

E-Companion to “On Integer Programming for the Binarized Neural Network Verification Problem”

Woojin Kim

Department of Mathematics, University of Wisconsin-Madison, wkim73@wisc.edu

James R. Luedtke

Department of Industrial and Systems Engineering, University of Wisconsin-Madison, jim.luedtke@wisc.edu

Abstract. This e-companion contains the proofs, implementation details, and additional computational results supporting the paper “On Integer Programming for the Binarized Neural Network Verification Problem.” Equations, results, sections, and tables referred to without the prefix “A” are numbered as in the main paper.

Key words: Integer Programming, Binarized Neural Networks, Verification

A. Appendix

A.1. Proof of Lemma 1

We prove following Lemma 1 on the formulation for the layer propagation constraint (3a) introduced in Section 2.1.1 with the definition on LB_i^ℓ , UB_i^ℓ , and R_i^ℓ for $\ell \in [L]$ and $i \in N^\ell$.

LEMMA 1. *Each $(\mathbf{x}^0, \mathbf{x}^1) \in X^0 \times \{0, 1\}^{n^1}$ satisfies (3a) for $\ell = 1$ if and only if it satisfies the following inequalities:*

$$2 \sum_{j \in N^0} W_{ij}^1 x_j^0 \geq \left(R_i^1 - LB_i^1 + \frac{1}{q} \right) x_i^1 + LB_i^1, \quad \forall i \in N^1, \quad (1)$$

$$2 \sum_{j \in N^0} W_{ij}^1 x_j^0 \leq \left(UB_i^1 - R_i^1 + \frac{1}{q} \right) x_i^1 + \left(R_i^1 - \frac{1}{q} \right), \quad \forall i \in N^1. \quad (2)$$

For $\ell \in \{2, \dots, L\}$, $(\mathbf{x}^{\ell-1}, \mathbf{x}^\ell) \in \{0, 1\}^{n^{\ell-1}} \times \{0, 1\}^{n^\ell}$ satisfies (3a) if and only if it satisfies the following inequalities:

$$2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} \geq (R_i^\ell - \text{LB}_i^\ell + 1)x_i^\ell + \text{LB}_i^\ell, \quad \forall i \in N^\ell, \quad (3)$$

$$2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} \leq (\text{UB}_i^\ell - R_i^\ell + 1)x_i^\ell + (R_i^\ell - 1), \quad \forall i \in N^\ell. \quad (4)$$

Proof of Lemma 1. The following constraints are equivalent to (3a):

$$\begin{aligned} x_i^\ell = 1 &\Rightarrow a_i^\ell(\mathbf{x}^{\ell-1}) \geq 0 \\ &\Leftrightarrow 2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} \geq \sum_{j \in N^{\ell-1}} W_{ij}^\ell - b_i^\ell, \quad \forall \ell \in [L], i \in N^\ell, \\ x_i^\ell = 0 &\Rightarrow a_i^\ell(\mathbf{x}^{\ell-1}) < 0 \\ &\Leftrightarrow 2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} < \sum_{j \in N^{\ell-1}} W_{ij}^\ell - b_i^\ell, \quad \forall \ell \in [L], i \in N^\ell. \end{aligned}$$

For $i \in N^1$ and $j \in N^0$, $W_{ij}^1 x_j^0$ is a multiple of $\frac{1}{q}$. Also, $R_i^1 + \frac{1}{q}$ is the smallest multiple of $\frac{2}{q}$ not smaller than $\sum_{j \in N^0} W_{ij}^1 - b_i^1$, and $R_i^1 - \frac{1}{q}$ is the largest multiple of $\frac{2}{q}$ smaller than $\sum_{j \in N^0} W_{ij}^1 - b_i^1$. Hence, the above constraints can be written as follows for $\ell = 1$:

$$\begin{aligned} x_i^1 = 1 &\Rightarrow 2 \sum_{j \in N^0} W_{ij}^1 x_j^0 \geq R_i^1 + \frac{1}{q}, \quad \forall i \in N^1, \\ x_i^1 = 0 &\Rightarrow 2 \sum_{j \in N^0} W_{ij}^1 x_j^0 \leq R_i^1 - \frac{1}{q}, \quad \forall i \in N^1. \end{aligned}$$

For $\ell \in \{2, \dots, L\}$, $i \in N^\ell$, and $j \in N^{\ell-1}$, $W_{ij}^\ell x_j^{\ell-1}$ is an integer. Also, $R_i^\ell + 1$ is the smallest even integer not smaller than $\sum_{j \in N^{\ell-1}} W_{ij}^\ell - b_i^\ell$, and $R_i^\ell - 1$ is the largest even integer smaller than $\sum_{j \in N^{\ell-1}} W_{ij}^\ell - b_i^\ell$. Hence, the above constraints can be written as follows for $\ell \in \{2, \dots, L\}$:

$$\begin{aligned} x_i^\ell = 1 &\Rightarrow 2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} \geq R_i^\ell + 1, \quad \forall i \in N^\ell, \\ x_i^\ell = 0 &\Rightarrow 2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1} \leq R_i^\ell - 1, \quad \forall i \in N^\ell. \end{aligned}$$

For $\ell \in [L]$, $i \in N^\ell$, and $j \in N^{\ell-1}$, $W_{ij}^\ell \in \{-1, 0, 1\}$ and $x_j^{\ell-1} \in [0, 1]$. Hence, LB_i^ℓ is a lower bound for $2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1}$ because it is minus two times the number of -1 in $\{W_{ij}^\ell : j \in N^{\ell-1}\}$. Also, UB_i^ℓ is an upper bound for $2 \sum_{j \in N^{\ell-1}} W_{ij}^\ell x_j^{\ell-1}$ because it is two times the number of 1 in $\{W_{ij}^\ell : j \in N^{\ell-1}\}$.

By exploiting this lower bound and upper bound, it can be concluded that $(\mathbf{x}^0, \mathbf{x}^1) \in X^0 \times \{0, 1\}^{n^1}$ satisfies (3a) if and only if it satisfies (1) and (2), and $(\mathbf{x}^{\ell-1}, \mathbf{x}^\ell) \in \{0, 1\}^{n^{\ell-1}} \times \{0, 1\}^{n^\ell}$ satisfies (3a) if and only if it satisfies (3) and (4) for $\ell \in \{2, \dots, L\}$. $\square$

A.2. Proof of Lemma 2

Proof. First, from a feasible solution $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ to (3) where t is considered as a decision variable, we obtain a feasible solution to (13) with the same objective value. From $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$, $\hat{\mathbf{y}}$ is defined as $q\hat{\mathbf{x}}^0$. Also, $\hat{z}_t$ is defined as $\mathbf{1}_{\{\hat{t}\}}(t)$, and $\hat{v}_{ti}$ is defined as $\hat{z}_t \hat{x}_i^L$.

By Lemma 1, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ satisfies (1)-(2) and (3)-(4) for $\ell \in \{2, \dots, L\}$. By the definition of $\hat{\mathbf{y}}$, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ satisfies (9)-(10) and (13f). By the definition of $\hat{\mathbf{z}}$ and $\hat{\mathbf{v}}$, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ satisfies (13a)-(13b) and (13g)-(13h). Also, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ satisfies (13c) because $\hat{\mathbf{z}}$ and $\hat{\mathbf{x}}^L$ are binary, so $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ is a feasible solution to (13).

The definitions of $\hat{\mathbf{z}}$ and $\hat{\mathbf{v}}$ imply $\hat{z}_t = 0$ for $t \neq \hat{t}$, $\hat{z}_{\hat{t}} = 1$, and $\hat{v}_{ti} = \hat{z}_t \hat{x}_i^L$. With this implication, the objective value of $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ in (3) is same as the objective value of $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ in (13) by following steps:

$$\begin{aligned}
 a_i^{L+1}(\hat{\mathbf{x}}^L) - a_i^{L+1}(\hat{\mathbf{x}}^L) &= \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \hat{z}_t (a_i^{L+1}(\hat{\mathbf{x}}^L) - a_i^{L+1}(\hat{\mathbf{x}}^L)) \\
 &= \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \hat{z}_t \left(\sum_{i \in N^L} (W_{ti}^{L+1} - W_{\hat{t}i}^{L+1})(2\hat{x}_i^L - 1) + (b_t^{L+1} - b_{\hat{t}}^{L+1}) \right) \\
 &= \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \sum_{i \in N^L} 2(W_{ti}^{L+1} - W_{\hat{t}i}^{L+1}) \hat{z}_t \hat{x}_i^L \\
 &\quad + \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \left(- \sum_{i \in N^L} (W_{ti}^{L+1} - W_{\hat{t}i}^{L+1}) + (b_t^{L+1} - b_{\hat{t}}^{L+1}) \right) \hat{z}_t \\
 &= \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \sum_{i \in N^L} 2(W_{ti}^{L+1} - W_{\hat{t}i}^{L+1}) \hat{v}_{ti} \\
 &\quad + \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \left(- \sum_{i \in N^L} (W_{ti}^{L+1} - W_{\hat{t}i}^{L+1}) + (b_t^{L+1} - b_{\hat{t}}^{L+1}) \right) \hat{z}_t.
 \end{aligned} \tag{5}$$

Next, from a feasible solution $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ to (13), we obtain a feasible solution to (3) with the same objective value where t is considered as a decision variable. From $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$, $\hat{t}$ is defined as t satisfying $\hat{z}_t = 1$, whose uniqueness is guaranteed by (13a) and (13g).

By (1)-(4) and Lemma 1, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ satisfies the layer propagation constraints (3a). By (9)-(11), (13d), and (13f), $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ satisfies the input conditions (3b)-(3c). Hence, $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ is a feasible solution to (3).

By (5), the objective value of $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{\mathbf{y}}, \hat{\mathbf{z}}, \hat{\mathbf{v}})$ in (13) is same as the objective value of $(\hat{\mathbf{x}}^0, \dots, \hat{\mathbf{x}}^L, \hat{t})$ in (3). The first equality holds because $\hat{z}_t = 0$ for $t \neq \hat{t}$, and $\hat{z}_{\hat{t}} = 1$. The last equality

holds because $\hat{v}_{ti} = \hat{z}_t \hat{x}_i^L$. For $t \neq \hat{t}$, $\hat{v}_{ti} \geq 0$ by (13h), and $\hat{v}_{ti} \leq \hat{z}_t = 0$ by (13c), so $\hat{v}_{ti} = 0 = \hat{z}_t \hat{x}_i^L$. Also, $\hat{v}_{\hat{t}i} = \hat{z}_{\hat{t}} \hat{x}_i^L$ by following steps:

$$\begin{aligned} \hat{v}_{\hat{t}i} &= \sum_{t \in N^{L+1} \setminus \{\hat{t}\}} \hat{v}_{ti} && \text{(For all } t \text{ other than } \hat{t}, \hat{v}_{ti} = 0) \\ &= \hat{x}_i^L && \text{(By (13b))} \\ &= \hat{z}_{\hat{t}} \hat{x}_i^L. \end{aligned}$$

For these reasons, (13) is equivalent to (3). $\square$

A.3. Proof of Convex Hull Characterization for a Single Neuron

We prove Theorem 1 on the characterization for the convex hull (14) for a single neuron introduced in Section 2.3, which is an extension of the main result in Han and Gómez (2021). To simplify the statement of this theorem, $\ell \in \{2, \dots, L\}$ and $i \in N^\ell$ are fixed, and the following notations are defined for $j \in N^{\ell-1}$ with LB_i^ℓ , UB_i^ℓ , and R_i^ℓ defined in Section 2.1.1:

$$\begin{aligned} \mathbf{x} &:= \mathbf{x}^{\ell-1}, \\ u &:= x_i^\ell, \\ w_j &:= W_{ij}^\ell, \\ \text{LB} &:= \text{LB}_i^\ell = \sum_{j \in N^{\ell-1}} (W_{ij}^\ell - |W_{ij}^\ell|), \\ \text{UB} &:= \text{UB}_i^\ell = \sum_{j \in N^{\ell-1}} (W_{ij}^\ell + |W_{ij}^\ell|), \\ R &:= R_i^\ell = 2 \left\lceil \frac{\sum_{j \in N^{\ell-1}} W_{ij}^\ell - b_i^\ell}{2} \right\rceil - 1. \end{aligned}$$

Then, this theorem can be restated as follows:

Theorem 1 (Restated) *The set of $(\mathbf{x}, u) \in [0, 1]^{n^{\ell-1}} \times [0, 1]$ satisfying the following inequalities for all $J \subset \{j \in N^{\ell-1} : w_j \neq 0\}$ is (14):*

$$\sum_{j \in J} (w_j(2x_j - 1) - (2u - 1)) \geq (R - \text{UB} + 1)u, \quad (6a)$$

$$\sum_{j \in J} (w_j(2x_j - 1) - (2u - 1)) \leq (R - \text{LB} - 1)(-u + 1). \quad (6b)$$

Proof. Consider the following sets:

$$X^+ = \{(\mathbf{x}, 1) : \mathbf{x} \in \{0, 1\}^{n^{\ell-1}}, a_i^\ell(\mathbf{x}) \geq 0\},$$

$$X^- = \{(\mathbf{x}, 0) : \mathbf{x} \in \{0, 1\}^{n^{\ell-1}}, a_i^\ell(\mathbf{x}) < 0\}.$$

By the proof of Lemma 1, X^+ and X^- can be written as follows:

$$X^+ = \left\{ (\mathbf{x}, 1) : \mathbf{x} \in \{0, 1\}^{n^{\ell-1}}, \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j \geq \frac{R+1}{2} \right\},$$

$$X^- = \left\{ (\mathbf{x}, 0) : \mathbf{x} \in \{0, 1\}^{n^{\ell-1}}, \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j \leq \frac{R-1}{2} \right\}.$$

By exploiting total unimodularity of the constraints defining X^+ and X^- arising from $w_j \in \{-1, 0, 1\}$ and $\frac{R+1}{2} \in \mathbb{Z}$, $\text{conv}(X^+)$ and $\text{conv}(X^-)$ can be obtained as follows:

$$\text{conv}(X^+) = \left\{ (\mathbf{x}, 1) : \mathbf{x} \in [0, 1]^{n^{\ell-1}}, \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j \geq \frac{R+1}{2} \right\},$$

$$\text{conv}(X^-) = \left\{ (\mathbf{x}, 0) : \mathbf{x} \in [0, 1]^{n^{\ell-1}}, \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j \leq \frac{R-1}{2} \right\}.$$

These convex hulls can be used to describe (14) as follows where the last statement holds because of compactness of $\text{conv}(X^+)$ and $\text{conv}(X^-)$ arising from finiteness of X^+ and X^- :

$$\begin{aligned} \text{conv}(X^+ \cup X^-) &= \text{conv}(\text{conv}(X^+) \cup \text{conv}(X^-)) \\ &= \text{clconv}(\text{conv}(X^+) \cup \text{conv}(X^-)). \end{aligned}$$

By Balas (1985)'s work on disjunctive programming, $(\mathbf{x}, u) \in \mathbb{R}^{n^{\ell-1}} \times \mathbb{R}$ is in (14) if and only if there exist $(\mathbf{x}^+, u^+), (\mathbf{x}^-, u^-) \in \mathbb{R}^{n^{\ell-1}} \times \mathbb{R}$ and $\lambda \in [0, 1]$ satisfying the following inequalities:

$$\begin{aligned} \mathbf{x} &= \mathbf{x}^+ + \mathbf{x}^-, \\ u &= u^+ + u^-, \\ 0 &\leq \mathbf{x}^+ \leq \lambda \cdot \mathbf{1}, \\ u^+ &= \lambda, \\ 2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j^+ &\geq (R+1)\lambda, \\ 0 &\leq \mathbf{x}^- \leq (1-\lambda) \cdot \mathbf{1}, \\ u^- &= 0, \\ 2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j^- &\leq (R-1)(1-\lambda). \end{aligned}$$

Existence of $(\mathbf{x}^+, u^+), (\mathbf{x}^-, u^-) \in \mathbb{R}^{n^{\ell-1}} \times \mathbb{R}$ and $\lambda \in [0, 1]$ satisfying the above inequalities is identical to existence of $\mathbf{x}^+ \in \mathbb{R}^{n^{\ell-1}}$ satisfying the following inequalities, which are provided by substituting u^- with 0, u^+ and λ with u , and $\mathbf{x}^-$ with $\mathbf{x} - \mathbf{x}^+$:

$$-\frac{u}{2} \cdot \mathbf{1} \leq \mathbf{x}^+ - \frac{u}{2} \cdot \mathbf{1} \leq \frac{u}{2} \cdot \mathbf{1}, \quad (7)$$

$$-\left(\frac{1-u}{2}\right) \cdot \mathbf{1} \leq \mathbf{x} - \mathbf{x}^+ - \left(\frac{1-u}{2}\right) \cdot \mathbf{1} \leq \left(\frac{1-u}{2}\right) \cdot \mathbf{1}, \quad (8)$$

$$2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j^+ \geq (R+1)u, \quad (9)$$

$$2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j^+ \geq 2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j - (R-1)(1-u). \quad (10)$$

For j satisfying $w_j \neq 0$, (7)-(8) are equivalent to the following inequalities because $w_j \in \{-1, 1\}$:

$$\begin{aligned} -\frac{u}{2} \cdot \mathbf{1} &\leq w_j \left(\mathbf{x}^+ - \frac{u}{2} \cdot \mathbf{1} \right) \leq \frac{u}{2} \cdot \mathbf{1}, \\ -\frac{(1-u)}{2} \cdot \mathbf{1} &\leq w_j \left(\mathbf{x} - \mathbf{x}^+ - \frac{1-u}{2} \cdot \mathbf{1} \right) \leq \frac{(1-u)}{2} \cdot \mathbf{1}. \end{aligned}$$

By replacing $w_j x_j^+$ with its maximum attained from the above inequalities in (9)-(10) and employing Fourier-Motzkin Elimination to (7)-(8) to remove $\mathbf{x}^+ - \frac{u}{2}$, existence of $\mathbf{x}^+ \in \mathbb{R}^{n^{\ell-1}}$ satisfying (7)-(10) is equivalent to whether the following inequalities are satisfied:

$$\begin{aligned} \max \left(-\frac{u}{2}, x_j + \frac{u}{2} - 1 \right) &\leq \min \left(\frac{u}{2}, x_j - \frac{u}{2} \right), \quad \forall j \in N^{\ell-1}, \\ \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} \min((w_j + 1)u, 2w_j x_j + (-w_j + 1)(1-u)) &\geq (R+1)u, \\ \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} \min((w_j + 1)u, 2w_j x_j + (-w_j + 1)(1-u)) &\geq 2 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} w_j x_j - (R-1)(1-u). \end{aligned}$$

These inequalities are satisfied if and only if the following inequalities are satisfied because $|w_j| = 1$ if $w_j \neq 0$, $\sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} (-w_j + 1) = \sum_{j \in N^{\ell-1}} (-w_j + |w_j|) = -\text{LB}$, and $\sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} (w_j + 1) = \sum_{j \in N^{\ell-1}} (w_j + |w_j|) = \text{UB}$.

$|w_j|) = \text{UB}$:

$$\begin{aligned}
 0 &\leq x_j \leq 1, \quad \forall j \in N^{\ell-1}, \\
 0 &\leq u \leq 1, \\
 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} \min(w_j(2x_j - 1), 2u - 1) &\geq (R - \text{LB} + 1)u - \sum_{j \in N^{\ell-1}} |w_j|, \\
 \sum_{\substack{j \in N^{\ell-1} \\ w_j \neq 0}} \max(w_j(2x_j - 1), 2u - 1) &\leq (\text{UB} - R + 1)u + R - \sum_{j \in N^{\ell-1}} w_j - 1.
 \end{aligned}$$

If $w_j \neq 0$, $|w_j| = 1$, so $|\{j \in N^{\ell-1} : w_j \neq 0\}| = \sum_{j \in N^{\ell-1}} |w_j|$. With this equality, by replacing min and max in the last two inequalities with linear expressions involving $J \subset \{j \in N^{\ell-1} : w_j \neq 0\}$, the set of $(\mathbf{x}, u)$ satisfying the last two inequalities can be written as the set of $(\mathbf{x}, u)$ satisfying the following linear inequalities for all $J \subset \{j \in N^{\ell-1} : w_j \neq 0\}$:

$$\begin{aligned}
 \sum_{j \in J} (w_j(2x_j - 1) - (2u - 1)) &\geq (R - \text{LB} + 1)u - \sum_{j \in N^{\ell-1}} |w_j| - \left(\sum_{j \in N^{\ell-1}} |w_j| \right) (2u - 1), \\
 \sum_{j \in J} (w_j(2x_j - 1) - (2u - 1)) &\leq (\text{UB} - R + 1)u + R - \sum_{j \in N^{\ell-1}} w_j - 1 - \left(\sum_{j \in N^{\ell-1}} |w_j| \right) (2u - 1).
 \end{aligned}$$

These inequalities are equivalent to (6a) and (6b) because $\sum_{j \in N^{\ell-1}} |w_j| = \frac{\text{UB} - \text{LB}}{2}$ and $\sum_{j \in N^{\ell-1}} (w_j - |w_j|) = \text{LB}$, so (14) is the set of $(\mathbf{x}, u) \in [0, 1]^{N^{\ell-1}} \times [0, 1]$ satisfying (6) for all $J \subset \{j \in N^{\ell-1} : w_j \neq 0\}$. $\square$

A.4. Implementation Details for Infinity-norm and 2-norm

We explain implementation details for the case that the maximum perturbation from $\bar{\mathbf{x}}$ is defined using an ℓ_∞ norm or ℓ_2 norm. These details are about how to solve the IP subproblem (18) without an IP solver in the case of $\ell = 1$ and how to implement the input perturbation constraint (11).

We first consider solving (18) for the case of layer $\ell = 1$ and $p = \infty$. In this case, the optimal solution is obtained by setting x_j^0 to $\min(\bar{x}_j + \epsilon, 1)$ for j satisfying $c_i W_{ij}^1 = 1$, setting x_j^0 to $\max(\bar{x}_j - \epsilon, 0)$ for j satisfying $c_i W_{ij}^1 = -1$, and setting x_j^0 to $\bar{x}_j$ for j satisfying $c_i W_{ij}^1 = 0$. All constraints defining X^0 are of the form $|x_j^0 - \bar{x}_j| \leq \epsilon$, so this solution is feasible, and it immediate that no other solution can yield a better objective value.

We next consider solving (18) for the case of layer $\ell = 1$ and $p = 2$. First, observe that given a feasible solution $\hat{\mathbf{x}}^0 \in \frac{1}{q} \mathbb{Z}_+^{n^0} \cap [0, 1]^{n^0}$ to (18), if for some $j \in N^0$ it holds that $c_i W_{ij}^1 (\hat{x}_j^0 - \bar{x}_j) \leq 0$, then another feasible solution with the same or better objective value can be obtained by replacing

$\hat{x}_j^0$ with $\bar{x}_j$. Hence, we can restrict our search for an optimal solution of (18) to solutions $\hat{\mathbf{x}}^0$ that satisfy:

$$\begin{aligned}\hat{x}_j^0 &\geq \bar{x}_j, & \text{for } j \text{ such that } c_i W_{ij}^1 = 1, \\ \hat{x}_j^0 &\leq \bar{x}_j, & \text{for } j \text{ such that } c_i W_{ij}^1 = -1, \\ \hat{x}_j^0 &= \bar{x}_j, & \text{for } j \text{ such that } W_{ij}^1 = 0.\end{aligned}$$

Let $N_0^+ = \{j \in N_0 : W_{ij}^1 \neq 0\}$. Thus, we can restrict our attention to solutions defined by a vector $z \in \{0, 1, \dots, q\}^{N_0^+}$ as follows:

$$\hat{x}_j^0(z) = \begin{cases} \min(\bar{x}_j + \frac{z_j}{q}, 1) & \text{if } c_i W_{ij}^1 = 1, \\ \max(\bar{x}_j - \frac{z_j}{q}, 0) & \text{if } c_i W_{ij}^1 = -1, \\ \bar{x}_j & \text{if } W_{ij}^1 = 0. \end{cases}$$

Observe that the objective in (18) and the expression $\|\hat{\mathbf{x}}(z) - \bar{\mathbf{x}}\|_2$ are monotone increasing in z , and hence an optimal solution will be such that increasing z_j for any $j \in N_0^+$ would be infeasible. Next, for $z \in \{0, 1, \dots, q\}^{N_0^+}$, define the set

$$N_0^S(z) = \left\{ j \in N_0^+ : (c_i W_{ij}^1 = 1 \text{ and } \hat{x}_j^0(z) \leq 1 - 1/q) \text{ or } (c_i W_{ij}^1 = -1 \text{ and } \hat{x}_j^0(z) \geq 1/q) \right\}.$$

If there exists $z \in \{0, 1, \dots, q\}^{N_0^+}$ in which $\hat{\mathbf{x}}(z)$ is feasible to (18) and $N_0^S(z) = \emptyset$, then $\hat{\mathbf{x}}(z)$ is optimal to (18) since this solution obtains the best possible objective. Otherwise, we claim that there exists an optimal solution $\hat{\mathbf{x}}(z)$ that satisfies:

$$\max\{z_j : j \in N_0^S(z)\} - \min\{z_j : j \in N_0^S(z)\} \leq 1.$$

Consider a solution that violates this condition. Another feasible solution with the same objective value can be obtained by decreasing z_{j_1} by one and increasing z_{j_2} by one, where $j_1 \in \arg \max\{z_j : j \in N_0^S(z)\}$ and $j_2 \in \arg \min\{z_j : j \in N_0^S(z)\}$. Repeating this process will eventually yield a vector z which satisfies this condition since there only finitely many elements achieving the max and min in the condition, and an element will necessarily be removed from one or the other as long as the max is at least two larger than the min.

These arguments imply that an optimal solution to (18) can be obtained by first finding the maximum m such that the solution $\hat{\mathbf{x}}(z)$ satisfies $\|\hat{\mathbf{x}}(z) - \bar{\mathbf{x}}\|_2 \leq \epsilon$, where $z_j = m$ for $j \in N_0^+$. Having found this solution (e.g., by binary search), one would then iteratively select some $j \in N_0^S(z)$ and increase z_j , and repeat (without selecting any j more than once) until no more can be increased without violating $\|\hat{\mathbf{x}}(z) - \bar{\mathbf{x}}\|_2 \leq \epsilon$.

Finally, we describe how the constraint (11) is formulated when using a MIP solver to solve the verification problem in the case of $p = 2$. We define a decision variable u_j to represent $|x_j^0 - \bar{x}_j|$

Norm	# of instances	Many-IP	1-IP
ℓ_∞	47	143.1(16)	78.1(6)
ℓ_2	17	502.9(12)	311.6(2)

Table 1 Verification time (seconds) of Many-IP and 1-IP for ℓ_∞ norm and ℓ_2 norm

for each $j \in N^0$. The following inequalities are added as constraints because (11) is satisfied if and only if there exists $\mathbf{u} \in \mathbb{R}_+^{n^0}$ satisfying the following inequalities:

$$\begin{aligned} u_j &\geq x_j^0 - \bar{x}_j, \quad \forall j \in N^0, \\ u_j &\geq -x_j^0 + \bar{x}_j, \quad \forall j \in N^0, \\ \sum_{j \in N^0} u_j^2 &\leq \epsilon^2. \end{aligned}$$

We remark that we found through preliminary empirical study that this formulation technique was computationally superior to the more direct approach of simply formulating the constraint as follows:

$$\sum_{j \in N_0} (x_j^0 - \bar{x}_j)^2 \leq \epsilon^2.$$

A.5. Detailed Computational Results for Infinity-norm and 2-norm

We present more detailed computational results for the case that the maximum perturbation from $\bar{\mathbf{x}}$ is defined using an ℓ_∞ norm or ℓ_2 norm. Test instances for these cases are formed with Network 5 in Table 1, $\bar{\mathbf{x}}$, and ϵ that are chosen as explained in Section 4.1.

We first investigate the time required to use the IP problem (13) (resp. (12) for all t) to solve the verification problem. The shifted geometric mean (with a shift of 1) of times over all instances tested by both IP method Many-IP and 1-IP is computed for each method and displayed in Table 1 for the case of $p = \infty$ and $p = 2$, along with the number of test instances. For Many-IP, the number in parenthesis is the number of test instances where the time limit is hit in solving (12) for at least one t . For 1-IP, the number in parenthesis is the number of test instances where the time limit is hit in solving (13). We find that 1-IP's verification times are smaller than Many-IP's, indicating that our technique for obtaining a linear objective also leads to faster BNN verification in the case of $p = \infty$ and $p = 2$.

Table 2 presents results analogous to those of Table 6 in the main sections, but on instances with $p = \infty$. We find that in this case, neither 1-IP+HG nor 1-IP+Fix yield improvement compared to 1-IP, so generating (15) and variable fixings do not improve BNN verification. Generating variable fixings decreases LP gaps, but this decrease does not lead to more effective BNN verification in the case of $p = \infty$. On the other hand, 1-IP+Fix+2Var yields improvement compared to the other IP methods based on 1-IP. It implies that our technique for generating layerwise derived valid inequalities, mainly two-variable inequalities, also leads to more efficient BNN verification in the case of $p = \infty$.

	1-IP	1-IP +HG	1-IP +Fix	1-IP +Fix +2Var
Preprocessing time (seconds)	0.0	10.6	7.5	27.4
Verification time (seconds)	98.6	147.2	100.6	44.9
# of solved instances (veri.)	38	35	37	44
# of nodes (veri.)	1297.6	1283.6	1265.3	17.8
Optimization time (seconds)	115.5	178.4	117.5	57.4
# of solved instances (opt.)	37	33	37	42
# of nodes (opt.)	2182.8	2587.9	2133.7	86.4
LP gap	153.4 %	156.3 %	103.4 %	35.2 %
Optimality gap	31.8 %	46.8 %	33.6 %	11.0 %

Table 2 Metrics of IP methods based on 1-IP for ℓ_∞ norm (49 instances)

	1-IP	1-IP +HG	1-IP +Fix	1-IP +Fix +2Var
Preprocessing time (seconds)	0.0	35.1	6.7	9.2
Verification time (seconds)	1215.6	1305.9	9.3	10.3
# of solved instances (veri.)	12	12	22	22
# of nodes (veri.)	9844.0	9811.1	0.8	0.7
Optimization time (seconds)	1549.9	1632.5	12.2	12.4
# of solved instances (opt.)	11	11	21	22
# of nodes (opt.)	16 647.4	16 607.7	7.1	5.0
LP gap	165.1 %	165.1 %	12.5 %	2.9 %
Optimality gap	46.5 %	46.6 %	1.8 %	0.0 %

Table 3 Metrics of IP methods based on 1-IP for ℓ_2 norm (22 instances)

In the case of $p = 2$, the same metrics are computed over all 22 instances tested by all IP methods based on 1-IP to compare these IP methods. Table 3 shows these metrics. 1-IP+HG does not result in improvement compared to 1-IP, which means that generating (15) also does not improve BNN verification in the case of $p = 2$. 1-IP+Fix and 1-IP+Fix+2Var yield similar improvements compared to 1-IP, which implies that generating variable fixings improves BNN verification in the case of $p = 2$, but on these instances there does not appear to be further improvement from two-variable inequalities.

To better compare 1-IP+Fix and 1-IP+Fix+2Var, we report in Table 4 the results comparing these instances on all 49 instances solved by these two methods (many of these were excluded in Table 3 since they were not solved by 1-IP or 1-IP+HG). From this table we observe that spending more time in generating more layerwise derived valid inequalities, mainly two-variable inequalities, results in reducing LP gaps and solving the verification problem more quickly on these instances.

	1-IP +Fix	1-IP +Fix +2Var
Preprocessing time (seconds)	7.0	24.0
Verification time (seconds)	66.3	41.5
# of solved instances (veri.)	35	42
# of nodes (veri.)	33.6	4.8
Optimization time (seconds)	82.3	82.9
# of solved instances (opt.)	32	34
# of nodes (opt.)	90.7	75.7
LP gap	51.8 %	24.0 %
Optimality gap	29.5 %	16.9 %

Table 4 Metrics of 1-IP+Fix and 1-IP+Fix+2Var for ℓ_2 norm (49 instances)

Network	L	n¹	n²
1	1	32	*
2	1	64	*
3	1	128	*
4	2	32	32
5	2	64	64
6	2	128	128

Table 5 Networks in additional computational study

A.6. Computational Study on Convex Hull Characterization for a Single Neuron

We pursue an additional computational study to validate our implementation for IP methods exploiting Theorem 1 on convex hull characterization for a single neuron. As we see in Table 5, the IP method 1-IP+HG employing the valid inequalities presented Theorem 1 does not yield significant decreases in LP gaps compared to the IP method 1-IP. However, using these valid inequalities resulted in smaller LP gaps in Han and Gómez (2021). One possible reason for this discrepancy is that (15) cannot be used for $\ell = 1$ in our computational study because $q = 255$, but these valid inequalities can be used in the computational study of Han and Gómez (2021) because $q = 1$. To examine whether this guess is correct, an additional computational study is conducted on test instances based on ones in Han and Gómez (2021) to assess the impact of exploiting Theorem 1. In this computational study, the IP method Many-IP and Many-IP+HG, which solves the IP problem (12) by employing a constraint generation approach with (15) as 1-IP+HG for each t , are compared because t is fixed in Han and Gómez (2021).

Each test instance consists of a BNN, $\bar{\mathbf{x}}$, and ϵ . Six BNNs pretrained from Han and Gómez (2021) are used in this computational study. These networks are trained on the MNIST training dataset by using Hubara et al. (2016)'s method, which implies $n^0 = 784$ and $n^{L+1} = 10$. The numbers of hidden layers and the number of neurons in hidden layers of each network are reported in Table 5. Feature vectors in the MNIST dataset are scaled to binary vectors by converting coordinates smaller than 128 to 0 and the other coordinates to 1, which indicates $q = 1$. Ten feature vectors are

Network	ϵ	LP value		Verification time (seconds)	
		Many-IP	Many-IP+HG	Many-IP	Many-IP+HG
1	1.0	24.5	6.2	1.2	1.7
	2.0	24.6	6.3	1.3	5.0
	3.0	24.7	7.9	1.4	5.8
	4.0	24.8	7.7	1.4	6.7
	5.0	24.8	7.9	1.5	8.6
2	1.0	50.2	12.9	2.3	3.8
	2.0	50.4	16.9	4.2	9.9
	3.0	50.5	16.4	4.3	13.4
	4.0	50.7	18.5	4.3	16.9
	5.0	50.8	22.9	4.1	17.2
3	1.0	80.7	15.9	4.5	8.6
	2.0	80.9	19.1	9.0	27.5
	3.0	81.2	20.3	9.2	34.1
	4.0	81.4	29.4	9.2	36.6
	5.0	81.6	31.8	9.3	49.3
4	1.0	22.1	4.5	1.2	5.0
	2.0	22.1	11.0	1.4	21.1
	3.0	22.1	14.4	1.5	20.2
	4.0	22.1	16.6	1.4	22.6
	5.0	22.1	18.1	1.5	25.6
5	1.0	29.9	12.7	2.5	8.6
	2.0	29.9	19.9	6.6	53.2
	3.0	29.9	23.6	6.9	47.5
	4.0	29.9	25.7	7.2	68.4
	5.0	29.9	27.0	7.5	84.8
6	1.0	45.0	26.4	5.3	16.3
	2.0	45.0	36.2	28.7	1347.6(3)
	3.0	45.0	40.0	37.1	1312.6(3)
	4.0	45.0	42.2	50.4	1287.8(5)
	5.0	45.0	43.3	64.9	1175.9(4)

Table 6 Metrics of Many-IP and Many-IP+HG

selected for $\bar{x}$. For each digit from 0 to 9, one feature vector in the MNIST test dataset whose $\bar{t}$ is this digit is randomly chosen. Positive integers from 1 to 5 are used as ϵ .

For each network and ϵ , the arithmetic mean of optimal objective values of the LP relaxation problem of (12) over all $\bar{x}$ and t (LP value) and the shifted geometric mean of times to solve the verification problem for all t with a shift of 1 over all $\bar{x}$ (verification time) are computed for Many-IP and Many-IP+HG to compare these IP methods. Table 6 reports LP values and verification times. The number in parenthesis for verification time is the number of $\bar{x}$ where the time limit is hit in solving (12) for at least one t for each network and ϵ . Many-IP+HG yields smaller LP values than Many-IP as in Han and Gómez (2021), so our additional computational study validates our

implementation for IP methods employing the valid inequalities in Theorem 1. In particular, the gap in LP values between Many-IP and Many-IP+HG becomes smaller for larger L and ϵ as in Han and Gómez (2021). However, Many-IP+HG results in larger verification times than Many-IP, which implies that even though using the inequalities in Theorem 1 improves LP relaxation values, it does not reduce BNN verification time.

References

- Balas E (1985) Disjunctive programming and a hierarchy of relaxations for discrete optimization problems. *SIAM Journal on Algebraic Discrete Methods* 6(3):466–486.
- Han S, Gómez A (2021) Single-neuron convexification for binarized neural networks. <https://optimization-online.org/wp-content/uploads/2021/05/8419.pdf>, accessed May 27, 2021.
- Hubara I, Courbariaux M, Soudry D, El-Yaniv R, Bengio Y (2016) Binarized neural networks. Lee D, Sugiyama M, von Luxburg U, Guyon I, Garnett R, eds., *Adv. in Neural Information Processing Systems*, volume 29, 4107—4115 (Curran Associates, Inc.).