1 Finding the minimal change that will get rid of the network's WaterMark

Given a watermarked trained neural network as described here. We tested what is the minimal change to the network last layer in order to "remove" some watermarks from the network.

1.1 Defining the problem

Given a neural network N with an output size m the network decision for an input x is defined as the coordinate with the maximal value, if the network output is the vector y the decision is $argmax_{i\in[m]}\left\{y_i\right\}$

Given a watermarked network N with a set of K watermarks (A set of inputs to the network) $\{x_1, \cdots, x_K\}$ we'll mark the network last layer L such that L is a $m \times n$ matrix were n is the layer's number of neurons and m is the network output size. The change to the last layer will be a matrix with the same dimension as L we'll mark as ε, such that $\varepsilon_{i,j}$ is the change to the last layer matrix entry $L_{i,j}$. Well measure the overall change to the layer as $\|\varepsilon\|_\infty = max_{i,j}\left\{|\varepsilon_{i,j}|\right\}$.

For a certain input x we're only interested in the input to the last layer we'll mark the input to the last layer v. v is a $n \times 1$ vector. So the original network output $y = Lv$ and the changed network output is $y' = (L+\varepsilon)v$. For a single input x we need to find the minimal ε so that the $argmax_{i\in[m]}\left\{y_i\right\} \neq argmax_{i\in[m]}\left\{y'_i\right\}$

Denote $d := argmax_{i\in[m]}\left\{y_i\right\}$
For some $d' \in [m]\,, d' \neq d$ finding ε with minimal $\|\varepsilon\|_\infty$ such that $y' = (L+\varepsilon)v$ and $d' = argmax_{i\in[m]}\left\{y'_i\right\}$ can be described in a Linear Programming form like so:

$$\begin{aligned}
Minimize:&\quad c\\
Subject\ to:&\quad \forall i,j \quad -c \leq \varepsilon_{i,j} \leq c\\
&\quad y' = (L+\varepsilon)v\\
&\quad y'_d \leq y'_{d'}
\end{aligned}$$

*The variables are the entries in ε and y'

Using the same method we can find how to change the network to more than one input.
Given inputs $x_1, \cdots, x_k$ and their respective inputs to the last layer $v_1, \cdots, v_k$ and their respected outputs and decisions $\{y_1, \cdots, y_k\}$ $\{d_1, \cdots, d_k\}$ we want to find ε such that
$\forall 1 \leq j \leq k \quad d_j \neq argmax_{i\in[m]}\left\{\left((L+\varepsilon)\,v_j\right)_i\right\}$
Assuming we choose our new desired output $\{d'_1, \cdots, d'_k\}$ And now our LP looks like this:

$$\begin{aligned}
Minimize:&\quad c\\
Subject\ to:&\quad \forall i,j \quad -c \leq \varepsilon_{i,j} \leq c\\
&\quad \forall j \quad y'_j = (L+\varepsilon)v_j\\
&\quad \forall j \quad \left(y'_j\right)_{d_j} \leq \left(y'_j\right)_{d'_j}
\end{aligned}$$

*The variables are the entries in ε and y'_j

Using Marabou we can solve for the minimal ε under different norm $\|\varepsilon\|_1 = \sum_{i,j}|\varepsilon_{i,j}|$ since using this norm gives us a piece-wise linear problem.