CS771A: Assignment 1

Team : Technocrats

February 18, 2023

Part-1:

Breaking Simple XORRO PUF with a Linear Model

Frequency of XORRO gate given by :

$$\frac{1}{TimePeriod}$$

Time Period : Time in which output changes from 1 to 0 and then back to 1.
In the whole time period, time taken by any i$^{\text{th}}$ XOR gate will be

$$t_i = \delta^i_{00}(1-a_i)+\delta^i_{01}(a_i)+\delta^i_{10}(1-a_i)+\delta^i_{11}(a_i) = a_i(\delta^i_{01}+\delta^i_{11}-\delta^i_{00}-\delta^i_{10})+\delta^i_{00}+\delta^i_{10}$$

taking

$$\alpha_i = [\delta^i_{01} + \delta^i_{11} - \delta^i_{00} - \delta^i_{10}], \beta_i = \delta^i_{00} + \delta^i_{10}$$

Here α_i and β_i are the constants for a XOR gate.
Total time period will be

$$T = \sum_{i=0}^{r-1} t_i \ = \sum_{i=0}^{r-1}[(a_i \times \alpha_i) + \beta_i]$$

$$T = \sum_{i=0}^{r-1}(a_i \times \alpha_i) + \sum_{i=0}^{r-1}\beta_i$$

Similarly, for other XORRO gate, time period will be

$$T = \sum_{i=0}^{r-1}(a_i \times x_i) + \sum_{i=0}^{r-1} y_i$$

Time Period for Upper XORRO gate-

$$T_U = \sum_{i=0}^{r-1}(a_i \times \alpha_i) + \sum_{i=0}^{r-1} \beta_i$$

Time Period for Lower XORRO gate -

$$T_L = \sum_{i=0}^{r-1}(a_i \times x_i) + \sum_{i=0}^{r-1} y_i$$

The counter outputs 1 if upper XORRO has higher frequency or output is 1 if

$$T_L > T_U$$

or

$$\Delta T = T_L - T_U > 0$$

or

$$\Delta T > 0$$

and

$$\Delta T = T_L - T_U = \sum_{i=0}^{r-1} a_i \times (x_i - \alpha_i) + \sum_{i=0}^{r-1}(y_i - \beta_i)$$

Taking

$$x_i - \alpha_i = w_i, \sum_{i=0}^{r-1}(y_i - \beta_i) = b$$

$$\Delta T = \sum_{i=0}^{r-1} a_i \times w_i + b$$

Now since output is 1 for

$$\Delta T > 0$$

The response will be

$$\frac{1 + sign(\Delta T)}{2}$$

and

$$\Delta T = \sum_{i=0}^{r-1} a_i \times w_i + b$$

or

$$\Delta T = w^T \times \phi(c) + b$$

where b $\in R, w \in R^D, c \in \{0,1\}^{\mathrm{R}}$
$\phi : \{0,1\}^R, \rightarrow R^D, D > 0$
and in this case, D=R
So, the following explanation gives the correct response:

$$\frac{1 + sign(w^T \phi(c) + b)}{2}$$

Part-2:

Cracking a Simple XORRO PUF

To crack a simple XORRO PUF, the expression

$$\frac{1 + sign(w^\top \phi(c) + b)}{2}$$

is used.

Cracking an Advanced XORRO PUF

An advanced XORRO PUF can be treated as a collection of multiple simple XORRO PUFs. In 2^S available XORROs, $M = 2^{S-1}(2^S - 1)$ pairs of XORROs can be used in the XORRO PUF.

Hence, we need to have M [$M = 2^{S-1}(2^S - 1)$] number of linear models, one for each pair of XORROs, to crack the advanced XORRO PUF. The expression used to crack a simple XORRO PUF is :

$$\frac{1 + sign(w^\top \phi(c) + b)}{2}$$

Advanced XORRO PUF with R = 64, S = 4 i.e. it has 64 + 4 + 4 = 72 bit challenges.

M=$2^{(4-1)}(2^4 - 1) = 120$

For the $(i, j)th$ pair, the expression would be :

$$\frac{1 + sign(w_{i,j}^\top \phi(c) + b_{i,j})}{2}$$

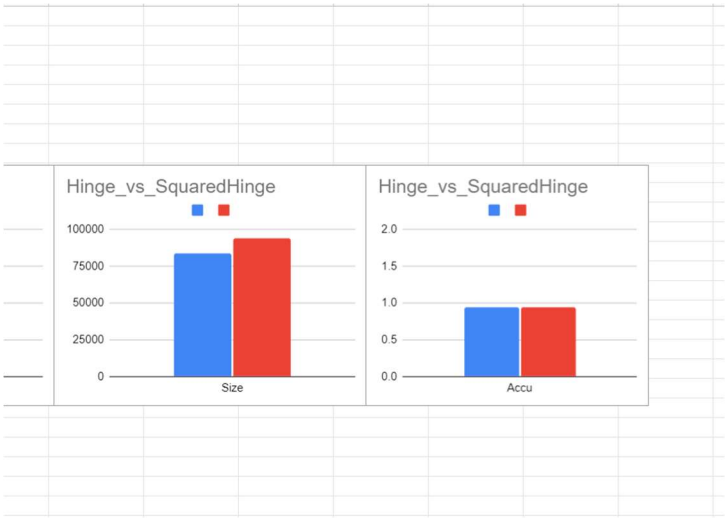
where c corresponds to the starting 64 bits of the challenge, and the i, j will be given by the last 8 bits, in which the first 4 bits correspond to the upper XORRO, and the last 4 bits correspond to the lower XORRO.

[For optmising solution, we have considered pair(1,3) and pair (3,1) as one unique pair, not two different pairs (adjusting the output accordingly)]

PART 4 :

Q- Report the affect of training time and test accuracy of at least 2 of the following :

a) changing the loss hyperparameter in LinearSVC (hinge vs squared hinge)



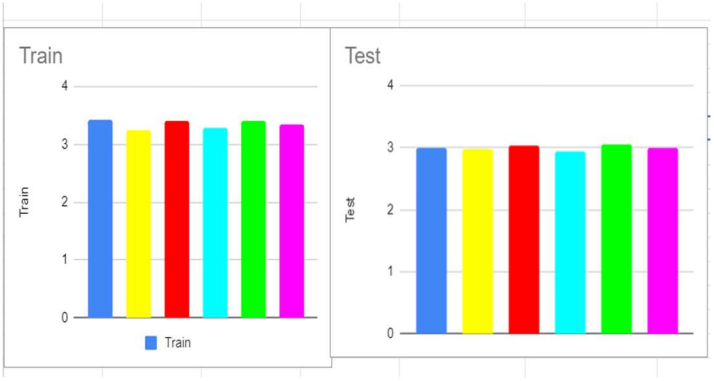
Training time was more when the loss hyperparameter was Hinge as compared to Squared Hinge.
Accuracy almost remained same for both hyperparameters.

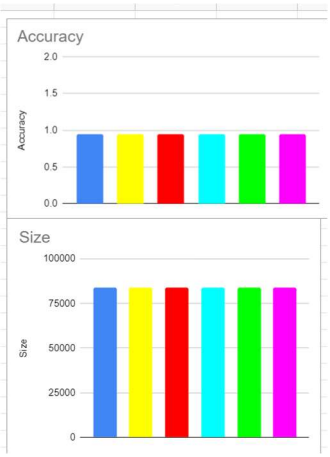
b) setting C hyperparameter in LinearSVC and LogisticRegression to high/low/medium value

Changing C HyperMeter

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

	High_c_SVC	Medium_C_SVC	Low_C_SVC	HIGH_C_LogiReg	Medium_C_LogiReg	Low_C_LogiReg
Train	3.42022	3.25133	3.4033304	3.279	3.409041	3.34219
Test	3.0063	2.9764925	3.03166	2.942272	3.050659	2.99966
Size	83743.4	83743.6	83743	83743.6	83743.6	83744
Accuracy	0.947425	0.947425	0.947425	0.947425	0.947425	0.947425





In LinearSVC when Hyperparameter C was set to Highest value , Training time was highest , when C was set to medium value , Training time was lowest , when C was set to lowest value, training time was in between the high and low medium value.

In LogisticRegression when Hyperparameter C was set to Highest value , Training time was lowest , when C was set to medium value , Training time was highest , when C was set to lowest value, training time was in between the high and low medium value.

On comparing in between the models , training time was more for High value C LinearSVC model than High value C Logistic Regression model. Training time was less for Medium value C LinearSVC model than Migh value C Logistic Regression model. Training time was less for Low value C LinearSVC model than Low value C Logistic Regression model.

Accuracy remained same for both the models (LinearSVC and LogisticRegression) on changing the C hyperparameter value to High, Medium and Low.