Ibrahim Johar Farooqi
23K-0074
BAI-4A

Date ____ 20__

AI Assignment 2

Q.2) Dry run of genetic Algorithm

↳ encoding

[1,2,3,1,2,3,1] → where (Task1 → Facility1, Task4 → Facility1 etc)

↳ population – generation

randomly generated 6 chromosomes

↳ A: [2,1,1,3,2,2,1] 485
↳ B: [1,2,3,1,2,3,3] 471
↳ C: [3,3,2,2,1,1,2] 478
↳ D: [2,2,1,1,3,3,3] 495
↳ E: [1,3,2,3,1,2,1] 462
↳ F: [3,1,3,2,2,1,2] 475

↳ fitness function

chromosomes	cost	Fitness (1/cost)	Selection Probability
A [2,1,1,3,2,2,1]	485	0.00206	16.82%
B [1,2,3,1,2,3,3]	471	0.00212	17.31%
C [3,3,2,2,1,1,2]	478	0.00209	17.09%
D [2,2,1,1,3,3,3]	495	0.00202	16.49%
E [1,3,2,3,1,2,1]	462	0.00216	17.65%
F [3,1,3,2,2,1,2]	475	0.00211	17.11%

↳ selection (roulette wheel selection)

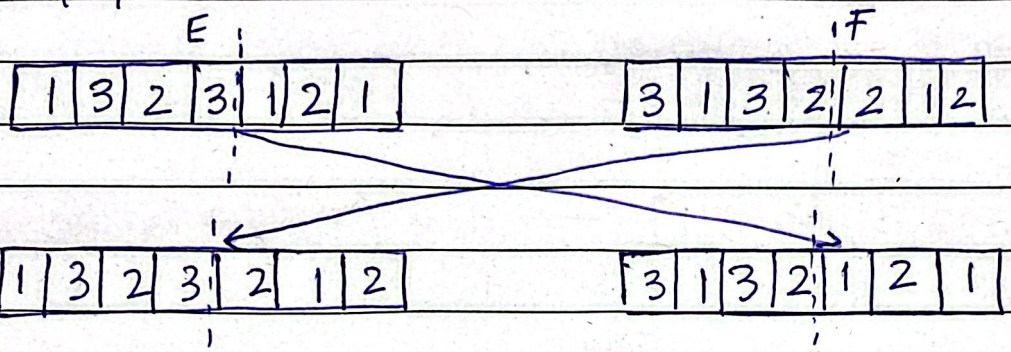
↳ random generated selection pt
↳ chromosomes w/ higher prob more likely to be chosen
↳ chromosome E & F chosen/ selected.

Date _____ 20___

↳ crossover point

↳ point at 4.

parent:



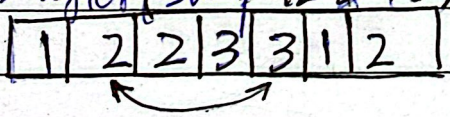
new children: G H

↳ mutation

↳ child G

↳ before:

↳ after (swap T2 & T5):



← new offspring

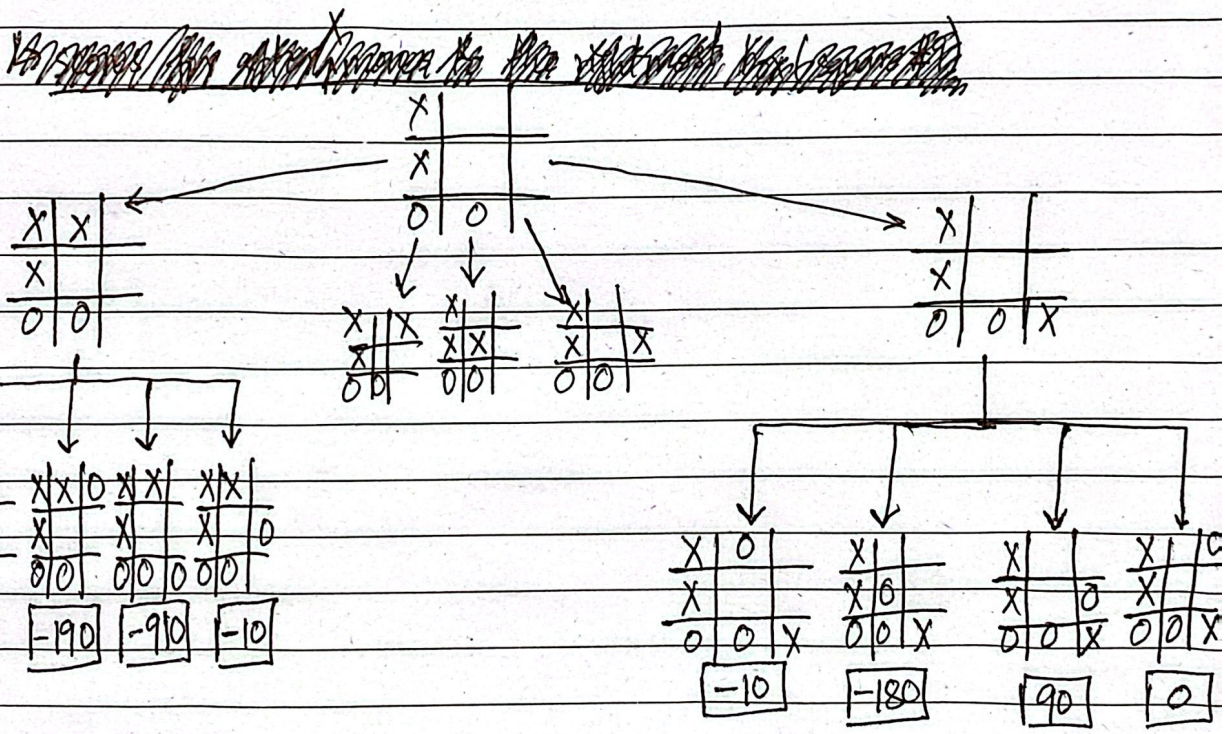
↳ new generation

↳ evaluate new population fitness

↳ repeat algorithm from fitness to mutation until convergence

Date _____ 20___

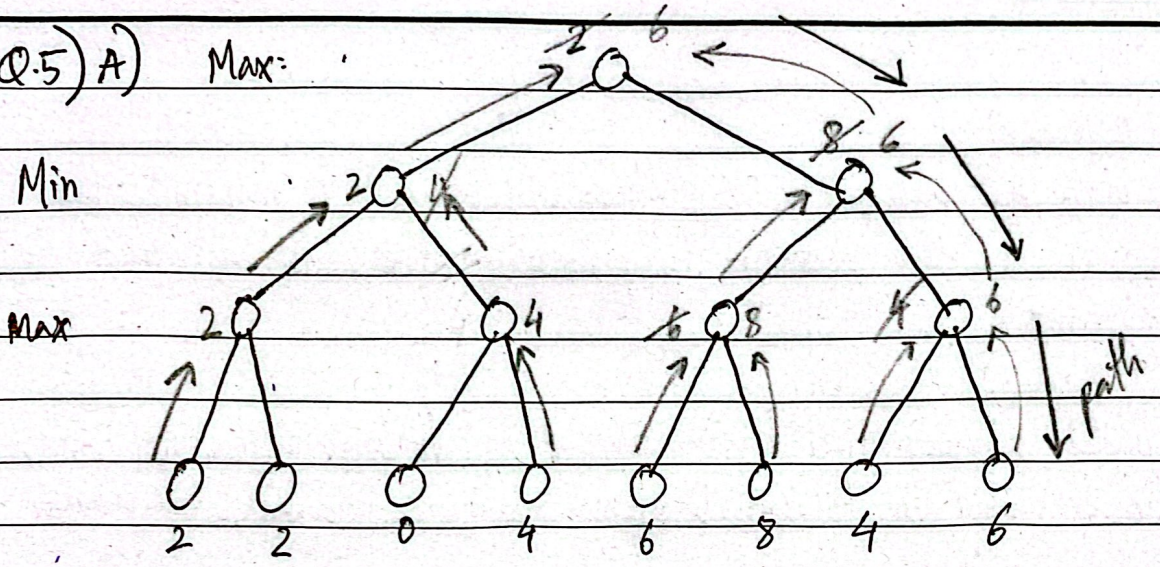
Q.4) value V = 0
do over all rows, columns, diagonals R:
if R contains three Xs; V = +1000
else if R contains three Os, V = -1000
else when R contains only two Xs, V = V + 100
else when R contains only one X, V = V + 10
else when R contains only two Os, V = V - 100
else when R contains only one O, V = V - 10
end do
return V



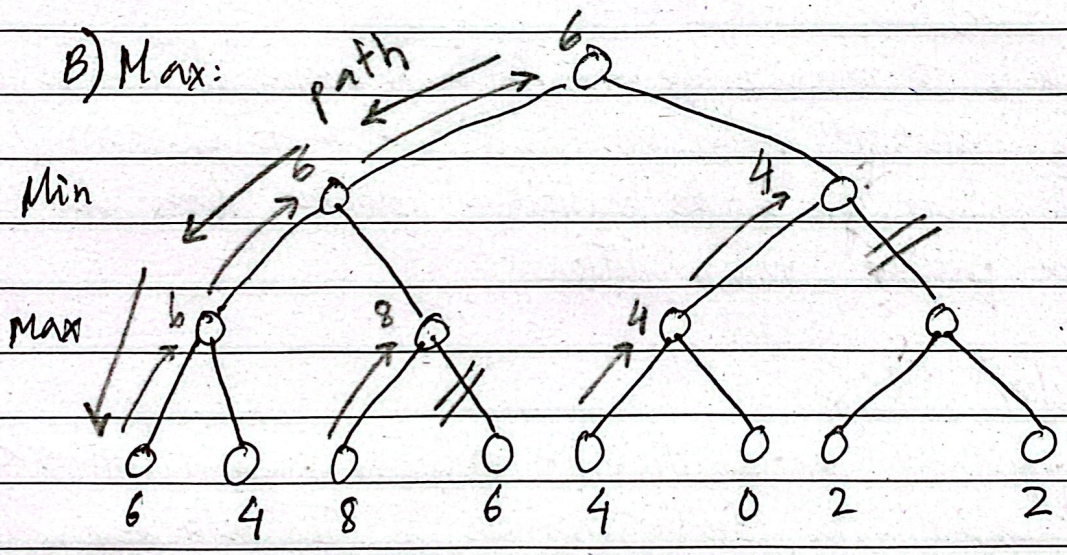
(PRUNE = //)

Date _____ 20___

Q.5) A) Max:



B) Max:



Date _____ 20__

Q.6) a)

↳ 1. Max (Defender)

↳ It is the AI powered IDS, whose objective is to minimize the damage to the network by preventing external attacks to the network

Min (Attacker)

↳ It is the adversarial entity attempting to breach the network, whose goal is to maximise damage through using various attacks.

↳ 2. Max (Defender)

↳ Objective is to minimize the probability of successful attacks, as it detects intrusions earlier on, as it continues to maintain integrity, where it blocks malicious attacks, alerts administrators or even patches vulnerabilities

Min (Attacker)

↳ This exploits the vulnerabilities in order to breach network. i.e stealing data, disrupt services, ... The attacker attempts to avoid being detected while simultaneously maximising the success rate of their exploits in the process.

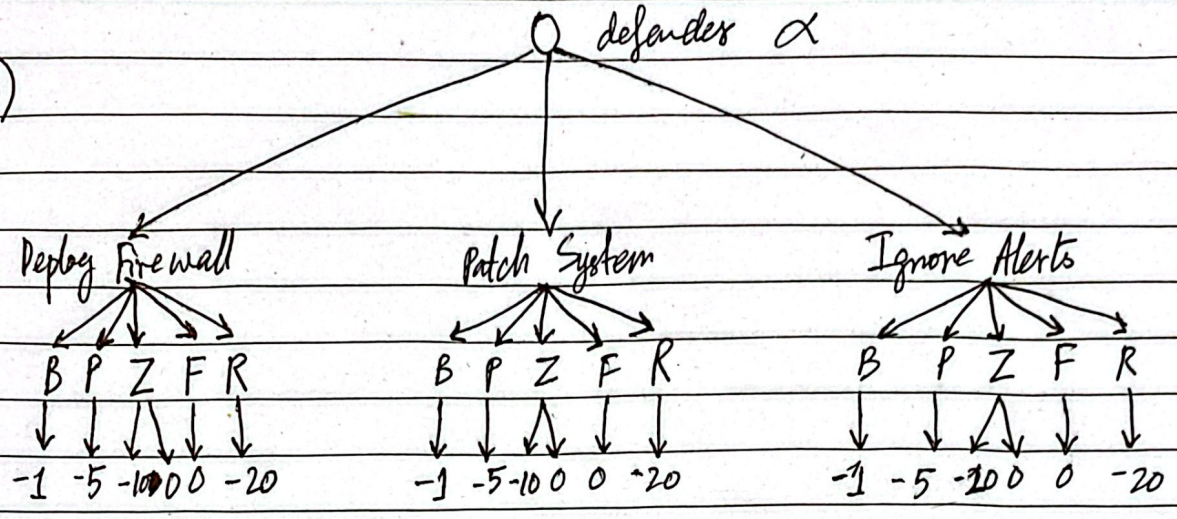
↳ 3. Stochastic Elements

↳ Probabilistic attacks like zero-day exploitation with 50% success rate, introduces uncertainty as the defender may very well need to prioritize its focus from worst-case to average case based on probability like expectimax

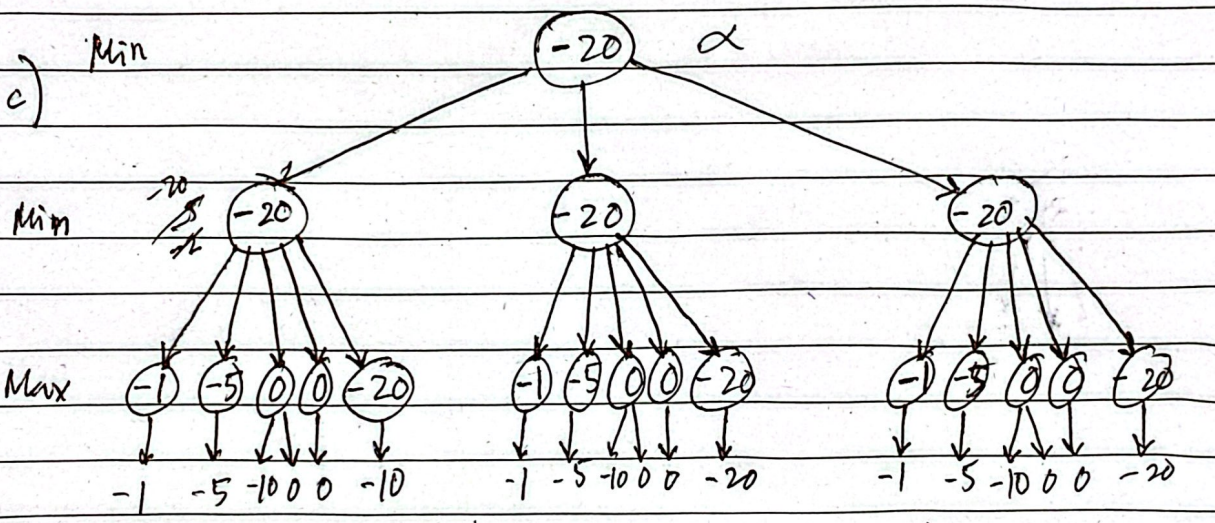
Date ____ 20 ____

Q.6)

b)



c)



d) ↳1.

success (50%) → damage = -10

failure (50%) → damage = 0

expected value = $(0.5 \times (-10)) + (0.5 \times 0) = -5$

2. Minimax

↳ defender assumes worst case scenario (zero-day exploits succeeds then -100), it is better to always deploy the firewall.

Expectimax — defender utilises & uses the expected value(0) which makes the zero day exploits on average less threatening. If fake attacks are likely then it may prefer patch sys or even ignore alerts, taking a much more balanced approach than over defending