Homework 2

1) In all of these, assuming that $a \leq b$.
(i.e $[a,b]$ represents a valid interval).

- It is easy to extend this to the $a > b$ case. Just say $T_f(a,b) = (1,0)$, i.e if $[a,b]$ is not a valid interval, then $T_f[a,b] = [1,0]$ & $[1,0]$ is not a valid interval.

(a) $f_1(x) = |x|$

$$T_{f_1}(a,b) = \begin{cases} (a,b) & a \geq 0 \\ (|b|,|a|) & a<0 \text{ \& } b \leq 0 \\ (0, \max(|a|,|b|)) & a<0 \text{ \& } b>0 \end{cases}$$

(b) $f_2(x) = x^3$

$$T_{f_2}(a,b) = (f(a), f(b))$$

{for mon. increasing & continuous functions, this is right}

(c) $f_3(x) = x - |x| = \begin{cases} 0 & x \geq 0 \\ 2x & x < 0 \end{cases}$

$$T_{f_3}(a,b) = (f(a), f(b))$$

(d) $f_4(x) = \min(x+|x|, x-|x|)$
$= x - |x|$

$$T_{f_4} = T_{f_3}$$

(e) $f_5(x) = \max(x^2, x^3)$

$$T_{f_5}(a,b) = \begin{cases} (f(a),f(b)) & a \geq 1 \\ (f(b),f(a)) & b \leq 0 \\ (0, \max\{f(a),f(b)\}) & a<0 \text{ \& } b>0 \\ (f(a),f(b)) & (a>0 \text{ \& } b>0 \text{ \& } a<1) \end{cases}$$

→ Using 23 shows 'onto' for all the transformers.
So, sound. Also, one can check that both lower and
upper values of T_f can be attained in f.
These, combined with continuousness of f gives optimality.

2)
Testing accuracy and doing FGSM & PGD on the model before the training.
Below are the name of the part of the ipynb file where this is done followed by the result (in percentages) when running.

Accuracy on test set:-
Accuracy(percentage): 10.22

Initial Attacks:-
Percent of examples where FGSM attack was not found: 2.1700000000000053
Percent of examples where PGD attack was not found: 2.1299999999999986

PGD attack is more successful.

Next, trained without the PDG attack.

Accuracy(percentage): 94.75
Percent of examples where FGSM attack was not found: 90.59
Percent of examples where PGD attack was not found: 90.53999999999999

Next, ran the code again from scratch but trained using PDG.

Accuracy(percentage): 96.36
Percent of examples where FGSM attack was not found: 93.77
Percent of examples where PGD attack was not found: 93.72