CS 771: Introduction To Machine Learning
Assignment 1

Akshat Agarwal
200081
akshatag20@iitk.ac.in

Muskan Kumari
200610
muskank20@iitk.ac.in

Navya Ratnan
200627
nratnan20@iitk.ac.in

Sejal Sahu
200911
sejals20@iitk.ac.in

Yash Goel
201142
yashgoel20@iitk.ac.in

Answer 1

Let $\delta^i_{0,0}, \delta^i_{0,1}, \delta^i_{1,0}$ and $\delta^i_{1,1}$ be the time intervals, when inputs are 00, 01, 10,11 respectively.
Then we have two cases:

Case-1: Output = 0
Then the time t_0 required to reach the output is

$$t_0 = \ \delta^0_{0,\ a_0} + \delta^1_{a_0,\ a1} + \delta^2_{a_0 \oplus a_1,\ a_2} + \delta^3_{a_0 \oplus a_1 \oplus a_2,\ a_3} + ... + \delta^{R-1}_{a_0 \oplus a_1 \oplus ... \oplus a_{R-2},\ a_{R-1}}$$

Case-2: Output = 1
Then the time t_1 required to reach the output is

$$t_1 = \ \delta^0_{1,\ a_0} + \delta^1_{\bar{a_0},\ a1} + \delta^2_{\bar{a_0} \oplus a_1,\ a_2} + \delta^3_{\bar{a_0} \oplus a_1 \oplus a_2,\ a_3} + ... + \delta^{R-1}_{\bar{a_0} \oplus a_1 \oplus ... \oplus a_{R-2},\ a_{R-1}}$$

We have, total time, $T_1 = t_0 + t_1$ and frequency $f_1 = \dfrac{1}{t_0 + t_1}$.

While simplifying the expression for $t_0 + t_1$, we observe the following patterns:

$$\delta^0_{0,\ a_0} + \delta^0_{1,\ a_0} = [(1 - a_0)\delta_{0,0} + a_0\delta_{0,1}] + [(1 - a_0)\delta_{1,0} + a_0\delta_{1,1}]$$

$$\begin{aligned}
\delta^1_{a_0,\ a_1} + \delta^1_{\bar{a_0},\ a_1} &= [(1 - a_0)(1 - a_1)\delta_{0,0} + (1 - a_0)a_1\delta_{0,1} + a_0(1 - a_1)\delta_{1,0} + a_0a_1\delta_{1,1}] \\
&\quad + [a_0(1 - a_1)\delta_{0,0} + a_0a_1\delta_{0,1} + (1 - a_0)(1 - a_1)\delta_{1,0} + (1 - a_0)a_1\delta_{1,1}] \\
&= (1 - a_1)\delta_{0,0} + a_1\delta_{0,1} + (1 - a_1)\delta_{1,0} + a_1\delta_{1,1}
\end{aligned}$$

$$\begin{aligned}
\delta^2_{a_0 \oplus a_1,\ a_2} + \delta^2_{\bar{a_0} \oplus a_1,\ a_2} &= [(1 - a_0)(1 - a_1) + a_0a_1](1 - a_2)\delta_{0,0} + [(1 - a_0)(1 - a_1) + a_0a_1]a_2\delta_{0,1} \\
&\quad + [a_0(1 - a_1) + (1 - a_0)a_1](1 - a_2)\delta_{1,0} + [a_0(1 - a_1) + (1 - a_0)a_1]a_2\delta_{1,1} \\
&\quad + [(1 - a_0)(1 - a_1) + a_0a_1](1 - a_2)\delta_{0,0} + [(1 - a_0)(1 - a_1) + a_0a_1]a_2\delta_{0,1} \\
&\quad + [a_0(1 - a_1) + (1 - a_0)a_1](1 - a_2)\delta_{1,0} + [a_0(1 - a_1) + (1 - a_0)a_1]a_2\delta_{1,1} \\
&= (1 - a_2)\delta_{0,0} + a_2\delta_{0,1} + (1 - a_2)\delta_{1,0} + a_2\delta_{1,1}
\end{aligned}$$

Hence, by observation we get

$$
\begin{aligned}
T_1 = t_0 + t_1 = {} & [(1-a_0)\delta_{0,0} + a_0\delta_{0,1} + (1-a_0)\delta_{1,0} + a_0\delta_{1,1}] \\
& + [(1-a_1)\delta_{0,0} + a_1\delta_{0,1} + (1-a_1)\delta_{1,0} + a_1\delta_{1,1}] + \\
& . \\
& . \\
& . \\
& + [(1-a_{R-1})\delta_{0,0} + a_{R-1}\delta_{0,1} + (1-a_{R-1})\delta_{1,0} + a_{R-1}\delta_{1,1}] \\
= {} & \left(R - \sum_{i=0}^{R-1} a_i\right)\delta_{0,0} + \left(\sum_{i=0}^{R-1} a_i\right)\delta_{0,1} + \left(R - \sum_{i=0}^{R-1} a_i\right)\delta_{1,0} + \left(\sum_{i=0}^{R-1} a_i\right)\delta_{1,1}
\end{aligned}
$$

Similarly for second XORRO, we get

$$
T_2 = t'_0 + t'_1 = \left(R - \sum_{i=0}^{R-1} a_i\right)\delta'_{0,0} + \left(\sum_{i=0}^{R-1} a_i\right)\delta'_{0,1} + \left(R - \sum_{i=0}^{R-1} a_i\right)\delta'_{1,0} + \left(\sum_{i=0}^{R-1} a_i\right)\delta'_{1,1}
$$

Now, let y be the output, then we know that

$$
y = \begin{cases} 1, & \text{if } T_1 < T_2 \\ 0, & \text{if } T_1 > T_2 \end{cases} = \frac{sgn(T_2 - T_1) + 1}{2}
$$

$$
\begin{aligned}
T_2 - T_1 = {} & \left(R - \sum_{i=0}^{R-1} a_i\right)[\delta'_{0,0} - \delta_{0,0}] + \left(\sum_{i=0}^{R-1} a_i\right)[\delta'_{0,1} - \delta_{0,1}] \\
& + \left(R - \sum_{i=0}^{R-1} a_i\right)[\delta'_{1,0} - \delta_{1,0}] + \left(\sum_{i=0}^{R-1} a_i\right)[\delta'_{1,1} - \delta_{1,1}] \\
= {} & \left(R - \sum_{i=0}^{R-1} a_i\right)\Delta_{0,0} + \left(\sum_{i=0}^{R-1} a_i\right)\Delta_{0,1} + \left(R - \sum_{i=0}^{R-1} a_i\right)\Delta_{1,0} + \left(\sum_{i=0}^{R-1} a_i\right)\Delta_{1,1} \\
= {} & \left(\sum_{i=0}^{R-1} a_i\right)[-\Delta_{0,0} + \Delta_{0,1} - \Delta_{1,0} + \Delta_{1,1}] + [R\Delta_{0,0} + R\Delta_{1,0}]
\end{aligned}
$$

where $\Delta_{i,j} = (\delta'_{i,j} - \delta_{i,j})$ and $i, j \,\epsilon\, \{0, 1\}$

Define vectors **w, a** and constant b as follows:

$\mathbf{w} := [\Delta_{0,0} \;\; \Delta_{0,1} \;\; \Delta_{1,0} \;\; \Delta_{1,1}]^T$

$\mathbf{a} := [a_0 \;\; a_1 \;\; a_2 \;\; ... \;\; a_{R-1}]$

$b := R\Delta_{0,0} + R\Delta 1, 0$

$$
\begin{aligned}
\left(\sum_{i=0}^{R-1} a_i\right)[-\Delta_{0,0} + \Delta_{0,1} - \Delta_{1,0} + \Delta_{1,1}] &= \mathbf{w}^T \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} [1 \;\; 1 \;\; 1 \;\; ... \;\; 1]_{1\times R} \cdot \mathbf{a} \\
&= \mathbf{w} \cdot \begin{bmatrix} -1 & -1 & ... & -1 \\ 1 & 1 & ... & 1 \\ -1 & -1 & ... & -1 \\ 1 & 1 & ... & 1 \end{bmatrix}_{4\times R} \cdot \mathbf{a} \\
&= \mathbf{w}^T \mathbf{P} \mathbf{a} \\
&= \mathbf{w}^T \phi(\mathbf{a})
\end{aligned}
$$

where $\phi(\mathbf{a}) := \mathbf{P} \cdot \mathbf{a}$

Then we get,

$$T_2 - T_1 = \mathbf{w}^T \phi(\mathbf{a}) + b$$

Hence, we can conclude,

$$y = \frac{sgn(\mathbf{w}^T \phi(\mathbf{a}) + b) + 1}{2}$$

where $\mathbf{a} \, \epsilon \{0, 1\}^R$

Answer 2

The parameters used to define the linear model **w** and b in the previous section are defined for a pair of XORROs.

Let us now define two vectors to select two XORROs from 2^S XORROs. Parameters **w** and b will be uniquely defined for each pair as $\mathbf{w}_{i,j} = -\mathbf{w}_{j,i}$ and $b_{i,j} = -b_{j,i}$, where i, j $\epsilon\{1, 2, 3, ..., 2^S\}$

Let's define a 3-dimensional vector **W** and 2-dimensional vector **B** as follows.

$$\mathbf{W} := \begin{bmatrix} 0 & \mathbf{w}_{1,2} & \mathbf{w}_{1,3} & ... & \mathbf{w}_{1,2^S} \\ \mathbf{w}_{2,1} & 0 & \mathbf{w}_{2,3} & ... & \mathbf{w}_{2,2^S} \\ \mathbf{w}_{3,1} & \mathbf{w}_{3,2} & 0 & ... & \mathbf{w}_{3,2^S} \\ \vdots & \vdots & \vdots & & \vdots \\ \mathbf{w}_{2^S,1} & \mathbf{w}_{2^S,2} & \mathbf{w}_{2^S,3} & ... & 0 \end{bmatrix}$$

$$\mathbf{B} := \begin{bmatrix} 0 & b_{1,2} & b_{1,3} & ... & b_{1,2^S} \\ b_{2,1} & 0 & b_{2,3} & ... & b_{2,2^S} \\ b_{3,1} & b_{3,2} & 0 & ... & b_{3,2^S} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{2^S,1} & b_{2^S,2} & b_{2^S,3} & ... & 0 \end{bmatrix}$$

$\mathbf{W}^T = -\mathbf{W}, \mathbf{B}^T = -\mathbf{B}$

Let $\mathbf{C}_i$ represent the vector used to select the i^{th} XORRO. It can generated once the 2S bit values are separated to two S bit values (they can be converted to decimal values i,j).

$$\mathbf{C}_i = [c_1 \quad c_2 \quad c_3 \quad ... \quad c_i \quad ...c_{2^S}]^T$$

where c_j = $\begin{cases} 1, & \text{if } j = i \\ 0, & \text{otherwise} \end{cases}$

Therefore,

$$\mathbf{w}_{i,j} = \mathbf{C}_i^T \mathbf{W} \mathbf{C}_j = -\mathbf{C}_j^T \mathbf{W} \mathbf{C}_i$$
$$\mathbf{b}_{i,j} = \mathbf{C}_i^T \mathbf{B} \mathbf{C}_j = -\mathbf{C}_j^T \mathbf{B} \mathbf{C}_i$$

From the previously derived linear model,

$$y = \frac{sgn(\mathbf{w}_{i,j}^T \mathbf{a} + b_{i,j}) + 1}{2}$$
$$= \frac{sgn(-\mathbf{C}_j^T \mathbf{W} \mathbf{C}_i \mathbf{a} - \mathbf{C}_j^T \mathbf{B} \mathbf{C}_i) + 1}{2}$$
$$y = \frac{sgn(\mathbf{C}_i^T (\mathbf{W}\mathbf{a} + \mathbf{B}) \mathbf{C}_j) + 1}{2}$$

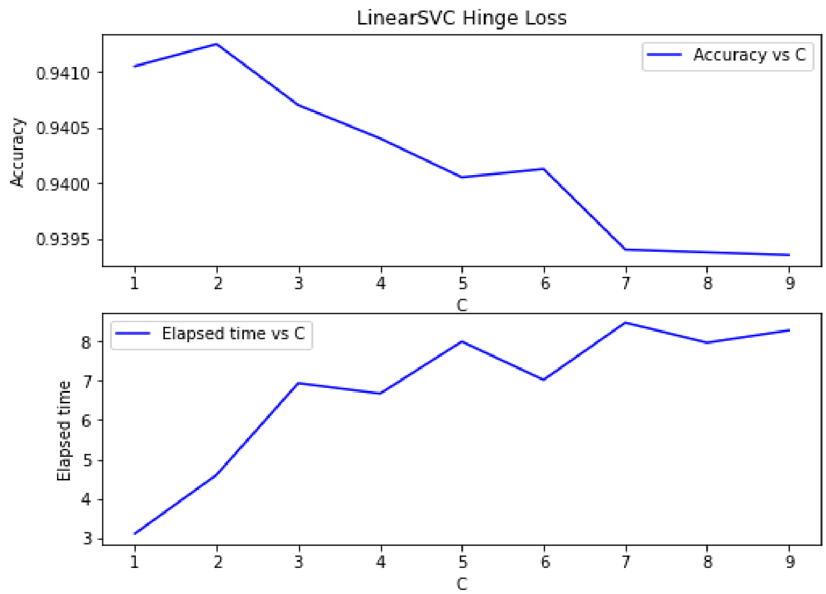
Hence, we have proved mathematically that the advanced XORRO PUF can be cracked using a collection of simple linear models.

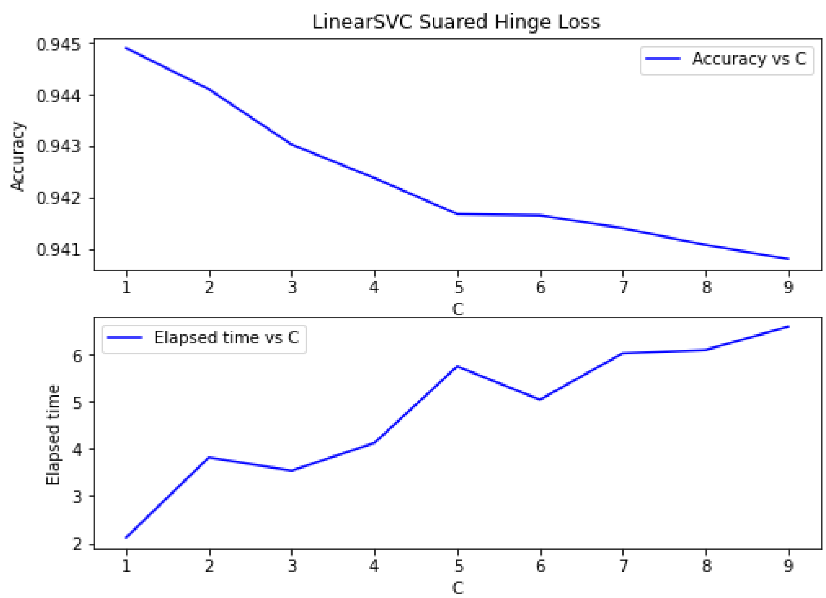
However, while implementing the code, we used a 2-dimensional list of linear models. We separated the data using select bits for each linear model and trained them individually.
During implementation, we did not use the C_i vectors to reduce computation time as data can be directly queried using array data structure. We created only $M = 2^{S-1}(2^S - 1)$ models instead the 2M models as we defined in the **W** matrix as the matrix is skew symmetric.

Answer 4

a)

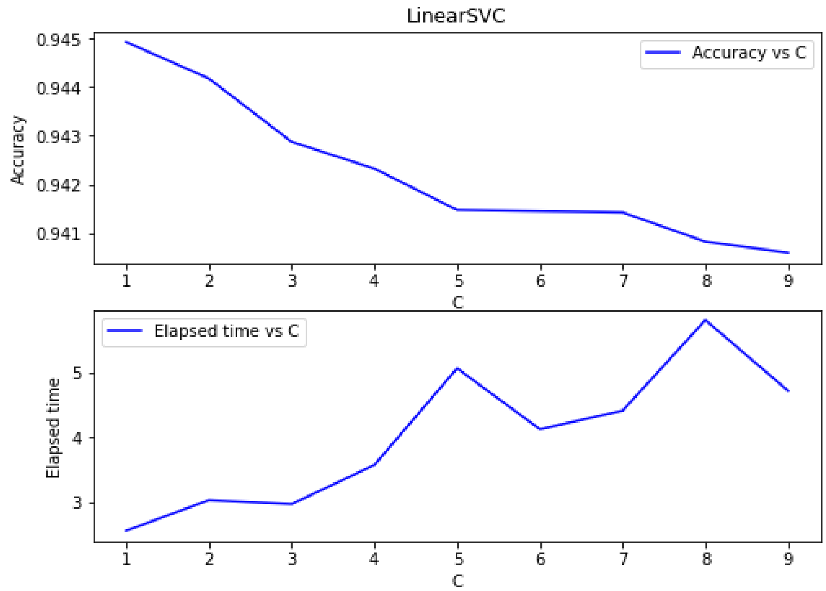
Affect of changing the loss hyperparameter in LinearSVC (hinge vs squared hinge)

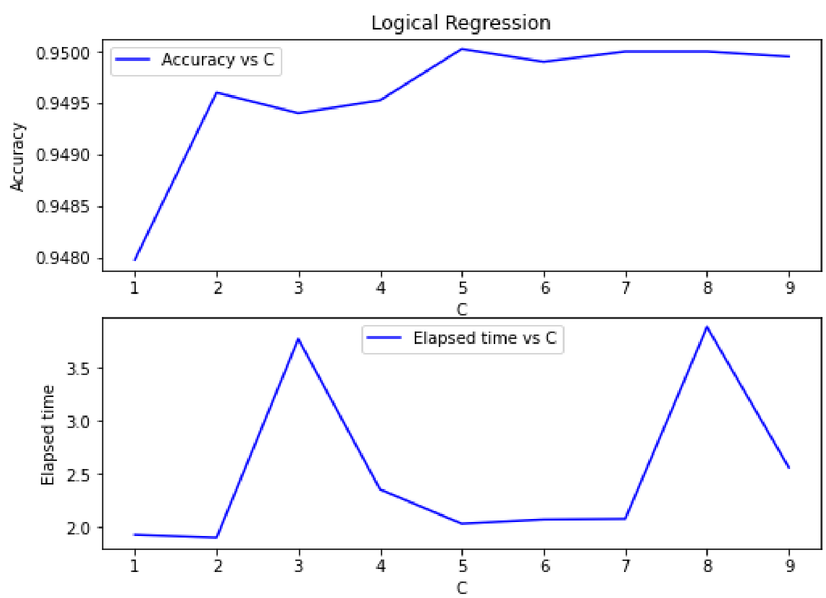




Fixed parameters: max iter = 100,000, tol = 0.01.
We conclude that with squared hinge loss, the time taken and accuracy has improved.

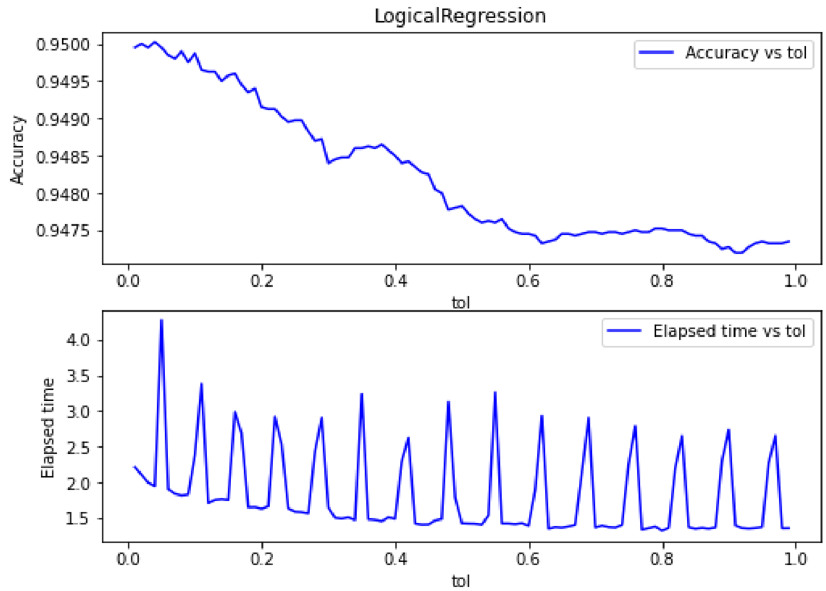
b)

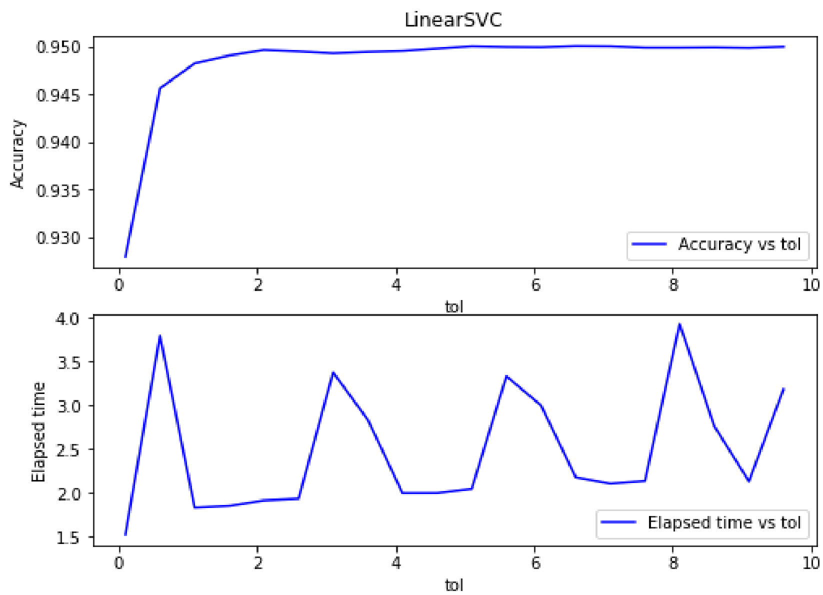




Fixed parameters: max iter = 100,000, tol = 0.02 As it can be observed, accuracy is maximum for C = 1 for LinearSVC and C = 7 for Logistic Regression while the trend in training time is difficult to judge.

c)





Fixed parameters: max iter = 100,000, C(SVC) = 1, C(logisticRegression) = 7 The trend in accuracy is the reverse as compared to the trend when C was varied.