CS771 project

Group Name: Aadityaamlan Panda
Members:-
Aadityaamlan Panda
Amit Kumar
Harish Choudhary
Jagdeesh Meena
Shivani Gupta
Sumit Neniwal

1 Question 1

Considering any i^th PUF in the series of seven PUFs for both series

PUFO

$$t_i^u = (1 - c_i)(t_{i-1}^u + p_i) + c_i(t_{i-1}^l + s_i)$$
$$t_i^l = (1 - c_i)(t_{i-1}^l + q_i) + c_i(t_{i-1}^u + r_i)$$

PUF1

$$T_i^u = (1 - C_i)(T_{i-1}^u + P_i) + c_i(T_{i-1}^l + S_i)$$
$$T_i^l = (1 - C_i)(T_{i-1}^l + Q_i) + c_i(T_{i-1}^u + R_i)$$

Arbiter 0

$$d_i = T_i^l - t_i^l$$

Arbiter 1

$$D_i = T_i^u - t_i^u$$

Tabulation

d_i	D_i	ARB 0	ARB 1	XOR Output
+ve	+ve	0	0	0
-ve	-ve	1	1	0
-ve	+ve	1	0	1
+ve	-ve	0	1	1

Output

$$Output = \frac{(1 + sign(-D_7 d_7))}{2} = \frac{(1 + sign(W^T \phi(c) + b))}{2}$$

Preprint. Under review.

Upon further analysis of the product

$$= \frac{((D_7 + d_7)^2 - (D_7 - d_7)^2)}{2} = \frac{-(A_7^2 - B_7^2)}{2}$$

$$\begin{aligned}
D_i &= T_i^u - t_i^u \\
&= (1 - c_i)(T_{i-1}^u - t_{i-1}^u + P_i - p_i) + c_i(T_{i-1}^l - t_{i-1}^l + S_i - s_i) \\
&= (1 - c_i)(D_{i-1} + k_p) + c_i(d_{i-1} + k_s) \\
&= (D_{i-1} + k_p) - c_i(D_{i-1} - d_{i-1} + k_p - k_s)
\end{aligned}$$

$$\begin{aligned}
d_i &= T_i^l - t_i^l \\
&= (1 - c_i)(T_{i-1}^l - t_{i-1}^l + Q_i - q_i) + c_i(T_{i-1}^u - t_{i-1}^u + R_i - r_i) \\
&= (1 - c_i)(d_{i-1} + k_q) + c_i(D_{i-1} + k_r) \\
&= (d_{i-1} + k_q) + c_i(D_{i-1} - d_{i-1} + k_r - k_q)
\end{aligned}$$

$$\begin{aligned}
A_i &= D_i + d_i \\
&= A_{i-1} + k_p + k_q + c_i(k_r - k_q - k_p + k_s)
\end{aligned}$$

$$\begin{aligned}
B_i &= D_i - d_i \\
&= B_{i-1} + k_p - k_q + c_i(-2B_{i-1} + k_q - k_p - k_r + k_s)
\end{aligned}$$

$$\begin{aligned}
A_0 &= \text{const}_1 + c_0 \cdot \text{const}_2 \quad (\text{since } A_{-1} = 0) \\
&= (1 - 2c_0)\text{const}_1 + \text{const}_2 \\
&= A_{0,\text{coeff}}^T \cdot \begin{bmatrix} 1 - 2c_0 \\ 1 \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
&\text{Let } f_i = 1 - 2c_i \quad \text{where } i \in \{1, 2, 3, \ldots, 7\} \\
&\quad A_0 = A_{0,\text{coeff}}^T \cdot [f_0, 1] \quad \Rightarrow \text{feature map} = \{f_0, 1\} \\
&\quad A_1 = A_0 + c_1 \cdot \text{const} \\
&\quad A_1 \Rightarrow \text{feature map} = \{f, f_0, 1\} \\
&\quad A_2 \Rightarrow \text{feature map} = \{f_2, f_1, f_0, 1\} \\
&\quad\quad \vdots \\
&\quad A_7 \Rightarrow \text{feature map} = \{f_7, f_6, f_5, \ldots, f_0, 1\}
\end{aligned}$$

Similarly since $B_{-1} = 0$

$$\begin{aligned}
B_0 &= const_1 + (1 - 2c_0)const_2 \Rightarrow featuremap = \{f_0, 1\} \\
B_1 &= (1 - 2c_1)B_0 + const \Rightarrow featuremap = \{f_1 f_0, f_1, 1\} \\
B_2 &= (1 - 2c_0)B_1 + const \Rightarrow featuremap = \{f_2 f_1 f_0, f_2 f_1, f_2, 1\} \\
&\vdots \\
B_7 &= (1 - 2c_1)B_0 + const \Rightarrow featuremap = \{f_7 f_6 f_5 \ldots f_0, f_7 f_6 \ldots f_1, \ldots, f_7 f_6, f_7, 1\}
\end{aligned}$$

$$\frac{A_7^2 - B_7^2}{2} = \frac{\left(A_{7,\text{coeff}}^T \cdot [f_7, f_6, f_5, \ldots, f_0, 1]\right)^2 \quad - B_{7,\text{coeff}}^T \cdot [f_7 f_6 f_5 \ldots f_0, f_7 f_6 \ldots f_1, \ldots, f_7 f_6, f_7, 1]}{2}$$

This will yield 45 terms in the feature maps of both A_7^2 and B_7^2.
The feature maps will have four terms in common: $1, f_7^2, f_7 f_6, f_7$.
Hence, the overall feature map will have 86 terms $(= 45 + 45 - 4 + 1$ bias term$)$.

2 Question 2

The total number of elements in the final feature map $\phi(c)$ (excluding the bias term) is 85, as shown in Question 1. Hence, the overall dimensionality is $D = 85$.

3 Question 3

$$
\begin{aligned}
A^2 &= (\langle\langle a_0, a_1, \ldots, a_7\rangle, a_9\rangle \cdot [f_7, f_6, \ldots, f_0, 1])^2 \\
&= (\langle\langle a_0, a_1, \ldots, a_7\rangle, a_9\rangle \cdot [c_7, c_6, \ldots, c_0, 1])^2 \\
&= K_1(\mathbf{a}, \mathbf{c}) \quad \text{where} \\
K_1(\mathbf{a}, \mathbf{c}) &= (\mathbf{a}^T \mathbf{c} + \text{const})^d \quad \text{where } d = 2 \quad \text{(Polynomial Kernel)}
\end{aligned}
$$

$$
\begin{aligned}
B^2 &= (\langle\langle b_0, b_1, \ldots, b_7, b'\rangle, [f_7 f_6 ... f_0, f_7 f_6 ... f_1, \ldots, f_7 f_6, f_7, 1]\rangle)^2 \\
&= \left(\sum b_i \cdot \prod_{i=1}^{7}(1 - 2c_i) + b'\right)^2 \\
&= \left(\sum b_i \cdot K_2(-2 \cdot \mathbf{1}, \mathbf{C}_i) + b'\right)^2 \quad \text{where} \\
\mathbf{C}_i &= [c_7, c_6, \ldots, c_i] \\
K_2(-2 \cdot \mathbf{1}, \mathbf{C}_i) &= \prod_{i=1}^{7}(1 - 2c_i) \quad \text{(Polynomial Kernel)}
\end{aligned}
$$

Final Form

$$
y = \frac{1 + \text{sign}\left(K_1(\mathbf{a}, \mathbf{c}) + (\sum b_i \cdot K_2(-2 \cdot \mathbf{1}, \mathbf{C}_i) + b')^2\right)}{2}
$$

4 Question 4

$$
\begin{aligned}
\alpha_i &= \frac{p_i - q_i + r_i - s_i}{2} \\
\beta_i &= \frac{p_i - q_i - r_i + s_i}{2}
\end{aligned}
$$

$$
\begin{aligned}
w_0 &= \alpha_0 = \frac{p_0 - q_0 + r_0 - s_0}{2} \\
w_i &= \alpha_i + \beta_{i-1} = \frac{p_i - q_i + r_i - s_i + p_{i-1} - q_{i-1} - r_{i-1} + s_{i-1}}{2}
\end{aligned}
$$

$$
\begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ \vdots \\ w_{63} \\ \beta_{63} \end{bmatrix} = A \begin{bmatrix} p_0 \\ q_0 \\ r_0 \\ s_0 \\ p_1 \\ q_1 \\ r_1 \\ s_1 \\ \vdots \\ p_{63} \\ q_{63} \\ r_{63} \\ s_{63} \end{bmatrix}
$$

Where matrix A has entries like:

$$
\begin{bmatrix}
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & \cdots & \\
\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \cdots & \\
0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \cdots & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \frac{1}{2} \\
-\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & & & & & & &
\end{bmatrix}
$$

Solving the System

$$
w = Ax
$$

$$
\min_x \|Ax - w\| \text{ will solve the problem}
$$

But there are more variables than equations. Hence infinitely many solutions will emerge out from such an approach.

For w_0, taking $p_0, q_0, s_0 = 0, r_0 = 2w_0$:

$$
r_1 = 2w_0 + r_0
$$

$$
r_2 = 2w_0 + r_2
$$

$\Rightarrow$ The conflict arises between point at 63rd and 64th term. By simultaneous solving:

$$
p_{63} = w_{63} + w_{64} - \frac{p_{62}}{2} \quad \text{when } p_{62} \geq 0
$$

$$
r_{63} = w_{63} - w_{64} - \frac{p_{62}}{2}
$$

So we get p, q, r, s vectors. To make sure that none of them are negative, we simply add the absolute value of overall smallest element to all (The equations don't change when a row is subtracted from other rows).

5 Question 5 and 6

Download amit.zip

6 Question 7

(a) LinearSVC training times and accuracies for different hyperparameters

C	tol	Loss	Penalty	Train Time (s)	Accuracy
1	1e-4	squared_hinge	l2	2.340000	1.0
1	1e-2	squared_hinge	l2	0.243000	1.0
1	1e-6	squared_hinge	l2	1.075770	1.0
0.01	1e-4	squared_hinge	l2	0.149589	0.9569
100	1e-4	squared_hinge	l2	3.650925	0.99625
1	1e-4	hinge	l2	0.470600	0.99625
1	1e-4	squared_hinge	l1	5.98538	1.0

(a) LinearSVC training times and accuracies for different hyperparameters

C	tol	Penalty	Train Time (s)	Accuracy
1	1e-2	l2	0.1407	0.9907
1	1e-4	l2	0.8381	0.9907
1	1e-6	l2	0.3756	0.9907
1	1e-4	l1	5.28	1
0.01	1e-4	l2	0.1122	0.89
100	1e-4	l2	0.8660	1