COL341 Spring 2023
Homework 2
(To be done Individually)

Due Date: 19th March 2023, Friday, 11:55 PM (No extensions)

Instructions

Type the solutions in LaTeX(you may use Overleaf for ease of use). Submit the `.tex` source and the compiled `pdf` in a single `.zip` file in Moodle. Name the file as `<your-entry-number>.zip`, e.g. `2019CSZ8406.zip`. The homework is to be done individually. Plagiarism and academic dishonesty will be penalized as per the course policy. No deadline extension will be provided.

Question 1 [$1 \times 10 = 10$ marks]

The SVM hard margin formulation assumes that the data is linearly separable and tries to draw the decision boundary with maximum margin so that the generalization error is less. In class, we have seen the primal and corresponding dual problem in this scenario.

The primal problem corresponding to the separable case:

$$\min_{\boldsymbol{w},b} \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} \qquad \text{s.t} \qquad y_n(\boldsymbol{w}^T\boldsymbol{x}_n + b) \geq 1 \qquad\qquad (n = 1, \dots N)$$

The corresponding dual problem is

$$\min_{\alpha \in \mathcal{R}^N} \frac{1}{2}\sum_{m=1}^{N}\sum_{n=1}^{N} y_n y_m \alpha_n \alpha_m \boldsymbol{x}_n^T \boldsymbol{x}_m - \sum_{n=1}^{N}\alpha_n$$

$$\text{s.t} \qquad \sum_{n=1}^{N} y_n \alpha_n = 0 \qquad \text{and} \quad \alpha_n \geq 0 \qquad (n = 1, \dots N)$$

However, in practice, the training data is not linearly separable, and we need to introduce slack variables to handle the noise. Again, as discussed in the class, the primal problem corresponding to the soft SVM is:

$$\min_{\boldsymbol{w},b} \ \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} + C\sum_{n=1}^{N}\zeta_n$$

$$\text{s.t} \qquad y_n(\boldsymbol{w}^T\boldsymbol{x}_n + b) \geq 1 - \zeta_n \quad \text{and} \quad \zeta_n \geq 0 \qquad (n = 1, \ldots N)$$

The task in this homework is to derive the dual of the soft SVM, which is:

$$\min_{\alpha\in\mathcal{R}^N} \ \frac{1}{2}\sum_{m=1}^{N}\sum_{n=1}^{N} y_n y_m \alpha_n \alpha_m \boldsymbol{x}_n^T\boldsymbol{x}_m - \sum_{n=1}^{N}\alpha_n$$

$$\text{s.t} \qquad \sum_{n=1}^{N} y_n\alpha_n = 0 \qquad \text{and} \quad C \geq \alpha_n \geq 0 \qquad (n = 1, \ldots N)$$

[Hint: Find the Lagrangian of the primal problem. Use the KKT conditions to get certain relationships among the variables and substitute these into the Lagrangian to get the dual.]

Question 2 [1+2+3+2+1=10 marks]

In this question, we will find an upper bound of the VC-dimension of SVM. Suppose the input space is the ball of radius R in $\mathcal{R}^d$, so $||x|| \leq R$. Then,

$$d_{VC}(\rho) \leq \left\lceil R^2/\rho^2 \right\rceil + 1 \tag{1}$$

where $\left\lceil R^2/\rho^2 \right\rceil$ is the smallest integer greater than or equal to R^2/ρ^2.

To start the proof, fix $x_1, \ldots, x_n$ that are shattered by hyperplanes with margin ρ. We will show when N is even, $N \leq R^2/\rho^2 + 1$. When N is odd, a similar analysis can show that $N \leq R^2/\rho^2 + 1 + \frac{1}{N}$. In both cases, $N \leq \left\lceil R^2/\rho^2 \right\rceil + 1$.

Use the following **proof of sketch** to show that there exist a balanced dichotomy $y_1, \ldots, y_n$ s.t.

$$\sum_{n=1}^{N} y_n = 0, \text{and} \left\| \sum_{n=1}^{N} y_n\boldsymbol{x}_n \right\| \leq \frac{NR}{\sqrt{N-1}}$$

As these N points are being shattered, they can be separated by the SVM with margin at least ρ. So, for some W and b, we have

$$\rho\|\boldsymbol{w}\| \leq y_n(\boldsymbol{w}^T\boldsymbol{x}_n + b)\forall n$$

Then, use Cauchy- Schwartz inequality to prove the given upper bound for VC dimension.

Proof sketch (N is even)

Suppose you randomly select $N/2$ of the labels $y_1, \dots, y_n$ to be +1, the others being -1. By construction, $\sum_{n=1}^{N} y_n = 0$.

1. Show $\left\|\sum_{n=1}^{N} y_n \boldsymbol{x}_n\right\|^2 = \sum_{n=1}^{N} \sum_{m=1}^{N} y_n y_m \boldsymbol{x}_n^T \boldsymbol{x}_m$

2. When $n = m$, what is $y_n y_m$? Show that $\mathbb{P}[y_n y_m = 1] = (\frac{N}{2} - 1)/(N-1)$ when $n \neq m$. Hence show that

$$\mathbb{E}[y_n y_m] = \begin{cases} 1 & m = n; \\ -\frac{1}{N-1} & m \neq n. \end{cases}$$

3. Show that

$$\mathbb{E}\left[\left\|\sum_{n=1}^{N} y_n \boldsymbol{x_n}\right\|^2\right] = \frac{N}{N-1} \sum_{n=1}^{N} \|\boldsymbol{x}_n - \bar{\boldsymbol{x}}\|^2,$$

   where the average vector $\bar{\boldsymbol{x}} = \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{x}_n$. [Hint: Use linearity of expectation in (1), and consider the case $m = n$ and $m \neq n$ separately.]

4. Show that $\|\boldsymbol{x}_n - \bar{\boldsymbol{x}}\|^2 \leq \sum_{n=1}^{N} \|\boldsymbol{x}_n\|^2 \leq NR^2$

$$\text{[Hint: } \sum_{n=1}^{N} \|\boldsymbol{x}_n - \boldsymbol{\mu}\|^2 \text{ is minimized at } \boldsymbol{\mu} = \frac{1}{N} \sum_{n=1}^{N} \boldsymbol{x}_n]$$

5. Conclude that

$$\mathbb{E}\left[\left\|\sum_{n=1}^{N} y_n \boldsymbol{x}_n\right\|^2\right] \leq \frac{N^2 R^2}{N-1},$$

   and hence that

$$\mathbb{P}\left[\left\|\sum_{n=1}^{N} y_n \boldsymbol{x}_n\right\| \leq \frac{NR}{\sqrt{N-1}}\right] > 0$$

   This means for some choice of y_n, $\left\|\sum_{n=1}^{N} y_n \boldsymbol{x}_n\right\| \leq NR/\sqrt{N-1}$

   This proof is called a *probabilistic existence proof: if some random process can generate an object with positive probability, then that object must exist. Note that you prove the existence of the required dichotomy without actually constructing it. In this case, the easiest way to construct a desired dichotomy is to randomly generate the balanced dichotomies until you have one that works*