & 1 & -1 \\ \text{Org} & 0 & 0 & 1 \\ & 1 & 0 & 1 \end{array}$$



$$\begin{array}{ccccccccc} \text{CInv} & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \text{Challenge} & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{array}$$

FT Cross



$$\begin{array}{cccccccccc} b-a & c-a & b-a & b-a & c-d & b-a & b-a & b-a & c-d & c-d-c-d \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{array}$$

$$\text{dir_path} = (\text{dir_path} * C_{\text{Inv}} + \text{cro_path} * C) * [1 \text{ FT}(C)(1:\text{end}-1)]$$

$$\begin{array}{cccccccccc} \text{dir_path} & \frac{\delta_0 + \delta_1}{2} \\ \text{cro_path} & \frac{\delta_0 + \delta_1 + \delta_2}{2} \end{array}$$

$$\delta_0 + \delta_1 + \delta_2 + \delta_3 = \delta_1$$

$$\frac{\delta_0 + \delta_1 + \delta_2}{2} - \frac{\delta_1}{2} = \delta_1$$

$$\frac{\delta_1 + \delta_2 + \delta_3}{2} + \frac{\delta_0 + \delta_1}{2} = -\delta_1$$

$$\frac{\delta_0 + \delta_1}{2} - \frac{\delta_1 + \delta_2}{2} = -\delta_1$$

No.

Date

No.

Date

$$\frac{a}{b} \quad \begin{matrix} c \\ d \end{matrix}$$

$$\delta_0 = b - a \quad \delta_1 = c - d$$

$$\begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \delta_0^1 + \delta_0^2 + \delta_0^3 \quad w_4 + w_3 + w_2 + w_1 = \delta_0^1 + \delta_0^2 + \delta_0^3$$

$$\begin{matrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \delta_0^1 + \delta_0^2 + \delta_1^3 \quad w_4 + w_3 + w_2 - w_1 = \delta_0^1 + \delta_0^2 + \delta_1^3$$

$$\begin{matrix} 0 & 1 & 0 \\ 1 & -1 & 1 \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \delta_0^1 + \delta_1^2 - \delta_0^3 \quad w_4 + w_3 - w_2 - w_1 = \delta_0^1 + \delta_1^2 - \delta_0^3$$

$$\begin{matrix} 0 & 1 & 1 \\ 1 & -1 & -1 \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \delta_0^1 + \delta_1^2 - \delta_1^3 \quad w_4 + w_3 - w_2 + w_1 = \delta_0^1 + \delta_1^2 - \delta_1^3$$

$$\begin{matrix} 1 & 0 & 0 \\ 1 & -1 & 1 \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \delta_1^1 - \delta_0^2 - \delta_0^3 \quad w_4 - w_3 - w_2 - w_1 = \delta_1^1 - \delta_0^2 - \delta_0^3$$

$$\begin{matrix} 1 & 0 & 1 \\ 1 & -1 & -1 \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \delta_1^1 - \delta_0^2 - \delta_1^3 \quad w_1 = \frac{\delta_0^3 - \delta_1^3}{2}$$

$$\begin{matrix} 1 & 1 & 0 \\ 1 & -1 & 1 \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \delta_1^1 - \delta_1^2 + \delta_0^3 \quad w_2 = \frac{\delta_0^2 - \delta_1^2 + \delta_1^3 + \delta_0^3}{2}$$

$$\begin{matrix} 1 & 1 & 1 \\ 1 & -1 & -1 \end{matrix} \quad \begin{matrix} \times \\ \times \end{matrix} \quad \begin{matrix} a \\ b \end{matrix} \quad \delta_1^1 - \delta_1^2 + \delta_1^3 \quad w_3 = \frac{\delta_0^1 + \delta_0^2 + \delta_1^2 - \delta_1^1}{2}$$

$$w_4 = \frac{\delta_0^1 + \delta_1^1}{2}$$

$$\frac{\delta_1^0 - \delta_1^1}{2} \quad \frac{\delta_1^0 + \delta_1^1}{2}$$

\rightarrow

$$\begin{matrix} 0 & \Delta t = \delta_1^0 \\ | & | \\ | & | \\ -1 & 1 \end{matrix} \quad \Delta t = \delta_1^1$$

\rightarrow

$\times \quad \times$

$$\begin{matrix} c_1 & c_2 & 1 \\ \frac{\delta_1^0 - \delta_1^1}{2} & \frac{\delta_1^0 + \delta_1^1 + \delta_2^0 - \delta_2^1}{2} & \frac{\delta_2^0 + \delta_2^1}{2} \end{matrix}$$

$$\begin{array}{l} \begin{matrix} 0(1) & 0(1) & 1 \\ \rightarrow & 1 & 1 \end{matrix} \Rightarrow \frac{\delta_1^0 - \delta_1^1}{2} + \frac{\delta_1^0 + \delta_1^1 + \delta_2^0 - \delta_2^1}{2} + \frac{\delta_2^0 + \delta_2^1}{2} = \delta_1^0 + \delta_2^0 \\ \begin{matrix} 0(1) & 1(-1) & 1 \\ \rightarrow & 1 & 1 \end{matrix} \quad \frac{-\delta_1^0 + \delta_1^1}{2} + \frac{-\delta_1^0 - \delta_1^1 + \delta_2^0 + \delta_2^1}{2} + \frac{\delta_2^0 + \delta_2^1}{2} = -\delta_1^0 + \delta_2^1 \\ \begin{matrix} 1(-1) & 0(1) & 1 \\ \rightarrow & 1 & 1 \end{matrix} \quad \frac{\delta_1^0 + \delta_1^1}{2} + \frac{\delta_1^0 + \delta_1^1 + \delta_2^0 + \delta_2^1}{2} + \frac{\delta_2^0 + \delta_2^1}{2} = \delta_1^1 + \delta_2^0 \\ \begin{matrix} 1(-1) & 1(-1) & 1 \\ \rightarrow & 1 & -1 \end{matrix} \quad \frac{\delta_1^0 - \delta_1^1}{2} + \frac{\delta_1^0 - \delta_1^1 + \delta_2^0 + \delta_2^1}{2} + \frac{\delta_2^0 + \delta_2^1}{2} = -\delta_1^1 + \delta_2^1 \end{array}$$

$$\begin{matrix} 1 & 1 & 1 & 1 & \dots \\ 1 & -1 & 1 & 1 & \dots \\ -1 & -1 & 1 & 1 & \dots \\ -1 & 1 & 1 & 1 & \dots \end{matrix} \quad \delta_1^0 + \delta_2^0$$

Sub

32-bit C ✓

8-bit × 4

A B C D
111111
111111
111111
111111

16-bit

32-bit {

1) 1 → 1 ✓

2)

4) 1 → 1 ✓

5) Sy AB CD → BA DC

1) Seed → challenge → 16-region - multi-bit

2) - - - 16-res → Sub →

3) Sub both

4) Permutation

No. _____

Date _____

12.08

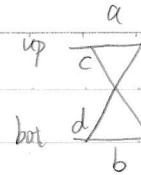
d-c. ^{up}
b-a _{bot}

No.

Date

bot-up > 0 $\rightarrow 1$
bot-up < 0 $\rightarrow 0$

$$X = \lceil Y \rceil$$



c=0 1 0 0 0 1 1 0 bot

up ~~X~~ --- ~~X~~ X ---

bot ~~b-a~~ ~~d-c~~ ~~a-b~~ ~~a-b~~ ~~a-b~~ ~~c-d~~ ~~d-c~~ ~~a-b~~

1-2c 1 -1 1 1 1 -1 1

f(cc) +1 -1 -1 -1 1 -1 1

1 1 -1 -1 -1 1 -1 C

at 1: delay-bot > 0
1 1 0 1 1 0 1

v=1

co

v=0
0: delay-bot > 0
1 1 0 1 1 0 1

v=0

v=1

1 0 1 0 1 1 0 0

up ~~X~~ - ~~X~~ - ~~X~~ X --- up

bot ~~d-c~~ ~~a-b~~ ~~c-d~~ ~~b-a~~ ~~d-c~~ ~~c-d~~ ~~b-a~~ ~~b-a~~

+ - - + + - + +

1 -1 1 -1 1 -1 -1 1

f(c) -1 -1 1 1 -1 1 1

1 -1 -1 1 1 -1 1 1 D

sign(delay)

sign(bit * delay)

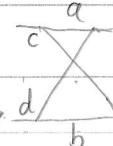
$$\delta_0 = b-a$$

$$\delta_1 = d-c$$

27
2

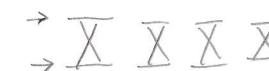
$$\delta_0^0$$

$$\delta_0^0 = b - a$$



bot

$$\delta_0^1 = d - c$$

G G₂ G₃ G₄

$$f_t(c) = [f_1, f_2, f_3, f_4]$$

$$[1, f_1, f_2, f_3, f_4] \cdot [w_1 + w_2 + w_3 + w_4] \cdot f_4$$

$$[f_4, f_1 f_4, f_2 f_4, f_3 f_4, f_4^2] \cdot [w_1 + w_2 + w_3 + w_4]$$

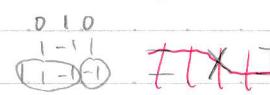
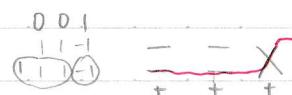
$$\cancel{\Rightarrow} \underbrace{[f_4, f_1 f_4, f_2 f_4, f_3 f_4, 1]}_{\text{feature transformation}} \cdot [w_1 + w_2 + w_3 + w_4]$$

feature transformation

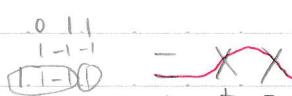
$$1 \quad \delta_1^0 + \delta_2^0 + \delta_3^0 = w_1 + w_2 + w_3 + w_4$$



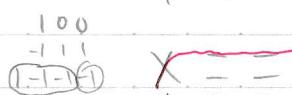
$$2 \quad \delta_1^0 + \delta_2^0 + \delta_3^1 = w_1 + w_2 + w_3 - w_4$$



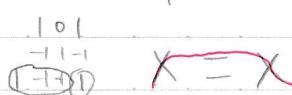
$$3 \quad \delta_1^0 + \delta_2^1 - \delta_3^0 = w_1 + w_2 - w_3 - w_4$$



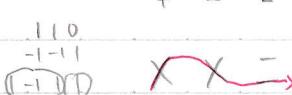
$$4 \quad \delta_1^0 + \delta_2^1 - \delta_3^1 = w_1 + w_2 - w_3 + w_4$$



$$5 \quad \delta_1^1 - \delta_2^0 - \delta_3^0 = w_1 - w_2 - w_3 - w_4$$



$$6 \quad \delta_1^1 - \delta_2^0 - \delta_3^1 = w_1 - w_2 - w_3 + w_4$$



$$7 \quad \delta_1^1 - \delta_2^1 + \delta_3^0 = w_1 - w_2 + w_3 - w_4$$



$$8 \quad \delta_1^1 - \delta_2^1 + \delta_3^1 = w_1 - w_2 + w_3 + w_4$$

$$\{ ① \delta_1^0 + \delta_2^0 + \delta_3^0 = w_1 + w_2 + w_3 + w_4$$

$$\{ ② \delta_1^0 + \delta_2^0 + \delta_3^1 = w_1 + w_2 + w_3 - w_4$$

$$\Rightarrow w_4 = \frac{\delta_3^0 - \delta_3^1}{2}$$

$$\{ ③ \delta_1^0 + \delta_2^1 - \delta_3^0 = w_1 + w_2 - w_3 - w_4$$

$$\{ ④ \delta_1^1 - \delta_2^0 - \delta_3^0 = w_1 - w_2 - w_3 - w_4$$

$$\Rightarrow w_2 = \frac{\delta_1^0 - \delta_1^1 + \delta_2^1 - \delta_2^0}{2}$$

$$\{ ⑤ \delta_1^0 + \delta_2^0 + \delta_3^1 = w_1 + w_2 + w_3 - w_4$$

$$\{ ⑥ \delta_1^0 + \delta_2^1 - \delta_3^0 = w_1 + w_2 - w_3 - w_4$$

$$\Rightarrow w_3 = \frac{\delta_2^0 - \delta_2^1 + \delta_3^1 - \delta_3^0}{2}$$

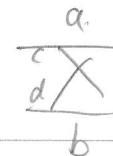
$$\{ ⑦ \delta_1^1 - \delta_2^0 - \delta_3^1 = w_1 - w_2 + w_3 + w_4$$

$$\{ ⑧ \delta_1^1 - \delta_2^1 + \delta_3^0 = w_1 - w_2 + w_3 - w_4$$

No.

Date

3-bit



T

0 0 0 — — —

bot. $\rightarrow \overline{b-a} \quad \overline{b-a} \quad \overline{b-a}$

0 0 1 — —

 $\rightarrow \overline{b-a} \quad \overline{b-a} \quad \cancel{d-c}$

0 1 0 — —

 $\rightarrow \overline{b-a} \quad \cancel{d-c} \quad \overline{a-b}$

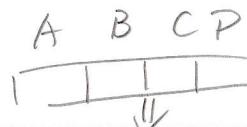
0 1 1 — —

 $\cancel{b-a} \quad \cancel{d-c} \quad \cancel{c-d}$ 1 0 0 — \rightarrow $\cancel{d-c} \quad \cancel{a-b} \quad \overline{a-b}$ 1 0 1 — \rightarrow $\cancel{d-c} \quad \overline{a-b} \quad \cancel{c-d}$ 1 1 0 — $\times \times =$ 1 1 1 $\times \times \times$

(15000)

End Note

16

No. 65535
Date

B A D C

$$w^1 = \frac{s_1^0 - s_1^1}{2}$$

$$w^2 = \frac{s_1^0 + s_1^1 + s_2^0 - s_2^1}{2}$$

$$w^3 = \frac{s_2^0 + s_2^1}{2}$$

$$\Phi_j = \prod_{i=1}^2 (1 - 2s_i) \text{ for } j=1, \dots, 2.$$

$$\begin{array}{ll} 1 & s_1^0 - s_1^1 \\ 0 0 & \rightarrow 1, 1, 1 \\ 1 & \frac{s_1^0 - s_1^1}{2} + \frac{s_1^0 + s_1^1 + s_2^0 - s_2^1}{2} + \frac{s_2^0 + s_2^1}{2} = s_1^0 + s_2^0 \\ 0 1 & \rightarrow -1, -1, 1 \\ 1 & \frac{-s_1^0 + s_1^1}{2} + \frac{-s_1^0 - s_1^1 - s_2^0 + s_2^1}{2} + \frac{-s_2^0 + s_2^1}{2} = -s_1^0 + s_2^1 \\ 1 0 & \rightarrow -1, 1, 1 \\ -1 & \frac{s_1^0 + s_1^1}{2} + \frac{s_1^0 + s_1^1 + s_2^0 - s_2^1}{2} + \frac{s_2^0 + s_2^1}{2} = s_1^1 + s_2^0 \\ -1 1 & \rightarrow 1 - 1 \\ 1 & \frac{s_2^0 - s_2^1}{2} + \frac{s_1^0 - s_1^1 - s_2^0 + s_2^1}{2} + \frac{s_2^0 + s_2^1}{2} = -s_1^1 + s_2^1 \end{array}$$

$$\begin{array}{ll} 00 & \overline{\overline{\overline{\overline{a}}}} \quad s_1^0 + s_2^0 \\ 01 & \cancel{\overline{\overline{\overline{a}}}} \quad s_1^0 + s_2^0 \\ 10 & \cancel{\overline{\overline{a}}} \quad s_1^1 - s_2^0 \\ 11 & \cancel{\overline{\overline{a}}} \quad \cancel{\overline{\overline{a}}} \quad s_1^1 - s_2^1 \end{array}$$

$$\begin{array}{ll} 1 & s_1^0 + s_2^0 \\ 00 & \overline{\overline{\overline{\overline{a}}}} \quad s_1^0 + s_2^0 \\ 01 & \cancel{\overline{\overline{\overline{a}}}} \quad -s_1^0 + s_2^0 \\ 10 & \cancel{\overline{\overline{a}}} \quad s_1^1 + s_2^0 \\ 11 & \cancel{\overline{\overline{a}}} \quad \cancel{\overline{\overline{a}}} \quad -s_1^1 + s_2^0 \end{array}$$

Map seed \rightarrow 16 bits5th \rightarrow 1th

Thesis

3 { Chapter 1 motivation → 3 Page
Stating actual problem
PUF can be modeled by ML secondary application
— Structure

2 Background

- PUF description *detailed*
- ML alg LR (Example) *NN, SVM*
- design part { per sub

3 Design (cheap cost)

- goal
- experiment (setup) visio (figures)
- what have been done

Arbiter

{ original
sub / Input/Output security and reliability
4X per Input [0, 1%]
Combination of sub & per (Input) Error

5000 samples
(At least 8 bits)

4. Evaluation

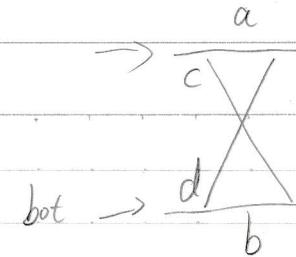
6.5nm Cost arbiter + sub / per benefit
arbiter + hash function

5 Conclusion
future

EndNote for referencing

env access to CRB other In design goal threat model Switch

a b c d
b a d c

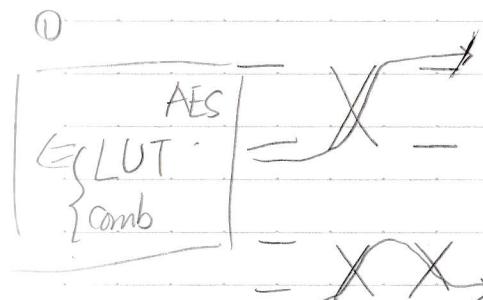


$$\delta_1 = b - a$$

$$\delta_1' = d - c$$

$$\begin{aligned} \text{bot} \rightarrow & \quad \overline{\quad} \quad \overline{\quad} \\ & \overline{b-a} \quad \overline{d-c} \quad \overline{a-b} \\ & \delta_1^0 \quad \delta_2^1 - \delta_3^0 \end{aligned}$$

$\begin{array}{l} 1001 \\ 1010 \\ 1011 \\ 1100 \end{array}$ G



(1)
permutation

per + Seed + sub
sub + Seed + per

Two ① hash function

② Multiply the prediction of all bits

③ Area (GE)