Homework1

Haoyu Guan[1]

[1]Questrom School of Business, Boston University

2020.02.11

1 Exercise 1

One extension of the model of the double spending problem for the blockchain is to allow the attacker to give up after the attacked is n blocks behind. This is related to the following problem. Suppose that the gambler continues to bet until either wins n dollars or loses m dollars. What is the probability that the gambler quits as a winner?

Those two things are the same with gambler's ruin problem with $N = n + m$

$$Q_i = pQ_{i+1} + (1-p)Q_{i-1}$$

Q_m means the pro. of win n dollars to N before lose m dollars to 0

so. $$Q_{i+1} - Q_i = \frac{q}{p}(Q_i - Q_{i-1})$$

$$\Rightarrow Q_i = \begin{cases} \dfrac{1-(q/p)^i}{1-(q/p)^N} & \text{if } p \neq \frac{1}{2} \\ \dfrac{i}{N} & p = \frac{1}{2} \end{cases}$$

$$\Rightarrow Q_m = \begin{cases} \dfrac{1-(q/p)^m}{1-(q/p)^{m+n}} & p \neq \frac{1}{2} \\ \dfrac{m}{m+n} & p = \frac{1}{2} \end{cases}$$

2 Exercise 2

One extension of the model of the double spending problem for the blockchain is to allow the winning probability depending on the state variable. This is related to the following problem. Suppose in the gamblers ruin problem that the probability of winning depending on the gamblers current fortune, i.e. pj is the probability that the gambler wins a bet when the wealth is j. Compute Q_i

$$Q_0 = 0 \qquad Q_N = 1$$

$$Q_i = p_i Q_{i+1} - (1-p_i) Q_{i-1}$$

$$\Rightarrow Q_{i+1} - Q_i = \frac{1-P_i}{P_i}(Q_i - Q_{i-1})$$

$$\Rightarrow Q_{i+1} - Q_i = \frac{1-P_i}{P_i} \cdot \frac{1-P_{i-1}}{P_{i-1}} \cdots \frac{1-P_1}{P_1} Q_1$$

$$\Rightarrow Q_i - Q_{i-1} = \frac{1-P_{i-1}}{P_{i-1}} \cdots \frac{1-P_1}{P_1} Q_1$$

$$Q_i - Q_1 = Q_i - Q_{i-1} + Q_{i-1} - Q_{i-2} + \cdots + Q_2 - Q_1$$

$$= \left[\frac{1-P_1}{P_1} + \frac{1-P_2}{P_2} \frac{1-P_1}{P_1} + \cdots + \prod_{k=1}^{i-1} \frac{1-P_k}{P_k}\right] Q_1$$

$$= \quad \text{let} \quad C_i = \prod_{k=1}^{i} \frac{1-P_k}{P_k}$$

$$\Rightarrow Q_i = [1 + C_1 + C_2 + \cdots + C_{i-1}] Q_1$$

$$1 = Q_N = [1 + C_1 + C_2 + \cdots + C_{N-1}] Q_1$$

$$\Rightarrow Q_1 = \frac{Q_N}{[1 + c_1 + c_2 + \cdots + c_{N-1}]}$$

$$= \frac{1}{1 + c_1 + c_2 + \cdots + c_{N-1}}$$

$$\Rightarrow Q_i = \frac{1 + c_1 + c_2 + \cdots + c_{i-1}}{1 + c_1 + c_2 + \cdots + c_{N-1}}$$