CS973: Machine Learning for Cyber Security

Quiz I (06 Oct 2024)

Q3. Will ML Work? (2 marks)

Consider the following tasks and tick all options where the task is an appropriate candidate to be solved using machine learning (more than one option may be correct). Do not tick an option if that task can be easily solved without ML, say by writing a simple piece of C/Java/Python code. (2 marks)

[ ] Deciding if the electricity consumption of my household for the last month was more than 500 units or not?

[✓] Predicting if the electricity consumption of my household for the next month will be more than 500 units or not?

[✓] Given audio file of a song, deciding if the song was sung by Shreya Ghoshal or Palak Muchhal using the audio file alone.

[ ] Given the image file of a QR code, finding out what URL is encoded in the QR code using the image file alone.

Q4. Perpendicular inside a parabola (9 marks)

Consider vectors on the 2D Euclidean plane of the form $\mathbf{v} = (v_1, v_2)$ that lie on the standard parabola $y = x^2$ i.e. $v_2 = v_1^2$ for all such vectors $\mathbf{v}$.

Part 1 (1+2 marks). Find a non-zero 2D vector $\mathbf{p}$ that lies on the parabola and is also perpendicular to the 2D vector $\mathbf{q} = \left(\frac{1}{2}, \frac{1}{4}\right)$. First write down the value of $\mathbf{p}$ then give a brief derivation.

Let $\mathbf{p} = (t, t^2)$ so that it lies on the parabola. To have perpendicularity, we need $\frac{t}{2} + \frac{t^2}{4} = 0$. As we cannot have $t = 0$ as $\mathbf{p} \neq \mathbf{0}$, the other solution is $t = -2$ which gives us $\mathbf{p} = (-2,4)$.

Part 2 (1+2 marks). Given a general non-zero 2D vector $\mathbf{q} = (s, t)$ that lies on the parabola (i.e. $t = s^2$ and $\mathbf{q} \neq \mathbf{0}$), find a non-zero 2D vector $\mathbf{p} = (m, n)$ so that

$\mathbf{p}$ lies on the parabola and is perpendicular to $\mathbf{q}$. First write down the value of m, n then give a brief derivation. Your answer for m, n must be in terms of s, t.

Let $\mathbf{p} = (m, m^2)$. To have perpendicularity, we need $ms + m^2 s^2 = 0$ which gives us two solutions $ms = 0$ and $ms = -1$. Since we have non-zero vectors, we cannot have $ms = 0$ which means we must have $m = -\frac{1}{s}$ i.e., $\mathbf{p} = \left(-\frac{1}{s}, \frac{1}{s^2}\right)$.

Part 3 (1+2 marks). Find two 2D vectors $\mathbf{c}, \mathbf{d}$ that satisfy 4 properties given below

- Both vectors are non-zero
- Both vectors lie on the parabola
- Both vectors are also perpendicular to each other
- Both vectors also have the same Euclidean length.

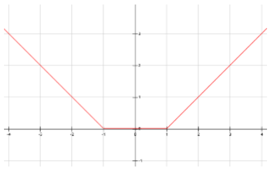
Write down the value of $\mathbf{c}, \mathbf{d}$ and give brief derivation. Note that your answer for $\mathbf{c}, \mathbf{d}$ must be actual numbers. For example, you could say $\mathbf{c} = (2,4)$ or $\mathbf{d} = (1,1)$.

From part 2, we know the vectors must be of the form $\mathbf{c} = (u, u^2), \mathbf{d} = \left(-\frac{1}{u}, \frac{1}{u^2}\right)$ to satisfy the parabola and perpendicularity conditions. However, $\|\mathbf{c}\|_2^2 = u^2 + u^4$ while $\|\mathbf{d}\|_2^2 = \frac{1}{u^2} + \frac{1}{u^4} = \frac{u^2+u^4}{u^6}$. Thus, to have $\|\mathbf{c}\|_2 = \|\mathbf{d}\|_2$ we need $u^6 = 1$ i.e. $u = 1$. Thus, $\mathbf{c} = (1,1), \mathbf{d} = (-1,1)$.

Q5. Deriving the PLP **(5 marks)**

Consider the following function $f: \mathbb{R} \to \mathbb{R}$ that looks like a piecewise linear approximation to the standard parabola (function plot given below as an image):

$$f = \begin{cases} -1 - x & x \leq -1 \\ 0 & x \in (-1,1) \\ -1 + x & x \geq 1 \end{cases}$$



Give below a derivation of the subgradient of f at all points on the real number line. Recall that the subgradient makes sense even for non-differentiable functions so long as they are convex. In particular, explicitly state the subdifferential (with brief calculations) at

- (1 mark) Points of the form $x < -1$
- (1 mark) The point $x = -1$
- (1 mark) Points of the form $x \in (-1,1)$
- (1 mark) The point $x = 1$
- (1 mark) Points of the form $x > 1$

We calculate the various subdifferentials below:

- When $x < -1$, the function is of the form $-1 - x$ hence differentiable. Thus, the subdifferential is $\partial f(x) = \{-1\}$ for all $x < -1$.
- In the vicinity of $x = -1$, the function looks like the hinge function i.e. of the from $\max\{-1 - x, 0\}$. Using the max rule tells us that $\partial f(x) = [-1,0]$ i.e., the set of all numbers between -1 and 0.
- When $x \in (-1,1)$, the function is constant hence differentiable. Thus, the subdifferential is $\partial f(x) = \{0\}$ for all $x \in (-1,1)$.
- In the vicinity of $x = 1$, the function looks like the ReLU function i.e. of the from $\max\{-1 + x, 0\}$. Using the max rule tells us that $\partial f(x) = [0,1]$ i.e., the set of all numbers between 0 and 1.
- When $x > 1$, the function is of the form $-1 + x$ hence differentiable. Thus, the subdifferential is $\partial f(x) = \{+1\}$ for all $x > 1$.

Q6. Decomposable Classifiers **(4 marks)**

Melbo has learnt the following quadratic classifier to solve a difficult binary classification problem: $\text{sign}(12x^2 + x - 35)$. This classifier takes a real number $x \in \mathbb{R}$ and gives a binary verdict by looking at the sign of the value $12x^2 + x - 35$.

Part 1 (1 mark) What point(s) lie on the decision boundary of this classifier? Just give the final answer below -- no derivation needed

$$x = \frac{5}{3}, x = -\frac{7}{4}$$

Part 2 (1+2 marks) Melbo suspects that the verdict of this quadratic classifier can be expressed as the product of the verdicts of two linear classifiers i.e. there exist real numbers $a, b, p, q \in \mathbb{R}$ such that for every $x \in \mathbb{R}$, we have

$$\text{sign}(12x^2 + x - 35) = \text{sign}(ax + b) \cdot \text{sign}(px + q)$$

Help confirm Melbo's suspicion. First give values of a, b, p, q below then give brief derivation. *Hint: use the fact that* $\text{sign}(ab) = \text{sign}(a) \cdot \text{sign}(b)$

We have $12x^2 + x - 35 = (4x + 7)(3x - 5)$ which gives us $a = 4, b = 7, p = 3, q = -5$. Such a decomposition of a classifier is possible when the polynomial corresponding to the classifier decomposes.