Abstract

This paper introduces a class of mixed-integer formulations for trained ReLU neural networks. The approach balances model size and tightness by partitioning node inputs into a number of groups and forming the convex hull over the partitions via disjunctive programming. At one extreme, one partition per input recovers the convex hull of a node, i.e., the tightest possible formulation for each node. For fewer partitions, we develop smaller relaxations that approximate the convex hull, and show that they outperform existing formulations. Specifically, we propose strategies for partitioning variables based on theoretical motivations and validate these strategies using extensive computational experiments. Furthermore, the proposed scheme complements known algorithmic approaches, e.g., optimization-based bound tightening captures dependencies within a partition.

1 Introduction

Many applications use mixed-integer linear programming (MILP) to optimize over trained feed-forward ReLU neural networks (NNs) [5, 14, 18, 23, 33, 37]. A MILP encoding of a ReLU-NN enables network properties to be rigorously analyzed, e.g., maximizing a neural acquisition function [34] or verifying robustness of an output (often classification) within a restricted input domain [6]. MILP encodings of ReLU-NNS have also been used to determine robust perturbation bounds [9], compress NNs [28], count linear regions [27], and find adversarial examples [17]. The so-called big-M formulation is the main approach for encoding NNs as MILPs in the above references. Optimizing the resulting MILPs remains challenging for large networks, even with state-of-the-art software.

Effectively solving a MILP hinges on the strength of its continuous relaxation [10]; weak relaxations can render MILPs computationally intractable. For NNs, Anderson et al. [3] showed that the big-M formulation is not tight and presented formulations for the convex hull (i.e., the tightest possible formulation) of individual nodes. However, these formulations require either an exponential (w.r.t. inputs) number of constraints or many additional/auxiliary variables. So, despite its weaker continuous relaxation, the big-M formulation can be computationally advantageous owing to its smaller size.

Given these challenges, we present a novel class of MILP formulations for ReLU-NNs. The formulations are hierarchical: their relaxations start at a big-M equivalent and converge to the convex hull. Intermediate formulations can closely approximate the convex hull with many fewer variables/constraints. The formulations are constructed by viewing each ReLU node as a two-part
disjunction. Kronqvist et al. [21] proposed hierarchical relaxations for general disjunctive programs. This work develops a similar hierarchy to construct strong and efficient MILP formulations specific to ReLU-NNs. In particular, we partition the inputs of each node into groups and formulate the convex hull over the resulting groups. With fewer groups than inputs, this approach results in MILPs that are smaller than convex-hull formulations, yet have stronger relaxations than big-M.

Three optimization tasks evaluate the new formulations: optimal adversarial examples, robust verification, and $\ell_1$-minimally distorted adversaries. Extensive computation, including with convex-hull-based cuts, shows that our formulations outperform the standard big-M approach with 25% more problems solved within a 1h time limit (average 2.2X speedups for solved problems).

Related work. Techniques for obtaining strong relaxations of ReLU-NNs include linear programming [16, 35, 36], semidefinite programming [12, 25], Lagrangian decomposition [7], combined relaxations [31], and relaxations over multiple nodes [30]. Recently, Tjandraatmadja et al. [32] derived the tightest possible convex relaxation for a single ReLU node by considering its multivariate input space. These relaxation techniques do not exactly represent ReLU-NNs, but rather derive valid bounds for the network in general. These techniques might fail to verify some properties, due to their non-exactness, but they can be much faster than MILP-based techniques. Strong MILP encoding of ReLU-NNs was also studied by Anderson et al. [3], and a related dual algorithm was later presented by De Palma et al. [13]. Our approach is fundamentally different, as it constructs computationally cheaper formulations that approximate the convex hull, and we start by deriving a stronger relaxation instead of strengthening the relaxation via cutting planes. Furthermore, our formulation enables input node dependencies to easily be incorporated.

Contributions of this paper. We present a new class of strong, yet compact, MILP formulations for feed-forward ReLU-NNs in Section 3. Section 3.1 observes how, in conjunction with optimization-based bound tightening, partitioning input variables can efficiently incorporate dependencies into MILP formulations. Section 3.2 builds on the observations of Kronqvist et al. [21] to prove the hierarchical nature of the proposed ReLU-specific formulations, with relaxations spanning between big-M and convex-hull formulations. Sections 3.3–3.4 show that formulation tightness depends on the specific choice of variable partitions, and we present efficient partitioning strategies based on both theoretical and computational motivations. The advantages of the new formulations are demonstrated via extensive computational experiments in Section 4.

2 Background

2.1 Feed-forward Neural Networks

A feed-forward neural network (NN) is a directed acyclic graph with nodes structured into $k$ layers. Layer $k$ receives the outputs of nodes in the preceding layer $k - 1$ as its inputs (layer 0 represents inputs to the NN). Each node in a layer computes a weighted sum of its inputs (known as the preactivation), and applies an activation function. This work considers the ReLU activation function:

$$ y = \max(0, w^T x + b) $$

where $x \in \mathbb{R}^\eta$ and $y \in [0, \infty)$ are, respectively, the inputs and output of a node ($w^T x + b$ is termed the preactivation). Parameters $w \in \mathbb{R}^\eta$ and $b \in \mathbb{R}$ are the node weights and bias, respectively.

2.2 ReLU Optimization Formulations

In contrast to the training of NNs (where parameters $w$ and $b$ are optimized), optimization over a NN seeks extreme cases for a trained model. Therefore, model parameters $(w, b)$ are fixed, and the inputs/outputs of nodes in the network $(x, y)$ are optimization variables instead.

Big-M Formulation. The ReLU function (1) is commonly modeled [9, 23]:

$$ y \geq (w^T x + b) $$

$$ y \leq (w^T x + b) - (1 - \sigma) LB^0 $$

$$ y \leq \sigma UB^0 $$

where $\sigma = 0$.
where \( y \in [0, \infty) \) is the node output and \( \sigma \in \{0, 1\} \) is a binary variable corresponding to the on-off state of the neuron. The formulation requires the bounds (big-M coefficients) \( LB^0, UB^0 \in \mathbb{R} \), which should be as tight as possible, such that \((w^Tx + b) \in [LB^0, UB^0] \).

**Disjunctive Programming** \(^4\). We observe that \([1]\) can be modeled as a disjunctive program:

\[
\begin{cases}
y = 0 \\
w^Tx + b \leq 0 \\
w^Tx + b \geq 0
\end{cases}
\]

The extended formulation for disjunctive programs introduces auxiliary variables for each disjunction. Instead of directly applying the standard extended formulation, we first define \( z := w^T x \) and assume \( z \) is bounded. The auxiliary variables \( z^a \in \mathbb{R} \) and \( z^b \in \mathbb{R} \) can then be introduced to model \([5]\):

\[
\begin{align}
w^Tx &= z^a + z^b \\
z^a + \sigma b &\leq 0 \\
z^b + (1 - \sigma)b &\geq 0 \\
y &= z^b + (1 - \sigma)b \\
\sigma LB^a &\leq z^a \leq \sigma UB^a \\
(1 - \sigma)LB^b &\leq z^b \leq (1 - \sigma)UB^b
\end{align}
\]

where again \( y \in [0, \infty) \) and \( \sigma \in \{0, 1\} \). Bounds \( LB^a, UB^a, LB^b, UB^b \in \mathbb{R} \) are required for this formulation, such that \( z^a \in \sigma[LB^a, UB^a] \) and \( z^b \in (1 - \sigma)[LB^b, UB^b] \). Note that the inequalities in \([5]\) may cause the domains of \( z^a \) and \( z^b \) to differ. The summation in \([6]\) can be used to eliminate either \( z^a \) or \( z^b \); therefore, in practice, only one auxiliary variable is introduced by formulation \([6–11]\).

**Importance of relaxation strength.** MILP is often solved with branch-and-bound, a strategy that bounds the objective function between the best feasible point and its tightest optimal relaxation. The integral search space is explored by “branching” until the gap between bounds falls below a given tolerance. A *tighter*, or stronger, relaxation can reduce this search tree considerably.

### 3 Disaggregated Disjunctions: Between Big-M and the Convex Hull

Our proposed formulations split the sum \( z = w^T x \) into partitions: we will show these formulations have tighter continuous relaxations than \([6–11]\). In particular, we partition the set \( \{1, ..., \eta\} \) into subsets \( S_1 \cup S_2 \cup ... \cup S_N = \{1, ..., \eta\}, S_n \cap S_n' = \emptyset \forall n \neq n' \). An auxiliary variable is then introduced for each partition, i.e., \( z_n = \sum_{i \in S_n} w_i x_i \). Replacing \( z = w^T x \) with \( \sum_{n=1}^N z_n \), the disjunction \([5]\) becomes:

\[
\begin{cases}
y = 0 \\
\sum_{n=1}^N z_n + b \leq 0
\end{cases}
\]

Assuming now that each \( z_n \) is bounded, the extended formulation can be expressed using auxiliary variables \( z^a_n \) and \( z^b_n \) for each \( z_n \). Eliminating \( z^a_n \) via the summation \( z_n = z^a_n + z^b_n \) results in our proposed formulation (complete derivation in appendix A.1):

\[
\begin{align}
\sum_{n} \left( \sum_{i \in S_n} w_i x_i - z^b_n \right) + \sigma b &\leq 0 \\
\sum_{n} z^b_n + (1 - \sigma)b &\geq 0 \\
y &= \sum_{n} z^b_n + (1 - \sigma)b \\
\sigma LB^a_n &\leq \sum_{i \in S_n} w_i x_i - z^b_n \leq \sigma UB^a_n, \quad \forall n = 1, ..., N \\
(1 - \sigma)LB^b_n &\leq z^b_n \leq (1 - \sigma)UB^b_n, \quad \forall n = 1, ..., N
\end{align}
\]

where \( y \in [0, \infty) \) and \( \sigma \in \{0, 1\} \). We observe that \([13–17]\) exactly represents the ReLU node (given that the partitions \( z_n \) are bounded in the original disjunction): the sum \( z_n = \sum_{i \in S_n} w_i x_i \) is
substituted in the extended convex hull formulation [4] of disjunction (12). Note that, compared to
the general case presented by Kronqvist et al. [21], both sides of disjunction (12) can be modeled using
the same partitions, resulting in fewer auxiliary variables. We further note that domains \([LB^u_n, UB^u_n]\)
and \([LB^b_n, UB^b_n]\) may not be equivalent, owing to inequalities in (12).

### 3.1 Obtaining and Tightening Bounds

The big-M formulation (2)–(4) requires valid bounds \((w^T x + b) \in [LB^0, UB^0]\). Given bounds for
each input variable, \(x_i \in [\xi_i, \bar{\xi}_i]\), interval arithmetic gives valid bounds:

\[
LB^0 = \sum_i (\xi_i \max(0, w_i) + \bar{\xi}_i \min(0, w_i)) + b
\]

\[
UB^0 = \sum_i (\bar{\xi}_i \max(0, w_i) + \xi_i \min(0, w_i)) + b
\]

But (18)–(19) do not provide the tightest valid bounds in general, as dependencies between the input
variables are ignored. Propagating the resulting over-approximated bounds from layer to layer leads
to increasingly large over-approximations, i.e., propagating weak bounds through layers results in a
significantly weakened model. These bounds remain in the proposed formulation (13)–(17) in the
form of bounds on both the output \(y\) and the original variables \(x\) (i.e., outputs of the previous layer).

![Hierarchical relaxations from N = 1 (equiv. big-M) to N = 20 (convex hull of each
node over a box domain) for a two-input \((x_1, x_2)\) NN trained on scaled Ackley function, with output
\(f(x)\). Top row: \(z^h_n\) bounds obtained using interval arithmetic; Bottom row: \(z^b_n\) bounds obtained by
optimization-based bound tightening. The partitions are formed using the equal size
strategy.](image)

**Optimization-Based Bound Tightening (OBBT)** or progressive bounds tightening [33], tightens
variable bounds and constraints [15]. For example, solving the optimization problem with the
objective set to minimize/maximize \((w^T x + b)\) gives bounds: \(\min(w^T x + b) \leq w^T x + b \leq \max(w^T x + b)\).
To simplify these problems, OBBT can be performed using the relaxed model (i.e.,
\(\sigma \in [0, 1]\) rather than \(\sigma \in \{0, 1\}\), resulting in a linear program (LP). In contrast to (18)–(19), bounds
from OBBT incorporate variable dependencies. We apply OBBT by solving one LP per bound.

The partitioned formulation (13)–(17) requires bounds such that \(z^a_n \in \sigma[LB^u_n, UB^u_n]\), \(z^b_n \in (1 - \sigma)[LB^b_n, UB^b_n]\). In other words, \([LB^u_n, UB^u_n]\) is a valid domain for \(z^a_n\) when the node is inactive
\((\sigma = 1)\) and vice versa. These bounds can also be obtained via OBBT: \(\min(\sum_{i \in S_n} w_ia_i) \leq z^a_n \leq \max(\sum_{i \in S_n} w_ia_i); w^T x + b \leq 0\). The constraint on the right-hand side of disjunction (12)
can be similarly enforced in OBBT problems for \(z^b_n\). In our framework, OBBT additionally captures
dependencies within each partition \(S_n\). Specifically, we observe that the partitioned OBBT problems
effectively form the convex hull over a given polyhedron of the input variables, in contrast to the
convex hull formulation, which only considers the box domain defined by the min/max of each
input node [3]. Since \(\sum_{i \in S_n} w_ia_i = z^a_n + z^b_n\) and \(z^a_n \geq 0\), the bounds \(\min(\sum_{i \in S_n} w_ia_i), \max(\sum_{i \in S_n} w_ia_i)\) are valid for both \(z^a_n\) and \(z^b_n\). These bounds can be from (18)–(19), or by solving
two OBBT problems for each partition (2N LPs total). This simplification uses equivalent bounds for
\(z^a_n\) and \(z^b_n\), but tighter bounds can potentially be found by performing OBBT for \(z^a_n\) and \(z^b_n\) separately
(4N LPs total).
Figure 1 compares the proposed formulation with bounds from interval arithmetic (top row) vs OBBT (bottom row). The true model outputs (blue), and minimum (orange) and maximum (green) outputs of the relaxed model are shown over the input domain. The NNs comprise two inputs, three hidden layers with 20 nodes each, and one output. As expected, OBBT greatly improves relaxation tightness.

3.2 Tightness of the Proposed Formulation

**Proposition 1.** (13–17) has the equivalent non-lifted (i.e., without auxiliary variables) formulation:

\[
y \leq \sum_{i \in I_j} w_i x_i + \sigma (b + \sum_{i \in I \setminus I_j} UB_i) + (\sigma - 1) (\sum_{i \in I_j} LB_i), \quad \forall j = 1, \ldots, 2^N \tag{20}
\]

\[
y \geq w^T x + b \tag{21}
\]

\[
y \leq \sigma UB \tag{22}
\]

where \( UB_i \) and \( LB_i \) denote the upper and lower bounds of \( w_i x_i \). The set \( I \) denotes the input indices \{1, \ldots, \eta\}, and the subset \( I_j \) denotes the indices contained by the union of the \( j \)-th combination of partitions in \( \{S_1, \ldots, S_N\} \).

**Proof.** Formulation (13–17) introduces \( N \) auxiliary variables \( z_n^b \), which can be projected out using Fourier-Motzkin elimination (appendix A.2), resulting in combinations \( I_1, \ldots, I_J, J = 2^N \).

**Remark.** When \( N < \eta \), the family of constraints in (20) represent a subset of the inequalities used to define the convex hull by Anderson et al. [3], where \( UB_i \) and \( LB_i \) would be obtained using interval arithmetic. Therefore, though a lifted formulation is proposed in this work, the proposed formulations have non-lifted relaxations equivalent to pre-selecting a subset of the convex hull inequalities.

**Proposition 2.** Formulation (13–17) is equivalent to the big-M formulation (2)–(4) when \( N = 1 \).

**Proof.** When \( N = 1 \), it follows that \( S_1 = \{1, \ldots, \eta\} \). Therefore, \( z_1 = \sum_{n=1}^\eta w_n x_n = w^T x \), and \( \sum_n z_n = z_1 = z \). Conversely, big-M can be seen as the convex hull over a single aggregated “variable,” \( z = w^T x \).

**Proposition 3.** Formulation (13–17) represents the convex hull of (1), given the inputs \( x \) are bounded, for the case of \( N = \eta \).

**Proof.** When \( N = \eta \), it follows that \( S_\eta = \\{\eta\}, \forall n = 1, \ldots, \eta \), and, consequently, \( z_n = w_n x_n \). Since \( z_n \) are linear transformations of each \( x_n \) (as are their respective bounds), forming the convex hull over \( z_n \), recovers the convex hull over \( x \). An extended proof is provided in appendix A.3.

**Proposition 4.** A formulation with \( N \) partitions is strictly tighter than any formulation with \((N - 1)\) partitions that is derived by combining two partitions in the former.

**Proof.** When combining two partitions, i.e., \( S'_{N-1} := S_{N-1} \cup S_N \), constraints in (20) where \( S'_{N-1} \subseteq I_j \) are also obtained by \( \{S_{N-1}, S_N\} \subseteq I_j \). In contrast, those obtained by \( S_{N-1} \cup S_N \subseteq I_j \) cannot be modeled by \( S'_{N-1} \). Since each constraint in (20) is facet-defining \[ and distinct from each other, omissions result in a less tight formulation.

**Remark.** The convex hull can be formulated with \( \eta \) auxiliary variables using (13–17) for \( N = \eta \), or \( 2^\eta \) constraints using (20). While these formulations have tighter relaxations, they can perform worse than big-M due to having more difficult branch-and-bound subproblems. Our proposed formulation balances this tradeoff by introducing a hierarchy of relaxations with increasing tightness and size. The convex hull is created over partitions \( z_n, n = 1, \ldots, N \), rather than the input variables \( x_n, n = 1, \ldots, \eta \). Therefore, only \( N \) auxiliary variables are introduced, with \( N \leq \eta \). The results in this work are obtained using this lifted formulation (13–17). Appendix A.5 compares the computational performance of equivalent non-lifted formulations, i.e., involving \( 2^N \) constraints.

Figure 1 shows a hierarchy of increasingly tight formulations from \( N = 1 \) (equiv. big-M) to \( N = 20 \) (convex hull of each node over a box input domain). The intermediate formulations approximate the convex-hull \((N = 20)\) formulation well, but need fewer auxiliary variables/constraints.
3.3 Effect of Input Partitioning Choice

Formulation (13) – (17) creates the convex hull over \( z_n = \sum_{i \in S_n} w_i x_i, n = 1, ..., N \). The hyperparameter \( N \) dictates model size, and the choice of subsets, \( S_1, ..., S_N \), can strongly impact the strength of its relaxation. By Proposition 4, (13) – (17) can in fact give multiple hierarchies of formulations. While all hierarchies eventually converge to the convex hull, we are primarily interested in those with tight relaxations for small \( N \).

**Bounds and Bounds Tightening.** Bounds on the partitions play a key role in the proposed formulation. For example, consider when a node is inactive: \( \sigma = 1 \), \( z_n = 0 \), and (16) gives the bounds \( \sigma LB_n^a \leq \sum_{i \in S_n} w_i x_i \leq \sigma UB_n^a \). Intuitively, the proposed formulation represents the convex hull over the auxiliary variables, \( z_n = \sum_{i \in S_n} w_i x_i \), and their bounds play a key role in model tightness. We hypothesize these bounds are most effective when partitions \( S_n \) are selected such that \( w_i x_i, \forall i \in S_n \) are of similar orders of magnitude. Consider for instance the case of \( w = [1, 1, 100, 100] \) and \( x_i \in [0, 1], i = 1, ..., 4 \). As all weights are positive, interval arithmetic gives \( 0 \leq \sum x_i w_i \leq \sum x_i w_i \).

With two partitions, the choices of \( S_1 = \{1, 2\} \) vs \( S_1 = \{1, 3\} \) give:

\[
\begin{align*}
\begin{bmatrix} x_1 + x_2 & \leq \sigma 2 \\
x_3 + x_4 & \leq \sigma 2 \end{bmatrix} & \text{ vs. } \begin{bmatrix} x_1 + 100 x_3 & \leq \sigma 101 \\
x_2 + 100 x_4 & \leq \sigma 101 \end{bmatrix}
\end{align*}
\]

where \( \sigma \) is a binary variable. The constraints on the right closely approximate the \( \eta \)-partition (i.e., convex hull) bounds: \( x_3 \leq \sigma \) and \( x_4 \leq \sigma \). But \( x_1 \) and \( x_2 \) are relatively unaffected by a perturbation \( \sigma = 1 - \delta \) (when \( \sigma \) is relaxed). Whereas the formulation on the left constrains the four variables equivalently. If the behavior of the node is dominated by a few inputs, the formulation on the right is strong, as it approximates the convex hull over those inputs (\( z_1 \approx x_3 \) and \( z_2 \approx x_4 \) in this case). For the practical case of \( N << \eta \), there are likely fewer partitions than dominating variables.

The size of the partitions can also be selected to be uneven:

\[
\begin{align*}
x_1 & \leq \sigma 1 \\
x_2 + 100 x_3 + 100 x_4 & \leq \sigma 201
\end{align*}
\]

\[
\begin{align*}
x_3 & \leq \sigma 1 \\
x_1 + x_2 + 100 x_3 + 100 x_4 & \leq \sigma 102
\end{align*}
\]

Similar tradeoffs are seen here: the first formulation provides the tightest bound for \( x_1 \), but \( x_2 \) is effectively unconstrained and \( x_3, x_4 \) approach “equal treatment.” The second formulation provides the tightest bound for \( x_3 \), and a tight bound for \( x_4 \), but \( x_1, x_2 \) are effectively unbounded for fractional \( \sigma \).

The above analyses also apply to the case of OBBT. For the above example, solving a relaxed model for \( \max(x_1 + x_2) \) obtains a bound that affects the two variables equivalently, while the same procedure for \( \max(x_1 + 100 x_3) \) obtains a bound that is much stronger for \( x_3 \) than for \( x_1 \). Similarly, \( \max(x_1 + x_2) \) captures dependency between the two variables, while \( \max(x_1 + 100 x_3) \approx \max(100 x_3) \).

**Relaxation Tightness.** The partitions (and their bounds) also directly affect the tightness of the relaxation for the output variable \( y \). The equivalent non-lifted realization (20) reveals the tightness of the above simple example. With two partitions, the choices of \( S_1 = \{1, 2\} \) vs \( S_1 = \{1, 3\} \) result in the equivalent non-lifted constraints:

\[
\begin{align*}
y & \leq x_1 + 100 x_3 + \sigma (b + 101) \\
y & \leq x_2 + 100 x_4 + \sigma (b + 101)
\end{align*}
\]

\[
\begin{align*}
y & \leq x_1 + x_2 + \sigma (b + 200) \\
y & \leq 100 x_3 + 100 x_4 + \sigma (b + 2)
\end{align*}
\]

Note that combinations \( I_1 = \emptyset \) and \( I_2 = \{1, 2, 3, 4\} \) in (20) are not analyzed here, as they correspond to the big-M/1-partition model and are unaffected by choice of partitions. The 4-partition model is the tightest formulation and (in addition to all possible 2-partition constraints) includes:

\[
\begin{align*}
y & \leq x_1 + \sigma (b + 201), i = 1, 2 \\
y & \leq 100 x_i + \sigma (b + 102), i = 3, 4
\end{align*}
\]

The unbalanced 2-partition, i.e., the left of (25), closely approximates two of the 4-partition (i.e., convex hull) constraints (27). Analogous to the tradeoffs in terms of bound tightness, we see that this formulation essentially neglects the dependence of \( y \) on \( x_1, x_2 \) and instead creates the convex hull over \( x_1 = x_1 + 100 x_3 \approx x_3 \) and \( z_2 = 100 x_4 \). For this simple example, the behavior of \( y \) is dominated by \( x_3 \) and \( x_4 \), and this turns out to be a relatively strong formulation. However, when \( N << \eta \), we expect neglecting the dependence of \( y \) on some input variables to weaken the model.

The alternative formulation, i.e., the right of (25), handles the four variables similarly and creates the convex hull in two new directions: \( z_1 = x_1 + x_2 \) and \( z_2 = 100(x_3 + x_4) \). While this does not
We consider perturbations defined by the \( \ell_2 \) weight vector, \( w \), and distributing them evenly among partitions (\( w \) is fixed during optimization). We propose two such strategies below, as well as two strategies in red for comparison.

### Equal-Size Partitions
One strategy is to create partitions of equal size, i.e., \( |S_1| = |S_2| = \cdots = |S_N| \) (note that they may differ by up to one if \( \eta \) is not a multiple of \( N \)). Indices are then assigned to partitions to keep the weights in each as close as possible. This is accomplished by sorting the weights \( w \) and distributing them evenly among partitions (\( \text{array\_split}(\text{argsort}(w), N) \) in Numpy).

### Equal-Range Partitions
A second strategy is to partition with equal range, i.e., \( \text{range}(w_i) = \cdots = \text{range}(w_i) \) for \( i \in S_n \). We define thresholds \( v \in \mathbb{R}^{N+1} \) such that \( v_1 \) and \( v_{N+1} \) are \( \min(w) \) and \( \max(w) \). To reduce the effect of outliers, we define \( v_2 \) and \( v_{N} \) as the 0.05 and 0.95 quantiles of \( w \), respectively. The remaining elements of \( v \) are distributed evenly in \( (v_2, v_N) \). Indices \( i \in \{1, \ldots, \eta\} \) are then assigned to \( S_n : w_i \in [v_n, v_{n+1}) \). This strategy requires \( N \geq 3 \), but, for a symmetrically distributed weight vector, \( w \), two partitions of equal size are also of equal range.

We compare our proposed strategies against the following:

#### Random Partitions
Input indices \( \{1, \ldots, \eta\} \) are assigned randomly to partitions \( S_1, \ldots, S_N \).

#### Uneven Magnitudes
Weights are sorted and “dealt” in reverse to partitions in snake-draft order.

### 4 Experiments

Computational experiments were performed using Gurobi v 9.1 [19], and models were implemented and trained using PyTorch [24]. The computational set-up, solver settings, and models for MNIST [22] and CIFAR-10 [20] are described in appendix A.4.

#### 4.1 Optimal Adversary Results

The optimal adversary problem takes a target image \( \bar{x} \), its correct label \( j \), and an adversarial label \( k \), and finds the image within a range of perturbations maximizing the difference in predictions. Mathematically, this is formulated as \( \max_{x} (f_k(x) - f_j(x)) \quad x \in X \), where \( f_k \) and \( f_j \) correspond to the \( k \)- and \( j \)-th elements of the NN output layer, respectively, and \( X \) defines the domain of perturbations. We consider perturbations defined by the \( \ell_1 \)-norm \( (||x - \bar{x}||_1 \leq \epsilon_1 \in \mathbb{R}) \), which promotes sparse perturbations [8]. For each dataset, we use the first 100 test-dataset images and randomly selected adversarial labels (the same 100 instances are used for models trained on the same dataset).

Table [1] gives the optimal adversary results. Perturbations \( \epsilon_1 \) were selected such that some big-M problems were solvable within 3600s (problems become more difficult as \( \epsilon_1 \) increases). While our
Table 1: Number of solved (in 3600s) optimal adversary problems and average solve times for big-M vs $N = \{2, 4\}$ equal-size partitions. Average times computed for problems solved by all 3 formulations. Grey indicates partition formulations strictly outperforming big-M.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_1$</th>
<th>Big-M solved</th>
<th>avg.time(s)</th>
<th>2 Partitions solved</th>
<th>avg.time(s)</th>
<th>4 Partitions solved</th>
<th>avg.time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>$2 \times 50$</td>
<td>5</td>
<td>100</td>
<td>57.6</td>
<td>100</td>
<td>42.7</td>
<td>100</td>
<td>83.9</td>
</tr>
<tr>
<td></td>
<td>$2 \times 50$</td>
<td>10</td>
<td>97</td>
<td>431.8</td>
<td>98</td>
<td>270.4</td>
<td>98</td>
<td>398.4</td>
</tr>
<tr>
<td></td>
<td>$2 \times 100$</td>
<td>2.5</td>
<td>92</td>
<td>525.2</td>
<td>100</td>
<td>285.1</td>
<td>94</td>
<td>553.9</td>
</tr>
<tr>
<td></td>
<td>$2 \times 100$</td>
<td>5</td>
<td>38</td>
<td>1587.4</td>
<td>59</td>
<td>587.8</td>
<td>48</td>
<td>1084.7</td>
</tr>
<tr>
<td>CNN1*</td>
<td>$0.25$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>$2 \times 100$</td>
<td>5</td>
<td>62</td>
<td>1982.3</td>
<td>69</td>
<td>1083.4</td>
<td>85</td>
<td>752.8</td>
</tr>
<tr>
<td></td>
<td>$2 \times 100$</td>
<td>10</td>
<td>23</td>
<td>2319.0</td>
<td>28</td>
<td>1320.2</td>
<td>34</td>
<td>1318.1</td>
</tr>
</tbody>
</table>

$^*$OBBT performed on all NN nodes

formulations consistently outperform big-M in terms of problems solved and solution times, the best choice of $N$ is problem-dependent. For instance, the 4-partition formulation performs best for the $2 \times 100$ network trained on CIFAR-10; Figure 2 (right) shows the number of problems solved for this case. The 2-partition formulation is best for easy problems, but is soon overtaken by larger values of $N$. Intuitively, simpler problems are solved with fewer branch-and-bound nodes and benefit more from smaller subproblems. Performance declines again near $N \geq 7$, supporting observations that the convex-hull formulation ($N = \eta$) is not always best [3].

Convex-Hull-Based Cuts. The cut-generation strategy for big-M by Anderson et al. [3] is compatible with our formulations (Section 3.3), i.e., we begin with a partition-based formulation and apply cuts during optimization. Figure 2 (left) gives results with these cuts added (via Gurobi callbacks) at various cut frequencies. Specifically, a cut frequency of $1/k$ corresponds to adding the most violated cut (if any) to each NN node at every $k$ branch-and-bound nodes. Performance is improved at certain frequencies; however, our formulations consistently outperform even the best cases using big-M with cuts. Moreover, cut generation is not always straightforward to integrate with off-the-shelf MILP solvers, and our formulations often perform just as well (if not better) without added cuts. Appendix A.5 gives results with most-violated cuts directly added to the model, as in De Palma et al. [13].

Figure 2: Number solved vs convex-hull-cut frequency/run time for optimal adversary problems ($\epsilon = 5$) for $2 \times 100$ models, without OBBT. Left: $N = 1$ (equivalent to big-M) performs worst on MNIST (dotted) and CIFAR-10 (solid) models for most cut frequencies. Right: each line shows 100 runs of CIFAR-10 model (no convex-hull cuts). $N = 1$ performs the worst; $N = 2$ performs well for easier problems; and intermediate values of $N$ balance model size and tightness well.

Partitioning Strategies. Figure 3 shows the result of the input partitioning strategies from Section 3.4 on the MNIST $2 \times 100$ model for varying $N$. Both proposed strategies (blue) outperform formulations with random and uneven partitions (red). With OBBT, big-M ($N = 1$) outperforms partition-based formulations when partitions are selected poorly. Figure 3 again shows that our formulations perform best for some intermediate $N$; random/uneven partitions worsen with increasing $N$. 

8
Figure 3: Number solved (left) and solution times (right) for optimal adversary problems for MNIST $2 \times 100$ ($\epsilon = 5$). Each point shows 100 runs, max time of 3600s. Dashed lines show runs with OBBT. The equal range strategy requires $N \geq 3$. Our proposed (blue) partitioning strategies solve more problems (top) faster (bottom) than random and uneven partitions (red).

Optimization-Based Bounds Tightening. OBBT was implemented by tightening bounds for all $z^b_n$. We found that adding the bounds from the 1-partition model (i.e., bounds on $\sum z^b_n$) improved all models, as they account for dependencies among all inputs. Therefore these bounds were used in all models, resulting in $2N + 2$ LPs per node ($N \geq 2$). We limited the OBBT LPs to 5s; interval bounds were used if an LP was not solved. Figure 3 shows that OBBT greatly improves the optimization performance of all formulations. OBBT problems for each layer are independent and could, in practice, be solved in parallel. Therefore, at a minimum, OBBT requires the sum of max solution times found in each layer (5s $\times$ # layers in this case). This represents an avenue to significantly improve MILP optimization of NNs via parallelization. In contrast, parallelizing branch-and-bound is known to be challenging and may have limited benefits [1, 26].

Table 2: Number of verification problems solved in 3600s and average solve times for big-M vs $N = \{2, 4\}$ equal-size partitions. Average times computed for problems solved by all 3 formulations. OBBT was performed for all problems. Grey indicates formulations strictly outperforming big-M.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_\infty$</th>
<th>Big-M</th>
<th>2 Partitions</th>
<th>4 Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sol. (#)</td>
<td>avg. time (s)</td>
<td>sol. (#)</td>
<td>avg. time (s)</td>
<td>sol. (#)</td>
</tr>
<tr>
<td>MNIST</td>
<td>CNN1</td>
<td>0.050</td>
<td>82</td>
<td>198.5</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.075</td>
<td>30</td>
<td>632.5</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.075</td>
<td>21</td>
<td>667.1</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.100</td>
<td>1</td>
<td>505.3</td>
<td>5</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>CNN1</td>
<td>0.007</td>
<td>99</td>
<td>100.6</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.010</td>
<td>98</td>
<td>119.1</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.007</td>
<td>80</td>
<td>300.5</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.010</td>
<td>40</td>
<td>743.6</td>
<td>72</td>
</tr>
</tbody>
</table>

4.2 Verification Results

The verification problem is similar to the optimal adversary problem, but terminates when the sign of the objective function is known (i.e., the lower/upper bounds of the MILP have the same sign). This problem is typically solved for perturbations defined by the $\ell_\infty$-norm ($||x - \bar{x}||_\infty \leq \epsilon_\infty \in \mathbb{R}$). Here, problems are difficult for moderate $\epsilon_\infty$: at large $\epsilon_\infty$ a mis-classified example (positive objective) is easily found. Several verification tools rely on an underlying big-M formulation, e.g., MIPVerify [33], NSVerify [2], making big-M an especially relevant point of comparison. Owing to the early termination, larger NNs can be tested compared to the optimal adversary problems. We turned off cuts ($\text{cuts} = 0$) for the partition-based formulations, as the models are relatively tight over the box-domain perturbations and do not seem to benefit from additional cuts. On the other hand, removing cuts improved some problems using big-M and worsened others. Results are presented in Table 2. Our formulations again generally outperform big-M ($N = 1$), except for a few of the 4-partition problems.
Table 3: Number of $\ell_1$-minimally distorted adversary problems solved in 3600s and average solve times for big-M vs $N = \{2, 4\}$ equal-size partitions. Average times and $\epsilon_1$ are computed for problems solved by all 3 formulations. OBBT was performed for all problems. Grey indicates partition formulations strictly outperforming big-M.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>avg$(\epsilon_1)$</th>
<th>Big-M solved</th>
<th>avg.time(s)</th>
<th>2 Partitions solved</th>
<th>avg.time(s)</th>
<th>4 Partitions solved</th>
<th>avg.time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>$2 \times 50$</td>
<td>6.51</td>
<td>52</td>
<td>675.0</td>
<td>93</td>
<td>150.9</td>
<td>89</td>
<td>166.6</td>
</tr>
<tr>
<td></td>
<td>$2 \times 75$</td>
<td>4.41</td>
<td>16</td>
<td>547.3</td>
<td>37</td>
<td>310.5</td>
<td>31</td>
<td>424.0</td>
</tr>
<tr>
<td></td>
<td>$2 \times 100$</td>
<td>2.73</td>
<td>7</td>
<td>710.8</td>
<td>13</td>
<td>572.9</td>
<td>10</td>
<td>777.9</td>
</tr>
</tbody>
</table>

4.3 Minimally Distorted Adversary Results

In a similar vein as Croce and Hein [11], we define the $\ell_1$-minimally distorted adversary problem: given a target image $\bar{x}$ and its correct label $j$, find the smallest perturbation over which the NN predicts an adversarial label $k$. We formulate this as $\min_{\epsilon_1, x} ||x - \bar{x}||_1 \leq \epsilon_1; f_k(x) \geq f_j(x)$. The adversarial label $k$ is selected as the second-likeliest class of the target image. Figure 4 provides examples illustrating that the $\ell_1$-norm promotes sparse perturbations, unlike the $\ell_\infty$-norm. Note that the sizes of perturbations $\epsilon_1$ are dependent on input dimensionality; if it were distributed evenly, $\epsilon_1 = 5$ would correspond to an $\ell_\infty$-norm perturbation $\epsilon_\infty \approx 0.006$ for MNIST models.

![Figure 4](image-url)

Figure 4: Sample $\ell_1$- vs $\ell_\infty$-based minimally distorted adversaries for the MNIST $2 \times 50$ model. The true label ($j$) is ‘9,’ and the adversarial label ($k$) is ‘4.’

Table 3 presents results for the minimally distorted adversary problems. As input domains are unbounded, these problems are considerably more difficult than the above optimal adversary problems. Therefore, only smaller MNIST networks were manageable (with OBBT) for all formulations. Again, partition-based formulations consistently outperform big-M, solving more problems and in less time.

5 Conclusions

This work presented MILP formulations for ReLU NNs that balance having a tight relaxation and manageable size. The approach forms the convex hull over partitions of node inputs; we presented theoretical and computational motivations for obtaining good partitions for ReLU nodes. Furthermore, our approach expands the benefits of OBBT, which, unlike conventional MILP tools, can easily be parallelized. Results on three classes of optimization tasks show that the proposed formulations consistently outperform standard MILP encodings, allowing us to solve 25% more of the problems (average >2X speedup for solved problems). Implementations of the proposed formulations and partitioning strategies are available at [https://github.com/cog-imperial/](https://github.com/cog-imperial/PartitionedFormulations_NN)

Acknowledgments

This work was supported by Engineering & Physical Sciences Research Council (EPSRC) Fellowships to CT and RM (grants EP/T001577/1 and EP/P016871/1), an Imperial College Research Fellowship to CT, a Royal Society Newton International Fellowship (NIF/1/182194) to JK, a grant by the Swedish Cultural Foundation in Finland to JK, and a PhD studentship funded by BASF to AT.
References


[29] Gagandeep Singh, Jonathan Maurer, Christoph Müller, Matthew Mirman, Timon Gehr, Adrian Hoffmann, Petar Tsankov, Dana Drachsler Cohen, Markus Püschel, and Martin Vechev. ERAN verification dataset. URL http://github.com/eth-sri/eran


Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper’s contributions and scope? [Yes]

   (b) Did you describe the limitations of your work? [Yes] Section 3.3 describes how the proposed method introduces a hyperparameter and is strongly dependent on the chosen partitions (Figure 3 show that computational performance can suffer if these are poorly chosen). Section 4.2 details a case where the proposed formulation does not integrate well with default cuts in an off-the-shelf solver.

   (c) Did you discuss any potential negative societal impacts of your work? [N/A] No new adversarial methodologies or applications are presented; our test cases compare optimization formulations on standard instances.

   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes] Our work does not involve human subjects, and only openly available datasets (MNIST and CIFAR-10) are used.

2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes] Section 2.2 states mathematical preliminaries, including assumptions, on which the theoretical result are based.

   (b) Did you include complete proofs of all theoretical results? [Yes] Brief proofs are provided in Section 3.2 and extended proofs are in Appendices A.1–A.3

3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] Code to reproduce the proposed formulation is provided as supplemental material. This will be made available on Github upon publication.

   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] These are not central to our results, so they are provided in Appendix A.4.

   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [N/A] All optimization runs are deterministic.

   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] Computational resources are described in Appendix A.4.

4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] The MNIST [22] and CIFAR datasets [20] are cited.

   (b) Did you mention the license of the assets? [Yes] See Appendix A.4.

   (c) Did you include any new assets either in the supplemental material or as a URL? [N/A] Only optimization codes are produced, which are in supplemental material.

   (d) Did you discuss whether and how consent was obtained from people whose data you’re using/curating? [N/A] Datasets are openly available under CC BY-SA 3.0 (MNIST) and MIT License (CIFAR-10).

   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A]

5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]

   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]

   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]
A Appendix

A.1 Derivation of Proposed Formulation

Given the disjunction:

\[
\begin{align*}
& y = 0 \\
& \sum_{n=1}^{N} z_n + b \leq 0
\end{align*}
\]

The extended, or “multiple choice,” formulation for disjunctions [4] introduces auxiliary variables \(z^a_n\) and \(z^b_n\) for each \(z_n\):

\[
\begin{align*}
\sum_{i \in S_n} w_i x_i &= z^a_n + z^b_n \quad (29) \\
\sum_n z^a_n + \sigma b &\leq 0 \quad (30) \\
\sum_n z^b_n + (1 - \sigma) b &\geq 0 \quad (31) \\
y &= \sum_n z^b_n + (1 - \sigma) b \quad (32)
\end{align*}
\]

where again \(\sigma \in \{0, 1\}\). We observe that (29)–(34) exactly represents the ReLU node described by (12): substituting \(z_n = \sum_{i \in S_n} w_i x_i\) in the extended convex hull formulation [4] of the original disjunction (5), directly gives (29)–(34). Eliminating \(z^a_n\) via (29) results in our proposed formulation:

\[
\begin{align*}
\sum_n \left( \sum_{i \in S_n} w_i x_i - z^b_n \right) + \sigma b &\leq 0 \\
\sum_n z^b_n + (1 - \sigma) b &\geq 0 \\
y &= \sum_n z^b_n + (1 - \sigma) b \\
\sigma LB^a_n \leq z^a_n \leq \sigma UB^a_n, \quad \forall n = 1, ..., N \quad (33) \\
(1 - \sigma) LB^b_n \leq z^b_n \leq (1 - \sigma) UB^b_n, \quad \forall n = 1, ..., N \quad (34)
\end{align*}
\]

A.2 Derivation of Equivalent Non-Extended Formulation

We seek an equivalent (non-lifted) formulation to (35)–(39) without \(z^b_n\). The term \(\sum_n z^b_n\) can be isolated in (35)–(37), giving:

\[
\begin{align*}
\sum_n z^b_n \geq \sum_{i \in S_n} w_i x_i - \sigma b \quad (40) \\
\sum_n z^b_n \geq -(1 - \sigma) b \quad (41) \\
\sum_n z^b_n = y - (1 - \sigma) b \quad (42)
\end{align*}
\]

We observed in Section 3.1 that \([\min(\sum_{i \in S_n} w_i x_i), \max(\sum_{i \in S_n} w_i x_i)]\) are valid for both \(z^a_n\) and \(z^b_n\). Let \(UB_i\) and \(LB_i\) denote, respectively, valid upper and lower bounds of weighted input \(w_i x_i\).
Isolating $z_n^b$ in the bounds (38)–(39) gives:

$$z_n^b \leq \sum_{i \in S_n} w_i x_i - \sigma \sum_{i \in S_n} LB_i$$  \hspace{1cm} (43)

$$z_n^b \geq \sum_{i \in S_n} w_i x_i - \sigma \sum_{i \in S_n} UB_i$$  \hspace{1cm} (44)

$$z_n^b \leq (1 - \sigma) \sum_{i \in \tilde{S}_n} UB_i$$  \hspace{1cm} (45)

$$z_n^b \geq (1 - \sigma) \sum_{i \in \tilde{S}_n} LB_i$$  \hspace{1cm} (46)

**Fourier-Motzkin Elimination.** We will now eliminate the auxiliary variables using the above inequalities. Equations that appear in the non-extended formulation are marked in green. First, we examine the equations containing $\sum_n z_n^b$. Combining (40)+(42) and (41)+(42) gives, respectively:

$$y \geq w^T x + b$$  \hspace{1cm} (47)

$$y \geq 0$$  \hspace{1cm} (48)

Secondly, we examine equations containing only $z_n^b$. Combining (43)+(44) gives the trivial constraint $\sum_{i \in S_n} UB_i \geq \sum_{i \in \tilde{S}_n} LB_i$. Combining (45)+(46) gives the same constraint. The other combinations (43)+46 and (44)+45 recover the definition of lower and upper bounds on the partitions:

$$\sum_{i \in S_n} LB_i \leq \sum_{i \in \tilde{S}_n} w_i x_i \leq \sum_{i \in \tilde{S}_n} UB_i$$  \hspace{1cm} (49)

Now examining both equations containing $z_n^b$ and those containing $\sum_n z_n^b$, the combinations between (42) and (43)–(46) are most interesting. Here, each $z_n^b$ can be eliminated using either inequality (43) or (45). Note that combining these with (40) or (41) results in trivially redundant constraints. Defining $A$ as the indices of partitions for which (43) is used, and $\tilde{B}$ as the remaining indices:

$$y - (1 - \sigma)b \leq \sum_{n \in A} \sum_{i \in S_n} w_i x_i - \sigma \sum_{n \in A} \sum_{i \in \tilde{S}_n} LB_i + (1 - \sigma) \sum_{n \in \tilde{B}} \sum_{i \in S_n} UB_i$$  \hspace{1cm} (50)

Similarly, the inequalities of opposite sign can be chosen from either (43) or (46). Defining now $A'$ as the indices of partitions for which (44) is used, and $\tilde{B}'$ as the remaining indices:

$$y - (1 - \sigma)b \geq \sum_{n \in A'} \sum_{i \in S_n} w_i x_i - \sigma \sum_{n \in A'} \sum_{i \in \tilde{S}_n} UB_i + (1 - \sigma) \sum_{n \in \tilde{B}'} \sum_{i \in S_n} LB_i$$  \hspace{1cm} (51)

Defining $\mathcal{I}_j$ as the union of $S_n \forall n \in A$ and $\mathcal{I}'_j$ as the union of $S_n \forall n \in A'$, (50)–(51) become:

$$y \leq \sum_{i \in \mathcal{I}_j} w_i x_i - \sigma \sum_{i \in \mathcal{I}_j} LB_i + (1 - \sigma)(b + \sum_{i \in \mathcal{I} \setminus \mathcal{I}_j} UB_i)$$  \hspace{1cm} (52)

$$y \geq \sum_{i \in \mathcal{I}'_j} w_i x_i - \sigma \sum_{i \in \mathcal{I}'_j} UB_i + (1 - \sigma)(b + \sum_{i \in \mathcal{I} \setminus \mathcal{I}'_j} LB_i)$$  \hspace{1cm} (53)

The lower inequality (53) is redundant. Consider that $\sigma \in \{0, 1\}$. For $\sigma = 0$ and $\sigma = 1$, we recover:

$$y \geq \sum_{i \in \mathcal{I}'_j} w_i x_i + (b + \sum_{i \in \mathcal{I} \setminus \mathcal{I}_j} LB_i)$$  \hspace{1cm} (54)

$$y \geq \sum_{i \in \mathcal{I}'_j} (w_i x_i - UB_i)$$  \hspace{1cm} (55)

The former is less tight than $y \geq w^T x + b$, while the latter is less tight than $y \geq 0$. Finally, setting $\sigma' = 1 - \sigma$ in (52) gives:

$$y \leq \sum_{i \in \mathcal{I}_j} w_i x_i + (\sigma' - 1) \sum_{i \in \mathcal{I}_j} LB_i + \sigma'(b + \sum_{i \in \mathcal{I} \setminus \mathcal{I}_j} UB_i)$$  \hspace{1cm} (56)
The combination $\mathcal{I}_j = \emptyset$ removes all $x_i$, giving an upper bound for $y$:

$$y \leq \sigma'(b + \sum_{i \in \mathcal{I}} UB_i) \quad (57)$$

Combining all remaining equations gives a nonextended formulation:

$$y \leq \sum_{i \in \mathcal{I}_j} w_i x_i + \sigma'(b + \sum_{i \in \mathcal{I}_\mathcal{I}_j} UB_i) + (\sigma' - 1)(\sum_{i \in \mathcal{I}_j} LB_i) \quad (58)$$

$$y \geq w^T \mathbf{x} + b \quad (59)$$

$$y \leq \sigma' UB^0 \quad (60)$$

$$y \in [0, \infty) \quad (61)$$

A.3 Equivalence of $\eta$-Partition Formulation to Convex Hull

When $N = \eta$, it follows that $\mathcal{S}_n = \{n\}$, $\forall n = 1, \ldots, \eta$, and, consequently, $z_n = w_n x_n$. The auxiliary variables can be expressed in terms of $x_n$, rather than $z_n$ (i.e., $z^a_n = w_n x^a_n$ and $z^b_n = w_n x^b_n$). Rewriting (29)–(34) in this way gives:

$$x_n = x^a_n + x^b_n \quad (62)$$

$$w^T x^a + \sigma b \leq 0 \quad (63)$$

$$w^T x^b + (1 - \sigma) b \geq 0 \quad (64)$$

$$y = w^T x^b + (1 - \sigma) b \quad (65)$$

$$\frac{LB^a_n}{w_n} \leq x^a_n \leq \frac{UB^a_n}{w_n}, \quad \forall n = 1, \ldots, \eta \quad (66)$$

$$(1 - \sigma) \frac{LB^b_n}{w_n} \leq x^b_n \leq (1 - \sigma) \frac{UB^b_n}{w_n}, \quad \forall n = 1, \ldots, \eta \quad (67)$$

This formulation with a copy of each input—sometimes referred to as a “multiple choice” formulation—represents the convex hull of the node, e.g., see [3]; however, the overall model tightness still hinges on the bounds used for $x_n$, $n = 1, \ldots, \eta$. We note that (66)–(67) are presented here with $x^a_n$ and $x^b_n$ isolated for clarity. In practice, the bounds can be written without $w_n$ in their denominators, as in (13)–(17).

A.4 Experiment Details

Computational Set-Up. All computational experiments were performed on a 3.2 GHz Intel Core i7-8700 CPU (12 threads) with 16 GB memory. Models were implemented and solved using Gurobi v 9.1 [19] (academic license). The LP algorithm was set to dual simplex, cuts = 1 (moderate cut generation), TimeLimit = 3600s, and default termination criteria were used. We set parameter MIPFocus = 3 to ensure consistent solution approaches across formulations. Average times were computed as the arithmetic mean of solve times for instances solved by all formulations for a particular problem class. Thus, no time outs are included in the calculation of average solve times.

Neural Networks. We trained several NNs on MNIST [22] and CIFAR-10 [20], including both fully connected NNs and convolutional NNs (CNNs). MNIST (CC BY-SA 3.0) comprises a training set of 60,000 images and a test set of 10,000 images. CIFAR-10 (MIT License) comprises a training set of 50,000 images and a test set of 10,000 images. Dense models are denoted by $n_{\text{Layers}} \times n_{\text{Hidden}}$ and comprise $n_{\text{Layers}} \times n_{\text{Hidden}}$ hidden plus 10 output nodes. CNN2 is based on ‘ConvSmall’ of the ERAN dataset [29]: 

\[
\text{Conv2D}(16, (4,4), (2,2)), \text{Conv2D}(32, (4,4), (2,2)), \text{Dense}(100), \text{Dense}(10))
\]

CNN1 halves the channels in each convolutional layer: 

\[
\text{Conv2D}(8, (4,4), (2,2)), \text{Conv2D}(16, (4,4), (2,2)), \text{Dense}(100), \text{Dense}(10))
\]

The implementations of CNN1/CNN2 have 1,852/3,604 and 2,476/4,852 nodes for MNIST and CIFAR-10, respectively. NNs are implemented in PyTorch [24] and obtained using standard training (i.e., without regularization or methods to improve robustness). MNIST models were trained for ten epochs, and CIFAR-10 models were trained for 20 epochs, all using the Adadelta optimizer with default parameters.
A.5 Additional Computational Results

Comparing formulations. Proposition 1 suggests an equivalent, non-lifted formulation for each partition-based formulation. In contrast to our proposed formulation (13)-(17), which adds a linear (w.r.t. number of partitions $N$) number of variables, this non-lifted formulation involves adding an exponential (w.r.t. $N$) number of constraints. Table 4 computationally compares our proposed formulations against non-lifted formulations with equivalent relaxations on 100 optimal adversary instances of medium difficulty. These results clearly show the advantages of the proposed formulations; a non-lifted formulation equivalent to 20-partitions ($2^{20}$ constraints per node) cannot even be fully generated on our test machines due to its computational burden. Additionally, our formulations naturally enable OBBT on partitions. As described in Section 3.1, this captures dependencies among each partition without additional constraints.

<table>
<thead>
<tr>
<th>Partitions</th>
<th>Proposed Formulation</th>
<th>Non-Lifted Formulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N$</td>
<td>solvedavg.time(s)</td>
<td>solvedavg.time(s)</td>
</tr>
<tr>
<td>2</td>
<td>59</td>
<td>530.1</td>
</tr>
<tr>
<td>5</td>
<td>45</td>
<td>792.5</td>
</tr>
<tr>
<td>10</td>
<td>31</td>
<td>-</td>
</tr>
<tr>
<td>20</td>
<td>22</td>
<td>-</td>
</tr>
</tbody>
</table>

*The non-lifted formulation cannot be generated on our test machines.

As suggested in Proposition 1, the convex hull for a ReLU node involves an exponential (in terms of number of inputs) number of non-lifted constraints:

$$y \leq \sum_{i \in I_j} w_i x_i + \sigma(b + \sum_{i \in I \setminus I_j} UB_i) + (\sigma - 1)(\sum_{i \in I_j} LB_i), \quad \forall j = 1, \ldots, 2^n$$

(68)

where $UB_i$ and $LB_i$ denote the upper and lower bounds of $w_i x_i$. The set $I$ denotes the input indices $\{1, \ldots, \eta\}$, and the subset $I_j$ contains the union of the $j$-th combination of partitions $\{S_1, \ldots, S_\eta\}$.

Anderson et al. [3] provide a linear-time method for identifying the most-violated constraint in (68). First, the subset $\hat{I}$ is defined:

$$\hat{I} = \left\{ i \in I \mid w_i x_i < w_i \left(LB_{x_i}(1 - \sigma) + UB_{x_i}\sigma\right) \right\}$$

(69)

where $LB_{x_i}$ and $UB_{x_i}$ are, respectively, the lower and upper bounds of input $x_i$. Then, the constraint in (68) corresponding to the subset $\hat{I}$ is checked:

$$y \leq \sum_{i \in \hat{I}} w_i x_i + \sigma(b + \sum_{i \in I \setminus \hat{I}} UB_i) + (\sigma - 1)(\sum_{i \in \hat{I}} LB_i)$$

(70)

If this constraint (70) is violated, then it is the most violated in the family (68). If it is not, then no constraints in (68) are violated. This method can be used to solve the separation problem and generate cutting planes during optimization.

Figure 2 (left) shows that dynamically generated, convex-hull-based cuts only improve optimization performance when added at relatively low frequencies, if at all. Alternatively, De Palma et al. [13] only add the most violated cut (if one exists) at the initial LP solution to each node in the NN. Adding the cut before solving the MILP may produce different performance than dynamic cut generation: the De Palma et al. [13] approach to adding cuts includes the cut in the solver (Gurobi) pre-processing. Tables 5-8 give the results of the optimal adversary problem (cf. Table 1) with these single “most-violated” cuts added to each node. These cuts sometimes improve the big-M performance, but partition-based formulations still consistently perform best.
Table 5: Number of solved (in 3600s) optimal adversary problems for big-M vs $N = \{2, 4\}$ equal-size partitions. Columns marked “w/cuts” denote most violated convex-hull cut at root MILP node added to each NN node. Most solved for each set of problems is in bold. Green text indicates more solved compared to no convex-hull cuts.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_1$</th>
<th>Big-M w/ cuts</th>
<th>Big-M w/o cuts</th>
<th>2 Partitions w/ cuts</th>
<th>2 Partitions w/o cuts</th>
<th>4 Partitions w/ cuts</th>
<th>4 Partitions w/o cuts</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>2 x 50</td>
<td>5</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>2 x 50</td>
<td>10</td>
<td>98</td>
<td>97</td>
<td>97</td>
<td>98</td>
<td>98</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>2.5</td>
<td>95</td>
<td>92</td>
<td>100</td>
<td>100</td>
<td>97</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>5</td>
<td>51</td>
<td>50</td>
<td>55</td>
<td>59</td>
<td>45</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>CNN1*</td>
<td>0.25</td>
<td>91</td>
<td>68</td>
<td>85</td>
<td>86</td>
<td>83</td>
<td>87</td>
</tr>
<tr>
<td></td>
<td>CNN1*</td>
<td>0.5</td>
<td>7</td>
<td>2</td>
<td>18</td>
<td>16</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>2 x 100</td>
<td>5</td>
<td>45</td>
<td>62</td>
<td>65</td>
<td>69</td>
<td>61</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>10</td>
<td>11</td>
<td>23</td>
<td>30</td>
<td>28</td>
<td>26</td>
<td>34</td>
</tr>
</tbody>
</table>

*OBBT performed on all NN nodes

Table 6: Average solve times of optimal adversary problems for big-M vs $N = \{2, 4\}$ equal-size partitions. Columns marked “w/cuts” denote most violated convex-hull cut at root MILP node added to each NN node. Average times computed for problems solved by all 6 formulations. Lowest average time for each set of problems is in bold. Green text indicates lower time compared to no convex-hull cuts.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_\infty$</th>
<th>Big-M w/ cuts</th>
<th>Big-M w/o cuts</th>
<th>2 Partitions w/ cuts</th>
<th>2 Partitions w/o cuts</th>
<th>4 Partitions w/ cuts</th>
<th>4 Partitions w/o cuts</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>2 x 50</td>
<td>5</td>
<td>45.3</td>
<td>57.6</td>
<td>60.3</td>
<td>42.7</td>
<td>86.0</td>
<td>83.9</td>
</tr>
<tr>
<td></td>
<td>2 x 50</td>
<td>10</td>
<td>285.2</td>
<td>431.8</td>
<td>305.0</td>
<td>270.4</td>
<td>404.5</td>
<td>398.4</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>2.5</td>
<td>505.2</td>
<td>525.2</td>
<td>309.3</td>
<td>285.1</td>
<td>597.4</td>
<td>553.9</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>5</td>
<td>930.5</td>
<td>1586.0</td>
<td>691.7</td>
<td>536.9</td>
<td>1131.4</td>
<td>1040.3</td>
</tr>
<tr>
<td></td>
<td>CNN1*</td>
<td>0.25</td>
<td>420.7</td>
<td>1067.9</td>
<td>567.2</td>
<td>609.4</td>
<td>784.6</td>
<td>817.1</td>
</tr>
<tr>
<td></td>
<td>CNN1*</td>
<td>0.5</td>
<td>1318.2</td>
<td>2293.2</td>
<td>1586.7</td>
<td>1076.0</td>
<td>1100.9</td>
<td>2161.2</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>2 x 100</td>
<td>5</td>
<td>1739.2</td>
<td>1914.6</td>
<td>595.1</td>
<td>1192.4</td>
<td>834.8</td>
<td>538.4</td>
</tr>
<tr>
<td></td>
<td>2 x 100</td>
<td>10</td>
<td>1883.3</td>
<td>1908.9</td>
<td>1573.4</td>
<td>1621.4</td>
<td>1767.44</td>
<td>2094.5</td>
</tr>
</tbody>
</table>

*OBBT performed on all NN nodes

Table 7: Number of solved (in 3600s) verification problems for big-M vs $N = \{2, 4\}$ equal-size partitions. OBBT was performed for all partitions, and columns marked “w/cuts” denote most violated convex-hull cut at root MILP node added to each NN node. Most solved for each set of problems is in bold. Green text indicates more solved compared to no convex-hull cuts.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_\infty$</th>
<th>Big-M w/ cuts</th>
<th>Big-M w/o cuts</th>
<th>2 Partitions w/ cuts</th>
<th>2 Partitions w/o cuts</th>
<th>4 Partitions w/ cuts</th>
<th>4 Partitions w/o cuts</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>CNN1</td>
<td>0.050</td>
<td>78</td>
<td>82</td>
<td>91</td>
<td>92</td>
<td>89</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.075</td>
<td>25</td>
<td>30</td>
<td>53</td>
<td>52</td>
<td>45</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.075</td>
<td>16</td>
<td>21</td>
<td>34</td>
<td>36</td>
<td>11</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.100</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>CNN1</td>
<td>0.007</td>
<td>98</td>
<td>99</td>
<td>100</td>
<td>100</td>
<td>99</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.010</td>
<td>80</td>
<td>98</td>
<td>94</td>
<td>100</td>
<td>89</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.007</td>
<td>78</td>
<td>80</td>
<td>94</td>
<td>95</td>
<td>73</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.010</td>
<td>29</td>
<td>40</td>
<td>74</td>
<td>72</td>
<td>34</td>
<td>35</td>
</tr>
</tbody>
</table>

*OBBT performed on all NN nodes
Table 8: Average solve times of verification problems for big-M vs $N = \{2, 4\}$ equal-size partitions. OBBT was performed for all partitions, and columns marked “w/cuts” denote most violated convex-hull cut at root MILP node added to each NN node. Average times computed for problems solved by all 6 formulations. Lowest average time for each set of problems is in bold. Green text indicates lower time compared to no convex-hull cuts.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>$\epsilon_1$</th>
<th>Big-M 2 Partitions</th>
<th>4 Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>w/ cuts</td>
<td>w/o cuts</td>
</tr>
<tr>
<td>MNIST</td>
<td>CNN1</td>
<td>0.050</td>
<td>133.7</td>
<td>92.2</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.075</td>
<td>504.7</td>
<td>239.0</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.075</td>
<td>637.8</td>
<td>414.8</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>CNN1</td>
<td>0.007</td>
<td>102.5</td>
<td>74.7</td>
</tr>
<tr>
<td></td>
<td>CNN1</td>
<td>0.010</td>
<td>599.4</td>
<td>66.5</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.007</td>
<td>308.3</td>
<td>262.7</td>
</tr>
<tr>
<td></td>
<td>CNN2</td>
<td>0.010</td>
<td>525.9</td>
<td>394.2</td>
</tr>
</tbody>
</table>

*OBBT performed on all NN nodes