CS 521: Homework 2

Jamie Fulford

Due October 3, 2025

Link to files: https://github.com/jfulfo/cs521/tree/main/hw2

Problem 1

(a) Clearly the best choice is $I_1 + I_2 = [a_1 + a_2, b_1 + b_2] + i[c_1 + c_2, d_1 + d_2]$.

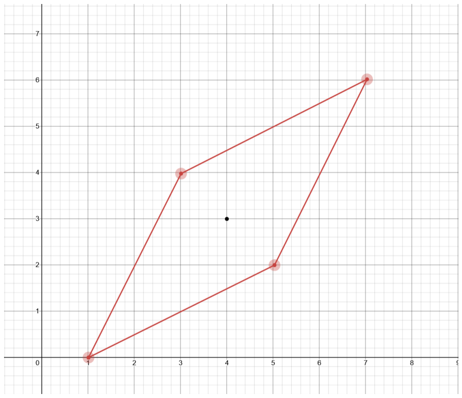
(b) Multiplication is less obvious. Let $x_1 = [a_1, b_1], x_2 = [a_2, b_2], y_1 = [c_1, d_1], y_2 = [c_2, d_2]$. We use

$$(x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2)$$

We need to find upper and lower bounds for both components. We use the fact that for a rectangular domain $[a, b] \times [c, d]$, the bilinear function $f(x, y) = xy$ has its extrema at the vertices of the rectangle. In other words, the maximum and minimum for real interval multiplication is one of ac, ad, bc, bd. Therefore we want to consider all endpoints of our intervals. Let $P_1 = \{a_1a_2, a_1b_2, b_1a_2, b_1b_2\}, P_2 = \{c_1c_2, c_1d_2, d_1c_2, d_1d_2\}, Q_1 = \{a_1c_2, a_1d_2, b_1c_2, b_1d_2\}, Q_2 = \{c_1a_2, c_1b_2, d_1a_2, d_2, a_3\}$. Then the most precise interval would be

$$I_1 \cdot I_2 = [\min P_1 - \max P_2, \max P_1 - \min P_2] + i[\min Q_1 + \min Q_2, \max Q_1 + \max Q_2]$$

Problem 2

(a) 

(b) We first compute x_3, x_4 using the affine form transformer. We get

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \end{pmatrix} \varepsilon_1 + \begin{pmatrix} 5 \\ 1 \end{pmatrix} \varepsilon_2 + \begin{pmatrix} 10 \\ -1 \end{pmatrix}$$

This gives bound $x_3 \in [1, 19], x_4 \in [-3, 1]$. Note that x_4 crosses zero, so we need to construct the proper ReLU transformer for x_4. Since the lower bound of x_3 is greater than 0 we just use $x_5 = x_3$ The slope is $\lambda = \frac{1}{1-(-3)} = \frac{1}{4}$. Then we get

$$\begin{aligned} x_6 &= \frac{1}{4}(-\varepsilon_1 + \varepsilon_2 - 1) - \varepsilon_3 \cdot \frac{\frac{1}{4} \cdot (-3)}{2} - \frac{\frac{1}{4} \cdot (-3)}{2} \\ &= -\frac{1}{4}\varepsilon_1 + \frac{1}{4}\varepsilon_2 + \frac{3}{8}\varepsilon_3 + \frac{1}{8} \end{aligned}$$

Thus our resulting zonotope is

$$\begin{pmatrix} x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 4 \\ -\frac{1}{4} \end{pmatrix} \varepsilon_1 + \begin{pmatrix} 5 \\ \frac{1}{4]} \end{pmatrix} \varepsilon_2 + \begin{pmatrix} 0 \\ \frac{3}{8} \end{pmatrix} \varepsilon_3 + \begin{pmatrix} 10 \\ \frac{1}{8} \end{pmatrix}$$

Then the bounds are $x_5 \in [1, 19]$ and $x_6 \in [-3/4, 1]$. Thus $x_6 \geq x_5$.

Problem 3

(a) For $y = \max(x_1, x_2)$, we get

$$\begin{aligned}
&y \geq x_1 \\
&y \geq x_2 \\
&y \leq x_1 + (b_2 - a_1)(1 - a) \\
&y \leq x_2 + (b_1 - a_2)a \\
&a \in \{0, 1\}
\end{aligned}$$

(b) First lets propagate the bounds. We are given $x_1, x_2 \in [0, 1]$. Then $x_3 \in [0, 2], x_4 \in [-2, -1], x_5 \in [-1, 1], x_6 \in [0, 1]$. For $x_7 = \max(x_3, x_4)$, since $x_3 > x_4$, then we can just substitute $x_7 = x_3$. For $x_8 = \max(x_5, x_6)$, we use our previous encoding to get the constraints

$$\begin{aligned}
&x_8 \geq x_5 \\
&x_8 \geq x_6 \\
&x_8 \leq x_5 + 2(1 - a) \\
&x_8 \leq x_6 + a
\end{aligned}$$

To show $x_9 > x_{10}$, we use contradiction, in particular adding the constraint $x_9 \leq x_{10}$. This gives:

$$\begin{aligned}
&x_7 \leq -x_7 + x_8 - 0.5 \\
\implies &x_8 \geq 2x_1 + 2x_2 + 0.5
\end{aligned}$$

Then $x_8 \geq 0.5$ always, but at $x_1 = x_2 = 0$, $x_8 = 0$, which is a contradiction.

Problem 4

I changed the given architecture slightly to make it work with the given bound propagation library. The library could not accept the `Normalize` or flatten steps in the given network so I moved these as transforms in the dataloader. The model achieved a clean accuracy of 97.07%. Below are the results of the robustness of the model against perturbations via interval analysis. These data

ε	Verified Accuracy
0.01	79.49
0.02	28.37
0.03	5.50
0.04	1.10
0.05	0.18
0.06	0.01
0.07	0.00
0.08	0.00
0.09	0.00
0.10	0.00

indicate that the model has good robustness against small perturbations (e.g. $\varepsilon = 0.01$), but experiences a sharp drop-off in accuracy as the perturbations increase in size. Discrepancies between my implementation and others may be caused by the way I did normalization with my model.