COS 445 - PSet 5, Problem 1

Odysseus

April 28, 2021

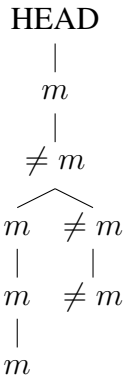
Problem 1: Super Selfish Mining

Part a

We wish to determine which of the six broadcasting cases is triggered during each round. We present the following sequence of broadcasts:

$$\boxed{\langle c_4, c_1, c_5, c_6, c_6, c_2, c_3 \rangle}$$

To help visualize these broadcasts, we draw a tree representing the blocks that are mined during each round and their connectivity. Let m denote blocks mined by miner m, and let $\neq m$ denote blocks mined by other miners. Let the label HEAD mark the end of the blockchain before the sequence of rounds begins.



Before the given sequence begins, we assume that no other blocks have been mined on top of HEAD at time step $t = 0$. This means that after m mines a block during $t = 1$, they will trigger broadcast case c_4 since $h_m(1) = h(1) + 1$ and because it is given that $M_2 \neq m$.

At $t = 2$, broadcast case c_1 is triggered since $h_m(2) \leq h(2)$ after M_2 mines a new block on top of the block m mined at $t = 1$.

At $t = 3$, it is given that $M_3 = m$ and that m will mine the next round as well. Therefore broadcast case c_5 will be triggered since with the addition of m's new block $h_m(3) = h(3) + 1$.

At $t = 4$, we know that $M_4 = m$. Since we now have $h_m(4) > h(4) + 1$, m will trigger broadcast case c_6.

At $t = 5$, the same situation occurs as in $t = 4$ so m will trigger case c_6 again.

At $t = 6$, it is given that $M_6 \neq m$ and that m will not mine the next round. Because we still have $h_m(t) > h(t) + 1$, m will trigger case c_2. Visually, what has happened is that a fork has appeared off the block that M_2 mined during $t = 2$.

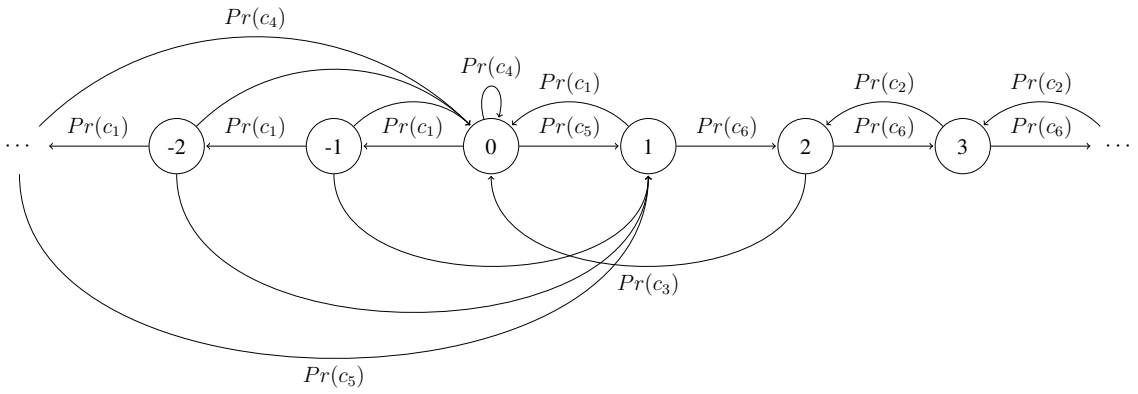
At $t = 7$, it is given that $M_7 \neq m$ in a similar fashion to $t = 6$. Since $M_7 \neq m$ but $h_m(7) = h(7) + 1$, m will trigger case c_3.

At the end of the sequence, m will have announced the blocks it previously hid from the rest of the network. Since m's additions are longer than the public chain, the public chain will effectively be "pruned" and m will claim the rewards.

Part b

We wish to analyze the expected reward achieved with the super selfish mining strategy using a Markov chain.

We present the following Markov chain:



Where the probability of each case is equal to the following:

Probability	Value
$Pr(c_1)$	$1-\alpha$
$Pr(c_2)$	$1-\alpha$
$Pr(c_3)$	$1-\alpha$
$Pr(c_4)$	$\alpha(1-\alpha)$
$Pr(c_5)$	α^2
$Pr(c_6)$	α

The value of each state is simply the difference calculated from $h_m(t) - h(t)$, hence there is an infinite list of states to correspond to every possible difference in height. For each state, we note that the sum of all transitions for that state is equal to 1.

The value of each probability follows relatively simply. $Pr(c_1)$, $Pr(c_2)$, and $Pr(c_3)$, for example, come from the probability that the miner for a particular time step is $\neq m$ (which is given as $1-\alpha$). Likewise, moving from a difference of 1 to a difference of 2, 3, and so on is just the probability that m is the miner (which is given as α). To maintain a difference of 0, it must be that m is the miner one round and not the following round (or vice versa). Thus the probability is equal to the product $\alpha(1-\alpha)$. Likewise, moving from any state with a difference < 0 to state 1 is proportional to the probability that m is the miner twice in a row (or α^2).