CS781 Mid-semester Exam (Autumn 2024)

Max marks: 35 Duration: 120 mins Roll No.

- *You are required to answer each question only in the space provided with each question.*
- *Only material written within the allotted answering space for each question will be graded.*
- *The spaces allotted for answering questions should give a rough indication of the relative lengths of correct answers to the questions.*
- *Please attach all your rough sheets.*
- *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.***

1. *[10 marks]* We have studied in class several abstractions of the ReLU constraint based on linear relaxations. A student proposes a new abstraction of the ReLU constraint, that she claims works for all ReLUs, and not just for unstable ReLUs.

   For $s = ReLU(t)$ where $l \leq t \leq u$ (note that it is not necessary that $l < 0 < u$), the abstraction is given by four inequalities:

   $$t \geq l; \quad t \leq u; \quad s \geq \mu(l,u) \times t; \quad s \leq \mu(l,u) \times t + \lambda(l,u),$$

   where $\mu(l,u)$ and $\lambda(l,u)$ are functions of l and u.

   Indicate, with clear justification, which of the following choices of $\mu(\cdot,\cdot)$ and $\lambda(\cdot,\cdot)$ functions constitute a *sound abstraction* of ReLU constraints, i.e. concretization of the abstraction must yield a superset of the set of points (s,t) related by the ReLU constraint.

   In case you think one of the choices below doesn't yield a sound justification, give concrete values of l and u, and show why concretizaton of the abstraction excludes some (s,t) points related by the ReLU constraint. Otherwise, prove that the abstraction is sound for all l and u s.t. $l < u$.

   (a) *[5 marks]* $\mu(l,u) = \frac{1}{2}$, $\lambda(l,u) = \max(-l,u)$

(b) *[5 marks]* $\mu(l,u) = \frac{ReLU(u)-ReLU(l)}{u-l}$, $\lambda(l,u) = \frac{ReLU(u)\times l}{l-u}$

2. *[15 marks]* The following sub-questions relate to the network shown in Fig. 1. Dashed nodes in this figure represent ReLUs. Let $\mathbf{x}$ denote the input vector $[x_1, x_2]^T$. Assume $||\mathbf{x} - \mathbf{x_0}||_2 \leq 2$, where $\mathbf{x_0}$ represents the input $[1, -1]^T$, i.e. $x_{1,0} = 1, x_{2,0} = -1$.

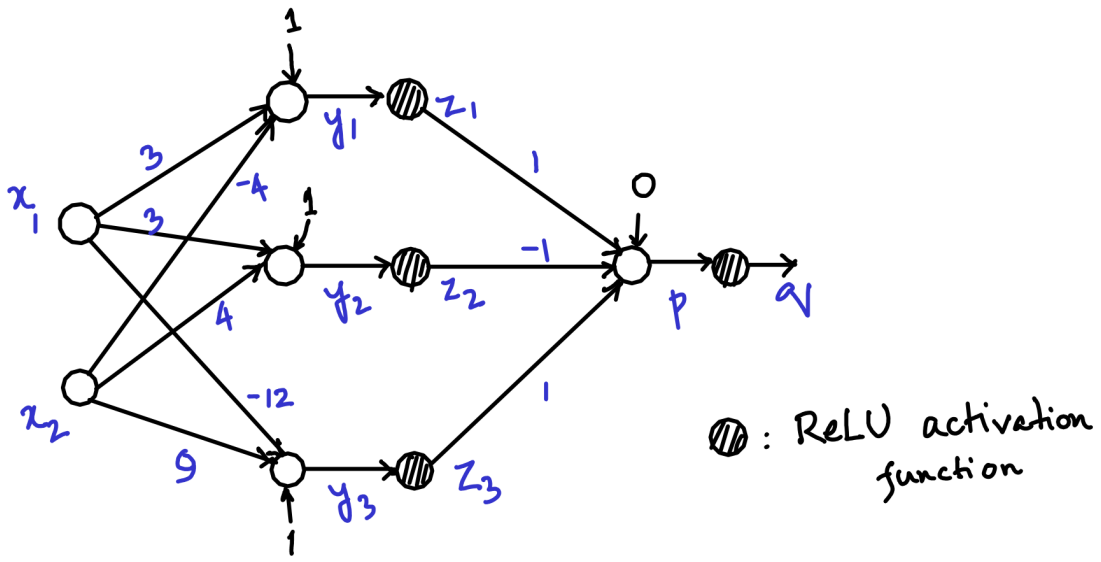

Figure 1: Neural network with ReLU activation

(a) *[4 marks]* Using Holder's inequality, find bounds l_i, u_i for $i \in \{1, 2, 3\}$ such that $l_i \leq y_i \leq u_i$. Refer to Fig. 1 to understand what the y_i's denote. You must show all steps of your calculation.

(b) *[5 marks]* Now assume $-5 \leq y_1 \leq 5$, $-3 \leq y_2 \leq 3$ and $-2 \leq y_3 \leq 2$. ***Do not worry about whether these are correct bounds of*** y_1, y_2, y_3 ***or not, and do not use the bounds computed by you in the previous sub-question.***

Using the provided **(not your computed)** bounds for y_i, calculate linear (in x_1, x_2) bounds of p using the technique of α-CROWN. Use a separate parameter α_i to relax each ReLU constraint $z_i = RelU(y_i)$. Assume $0 \leq \alpha_i \leq 1$. The coefficients in your linear expressions can be in terms of the α_i's.

(c) For this sub-question, ignore all calculations done in the previous two sub-questions.

i. *[2 marks]* Use simple interval propagation (and nothing else) to obtain lower and upper bounds of y_1, y_2, y_3 and p. You may assume that the output of a ReLU is always non-negative during interval propagation.

ii. *[2 marks]* Use the bounds computed by you above (in question 2ci) to find linear bounds of q in terms of x_1 and x_2. Use the relaxation of unstable ReLU constraints as used in DeepPoly. In other words, for each unstable ReLU $s = ReLU(t)$, use $s \geq 0$ if $-l_t \geq u_t$ and $s \geq t$ otherwise, for the lower bound constraint.

iii. *[2 marks]* Use Holder's inequality on the linear expressions computed above (in question 2cii) to find concrete upper and lower bounds of q.

3. *[10 marks]* A *binarized neural network (BNN)* is a neural network in which all inter-layer edge weights are either 1 or -1, and in which all activation functions are the *sign* function, defined as follows: $sign(t) = 1$ if $t \geq 0$ and -1 otherwise.

   A BNN can have arbitrary real numbers as biases of neurons. Thus, for a neuron in a BNN, pre-activation values can be real numbers, although post-activation values are always either -1 or 1. Every input of a BNN is an integer, either -1 or 1.

   It turns out we can model a (relaxation of a) BNN using a *special* set of linear constraints. Specifically, a *bounded integer linear expression* is a linear expression in which all variables are bounded integers, but constants and coefficients can be arbitrary real numbers. For example, $0.5x + 2y - 0.75$ is a bounded integer linear expression, where x, y are integers s.t. $-10 \leq x, y \leq 10$. A *bounded integer linear inequality* is obtained by comparing (using $<, >, \leq, \geq$) a bounded integer linear expression with zero. For example, $0.5x + 2y - 0.75 \leq 0$ is a bounded integer linear inequality. Finally, a conjunction of finite number of bounded integer linear inequalities is called a *bounded integer linear system of constraints*. For example, the conjunction of $0.5x + 2y - 0.75 \leq 0$, $-10 \leq x \leq 10$ and $-5 \leq y \leq 15$ is a bounded integer linear system of constraints.

   (a) *[5 marks]* Write the best bounded integer linear system of constraints you can for modeling the activation function $s = sign(t)$, where $t \in [a + l, b + u]$, a, b are real-valued constants, and l, u are integers s.t. $X \leq l, u \leq Y$, where X, Y are integer-valued constants. Assume $a + X < 0 < b + Y$.

   Remember your constraints should be a set of linear inequalities over only bounded integer variables (no real-valued variables allowed). The bounds on the integer variables should also be part of your bounded linear system of constraints.

(b) *[5 marks]* Consider the BNN shown in Fig. 2. Give bounded integer linear upper and lower bound expressions for the output of this network in terms of the BNN inputs x_1 and x_2. Give justification for each step of your calculation. You are free to use variables to represent intermediate results computed by the BNN. However, remember that ***all variables appearing in your bounded integer linear expressions must be bounded integers (no real-valued variables)***, and the bounds of these integer variables must also be included as part of your system of constraints.

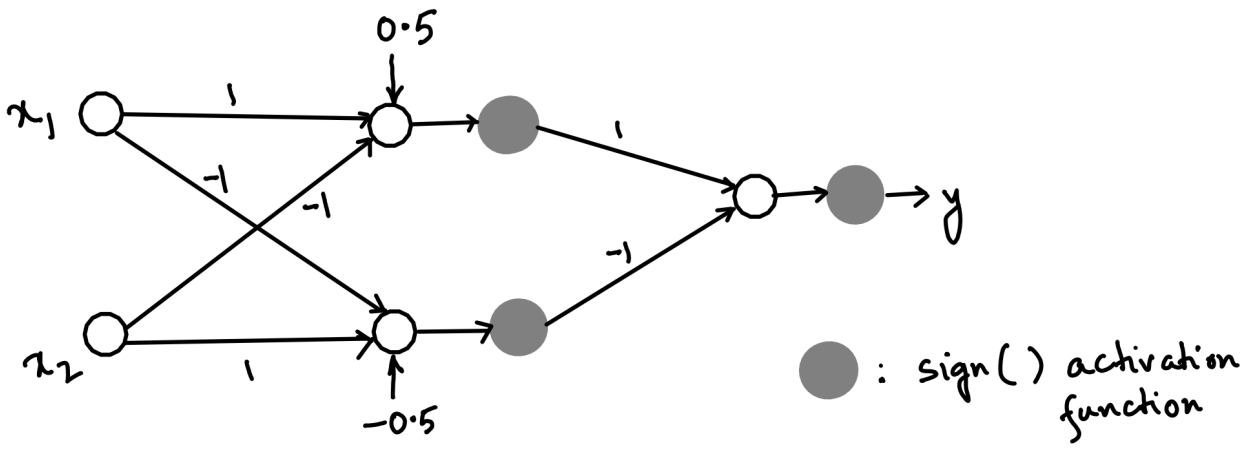

Figure 2: Binarized neural network with sign activation