Assignment 1

Divyansh Mathur
Department of Electrical Engineering
Indian Institute of Technology Kanpur
divyanshm21@iitk.ac.in

Khush Khandelwal
Department of Mechanical Engineering
Indian Institute of Technology Kanpur
khushk21@iitk.ac.in

Manan Kabra
Department of Mathematics
Indian Institute of Technology Kanpur
manank21@iitk.ac.in

Parv Chhabra
Department of Electrical Engineering
Indian Institute of Technology Kanpur
pchhabra21@iitk.ac.in

Vaibhav Methi
Department of Electrical Engineering
Indian Institute of Technology Kanpur
mvaivhav21@iitk.ac.in

1 Breaking Companion Arbiter PUF into a linear model

Let the *challenge* bits be $\mathbf{c} \stackrel{\text{def}}{=} [c_0, c_1, c_2, ..., c_{31}]$.
We define a new vector $\boldsymbol{\varphi}(c) \stackrel{\text{def}}{=} [\varphi_0, \varphi_1, \varphi_2, ..., \varphi_{31}]$, such that :-

$$\varphi_i \stackrel{\text{def}}{=} \prod_{k=i}^{31}(1 - 2c_k)$$

We also note that, since $c_i \in \{0, 1\} \Rightarrow (1 - 2c_i) \in \{-1, 1\} \Rightarrow \varphi_i \in \{-1, 1\}$

From Week 1 lecture slides, we know that the lag of an arbiter PUF can be broken up into a linear model given be :-

$$\Delta_{31} = \mathbf{w}^T.\boldsymbol{\varphi}(c) + \beta$$

Let ($\mathbf{u}$,p) be the linear model for *working* arbiter PUF and ($\mathbf{v}$,q) be the linear model for *reference* arbiter PUF, i.e.

$$\Delta_w = \mathbf{u}^T.\boldsymbol{\varphi}(c) + p$$
$$\Delta_r = \mathbf{v}^T.\boldsymbol{\varphi}(c) + q$$

The response of our CAR-PUF is 0 if $\left|\Delta_w - \Delta_r\right| \leq \tau$ and response is 1 if $\left|\Delta_w - \Delta_r\right| > \tau$
We have

$$\Delta_w - \Delta_r = (\mathbf{u}^T.\boldsymbol{\varphi}(c) + p) - (\mathbf{v}^T.\boldsymbol{\varphi}(c) + q)$$
$$\Delta_w - \Delta_r = (\mathbf{u} - \mathbf{v})^T.\boldsymbol{\varphi}(c) + (p - q)$$

Now for the response to be 0,

$$\left|\Delta_w - \Delta_r\right| \leq \tau$$
$$\left|(\mathbf{u} - \mathbf{v})^T.\boldsymbol{\varphi}(c) + (p - q)\right| \leq \tau$$

Given $\tau > 0$, squaring the above we get

$$\left|(\mathbf{u}-\mathbf{v})^T.\boldsymbol{\varphi}(c) + (p-q)\right|^2 \leq \tau^2$$

$$\Big|\sum_{i=0}^{31}((u_i - v_i)\varphi_i) + (p-q)\Big|^2 \leq \tau^2$$

$$\sum_{i=0}^{31}(u_i-v_i)^2\varphi_i^2 + (p-q)^2 + 2\sum_{i=0}^{31}\sum_{j=i+1}^{31}(u_i-v_i)(u_j-v_j)\varphi_i\varphi_j + 2(p-q)\sum_{i=0}^{31}(u_i-v_i)\varphi_i \leq \tau^2$$

Claim : $\varphi_i^2 = 1 \,\forall\, i \in \{0,1,2,...,31\}$
Proof : Since the challenge bit $c_i \in \{0,1\} \implies (1-2c_i) \in \{-1,1\}$
By the definition of φ_i, we have

$$\varphi_i \stackrel{\text{def}}{=} \prod_{k=i}^{31}(1-2c_k)$$

$$(1-2c_i) \in \{-1,1\} \implies \varphi_i \in \{-1,1\} \implies \varphi_i^2 = 1$$

$Therefore, \varphi_i^2 = 1 \,\forall\, i \in \{0,1,2,...,31\}$

Now, our inequality reduces to :-

$$\sum_{i=0}^{31}(u_i-v_i)^2 + (p-q)^2 + 2\sum_{i=0}^{31}\sum_{j=i+1}^{31}(u_i-v_i)(u_j-v_j)\varphi_i\varphi_j + 2(p-q)\sum_{i=0}^{31}(u_i-v_i)\varphi_i \leq \tau^2$$

$$2\sum_{i=0}^{31}\sum_{j=i+1}^{31}(u_i-v_i)(u_j-v_j)\varphi_i\varphi_j + 2(p-q)\sum_{i=0}^{31}(u_i-v_i)\varphi_i + \sum_{i=0}^{31}(u_i-v_i)^2 + (p-q)^2 - \tau^2 \leq 0$$

We choose our feature vectors to be :- $\{\varphi_i; 0 \leq i \leq 31\} \cup \{\varphi_i\varphi_j; 0 \leq i \leq 31, i+1 \leq j \leq 31\}$
With these feature vectors we note that the above model is linear, and we define our feature map $\phi : \{0,1\}^{32} \to \mathbb{R}^D$ where $D = 32 + \binom{32}{2} = 528$
Now we represent in terms of matrix as follows :

$$\begin{bmatrix} 2(p-q)(u_0-v_0) \\ \vdots \\ 2(p-q)(u_{31}-v_{31}) \\ 2(u_0-v_0)(u_1-v_1) \\ 2(u_0-v_0)(u_2-v_2) \\ \vdots \\ 2(u_{30}-v_{30})(u_{31}-v_{31}) \end{bmatrix}^T \begin{bmatrix} \varphi_0 \\ \vdots \\ \varphi_{31} \\ \varphi_0\varphi_1 \\ \varphi_0\varphi_2 \\ \vdots \\ \varphi_{30}\varphi_{31} \end{bmatrix} + \sum_{i=0}^{31}(u_i-v_i)^2 + (p-q)^2 - \tau^2 = \mathbf{W}^T.\boldsymbol{\phi}(\mathbf{c}) + b$$

where

$$\mathbf{W} = \begin{bmatrix} 2(p-q)(u_0-v_0) \\ \vdots \\ 2(p-q)(u_{31}-v_{31}) \\ 2(u_0-v_0)(u_1-v_1) \\ 2(u_0-v_0)(u_2-v_2) \\ \vdots \\ 2(u_{30}-v_{30})(u_{31}-v_{31}) \end{bmatrix}_{528} \qquad \boldsymbol{\phi}(\mathbf{c}) = \begin{bmatrix} \varphi_0 \\ \vdots \\ \varphi_{31} \\ \varphi_0\varphi_1 \\ \varphi_0\varphi_2 \\ \vdots \\ \varphi_{30}\varphi_{31} \end{bmatrix}_{528} \qquad b = \sum_{i=0}^{31}(u_i-v_i)^2 + (p-q)^2 - \tau^2$$

The response of this CAR-PUF is 0 if $\mathbf{W}^T.\phi(\mathbf{c}) + b \leq 0$ and response is 1 if $\mathbf{W}^T.\phi(\mathbf{c}) + b > 0$
Hence, the response to the challenge is given by the following expression:

$$\frac{1 + sign(\mathbf{W}^T\boldsymbol{\phi}(\mathbf{c}) + b)}{2} = r$$

We have defined φ_i as:

$$\varphi_i \overset{\text{def}}{=} \prod_{k=i}^{31}(1-2c_k) \implies \varphi_i\varphi_j = \prod_{k=i}^{j-1}(1-2c_k).\prod_{t=j}^{31}(1-2c_t)^2$$

$$\varphi_i\varphi_j = \prod_{k=i}^{j-1}(1-2c_k) \;\; since \;\; (1-2c_t)^2 = 1 \;\; \forall \; t \in \{0,1,2,...,31\}$$

Therefore, our map $\phi(\mathbf{c})$ is given by :

$$\phi(\mathbf{c}) = \begin{bmatrix} \prod_{k=0}^{31}(1-2c_k) \\ \prod_{k=1}^{31}(1-2c_k) \\ \vdots \\ \prod_{k=31}^{31}(1-2c_k) \\ \prod_{k=0}^{0}(1-2c_k) \\ \prod_{k=0}^{1}(1-2c_k) \\ \vdots \\ \prod_{k=30}^{30}(1-2c_k) \end{bmatrix}_{528} \qquad where \;\; \mathbf{c} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{31} \end{bmatrix}_{32}$$

2 Outcomes with different models while tuning hyperparameters

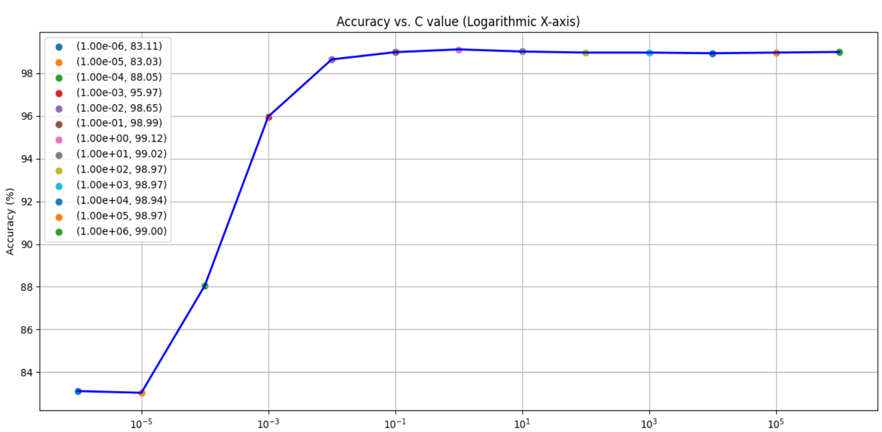
2.1 Changing loss hyperparameter in LinearSVC:

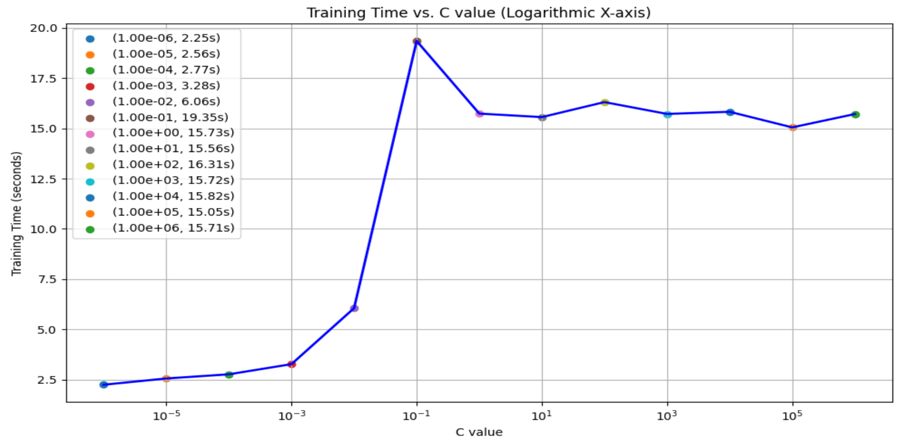
Accuracies and Training time on changing the loss function in the LinearSVC model, with default values of hyperparameters and max_iter = 10,000 are as shown:

Loss	Test Accuracy	Training Time
Hinge	98.82	14.23s
Squared Hinge	99.14	16.27s

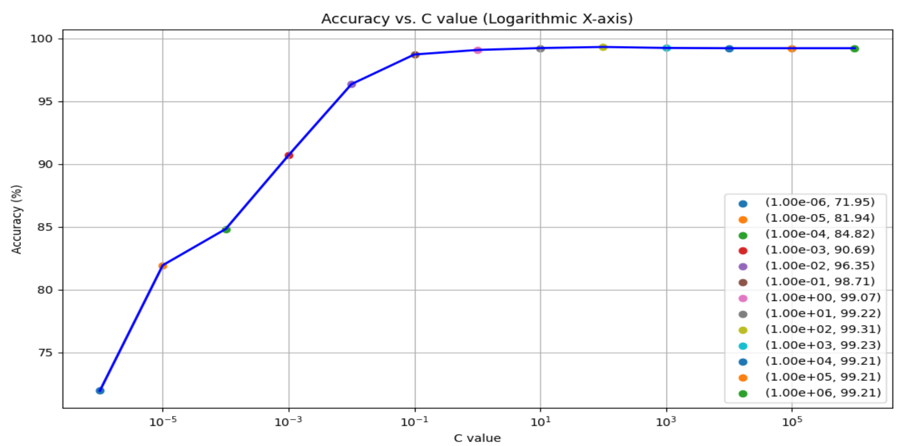
2.2 Tuning C hyperparameter in LinearSVC and LogisticRegression:

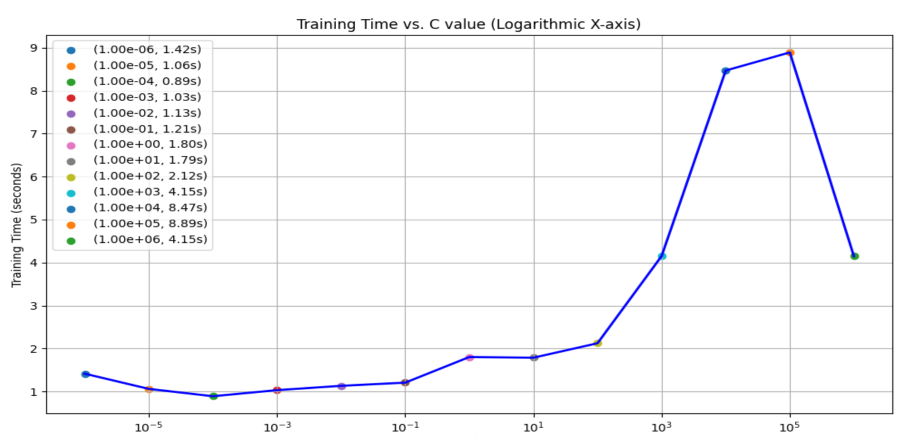
2.2.1 Linear SVC





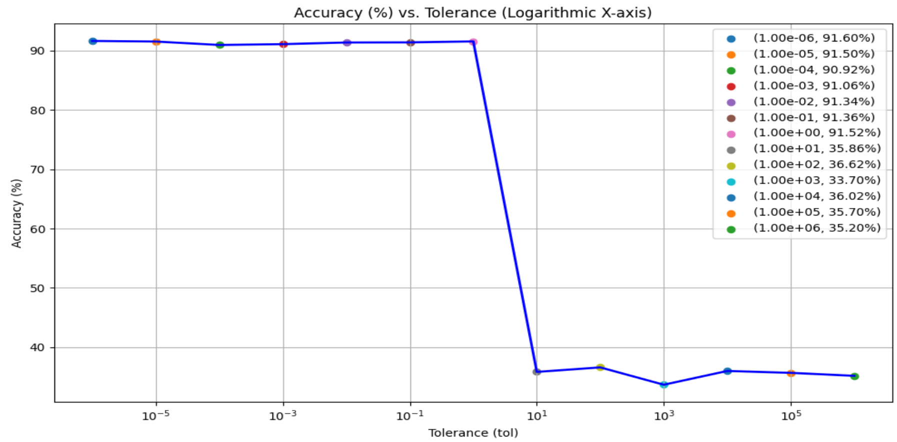
2.2.2 Logistic Regression

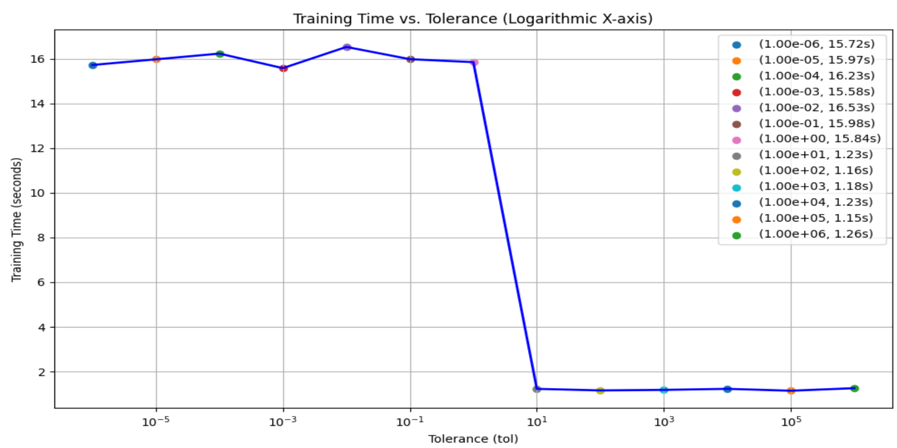




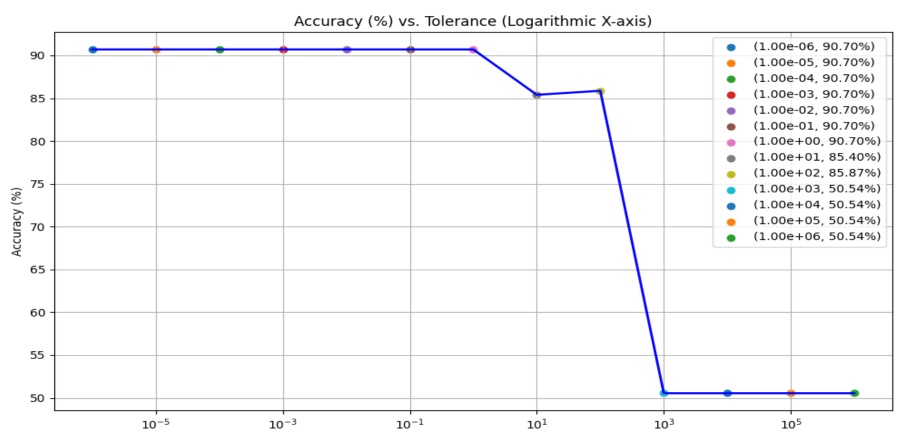
2.3 Tuning tol hyperparameter in LinearSVC and LogisticRegression:

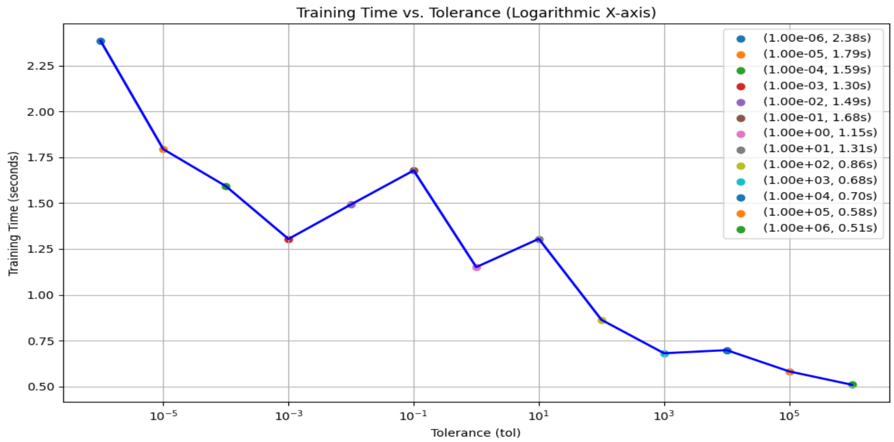
2.3.1 Linear SVC





2.3.2 Logistic Regression





2.4 Changing penalty (regularization) hyperparameter in LinearSVC and LogisticRegression:

Model	Test Accuracy	Training Time
LinearSVC	L1: 99.13 L2: 99.17	L1: 170s L2: 15.90s
Logistic Regression	L1: 99.18 L2: 99.08	L1: 234.79s L2: 2.85s