CS781 Quiz 1 (Autumn 2024)

Max marks: 25 **Duration: 90 mins**

- *The exam is open book and notes. However, you are not allowed to search on the internet or consult others over the internet for your answers.*
- *Be brief, complete and stick to what has been asked.*
- *Unless asked for explicitly, you may cite results/proofs covered in class without reproducing them.*
- ***If you need to make any assumptions, state them clearly.***
- ***Do not copy solutions from others. Penalty for offenders: FR grade.***

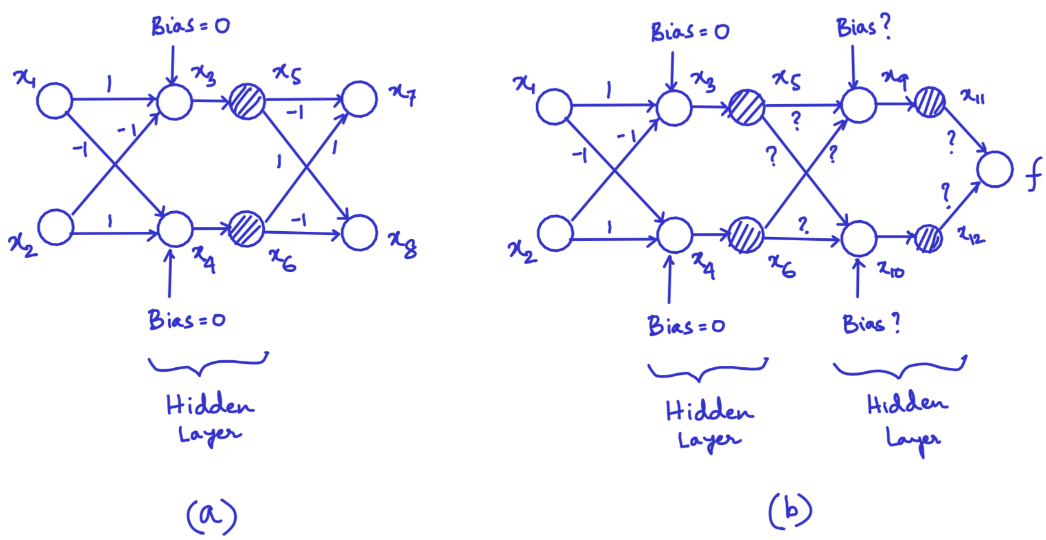


Figure 1: Neural networks

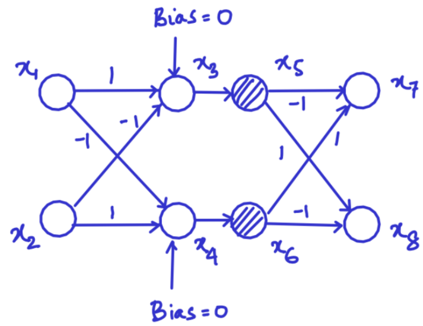
Consider the neural network N_1 shown in Fig. 1(a), where all neurons assume real values. The network has one hidden layer, which uses ReLU activation functions. ReLU nodes are shown shaded. No ReLUs are used in input or output layers. The bias for each neuron and all edge weights are as shown in Fig. 1(a). Note that $x_5 = ReLU(x_3)$ and $x_6 = ReLU(x_4)$.

Let $\boldsymbol{x} = (x_1, x_2)^T$ denote the input of the network. We wish to perturb the input such that $||\boldsymbol{x}||_1 \leq 1$, i.e the input lies in a 1-norm ball of radius 1 around the origin. You are given the following lower and upper bounds of various internal node values: $-1 \leq x_3, x_4, x_7, x_8 \leq 1$.

1. *[5 marks]* Let $z = x_5 - x_6$. We wish to find the best lower and upper bounds on z using a linear programming (LP) approach. Formulate the tightest set of linear constraints involving $z, x_1 and x_2$ such that minimizing (resp. maximizing) z subject to these constraints gives the best upper and lower bounds of z using LP.

   You are required to simply give the complete set of linear constraints, and not solve the linear program

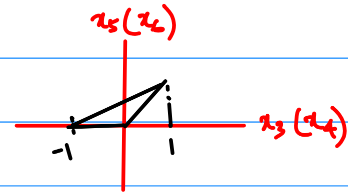
1



$$Z = x_5 - x_6$$

$$x_5 \geq 0$$
$$x_5 \geq x_3$$
$$x_5 \leq \frac{1}{2}x_3 + \frac{1}{2}$$

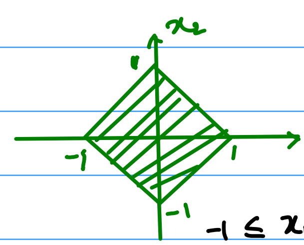
$$x_6 \geq 0$$
$$x_6 \geq x_4$$
$$x_6 \leq \frac{1}{2}x_4 + \frac{1}{2}$$



$$Z \geq -\frac{1}{2}x_4 - \frac{1}{2}$$
$$Z \geq x_3 - \frac{1}{2}x_4 - \frac{1}{2}.$$
$$Z \leq \frac{1}{2}x_3 + \frac{1}{2}$$
$$Z \leq \frac{1}{2}x_3 + \frac{1}{2} - x_4$$

$$x_3 = x_1 - x_2 + 0$$
$$x_4 = x_2 - x_1 + 0$$

$$\|x\|_1 \leq 1 \Leftrightarrow |x_1| + |x_2| \leq 1$$



$$-1 \leq x_1 + x_2 \leq 1$$
$$-1 \leq x_1 - x_2 \leq 1$$

$$\therefore \quad Z \geq -\frac{1}{2}x_2 + \frac{1}{2}x_1 - \frac{1}{2}$$
$$Z \geq \frac{3}{2}x_1 - \frac{3}{2}x_2 - \frac{1}{2}$$
$$Z \leq \frac{1}{2}x_1 - \frac{1}{2}x_2 + \frac{1}{2}$$
$$Z \leq \frac{3}{2}x_1 - \frac{3}{2}x_2 + \frac{1}{2}$$

min (or max) Z

$$x_1 + x_2 \leq 1$$
$$x_1 + x_2 \geq -1$$
$$x_1 - x_2 \leq 1$$
$$x_1 - x_2 \geq -1$$

2. *[5 marks]* A student wants to verify if $-1 \leq x_7 - x_8 \leq 1$ holds for the network N_1 in Fig. 1(a), when $||\boldsymbol{x}||_1 \leq 1$. Towards this end, the student claims that network N_1 can be transformed to network N_2 shown in Fig. 1(b), where the "?" represent weights and biases to be calculated, such that the above verification question reduces to check if $max_{||\boldsymbol{x}||_1 \leq 1} f \;\leq\; 0$ (see Fig. 1(b)). You are required to help the student come up with the right weights and biases in N_2. Indicate what each of the weights/biases should be with proper justification.

3. *[5 marks]* The student now wishes to find linear upper and lower bounds of f in terms of x_1 and x_2 using Linear Relaxation based Perturbation Analysis (LiRPA) applied to N_2. Assume that for each unstable ReLU $s = ReLU(t)$, the lower bound $s \geq t$ is used if $-l_t <= u_t$ and the lower bound $s \geq 0$ is used otherwise (i.e. DeepPoly like heuristic). Write the best linear upper and lower bounds of f in terms of x_1 and x_2 using the above lower bounds for unstable ReLUs. You must justify each step of your calculation.

4. *[10 marks]* The student now aims for higher accuracy, and wishes to solve the above sub-problem but after splitting the unstable ReLUs ($x_5 = ReLU(x_3)$ and $x_6 = ReLU(x_4)$). As a sub-problem to be solved, she considers the case corresponding to $x_3 \geq 0$ and $x_4 < 0$.

   (a) *[2 marks]* Draw the simplified network resulting from the above split constraints.

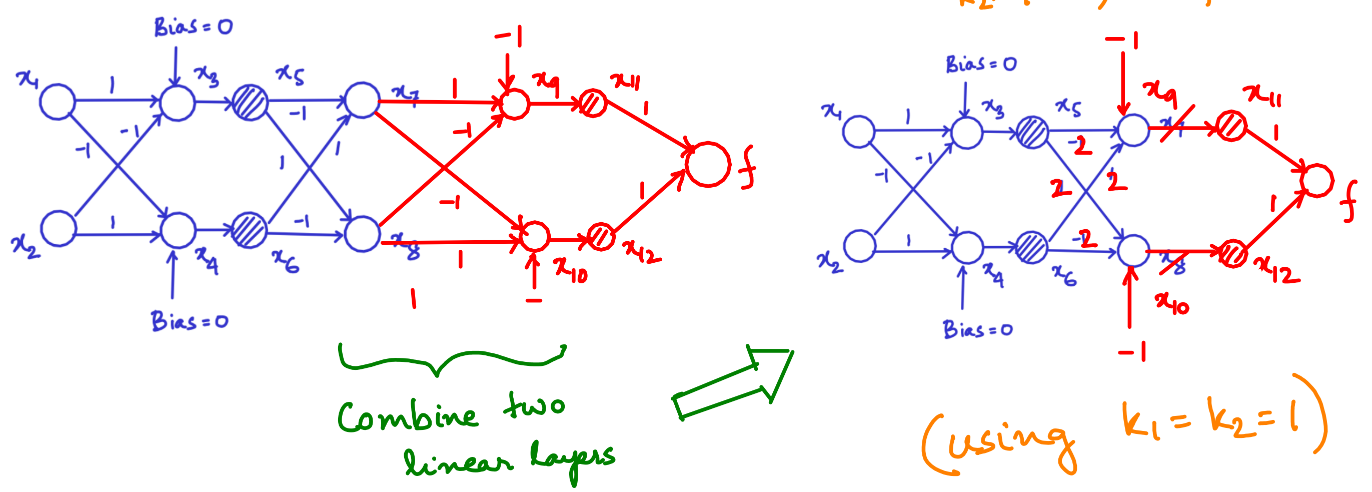
   (b) *[8 marks]* For each unstable ReLU $s = ReLU(t)$ in the simplified network, suppose the student uses the lower bound $s \geq \alpha.t$ in the linear relaxation of the ReLU (same α used for all unstable ReLUs). Furthermore, suppose the student uses the same Lagrangian multiplier β for all split neuron constraints. Assume $0 \leq \alpha \leq 1$ and $\beta \geq 0$. Write the best linear upper and lower bounds of f in terms of x_1 and x_2. Your bounds must be linear in x_1 and x_2, but the coefficients can be non-linear expressions in α and β.

(2) To verify: $-1 \leq x_7 - x_8 \leq 1$

$\Leftrightarrow \quad (x_7 - x_8 - 1 \leq 0) \wedge (x_8 - x_7 - 1 \leq 0)$

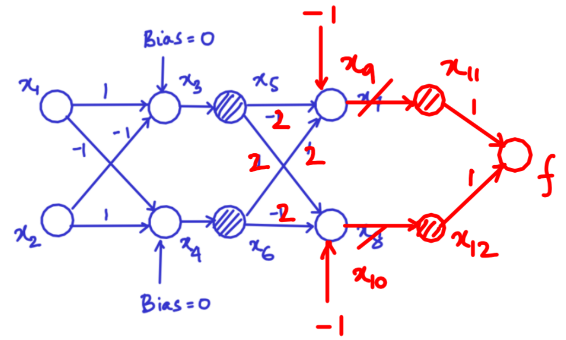
$\Leftrightarrow \quad ReLU(x_7 - x_8 - 1) + ReLU(x_8 - x_7 - 1) \leq 0 \quad (= 0)$

$\Leftrightarrow \quad ReLU(k_1 . x_7 - k_1 . x_8 - k_1) + ReLU(k_2 . x_8 - k_2 . x_7 - k_2) \leq 0$ for any $k_1, k_2 \geq 0$



3

N_2:



3. *[5 marks]* The student now wishes to find linear upper and lower bounds of f in terms of x_1 and x_2 using Linear Relaxation based Perturbation Analysis (LiRPA) applied to N_2. Assume that for each unstable ReLU $s = ReLU(t)$, the lower bound $s \geq t$ is used if $-l_t <= u_t$ and the lower bound $s \geq 0$ is used otherwise (i.e. DeepPoly like heuristic). Write the best linear upper and lower bounds of f in terms of x_1 and x_2 using the above lower bounds for unstable ReLUs. You must justify each step of your calculation.

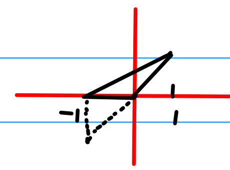
To apply LiRPA, we need l and u bounds for the input of each ReLU.

$-1 \leq x_3, x_4 \leq 1$

~~Lower~~ upper bounds in ReLU relaxation:

$x_5 \geq x_3$ $\qquad x_5 \leq \frac{1}{2}x_3 + \frac{1}{2}$

$x_6 \geq x_4$ $\qquad x_6 \leq \frac{1}{2}x_4 + \frac{1}{2}$



$x_9 = -2x_5 + 2x_6 - 1$

$x_{10} = 2x_5 - 2x_6 - 1$

x_9 and x_{10}, being ReLU inputs, we must determine their l and u bounds. Here, we will calculate them by expressing x_9 and x_{10} in terms of x_1 and x_2. As some students pointed out in class, we can obtain better bounds of x_9, x_{10} using $x_5, x_6 \geq 0$. That is also a perfectly correct approach, as long as we clearly describe the algorithmic step used to obtain the bounds.

$-x_3 - 1 + 2x_4 - 1 \leq x_9 \leq -2x_3 + x_4 \cancel{+1} \cancel{-1}$

$2x_3 - x_4 - 1 - 1 \leq x_{10} \leq x_3 \cancel{+1} - 2x_4 \cancel{-1}$

$2x_4 - x_3 - 2 \leq x_9 \leq -2x_3 + x_4$

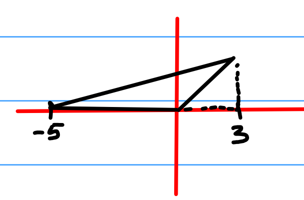
$2x_3 - x_4 - 2 \leq x_{10} \leq -2x_4 + x_3$

$3 \cdot (x_2 - x_1) - 2 = 2(x_2 - x_1) - (x_1 - x_2) - 2 \leq x_9 \leq -2(x_1 - x_2) + x_2 - x_1 = 3 \cdot (x_2 - x_1)$

$3(x_1 - x_2) - 2 \leq x_{10} \leq 3(x_1 - x_2)$

$-5 \leq x_9 \leq 3$

$-5 \leq x_{10} \leq 3$



~~Lower~~ upper bounds in ReLU relaxation: $\quad x_{11} \geq 0, \; x_{12} \geq 0$

$\left.\begin{aligned} x_{11} &\leq \frac{3}{8}x_9 + \frac{15}{8} \\ x_{12} &\leq \frac{3}{8}x_{10} + \frac{15}{8} \end{aligned}\right\}$ Upper bnds in ReLU relaxation

$0 \leq f = x_{11} + x_{12} \leq \frac{3}{8}(x_9 + x_{10}) + \frac{30}{8}$

$\leq 3/8\,(\cancel{3x_2} - \cancel{3x_1} + \cancel{3x_1} - \cancel{3x_2}) + 30/8 = 30/8$

In case we use $x_5 \geq 0$, $x_6 \geq 0$ (since they are outputs of ReLU) to obtain bounds on x_9, x_{10}, we'd get :

$$x_9 = -2x_5 + 2x_6 - 1 \qquad -2x_5 - 1 \leq x_9 \leq 2x_6 - 1$$

$$x_{10} = 2x_5 - 2x_6 - 1 \qquad -2x_6 - 1 \leq x_{10} \leq 2x_5 - 1$$

$$\therefore \quad -x_3 - 1 - 1 \leq x_9 \leq x_4 + \cancel{1} - \cancel{1}$$

i.e., $\quad -x_3 - 2 \leq x_9 \leq x_4$

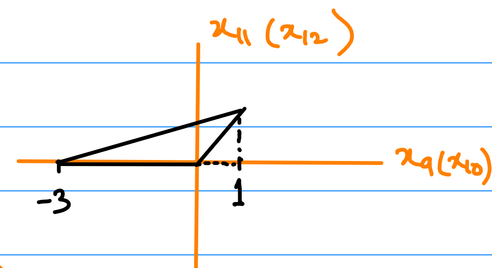
Similarly, $\quad -x_4 - 2 \leq x_{10} \leq x_3$

$$\therefore \quad -(x_1 - x_2) - 2 \leq x_9 \leq x_2 - x_1$$

$$-(x_2 - x_1) - 2 \leq x_{10} \leq x_1 - x_2$$

$$\therefore \quad -3 \leq x_9 \leq 1$$

$$-3 \leq x_{10} \leq 1$$



$\therefore$ Lower/upper bounds in ReLU relaxation of x_{11}, x_{12}:

$$0 \leq x_{11} \leq \frac{1}{4} x_9 + \frac{3}{4}$$

$$0 \leq x_{12} \leq \frac{1}{4} x_{10} + \frac{3}{4}$$

$$\therefore \quad 0 \leq f = x_{11} + x_{12} \leq \frac{1}{4} \cdot (x_9 + x_{10}) + \frac{6}{4}$$

$$\leq \frac{1}{4} \cdot (\cancel{x_2} - \cancel{x_1} + \cancel{x_1} - \cancel{x_2}) + \frac{6}{4}$$

$$= 6/4 = \frac{3}{2}$$

$$\therefore \quad 0 \leq f \leq \frac{3}{2}$$

[Note that this upper bound is tighter than $30/8 = \frac{15}{4}$, obtained earlier]

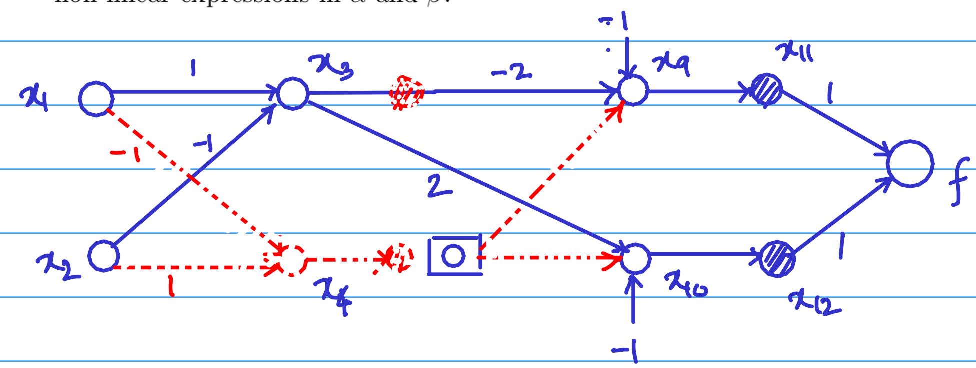
(4)

4. *[10 marks]* The student now aims for higher accuracy, and wishes to solve the above sub-problem but after splitting the unstable ReLUs ($x_5 = ReLU(x_3)$ and $x_6 = ReLU(x_4)$). As a sub-problem to be solved, she considers the case corresponding to $x_3 \geq 0$ and $x_4 < 0$.

   (a) *[2 marks]* Draw the simplified network resulting from the above split constraints.

   (b) *[8 marks]* For each unstable ReLU $s = ReLU(t)$ in the simplified network, suppose the student uses the lower bound $s \geq \alpha.t$ in the linear relaxation of the ReLU (same α used for all unstable ReLUs). Furthermore, suppose the student uses the same Lagrangian multiplier β for all split neuron constraints. Assume $0 \leq \alpha \leq 1$ and $\beta \geq 0$. Write the best linear upper and lower bounds of f in terms of x_1 and x_2. Your bounds must be linear in x_1 and x_2, but the coefficients can be non-linear expressions in α and β.

(a)



Dotted red are nodes & edges deleted to get the simplified network.

(b) There are 2 ReLUs remaining. Using α-approximation, we have $x_{11} \geq \alpha . x_9$ and $x_{12} \geq \alpha . x_{10}$, where $0 \leq \alpha \leq 1$

To find upper bound expressions for x_{11} and x_{12}, we need to know lower and upper bounds of x_9 and x_{10}.

* $x_9 = -2x_3 - 1$

Since we are using the split constraint $x_3 \geq 0$, we should use it here.

$\therefore \quad x_9 \leq -1 \Rightarrow x_{11} = ReLU(x_9) = 0$

(we don't need $x_{11} \geq \alpha . x_9$ any more)

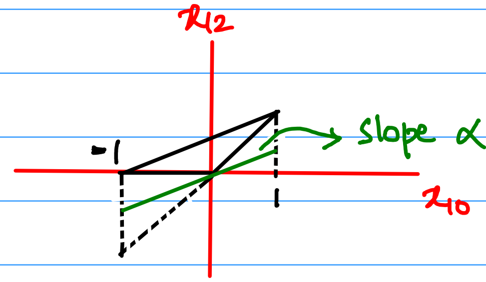
* $x_{10} = 2x_3 - 1$

Since we are using the split constraint $x_3 \geq 0$, we have $x_{10} \geq -1$

For an upper bound of x_{10}, we use

$$x_{10} = 2x_3 - 1 \leq 2(x_1 - x_2) - 1 \leq 2\times 1 - 1$$
$$= 1$$

$$\therefore \quad -1 \leq x_{10} \leq 1$$



$$\therefore \quad \alpha . x_{10} \leq x_{12} \leq \frac{1}{2} x_{10} + \frac{1}{2}$$

$$\therefore \quad f = x_{11} + x_{12} = 0 + x_{12} = x_{12}$$

$$\alpha . x_{10} \leq f \leq \frac{1}{2} x_{10} + \frac{1}{2}$$
$$= \alpha . (2x_3 - 1)$$
$$= \frac{1}{2} . (2x_3 - 1) - \frac{1}{2}$$
$$= x_3 - 1$$

$$\therefore \quad 2\alpha . x_3 - \alpha \leq f \leq x_3 - 1$$

Since $x_3 \geqslant 0$ and $x_4 < 0$ are split neuron constr., we need to add the β terms here, where $\beta \geqslant 0$

How do we do this?

(Please see next page)

Assume f has the largest value (say f^*) for $x_1 = x_1^*$, $x_2 = x_2^*$

s.t. the corresponding x_3, x_4 values, say x_3^* and x_4^*, satisfy our split neuron constraints.

Then
$$f^* \leq x_3^* - 1$$
$$\leq x_3^* - 1 + \beta . x_3^* - \beta . x_4^*.$$

for any $\beta \geq 0$, since $x_3^* \geq 0$ and $x_4^* < 0$

$$\therefore \quad f^* \leq \max_{\|x\|_1 \leq 1} \left(x_3 - 1 + \beta . x_3 - \beta . x_4 \right)$$

Since the above holds for any $\beta \geq 0$, we have

$$f^* \leq \min_{\beta \geq 0} \max_{\|x\|_1 \leq 1} \left(x_3 - 1 + \beta . x_3 - \beta . x_4 \right)$$

By a similar reasoning, if f has the smallest value, say f_*, when $x_1 = x_{1*}$, $x_2 = x_{2*}$, $x_3 = x_{3*}$, $x_4 = x_{4*}$ s.t. the the split neuron constraints are satisfied, then we have:

$$2\alpha x_{3*} - \alpha \leq f_*, \text{ for any } \alpha \in [0, 1]$$

$$2\alpha . x_{3*} - \alpha - \beta . x_{3*} + \beta . x_{4*} \leq$$

for any $\beta \geq 0$, since $x_3^* \geq 0$ and $x_4^* < 0$

$$\therefore \quad \min_{\|x\|_1 \leq 1} \left(2\alpha x_3 - \alpha - \beta . x_3 + \beta . x_4 \right) \leq f_*$$

Since the above inequality holds for all $0 \le \alpha \le 1$ and $\beta \geq 0$, we have

$$\max_{\substack{0 \le \alpha \le 1 \\ \beta \geq 0}} \min_{\|x\|_1 \le 1} \left(2\alpha x_3 - \alpha - \beta \cdot x_3 + \beta \cdot x_4\right) \le f_{*}$$

So, we know that

$$\max_{\substack{0 \le \alpha \le 1 \\ \beta \geq 0}} \min_{\|x\|_1 \le 1} \left(2\alpha x_3 - \alpha - \beta \cdot x_3 + \beta \cdot x_4\right) \le f \le \min_{\beta \geq 0} \max_{\|x\|_1 \le 1} \left(x_3 - 1 + \beta \cdot x_3 - \beta \cdot x_4\right)$$

Using $x_3 = x_1 - x_2$ and $x_4 = x_2 - x_1$, we get:

$$\boxed{\max_{\substack{0 \le \alpha \le 1 \\ \beta \geq 0}} \min_{\|x\|_1 \le 1} \left((2\alpha - 2\beta)\cdot x_1 - (2\alpha - 2\beta)\cdot x_2 - \alpha\right) \le f \le \min_{\beta \geq 0} \max_{\|x\|_1 \le 1} \left((1+2\beta) x_1 - (1+2\beta) x_2 - 1\right)}$$

However, does this allow us to say,

$$(2\alpha - 2\beta)\cdot x_1 - (2\alpha - 2\beta)\cdot x_2 - \alpha \le f \le (1+2\beta)\cdot x_1 - (1+2\beta)\cdot x_2 - 1$$

for all $\|x\|_1 \le 1$?
and for $0 \le \alpha \le 1$, $\beta \geq 0$

Not in general, but indeed when x_1 and x_2 take values that ensure $x_3 \geq 0$ and $x_4 < 0$.

So, under the given split neuron constraints, the above serve as bounds for f.

The boxed inequalities above allow us to ignore the bit about x_1, x_2 being s.t. they satisfy the split neuron constr, when doing the global optimization.