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

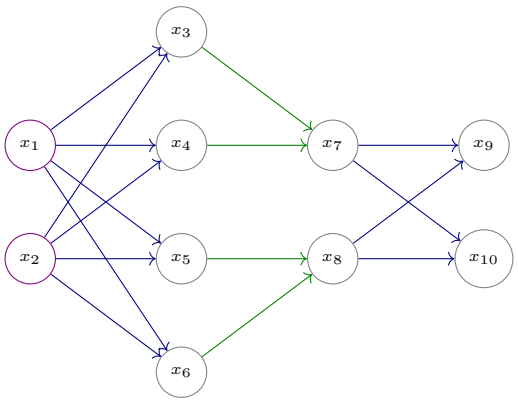

Figure 1: Fully-connected network with Affine and Maxpool operations.

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?

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?