AI Assignment 2

23K-0078
BAI-4A

Q1: query(x) = -1 * (x-7) ** 2 + 49.

Step	x	query(x)	query(x+1)	MoveDirection
1	0	0	13	→
2	1	13	24	→
3	2	24	33	→
...	...	...	...	...
7	7	49	48	Stop

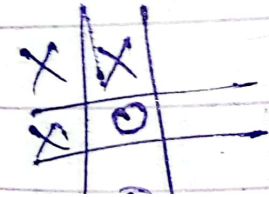
Peak at x=7
Elevation = 49

Q3: Differences in Implementations:
- My version uses simple backtracking with constraint checking.
- Google OR Tools applies constraint programming (optimized).
- GPT / Github version uses fast heuristics and pre-pruned states.

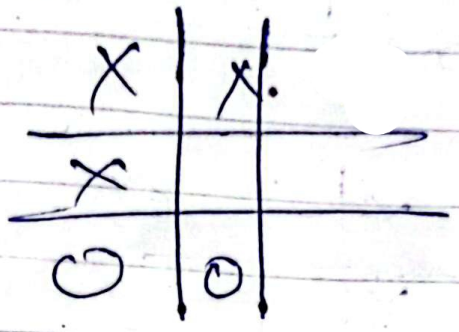
Time Comparisions:
- My Version: ~ 0.15s
- Google OR Tools ~ 0.03s
- GPT/Github ~ 0.02s

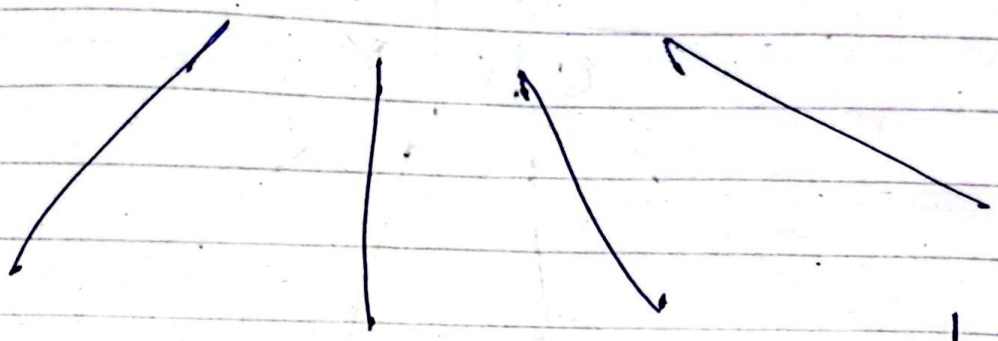
Improvement that can be done:
- Add variable ordering (MRV)
- Add Constraint propagation (like AC-3
- Reduce redundant constraint checks
- Use domain reduction + forward Checking.

Q4: leftmost



Q4: leftmost

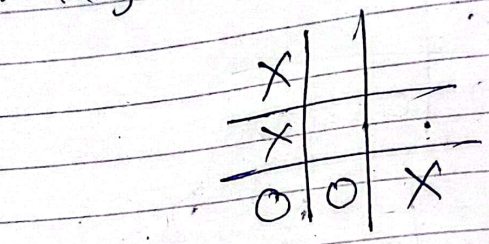


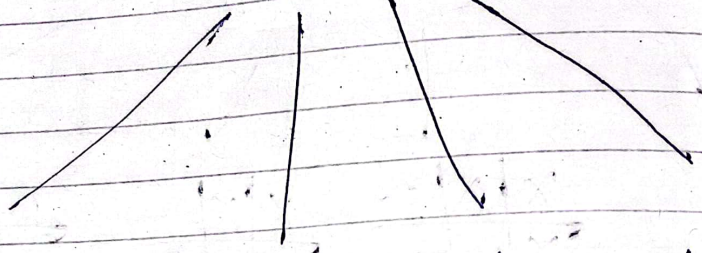


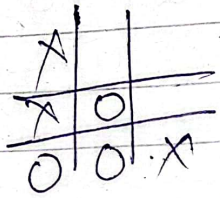
V = 100 V = 80 V = 80 V = -1000

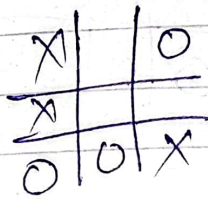
Best move to go with.

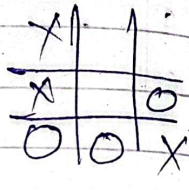
Q4: Right most.









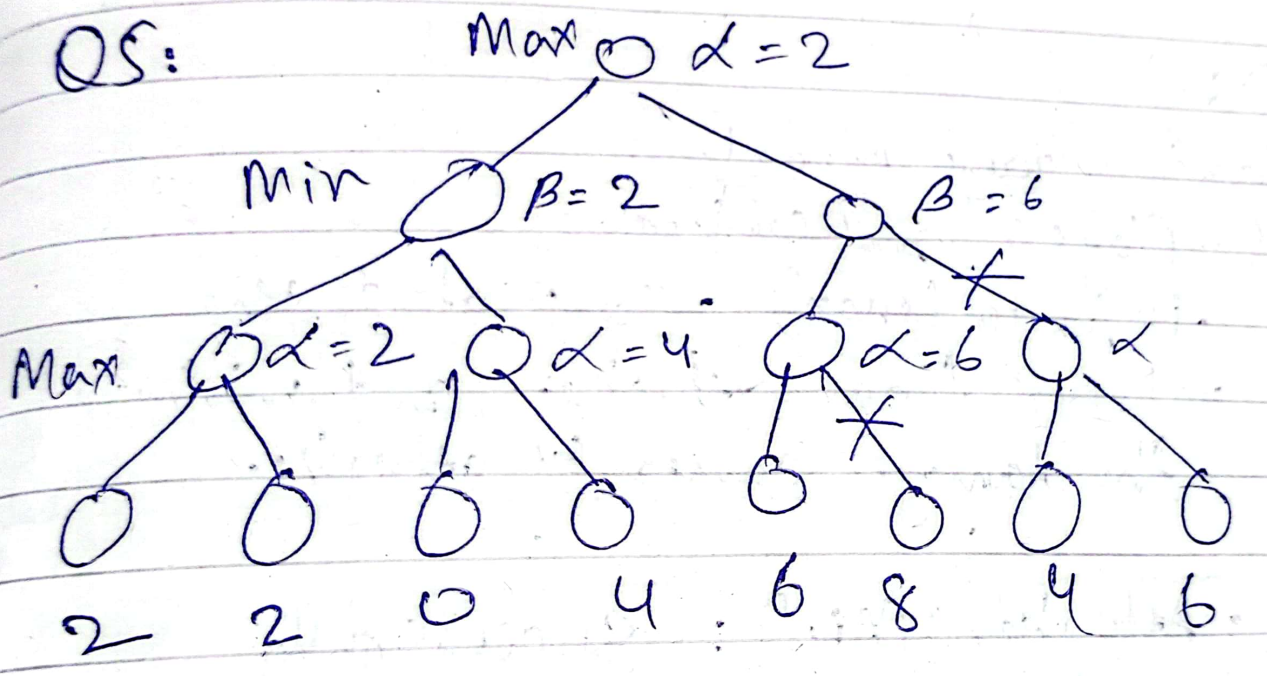


V=20 V=10 V=10 V=100

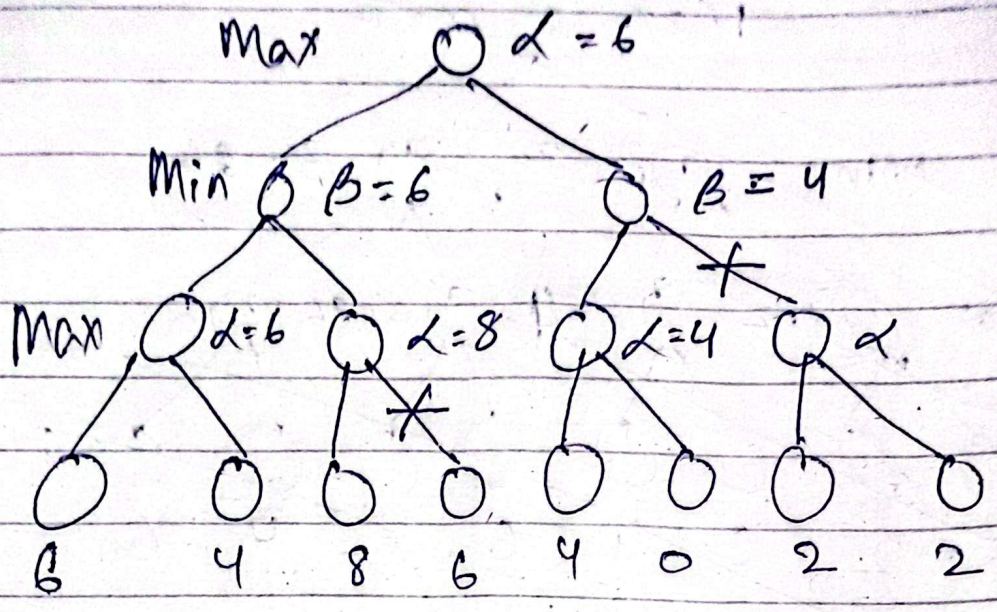
Best move to go with.

V=100

Q5:



B:



Q6:

Part(a): Game Model.

1- Players and Objectives.

- Defender (Max): To protect the network from attacker and minimize the damage caused by attacks.

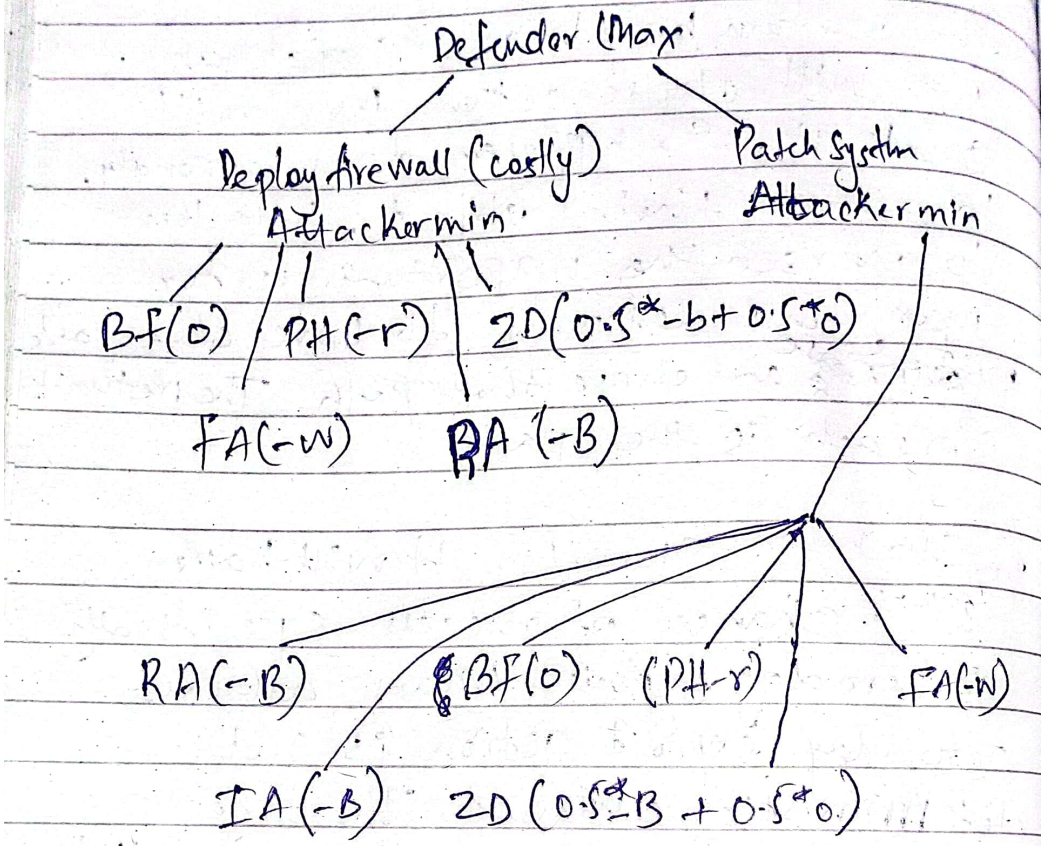
- Attacker (Min): Successfully penetrate the network and exploit the vulnerabilities.

2. Decision Making:

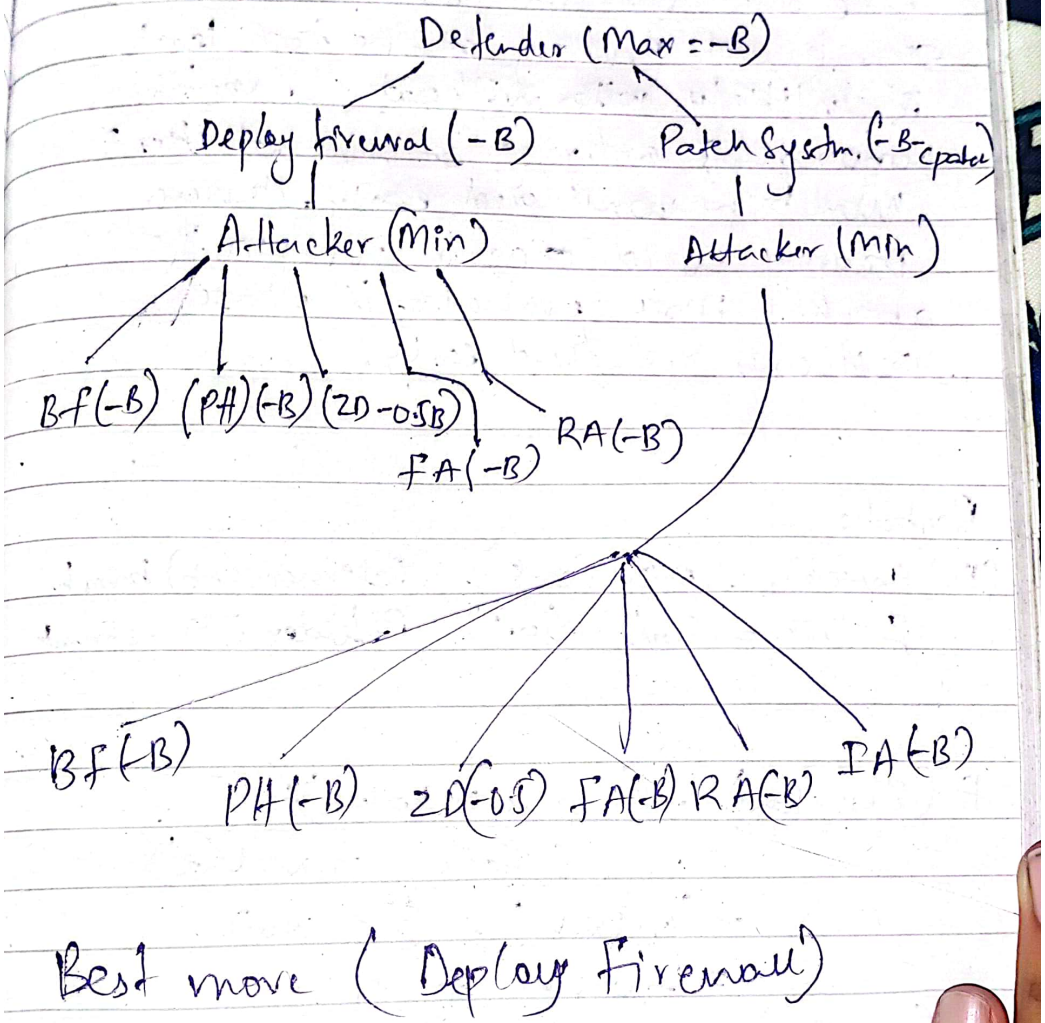
- This is a turn based adversarial game. Max will chose action Min will counter it. Each player does rationaly. to achieve their object. Attacker to worsen the opportunities for max and defender to have observable worst case and chose that path. The network breach is the path.

3. Stochastic Elements: It will have 50% chance of success specifically in zero day exploit. Means attacker. Zero day exploit action is not deterministic outcome. The tree will need account for these probabilities.

Part b:


Defender (Max)
Deploy Firewall (costly)
Patch System
Attacker min
BF(0)
PH(-r)
2D(0.5*-b+0.5*0)
FA(-W)
RA(-B)
RA(-B)
BF(0)
(PH-r)
FA(-W)
IA(-B)
2D(0.5*-B+0.5*0)

Part C:



Best move (Deploy Firewall)

2. Alpha beta pruning : In this simplified tree with one-level attacker response significant pruning at the top level is unlikely without a specific unfavorable ordering of the attacker's move being considered early. However pruning could occur within the attackers move evaluation if worse outcomes are found early.

Part d:

(1) Success = 50% (0.5) Defender (-b) breach
Failure = 50% (0.5) Defender (0) no breach

E (Zero-Day) = (Success × value) + (Failure × value)
= (0.5 × -b) + (0.5 × 0)
= -0.5b + 0
E (Zero Day) = -0.5b

simplified
response
level
pecific
tacker 3
never
the
se

(2) The Defender might favour the Patch System strategy more if the expected cost of zero day exploit combined with the patching cost is less severe than the guaranteed worst case scenario after deploy firewall.