WASP-AI Summer School 2020

Certification of neural networks

Gagandeep Singh
ETH Zurich and UIUC

Problem 1 (Box transformer for Maxpool)**.** The Maxpool operation is typically used in neural networks to reduce dimensionality. Given input neurons x_1, x_2, the output y of the Maxpool operation can be computed as $y := max(x_1, x_2)$.

1. Suppose the intervals for the inputs x_1, x_2 are given by $[a_1, b_1]$ and $[a_2, b_2]$ where $a_1, b_1, a_2, b_2 \in \mathbb{R}$, compute the most precise and sound interval for the output y of the Maxpool operation $y := max(x_1, x_2)$.

2. Now, consider the neural network shown in Fig. 1. The neural network has two input (x_1, x_2) and two output (x_9, x_{10}) neurons and consist of two layers with affine transformations (edges colored blue) and one layer with maxpool operation (edges

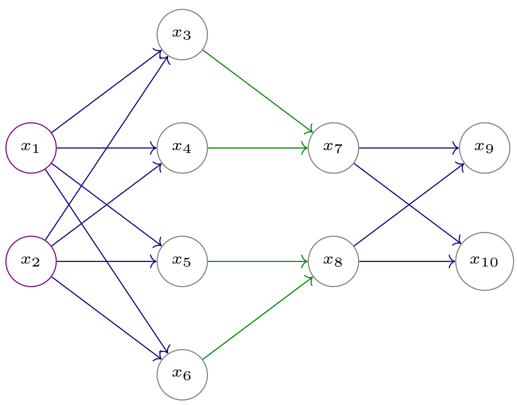

Figure 1: Fully-connected network with Affine and Maxpool operations.

colored green). The transformations in the network are given as:

$$
\begin{aligned}
x_3 &:= x_1 + x_2 \\
x_4 &:= x_1 - 2 \\
x_5 &:= x_1 - x_2 \\
x_6 &:= x_2 \\
x_7 &:= max(x_3, x_4) \\
x_8 &:= max(x_5, x_6) \\
x_9 &:= x_7 \\
x_{10} &:= -x_7 + x_8 - 0.5
\end{aligned}
$$

Use the Box Maxpool approximation designed above for verifying the property that for all values of $x_1, x_2 \in [0, 1]$, the output at $x_9 > x_{10}$. Can the box analysis prove this property?

Solution 1.

1. The interval for the output y is given by $[max(a_1, a_2), max(b_1, b_2)]$
2. The intervals for diffrent neurons in the network is given as:

$$
\begin{aligned}
x_1 &\in [0, 1] \\
x_2 &\in [0, 1] \\
x_3 &\in [0, 2] \\
x_4 &\in [-2, -1] \\
x_5 &\in [-1, 1] \\
x_6 &\in [0, 1] \\
x_7 &\in [0, 2] \\
x_8 &\in [0, 1] \\
x_9 &\in [0, 2] \\
x_{10} &\in [-2.5, 0.5].
\end{aligned}
$$

   The lower bound for $x_9 - x_{10}$ is -0.5 which is not sufficient to prove the property.

Problem 2 (MILP encoding for Maxpool)**.** In the lecture, we learned the Mixed Integer Linear Programming (MILP) based encoding of the ReLU operation. In this exercise, we our goal is to design an encoding of the Maxpool operation using MILP.

1. Design a MILP encoding for the Maxpool operation $y := max(x_1, x_2)$ where the input bounds for x_1 and x_2 are $[a_1, b_1]$ and $[a_2, b_2]$.

2. Now, use the Maxpool MILP encoding for verifying the same property as in the previous exercise. Can the resulting analysis prove the property?

Solution 2. 1. The MILP encoding for the output can be obtained by viewing the given maxpool as $y - x_1 = ReLU(x_2 - x_1)$. The result is:

$$
\begin{aligned}
&y \geq x_1\\
&y \geq x_2\\
&y \leq x_1 + (1-\alpha_1)\cdot(b_2 - a_1)\\
&y \leq x_2 + (1-\alpha_2)\cdot(b_1 - a_2)\\
&\alpha_1 + \alpha_2 = 1\\
&\alpha_1 = 1 \iff y = x_1 \text{ and } x_1 \geq x_2\\
&\alpha_2 = 1 \iff y = x_2 \text{ and } x_2 \geq x_1\\
&\alpha_1, \alpha_2 \in \{0, 1\}.
\end{aligned}
$$

2. We compute the lower bound of $x_9 - x_{10}$ starting by backsubstituting expressions for x_9 and x_{10}. This yields $x_9 - x_{10} = 2x_7 - x_8 + 0.5$, now we use MILP encoding for x_7 which gives us 2 branches. Exploring the first branch gives us:

$$\alpha_3 = 0, \alpha_4 = 1, x_7 = x_4, x_3 \leq x_4 \leq x_3 - 1$$

The branch condition $x_3 \leq x_4 \leq x_3 - 1$ is unsatisfiable so this branch is not explored. The MILP solver then explores the other branch which gives:

$$\alpha_3 = 1, \alpha_4 = 0, x_7 = x_3, x_4 \leq x_3 \leq x_4 + 4$$

The branch condition $x_4 \leq x_3 \leq x_4 + 4$ is satisfiable so this branch is taken. Substituting $x_7 = x_3$ we get, $x_9 - x_{10} = 2x_3 - x_8 + 0.5$. Now the solver explores both branches for x_8. Exploring the first branch gives us:

$$\alpha_5 = 0, \alpha_6 = 1, x_7 = x_6, x_5 \leq x_6 \leq x_5 + 2$$

The branch condition $x_5 \leq x_6 \leq x_5 + 2$ is satisfied. Substituting $x_8 = x_6$, we get $x_9 - x_{10} = 2x_3 - x_6 + 0.5 = 2x_1 + x_2 + 0.5 \geq 0.5$. Since the lower bound is > 0, the property holds in this branch. Now we explore the remaining branch which gives:

$$\alpha_5 = 1, \alpha_6 = 0, x_7 = x_5, x_6 \leq x_5 \leq x_6 + 1$$

The branch condition $x_6 \leq x_5 \leq x_6 + 1$ is satisfied. Substituting $x_8 = x_5$, we get $x_9 - x_{10} = 2x_3 - x_5 + 0.5 = x_1 + 3x_2 + 0.5 \geq 0.5$. Thus in this branch the property holds. Since the property holds in all explored branches, it holds for all inputs.