CS771 Introduction to Machine Learning

BY Learning Machine Learning

July 17, 2024

Here is a detailed mathematical derivation for constructing a linear model to predict the time $t_u(c)$ for the upper signal to reach the finish line in an arbiter Physically Unclonable Function (PUF), using the challenge vector c.

1 Problem Definition

Given:

- A 32-bit challenge vector $c = \{c_1, c_2, \dots, c_{32}\}$, where each $c_i \in \{0, 1\}$.
- The time $t_u(c)$ for the upper signal to reach the finish line, measured in milliseconds.

Objective:

- Create a mapping $\phi : \{0, 1\}^{32} \to R^D$.
- Find a linear model with parameters $W \in R^D$ and $b \in R$ such that:

$$W^\top \phi(c) + b = t_u(c)$$

Derivation of the Linear Model

1.1 Signal Propagation Time

The time t_i^u for the upper signal to propagate through the i-th stage in an arbiter PUF can be influenced by the configuration of the multiplexers and the challenge bits.

Given the challenge vector $c = \{c_1, c_2, \dots, c_{32}\}$, the time t_i^u can be expressed recursively:

$$t_i^u = (1 - c_i) \cdot (t_{i-1}^u + P_i) + c_i \cdot (t_{i-1}^l + S_i)$$

where:

- t_{i-1}^u and t_{i-1}^l are the upper and lower signal propagation times at stage $i - 1$.
- P_i and S_i are the delay terms specific to the i-th multiplexer.
- c_i is the challenge bit at stage i.

1.2 Deriving t^u_{32}

The t^u_i is:

$$t^u_i = P_i + t^u_{i-1} - c_i \cdot P_i + c_i \cdot S_i - c_i \cdot \Delta_{i-1}$$

(t$^u_i - t^l_i = \Delta_i$)

Now:

$$t^u_i - t^u_{i-1} = P_i - c_i \cdot P_i + c_i \cdot S_i - c_i \cdot \Delta_{i-1}$$

Taking i till 32

$$t^u_{32} = \sum_{i=1}^{32} (P_i + c_i \cdot S_i - c_i \cdot P_i) \;\; - \sum_{i=2}^{i=32} c_i \cdot \Delta_{i-1}$$

Simplifying Δ_i :

From sir's lecture notes

$$\Delta_i = \sum_{j=1}^{j=i} ((\alpha_j + \beta_{j-1}) \prod_{k=j}^{k=i} (1 - 2c_k)) + \beta_i$$

where

$$\beta_0 = 0, \alpha_j = (P_j - Q_j + R_j - S_j)/2$$
$$\beta_j = (P_j - Q_j - R_j + S_j)/2$$

and

Q_j and R_j are the delay terms specific to the j-th multiplexer

1.3 Mapping Function ϕ

We can transform above result such that:

$$t^u_{32} = W^T \phi(c) + b$$

where W^T and b depends only on PUFs-specific constant (α_j,β_j,P and Q)

b can shown as

$$b = \sum_{i=1}^{i=32} P_i$$

and W as from i=1 to i=31

$$W_i = -(\alpha_i + \beta_{i-1})$$

and from i=32 to i=63

$$W_i = S_{i-31} - P_{i-31} - \beta_{i-32}$$

Now $\phi(c)$ as

from i=1 to i=31

$$\phi(c)_i = \sum_{j=i}^{j=31} (c_{j+1} \prod_{k=i}^{k=j} (1 - 2c_k))$$

and from i=32 to i=63

$$\phi(c)_i = c_{i-31}$$

2 Problem

Dimensionality of the Linear Model

As from above we derived that our linear model W is: from i=1 to i=31

$$W_i = -(\alpha_i + \beta_{i-1})$$

and from i=32 to i=63

$$W_i = S_{i-31} - P_{i-31} - \beta_{i-32}$$

W is in form of : $R^{\tilde{63}}$. That is it contains 63 elements.

3 Problem Definition

Here is a detailed mathematical derivation for constructing a linear model to predict the responses $r_0(c)$ and $r_1(c)$ for a Cross-Connection Physically Unclonable Function (COCO-PUF), using the challenge vector c.

Given:

- A 32-bit challenge vector $c = \{c_1, c_2, \ldots, c_{32}\}$, where each $c_i \in \{0, 1\}$.
- Responses $r_0(c)$ and $r_1(c)$ for the challenge c.

Objective:

- Create a mapping $\tilde{\phi} : \{0, 1\}^{32} \to R^{\tilde{D}}$.
- Find linear models with parameters $\tilde{W}_0, \tilde{W}_1 \in R^{\tilde{D}}$ and $\tilde{b}_0, \tilde{b}_1 \in R$ such that:

$$r_0(c) = \frac{1 + \text{sign}(\tilde{W}_0^\top \tilde{\phi}(c) + \tilde{b}_0)}{2}$$

$$r_1(c) = \frac{1 + \text{sign}(\tilde{W}_1^\top \tilde{\phi}(c) + \tilde{b}_1)}{2}$$

3.1 Signal Propagation Time Differences

For COCO-PUF, consider the difference in reaching signal time of upper signal form PUF1 and PUF0.

$$\Delta_u = t_{32}^{u,1} - t_{32}^{u,0}$$

Similarly with lower siganl.

$$\Delta_l = t_{32}^{l,1} - t_{32}^{l,0}$$

Now from derivation of Q.1:

$$t_{32}^{u} = W^T \phi(c) + b$$

We can also say same thing for lower singal.

$$t_{32}^{l} = W^T \phi(c) + b$$

(Lower siganl expression would also derieve in same way as upper signal)

Let:

$$t_{32}^{u,1} = W_1^T \phi(c) + b_1$$

same with:

$$t_{32}^{u,0} = W_0^T \phi(c) + b_0$$

So

$$\Delta_u = W_1^T \phi(c) + b_1 - W_0^T \phi(c) - b_0$$
$$\Delta_u = (W_1^T - W_0^T)\phi(c) + (b_1 - b_0)$$

let

$$A_u^T = W_1^T - W_0^T$$
$$c_u = b_1 - b_0$$

So

$$\Delta_u = A_u^T \phi(c) + c_u$$

Similarly

$$\Delta_l = A_l^T \phi(c) + c_l$$

And we know that:

$$r_1(c) = \frac{1 + \text{sign}(\Delta_u)}{2}$$
$$r_0(c) = \frac{1 + \text{sign}(\Delta_l)}{2}$$

So

$$r_0(c) = \frac{1 + \text{sign}(A_0^T \phi(c) + c_0)}{2}$$
$$r_1(c) = \frac{1 + \text{sign}(A_1^T \phi(c) + c_1)}{2}$$

$\phi(c)$ is a map we derived in Q1

So: $\tilde{\phi} : \{0,1\}^{32} \rightarrow \tilde{R^{63}}$

and from i=1 to i=31

$$\phi(c)_i = \sum_{j=i}^{j=31} (c_{j+1} \prod_{k=i}^{k=j} (1 - 2c_k))$$

and from i=32 to i=63

$$\phi(c)_i = c_{i-31}$$

and W_1 and W_2 are same linear model but with different time constants.

4 Dimensionality of Model

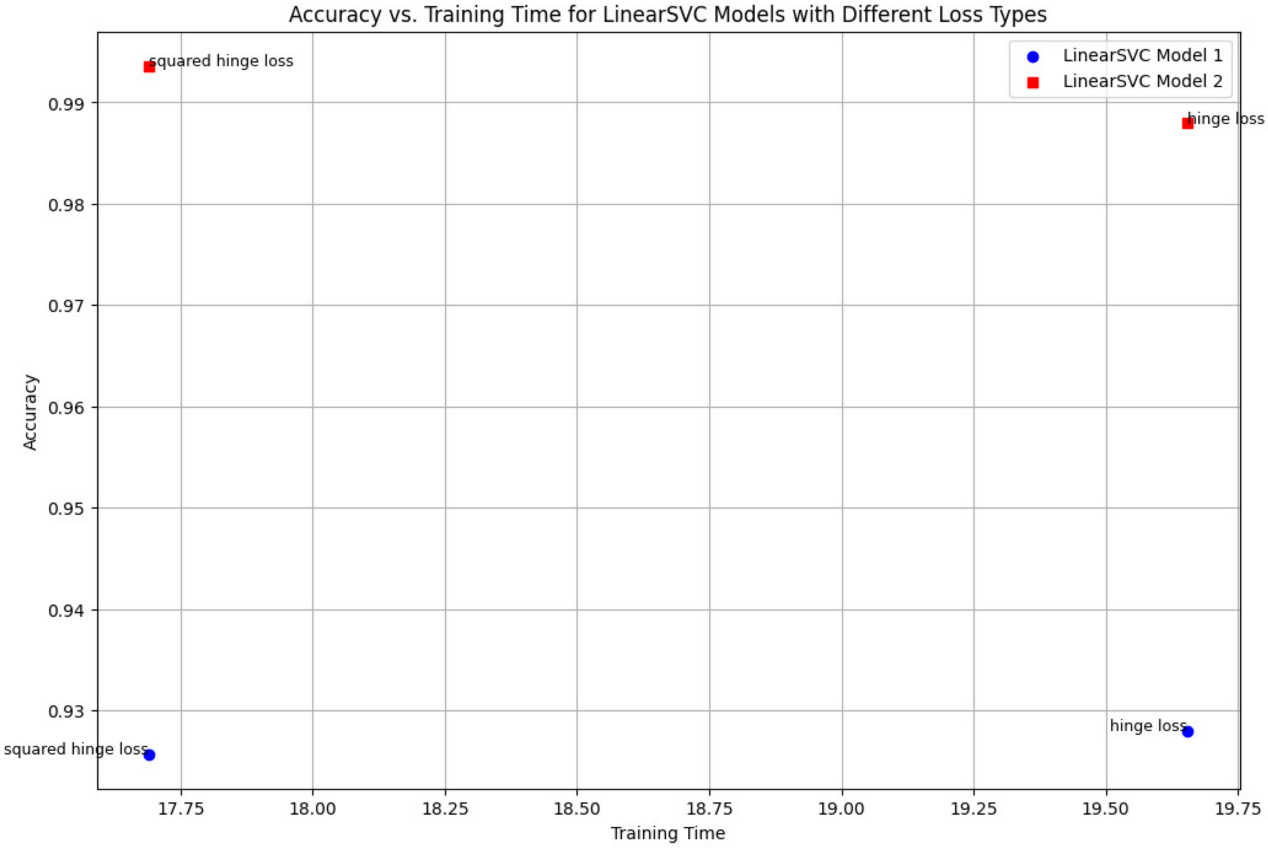
For both responses, dimensionality is same. That is 63. The model have same dimensionality as we derived from Q1. We just took difference of same model for upper and lower signal.

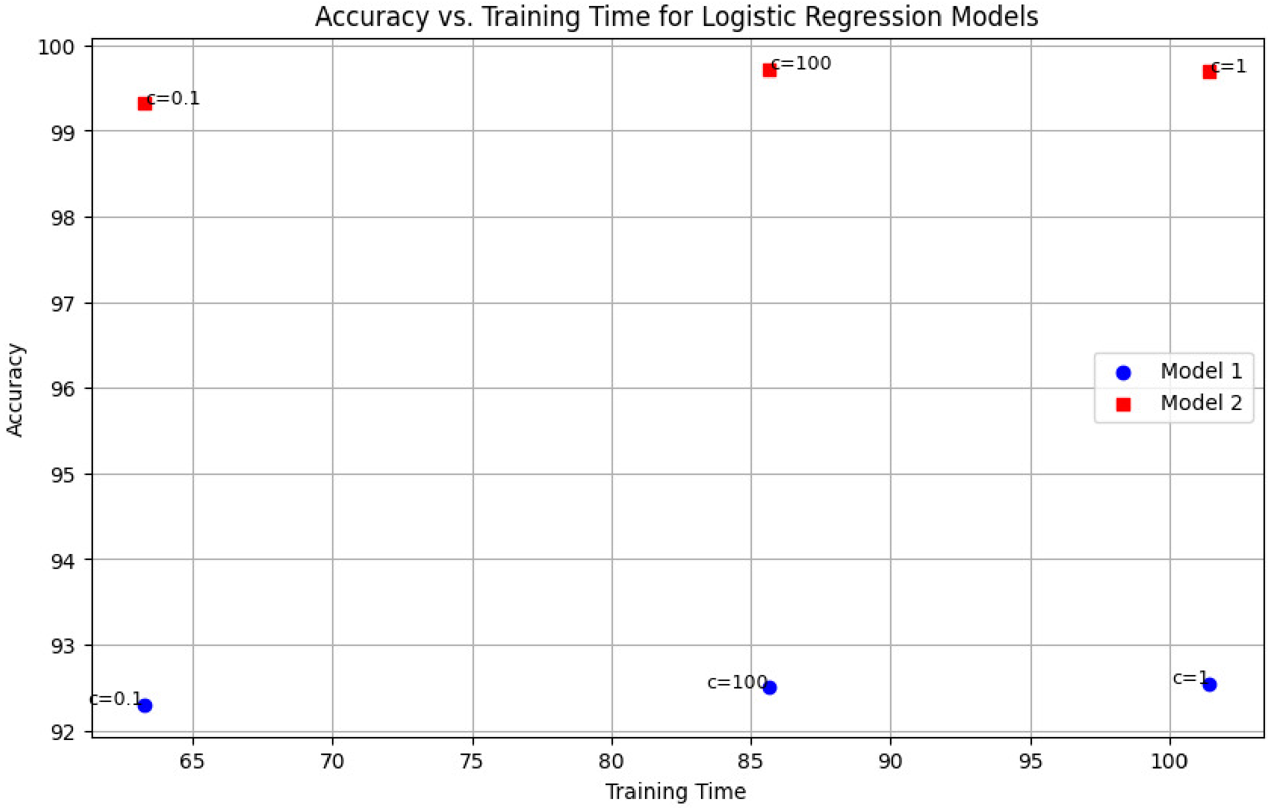
5 Code

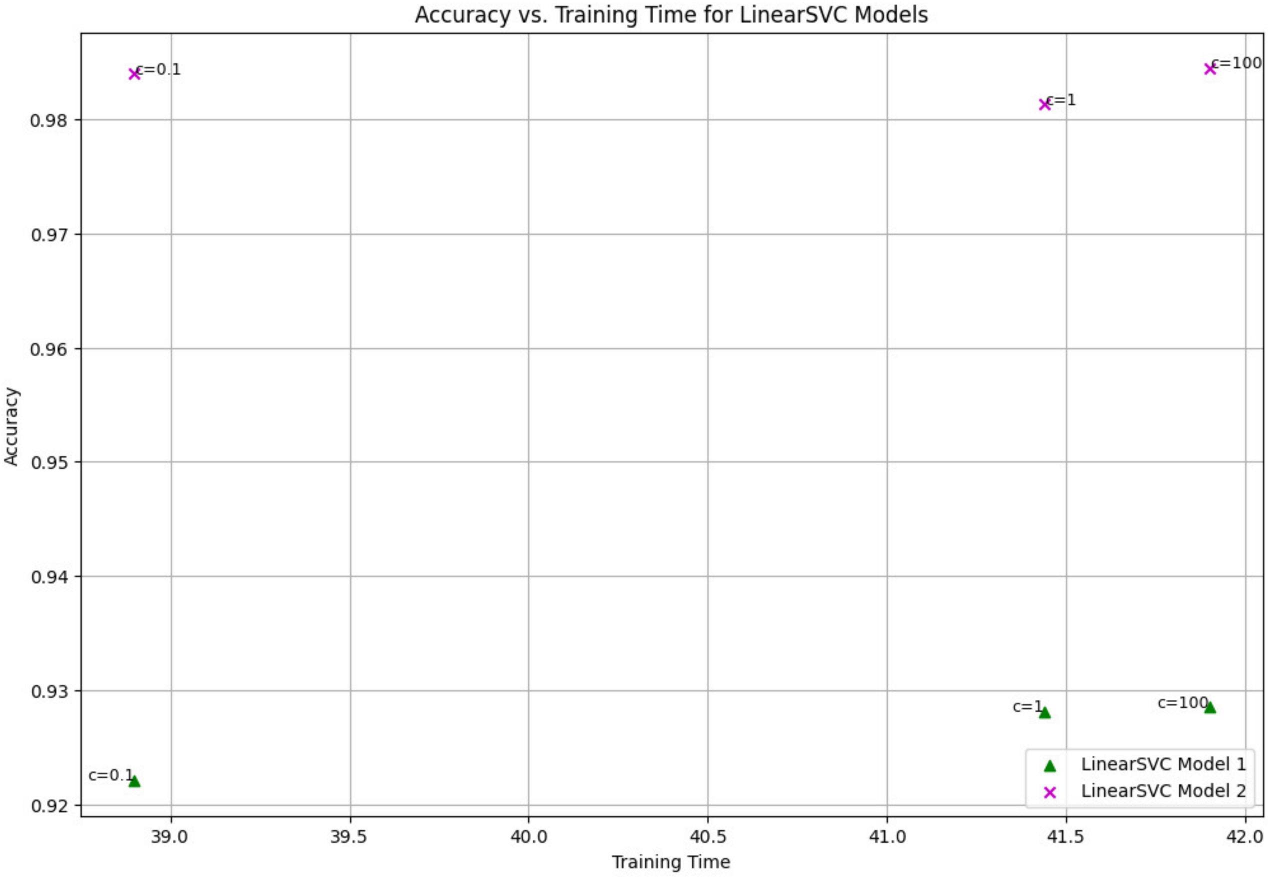
Uploaded separately.

6 Outcome

First image is for part A. Last two images for part B


Accuracy vs. Training Time for LinearSVC Models with Different Loss Types
● LinearSVC Model 1
■ LinearSVC Model 2
squared hinge loss
hinge loss
squared hinge loss
hinge loss
Accuracy
0.99
0.98
0.97
0.96
0.95
0.94
0.93
Training Time
17.75
18.00
18.25
18.50
18.75
19.00
19.25
19.50
19.75


Accuracy vs. Training Time for Logistic Regression Models
Accuracy
Training Time
100
99
98
97
96
95
94
93
92
65
70
75
80
85
90
95
100
c=0.1
c=100
c=1
c=0.1
c=100
c=1
● Model 1
■ Model 2


Accuracy vs. Training Time for LinearSVC Models
Accuracy
Training Time
0.98
0.97
0.96
0.95
0.94
0.93
0.92
39.0
39.5
40.0
40.5
41.0
41.5
42.0
c=0.1
c=1
c=100
c=0.1
c=1
c=100
▲ LinearSVC Model 1
× LinearSVC Model 2