Assignment 1

Aditya Gupta
Department of computer science
adityagu22@iitk.ac.in

Praveen Raj
Department of Mechanical Engineering
praveenr21@iitk.ac.in

1 Breaking CARPUFF into a linear model

Let $(\mathbf{u}, p)$ and $(\mathbf{v}, q)$ be the parameters for the linear model of the two Puffs. Where $u, v \in \mathbb{R}^{32}$

$$\mathbf{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{32} \end{bmatrix} \mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{32} \end{bmatrix}$$

$x_i = \prod_{j=i}^{32}(1 - 2c_j)$ for the challenges $c_1, c_2, \cdots, c_{32}$, then

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{32} \end{bmatrix}$$

then

$$\Delta_w = \mathbf{u}^T\mathbf{x} + p$$
$$\Delta_r = \mathbf{v}^T\mathbf{x} + q$$

For simplicity, let's just put bias terms inside vector. To do this we make

$$\tilde{\mathbf{u}} = \begin{bmatrix} u_1 \\ \vdots \\ u_{32} \\ p \end{bmatrix} \tilde{\mathbf{v}} = \begin{bmatrix} v_1 \\ \vdots \\ v_{32} \\ q \end{bmatrix} \text{ and } \tilde{\mathbf{x}} = \begin{bmatrix} x_1 \\ \vdots \\ x_{32} \\ x_{33} \end{bmatrix} \text{ where } x_{33} = 1$$

Where $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$ and $\tilde{\mathbf{x}} \in \mathbb{R}^{33}$
therefore,

$$\Delta_w = \tilde{\mathbf{u}}^T\tilde{\mathbf{x}}$$
$$\Delta_r = \tilde{\mathbf{v}}^T\tilde{\mathbf{x}}$$

Now for CAR-PUFF, we have

$$\text{Response} = \begin{cases} 0 & \text{if } |\Delta_w - \Delta_r| \leq \tau \\ 1 & \text{if } |\Delta_w - \Delta_r| > \tau \end{cases}$$

Or equivalently

$$\text{Response} = \begin{cases} 0 & \text{if } (\Delta_w - \Delta_r)^2 - \tau^2 \leq 0 \\ 1 & \text{if } (\Delta_w - \Delta_r)^2 - \tau^2 > 0 \end{cases}$$

Using sign Function we can write

$$\text{Response} = \frac{1 + \text{sign}\left((\Delta_w - \Delta_r)^2 - \tau^2\right)}{2}$$

For simplicity Let's define $\mathbf{z} \in \mathbb{R}^{33}$ as the difference between the two vectors $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{v}}$

$$\mathbf{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_{32} \\ z_{33} \end{bmatrix}$$

Where $\mathbf{z_i} = \mathbf{u_i} - \mathbf{v_i}$ for $i = 1, 2, \cdots, 32$ and $z_{33} = p - q$
Then we can write

$$\begin{aligned}
(\Delta_w - \Delta_r)^2 - \tau^2 &= \left(\mathbf{z}^T \tilde{\mathbf{x}}\right)^2 - \tau^2 \\
&= \left(\mathbf{z}^T \tilde{\mathbf{x}}\right)\left(\mathbf{z}^T \tilde{\mathbf{x}}\right) - \tau^2 \\
&= \left(\sum_{i=1}^{33} z_i \tilde{\mathbf{x}}_i\right)\left(\sum_{j=1}^{33} z_j \tilde{\mathbf{x}}_j\right) - \tau^2 \\
&= \sum_{i=1}^{33}\sum_{j=1}^{33} z_i z_j x_i x_j - \tau^2 \\
&= \sum_{i=1}^{33}\sum_{\substack{j=1 \\ j\neq i}}^{33} z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 x_i^2 - \tau^2
\end{aligned}$$

Note that the summation $\sum_{i=1}^{33}\sum_{\substack{j=1 \\ j\neq i}}^{33} z_i z_j x_i x_j$ is over all the pairs of indices i and j such that $i \neq j$.
So the term $z_i z_j x_i x_j$ is included **once for each pair of indices** i and j.
hence we can write

$$\sum_{i=1}^{33}\sum_{\substack{j=1 \\ j\neq i}}^{33} z_i z_j x_i x_j = \sum_{i=1}^{33}\sum_{\substack{j=1 \\ j>i}}^{33} 2 \times z_i z_j x_i x_j \tag{1}$$

Also $x_i = \pm 1$ for $i = 1, 2, \cdots, 32$ and $x_{33} = 1$
$\implies \mathbf{x_i^2} = \mathbf{1}$ for $i = 1, 2, \cdots, 33$
therefore

$$\sum_{i=1}^{33} z_i^2 x_i^2 = \sum_{i=1}^{33} z_i^2 \tag{2}$$

Therefore

$$\implies (\Delta_w - \Delta_r)^2 - \tau^2 = \sum_{i=1}^{33} \sum_{\substack{j=1 \\ j\neq i \\ j\neq i}}^{33} z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 x_i^2 - \tau^2$$

$$= \sum_{i=1}^{33} \sum_{\substack{j=1 \\ j>i}}^{33} 2 z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 - \tau^2 \qquad \text{(using 1 and 2)}$$

$\because$ Summation $\sum_{i=1}^{33} \sum_{j=1}^{33} z_i z_j x_i x_j$ has a total of 33×33 terms.
$\therefore \sum_{i=1}^{33} \sum_{\substack{j=1 \\ j\neq i}}^{33} z_i z_j x_i x_j$ has a total of $33 \times 33 - 33$ terms.
$\therefore \sum_{i=1}^{33} \sum_{\substack{j=1 \\ j\neq i \\ j>i}}^{33} 2 z_i z_j x_i x_j$ has a total of $\frac{33\times 33-33}{2} = \mathbf{528}$ terms.

$$\because (\Delta_w - \Delta_r)^2 - \tau^2 = \left(\sum_{i=1}^{33} \sum_{\substack{j=1 \\ j>i}}^{33} 2 z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 - \tau^2 \right)$$

$$\therefore \text{Response} = \frac{1 + \text{sign}\left(\sum_{i=1}^{33} \sum_{\substack{j=1 \\ j>i}}^{33} 2 z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 - \tau^2 \right)}{2}$$

Also the sum $\left(\sum_{i=1}^{33} \sum_{\substack{j=1 \\ j>i}}^{33} 2 z_i z_j x_i x_j + \sum_{i=1}^{33} z_i^2 - \tau^2 \right)$ can be written as $\mathbf{W}^T \phi(\mathbf{c}) + \mathbf{b}$ with

$$\mathbf{W} = \begin{bmatrix} 2z_1z_2 \\ 2z_1z_3 \\ \vdots \\ 2z_1z_{33} \\ 2z_2z_3 \\ \vdots \\ 2z_2z_{33} \\ 2z_3z_4 \\ \vdots \\ 2z_3z_{33} \\ \vdots \\ 2z_{32}z_{33} \end{bmatrix}_{528\times 1} \qquad \phi(\mathbf{c}) = \begin{bmatrix} x_1x_2 \\ x_1x_3 \\ \vdots \\ x_1x_{33} \\ x_2x_3 \\ \vdots \\ x_2x_{33} \\ x_3x_4 \\ \vdots \\ x_3x_{33} \\ \vdots \\ x_{32}x_{33} \end{bmatrix}_{528\times 1}$$

$\mathbf{b} = z_1^2 + z_2^2 + \cdots + z_{33}^2 - \tau^2$.
where $\mathbf{x_i} = 1 - 2\mathbf{c_i}$ for $i = 1, 2, \cdots, 32$ and $\mathbf{x_{33}} = \mathbf{1}$

$$\text{Response} = \frac{1 + \text{sign}\left(\mathbf{W}^T \phi(\mathbf{c}) + b\right)}{2}$$

with

$$\mathbf{W} = \begin{bmatrix} 2z_1z_2 \\ 2z_1z_3 \\ \vdots \\ 2z_1z_{33} \\ 2z_2z_3 \\ \vdots \\ 2z_2z_{33} \\ 2z_3z_4 \\ \vdots \\ 2z_3z_{33} \\ \vdots \\ 2z_{32}z_{33} \end{bmatrix}_{528\times 1} \qquad \phi(\mathbf{c}) = \begin{bmatrix} x_1x_2 \\ x_1x_3 \\ \vdots \\ x_1x_{33} \\ x_2x_3 \\ \vdots \\ x_2x_{33} \\ x_3x_4 \\ \vdots \\ x_3x_{33} \\ \vdots \\ x_{32}x_{33} \end{bmatrix}_{528\times 1}$$

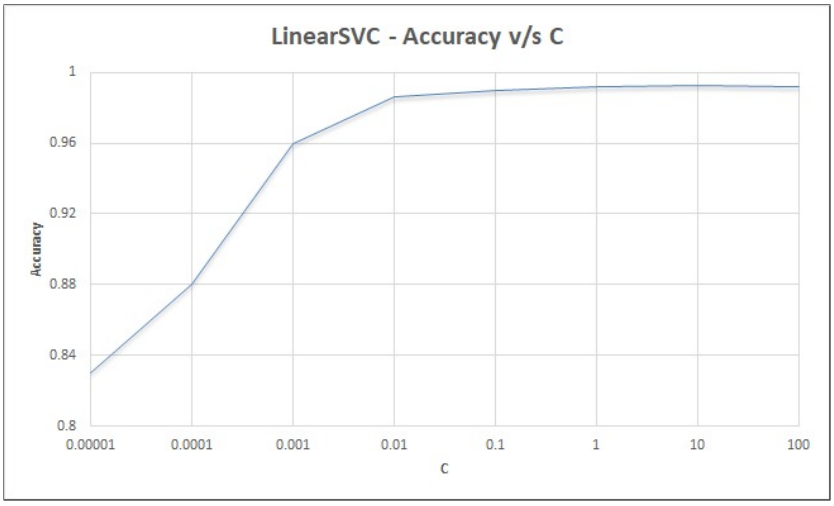
$$\mathbf{b} = z_1^2 + z_2^2 + \cdots + z_{33}^2 - \tau^2.$$

Where $\mathbf{x_i} = \prod_{\mathbf{j=i}}^{\mathbf{32}} (\mathbf{1} - \mathbf{2c_j})$ for the challenges $c_1, c_2, \cdots, c_{32}$ and $\mathbf{x_{33}} = \mathbf{1}$
and $\mathbf{z_i} = \mathbf{u_i} - \mathbf{v_i}$ for $i = 1, 2, \cdots, 32$ and $\mathbf{z_{33}} = \mathbf{p} - \mathbf{q}$
where $(\mathbf{u}, p)$ and $(\mathbf{v}, q)$ are the two linear models for the two arbiter PUFs sitting inside the CAR-PUF.

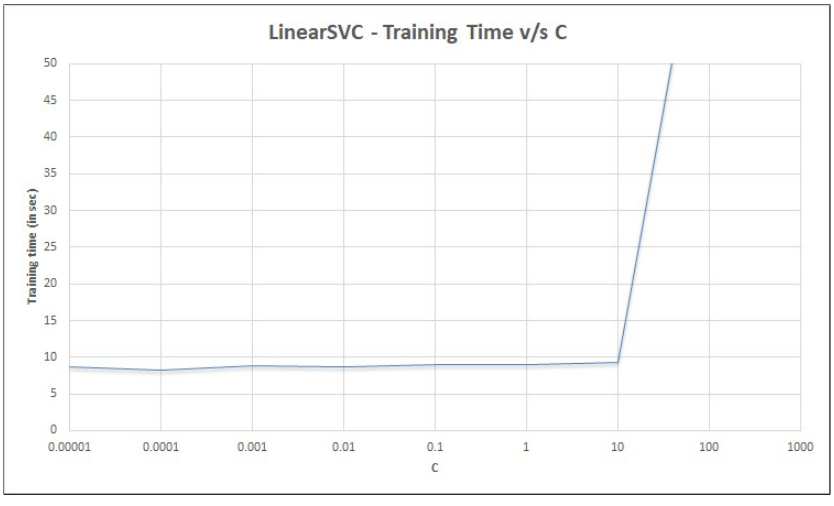
2 Outcomes with diffrent models with hyperparameters

2.1 Tuning C in LinearSVC and Logistic Regression

2.1.1 LinearSVC

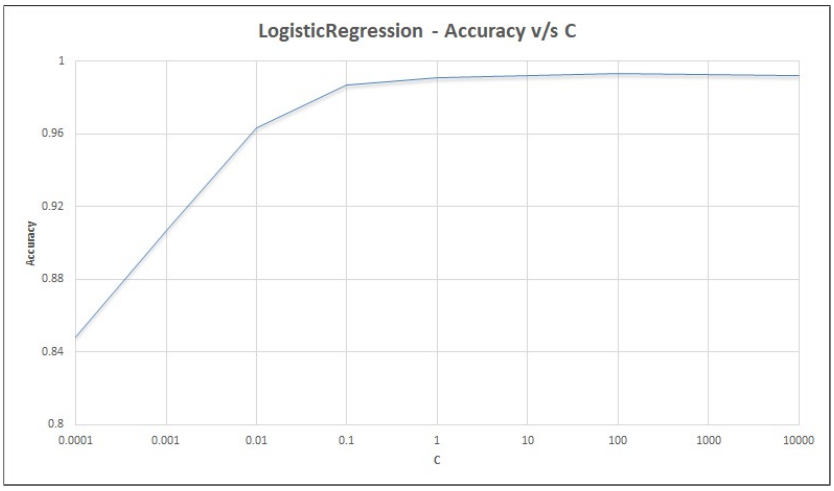


Variation of Accuracy with C in LinearSVC

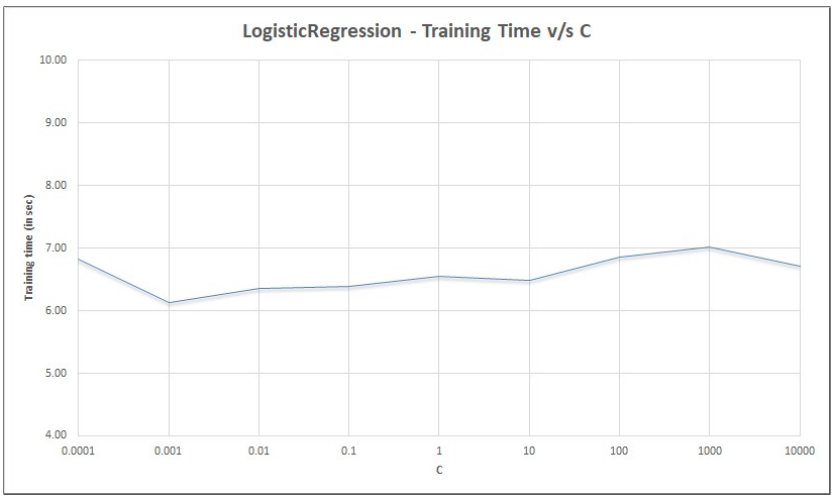


Variation of Training time with C in LinearSVC

2.1.2 Logistic Regression



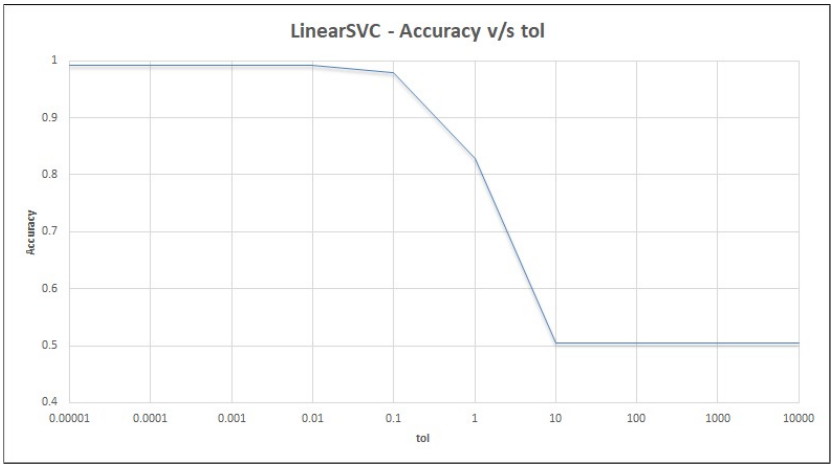
Variation of Accuracy with C in Logistic Regression



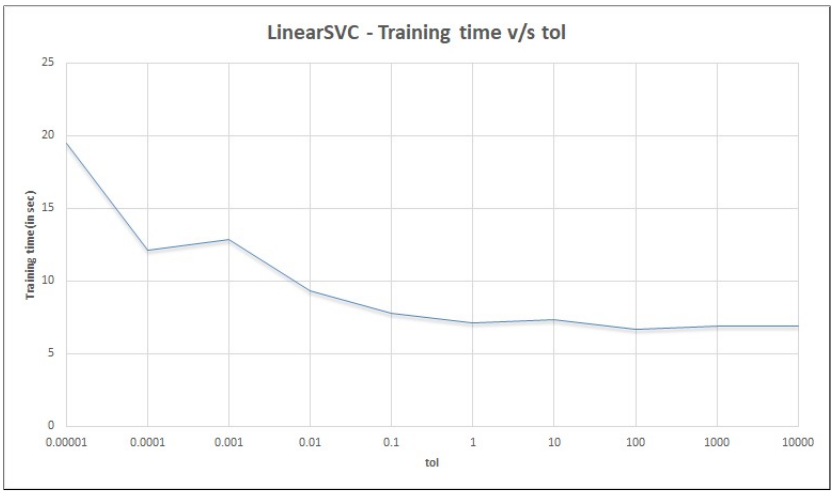
Variation of Training time with C in Logistic Regression

2.2 Tuning tol in LinearSVC and Logistic Regression

2.2.1 LinearSVC

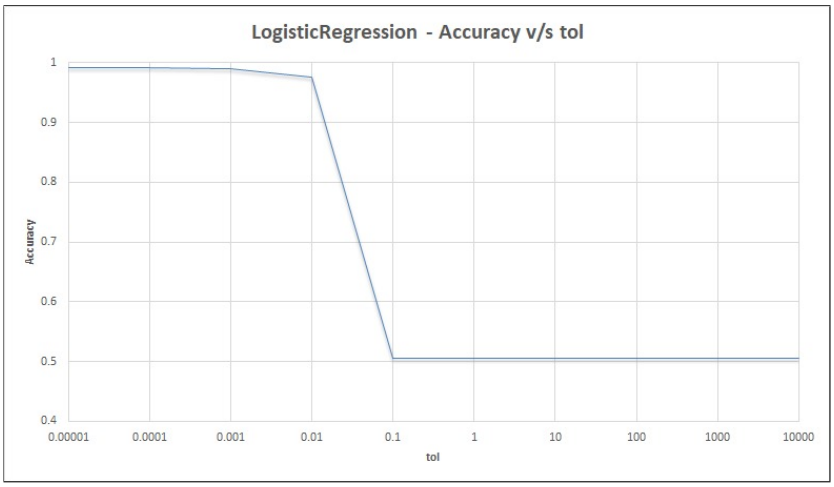


Variation of Accuracy with tol in LinearSVC

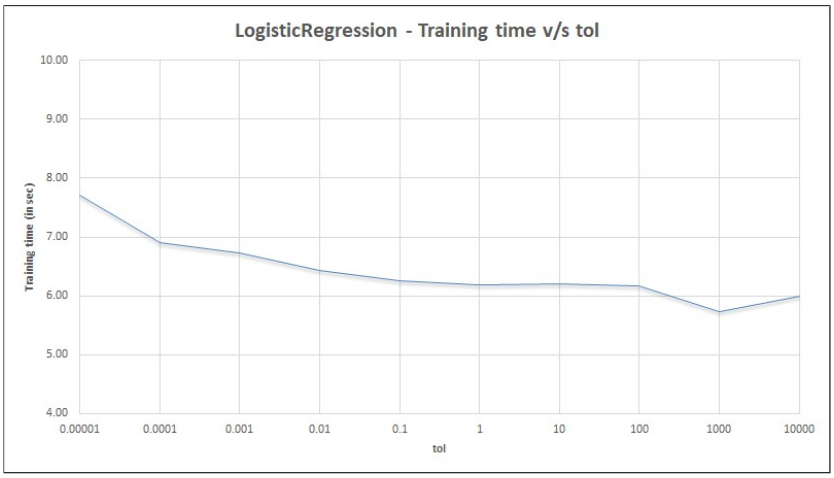


Variation of Training time with tol in LinearSVC

2.2.2 Logistic Regression



Variation of Accuracy with tol in Logistic Regression



Variation of Training time with tol in Logistic Regression