Speeding Up Neural Network Verification via Automated Algorithm Configuration

Matthias König, Holger H. Hoos, Jan N. van Rijn • Institute of Advanced Computer Science, Leiden University, Leiden, The Netherlands

Background

- Neural networks are vulnerable to adversarial examples
- Several neural network verification methods are based on mixed integer linear programming (MIP)
- Problem: High computational costs and many timeouts

Method

- Parallel portfolio of optimised solver configurations
- 1 CPU core per configuration

Conclusions

- Improved performance of state-of-the-art MIP-based verification engine MIPVerify:
  - 4.7-fold reduction in CPU time
  - 1.4 times fewer timeouts
  - 1.3-fold improvement on upper bound
- Future work considers further MIP-based verification engines, classifiers and datasets

Baselines & Results

- Task: Verify robust classifier over full MNIST dataset (n=10 000)
- Baselines: MIPVerify verification engine with Gurobi solver at default using (i) all available CPU cores, (ii) 4 CPU cores, (iii) 1 CPU core with same overall CPU time budget
- Avg. running time on subset of solvable instances (instances solved by any approach; n=8 646)

<table>
<thead>
<tr>
<th></th>
<th>Portfolio (4 Cores)</th>
<th>Default** (32 Cores)</th>
<th>Default (4 Cores)</th>
<th>Default (1 Core)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeouts</td>
<td>14.96%</td>
<td>21.29%</td>
<td>17.74%</td>
<td>17.66%</td>
</tr>
<tr>
<td>Adversarial error</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upper bound</td>
<td>23.86%</td>
<td>30.67%</td>
<td>27.49%</td>
<td>27.58%</td>
</tr>
<tr>
<td>Lower bound</td>
<td>14.43%</td>
<td>14.37%</td>
<td>14.40%</td>
<td>14.36%</td>
</tr>
<tr>
<td>Avg. running time</td>
<td>8 478</td>
<td>39 772</td>
<td>22 065</td>
<td>20 117</td>
</tr>
</tbody>
</table>

* Timeouts are penalised as $t \times 10$.
** As employed in MIPVerify