Problem 1.

(a) The prediction score for label i is always the top-1 score for all $x \in S$:

$$\exists x, x \in S \wedge (y = f(x)) \wedge \exists k \neq i, (y_k \geq y_i) \tag{1}$$

If the SMT solver reports "unsatisfiable", it means there is no x in S where any other label has a score equal to or greater than y_i, satisfying the requirement. Otherwise, a counterexample x_s exists where $y_k \geq y_i$ for some k $\neq$ i.

(b) The prediction score for label j can never be the top-1 score for all $x \in S$:

$$\exists x, x \in S \wedge (y = f(x)) \wedge (\forall k \neq j, y_j \geq y_k) \tag{2}$$

If the SMT solver finds a satisfying x_s, it means there exists an x where y_j is the highest score, contradicting the requirement. If the solver returns "unsatisfiable", then there is no y_j that would be top-1 score for any x in S, verifying the requirement.

Problem 2.

(1)

$$z_1^{(1)} = 1 \cdot x_1 - 1 \cdot x_2 + 1$$

$$\min: 1(-1) - 1(1) + 1 = -1, \quad \max: 1(1) - 1(-1) + 1 = 3$$

Thus, $z_1^{(1)} \in [-1, 3]$.

$$z_2^{(1)} = 2x_1 - 2x_2 + 1$$

$$\min: 2(-1) - 2(1) + 1 = -5, \quad \max: 2(1) - 2(-1) + 1 = 5$$

Thus, $z_2^{(1)} \in [-5, 5]$.
Since ReLU is defined as $\max(0, z)$:

$$\hat{z}_1^{(1)} \in [0, 3], \quad \hat{z}_2^{(1)} \in [0, 5].$$

$$z^{(2)} = W^{(2)} \hat{z}^{(1)} + b^{(2)}$$

$$z_1^{(2)} = 1 \cdot \hat{z}_1^{(1)} - 1 \cdot \hat{z}_2^{(1)} + 2$$

$$\min: 1(0) - 1(5) + 2 = -3, \quad \max: 1(3) - 1(0) + 2 = 5$$

Thus, $z_1^{(2)} \in [-3, 5]$.

$$z_2^{(2)} = 2\hat{z}_1^{(1)} - 2\hat{z}_2^{(1)} + 2$$

$$\min: 2(0) - 2(5) + 2 = -8, \quad \max: 2(3) - 2(0) + 2 = 8$$

Thus, $z_2^{(2)} \in [-8, 8]$.

$$\hat{z}_1^{(2)} \in [0, 5], \quad \hat{z}_2^{(2)} \in [0, 8].$$

$$y = W^{(3)}(\hat{z}^{(2)} + \hat{z}^{(1)})$$

$$\hat{z}_1^{(2)} + \hat{z}_1^{(1)} \in [0 + 0, 5 + 3] = [0, 8]$$

$$\hat{z}_2^{(2)} + \hat{z}_2^{(1)} \in [0 + 0, 8 + 5] = [0, 13]$$

Applying $W^{(3)}$:

$$y = -1 \cdot (\hat{z}_1^{(2)} + \hat{z}_1^{(1)}) + 1 \cdot (\hat{z}_2^{(2)} + \hat{z}_2^{(1)})$$

$$y_{\min} = -1(8) + 0 = -8$$

$$y_{\max} = -1(0) + 13 = 13$$

The lower bound of y using Interval Bound Propagation (IBP) is:

$$\mathbf{-8}$$

(2)
From IBP:

$$\hat{z}_1^{(1)} \in [0, 3], \quad \hat{z}_2^{(1)} \in [0, 5].$$

Using CROWN propagation:

$$z_1^{(2)} = 1 \cdot \hat{z}_1^{(1)} - 1 \cdot \hat{z}_2^{(1)} + 2$$

$$\min: 1(0) - 1(5) + 2 = -3$$

$$\max: 1(3) - 1(0) + 2 = 5$$

Thus,

$$z_1^{(2)} \in [-3, 5].$$

$$z_2^{(2)} = 2\hat{z}_1^{(1)} - 2\hat{z}_2^{(1)} + 2$$

$$\min : 2(0) - 2(5) + 2 = -8$$

$$\max : 2(3) - 2(0) + 2 = 8$$

Thus,

$$z_2^{(2)} \in [-8, 8].$$

The computed CROWN pre-activation bounds for $z^{(2)}$ are:

$$z_1^{(2)} \in [-3, 5], \quad z_2^{(2)} \in [-8, 8].$$

(3) From part 2, the pre-activation bounds for $z^{(2)}$ are:

$$z_1^{(2)} \in [-3, 5], \quad z_2^{(2)} \in [-8, 8].$$

Applying the ReLU function:

$$\hat{z}_1^{(2)} = \max(0, z_1^{(2)}) \Rightarrow \hat{z}_1^{(2)} \in [0, 5].$$

$$\hat{z}_2^{(2)} = \max(0, z_2^{(2)}) \Rightarrow \hat{z}_2^{(2)} \in [0, 8].$$

From part 1, the bounds for $\hat{z}^{(1)}$ were:

$$\hat{z}_1^{(1)} \in [0, 3], \quad \hat{z}_2^{(1)} \in [0, 5].$$

Summing these intervals:

$$\hat{z}_1^{(2)} + \hat{z}_1^{(1)} \in [0 + 0, 5 + 3] = [0, 8].$$

$$\hat{z}_2^{(2)} + \hat{z}_2^{(1)} \in [0 + 0, 8 + 5] = [0, 13].$$

$$y = -1 \cdot (\hat{z}_1^{(2)} + \hat{z}_1^{(1)}) + 1 \cdot (\hat{z}_2^{(2)} + \hat{z}_2^{(1)}).$$

Using the computed bounds:

$$y_{\min} = -1(8) + 0 = -8.$$

$$y_{\max} = -1(0) + 13 = 13.$$

The CROWN lower bound on y is:

$$\mathbf{-8}.$$

(4) To achieve the tightest possible lower bound on y using CROWN, we need to optimize the slope parameters α associated with the ReLU relaxations in the network. Since every ReLU neuron in the network is considered unstable, we have one α parameter for each neuron in every layer where ReLU is applied. The neural network consists of two hidden layers where ReLU is applied: the first hidden layer transforms $z^{(1)}$ into $\hat{z}^{(1)}$ via ReLU, and the second hidden layer transforms $z^{(2)}$ into $\hat{z}^{(2)}$ via ReLU. Each of these layers has two neurons, meaning that four total neurons undergo ReLU activation: $z_1^{(1)}$, $z_2^{(1)}$, $z_1^{(2)}$, and $z_2^{(2)}$. Since each unstable ReLU neuron introduces an independent α parameter, there are four independent α values to optimize. However, to obtain the tightest possible lower and upper bounds on y, we need two separate sets of α values: one optimized for the lower bound and another for the upper bound. Since each bound is independently optimized, the total number of α values used in this process is $4 \times 2 = 8$. Thus, we can optimize a total of **8** different α values to achieve the most precise bounds on the output y.

Problem 3.

(3) Perturbation of 0.1 hit timeout condition, below is the graph for 0 to 0.03.

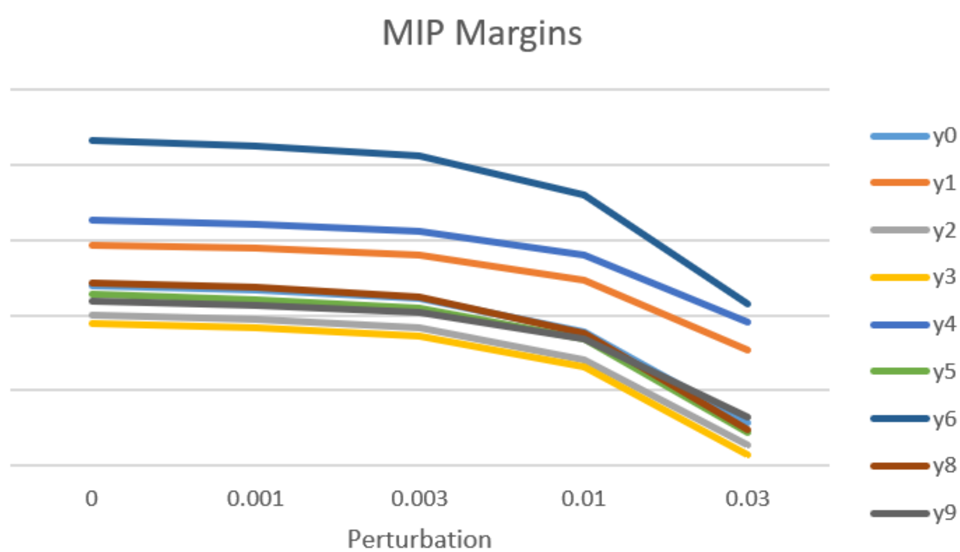

Figure 1: MIP Margins

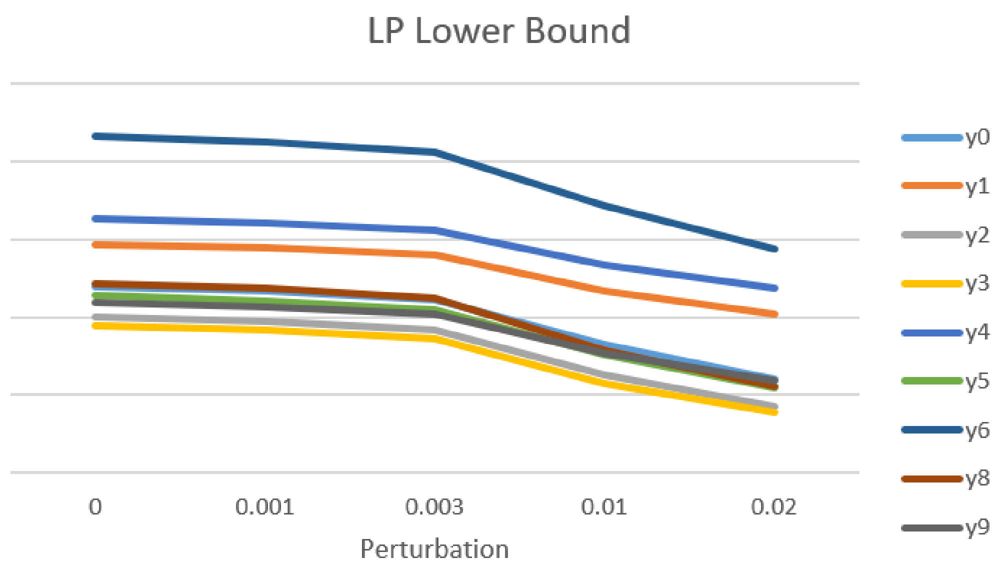

Figure 2: LP Lower Bound

Problem 4.

(2)
Case 1: $u \leq -1$

$$f_L(z) = -1, \tag{3}$$
$$f_U(z) = -1. \tag{4}$$

Case 2: $l \geq 1$

$$f_L(z) = 1, \tag{5}$$
$$f_U(z) = 1. \tag{6}$$

Case 3: $-1 \leq l \leq u \leq 1$

$$f_L(z) = z, \tag{7}$$
$$f_U(z) = z. \tag{8}$$

Case 4: $l < -1 < u \leq 1$

$$f_L(z) = -1, \tag{9}$$
$$f_U(z) = z. \tag{10}$$

Case 5: $-1 \leq l < 1 < u$

$$f_L(z) = z, \tag{11}$$
$$f_U(z) = 1. \tag{12}$$

Case 6: $l < -1 < u > 1$

$$f_L(z) = z, \tag{13}$$

$$f_U(z) = \frac{u-l}{2}z + \frac{u+l}{2}. \tag{14}$$

thus

Case	Lower Bound $f_L(z)$	Upper Bound $f_U(z)$
$u \leq -1$	-1	-1
$l \geq 1$	1	1
$-1 \leq l \leq u \leq 1$	z	z
$l < -1 < u \leq 1$	-1	z
$-1 \leq l < 1 < u$	z	1
$l < -1 < u > 1$	z	$\frac{u-l}{2}z + \frac{u+l}{2}$

Table 1: Linear lower and upper bounds for HardTanh