RIAI project

Thomas Cambier
Thibault Dardinier

December 20, 2018

1 General method

At the beginning of the program, we use ELINA to find bounds for every neuron in every layer, which gives arrays of bounds. During the whole analysis, we can improve these bounds with Gurobi and the interval analyser. Improving these bounds serves to improve the approximations of the RELUs in Gurobi (which is done via a triangle). The function **createNetwork** models the network (or a part of it) in Gurobi. This function is called by the functions **improveBounds** (which improves the bounds of a certain layer with Gurobi) and **analyzeEnd**. **analyzeEnd** models the network from a certain layer and tries to verify the label by finding the minimum of the output of the correct label minus the maximum of the outputs of the wrong labels. If this returns a positive number, then the network is verified.

2 Heuristics

Whatever the neural network, we start by running the interval analysis by ELINA because it is fast to run (there's no free lunch, except with ELINA). We have an optimal strategy with the tools that we set up: we analyze the network with Gurobi starting from the image and finishing to a certain layer starting from 2 (the only approximations being triangles for the RELUs), then we propagate the new bounds with ELINA (really fast) and finally, we encode all the network with Guroby and try to verify it. If it is not verified, we increase the end layer until we reach the end of the network. If it is still not verified at the end of the network, we know we cannot do better with the functions we have. After having run some timing tests with this strategy, we realized that it was fast enough to run for all networks except the one with 1024 neurons.

For the network with 1024 neurons, we only improve the bounds of the second layer considering only the best (based on our heuristic: If the bounds of the layer are a and b, then the best are the ones which maximize $b - max(a, 0)$, since it has the biggest potential for increasness) 200 neurons and then we do the interval analysis from ELINA again. Finally, we try to finish with Gurobi starting from the last layer and decreasing one by one.