Clearly, if

$$E(f) > 0,$$

then Charlie has chosen a better strategy over the null strategy. Thus we seek to maximize, if possible, the value $E(f)$ over all possible strategies. It is not so simple to develop a formula for each possible strategy. Short of maximizing over all strategies, we are happy to find at least one strategy that yields a positive expectation. We start with the simple strategy "mine only when not behind by more than k blocks."

Remark 5.1. We are presenting the analysis from Charlie's perspective, which is omniscient. It is possible in general that a double-spend attempt may involve a secret fork (see §5.3). Suppose you want perform a double-spend by sending an output to yourself and also to an exchange. You keep the output to yourself secret and mine this output onto a chain in secret, hoping to spring your chain onto the network once you have been credited by the exchange and are able to withdraw elsewhere or take possession of whatever you purchased. The analysis from the viewpoint of the exchange (how many blocks should pass before we credit the transaction in order to minimize risk?) is slightly more complicated as it involves the time variable as well. A much more general discussion of double-spends, taking other angles and considerations into account, is offered in a series of works by Cyril Grunspan and Ricardo Pérez-Marco [20, 22, 23].

5.1 Simplest strategy: Charlie elects to mine his own chain when less than k blocks behind

This game starts at state $(1, 0)$, meaning that Charlie is one block behind and has yet to mine any blocks on his forked chain. Charlie commits to a strategy of mining his own chain until the moment that his chain falls k blocks behind, at which point Charlie will switch back to the main chain.

First of all, we would like to know the probability that Charlie will win, given the current state. The probability of winning depends only on the first state variable, so we define

$$w_i := \text{probability that Charlie will win, given that Charlie is } i \text{ blocks behind.}$$

5.1.1 Recursion formulas

The analysis depends on the conditional probability formula (2.6). Note that by letting W denote the random variable that is 1 if Charlie wins and 0 if he loses, we have

$$w_i = \mathbb{E}[W \mid \text{Charlie is } i \text{ blocks behind}].$$

If Charlie is i blocks behind, there are two events that could happen immediately next, and we know these probabilities. We write

$$\begin{aligned}&\mathbb{E}[W \mid \text{Charlie is } i \text{ blocks behind}]\\ &\quad = \mathbb{E}\left[W \mid \begin{array}{c}\text{Charlie is } i \text{ blocks behind}\\ \text{and wins the next block}\end{array}\right] P(\text{Charlie wins the next block})\\ &\qquad + \mathbb{E}\left[W \mid \begin{array}{c}\text{Charlie is } i \text{ blocks behind}\\ \text{and loses the next block}\end{array}\right] P(\text{Charlie loses the next block})\end{aligned}$$

by (2.6). But

$$\mathbb{E}\left[W \mid \begin{array}{c}\text{Charlie is } i \text{ blocks behind}\\ \text{and loses the next block}\end{array}\right] = \mathbb{E}[W \mid \text{Charlie is } i+1 \text{ blocks behind}],$$

so we can write in simpler terms

$$w_i = pw_{i-1} + (1-p)w_{i+1}. \tag{5.3}$$

This is true for any i in between –1 and k, and it becomes most useful if we start working from the end points. We know that

$$w_{-1} = 1,$$

which simply states that if Charlie is –1 blocks behind, he has pulled ahead, and all miners now mine his chain; he has won. At the other end,

$$w_k = 0, \tag{5.4}$$

stating that Charlie gives up the fight and concedes defeat when he is k blocks behind. There are multiple ways to proceed in solving for the values w_i. We will offer two. The first method is somewhat straightforward and gives nice-looking formulas for smaller values of k. The second method uses difference equations and is somewhat more high-tech. The formulas are not as pretty but this method will lend itself to more complicated computations in later sections and will be easy to program using linear algebra.

5.1.2 A method for computing winning probability

Begin by noting that

$$\begin{aligned}w_{k-1} &= pw_{k-2} + (1-p)w_k\\ &= pw_{k-2}\end{aligned}$$

from (5.4). Proceed with the goal to continue to define w_i in terms of w_{i-1}, implicitly defining q_i by writing

$$w_i = q_i w_{i-1}. \tag{5.5}$$

We have determined that

$$q_{k-1} = p.$$

With this in mind, we may write, using (5.3) and (5.5),

$$\begin{aligned} w_{i-1} &= pw_{i-2} + (1-p)w_i \\ &= pw_{i-2} + (1-p)q_i w_{i-1} \end{aligned}$$

or

$$w_{i-1}(1-(1-p)q_i) = pw_{i-2},$$

which can be solved as

$$w_{i-1} = \frac{pw_{i-2}}{(1-(1-p)q_i)},$$

that is,

$$q_{i-1} = \frac{p}{(1-(1-p)q_i)}.$$

We can iterate this, until we get to

$$\begin{aligned} w_0 &= q_0 w_{-1} \\ &= q_0, \end{aligned}$$

where

$$\begin{aligned} q_0 &= \frac{p}{(1-(1-p)q_1)}, \\ q_1 &= \frac{p}{(1-(1-p)q_2)}, \\ &\dots \\ q_{k-1} &= p, \\ q_k &= 0. \end{aligned} \tag{5.6}$$

For example, when $k = 2$, we have

$$q_1 = p,$$

$$q_0 = \frac{p}{(1-(1-p)p)}.$$

Hence

$$w_0 = \frac{p}{(1-(1-p)p)},$$
$$w_1 = \frac{p^2}{(1-(1-p)p)}.$$

Exercise 5.1. Let $m = -(1-p)p$. Use (5.6) to show that there is a sequence of polynomials $\rho_i(m)$ such that for a given k, we have

$$q_{k-i} = p\frac{\rho_{i-2}(m)}{\rho_{i-1}(m)}$$

and

$$w_0 = p\frac{\rho_{k-2}(m)}{\rho_{k-1}(m)},$$
$$w_1 = p^2\frac{\rho_{k-3}(m)}{\rho_{k-1}(m)},$$
$$\cdots$$
$$w_{k-1} = p^k\frac{\rho_{-1}(m)}{\rho_{k-1}(m)},$$

where

$$\rho_{-1}(m) = 1,$$
$$\rho_0(m) = 1,$$

and the polynomials satisfy the recursion relation for $i \geq 1$

$$\rho_i(m) = \rho_{i-1}(m) + m\rho_{i-2}(m).$$

5.1.3 Another method: difference equations

While the above by-hand method will yield a formula for w_i in any given situation, there is another observation that offers us a streamlined computation. Consider the equation

$$w(x) = pw(x-1) + (1-p)w(x+1), \tag{5.7}$$

thinking here of w as a function of the continuous variable x on the interval $[-1, k]$. The equation appears to be a second-order finite difference equation. Drawing from intu-

ition from second-order homogeneous ordinary differential equations (ODEs) (cf. [32, Section 2.1]) we take a guess of the solution of the form

$$w(x) = e^{\tau x},$$

in which case (5.7) becomes

$$e^{\tau x} = pe^{\tau x - \tau} + (1-p)e^{\tau x + \tau}.$$

Dividing by $e^{\tau x}$,

$$1 = pe^{-\tau} + (1-p)e^{\tau}$$

which can be solved as

$$e^{\tau} = \frac{p}{(1-p)}.$$

Hence,

$$w(x) = \left(\frac{p}{1-p}\right)^x$$

is a solution to (5.7). Also note that if w is constant, (5.7) will be solved. So we define two solutions,

$$w_1(x) = \left(\frac{p}{1-p}\right)^x,$$
$$w_2(x) = 1,$$

which are independent solutions (two functions are independent if one function is not simply a real multiple of the other; more than two functions are independent if no function is a linear combination of multiples of the other functions). Noting that equation (5.7) can be written as a linear homogeneous equation,

$$w(x) - pw(x-1) - (1-p)w(x+1) = 0,$$

we may easily check that two solutions added together will also be a solution. By general theory for homogeneous equations, as in the case of linear second-order ODEs (cf. [32, Section 2.1]), we can write the general solution as

$$w(x) = c_1\left(\frac{p}{1-p}\right)^x + c_2.$$

By prescribing boundary values

$$w(-1) = 1,$$
$$w(k) = 0,$$

we may solve for the coefficients

$$c_1\left(\frac{p}{1-p}\right)^{-1} + c_2 = 1, \tag{5.8}$$

$$c_1\left(\frac{p}{1-p}\right)^{k} + c_2 = 0 \tag{5.9}$$

and obtain

$$c_1 = \frac{p}{1-p}\frac{1}{(1-(\frac{p}{1-p})^{k+1})}, \tag{5.10}$$

$$c_2 = -\left(\frac{p}{1-p}\right)^{k+1}\frac{1}{(1-(\frac{p}{1-p})^{k+1})}$$

$$= -\left(\frac{p}{1-p}\right)^{k} c_1. \tag{5.11}$$

Hence,

$$w(x) = \frac{(\frac{p}{1-p})^{x+1} - (\frac{p}{1-p})^{k+1}}{1-(\frac{p}{1-p})^{k+1}}. \tag{5.12}$$

For simplicity of computation in the future, we will let

$$m := \frac{p}{1-p}$$

and note that the coefficients are determined by the solution to the following linear system, which uses a matrix to express equations (5.8) and (5.9):

$$\begin{pmatrix} m^{-1} & 1 \\ m^{k} & 1 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{5.13}$$

Remark 5.2. The above expression (5.12) is reminiscent of the formula for computing sums of geometric series. This is not a coincidence. Most of the results in this section and the next could be derived using geometric series.

When $k = 2$ we have

$$w(0) = \frac{(\frac{p}{1-p})^{1} - (\frac{p}{1-p})^{3}}{1-(\frac{p}{1-p})^{3}},$$

$$w(1) = \frac{(\frac{p}{1-p})^2 - (\frac{p}{1-p})^3}{1 - (\frac{p}{1-p})^3}.$$

5.1.4 Computing expected values

We now compute the expected value to Charlie of the function f, defined by (5.2). We are most interested in

$$\mathbb{E}[f \mid (1,0)],$$

that is, the expected benefit of mining the reorg strategy when starting from one block behind.

From state $(1,0)$ there are two possible next states, $(2,0)$ and $(0,1)$, so we write, again using (2.6),

$$\mathbb{E}[f \mid (1,0)] = p\mathbb{E}[f \mid (0,1)] + (1-p)\mathbb{E}[f \mid (2,0)].$$

Introducing a less cumbersome notation,

$$e(x,s) := \mathbb{E}[f \mid (x,s)],$$

this relation becomes

$$e(1,0) = pe(0,1) + (1-p)e(2,0).$$

For brevity, we only present the solution method using difference equations. Unlike in the previous example, when there was only one state variable, in this case, we have two. Observe the following relation:

$$e(x,s) = pe(x-1,s+1) + (1-p)e(x+1,s). \tag{5.14}$$

Claim 5.1. *We have*

$$e(x,s+1) = e(x,s) + w(x) - 1. \tag{5.15}$$

Proof. Given we are at state (x,s) and following a given strategy that only depends on x, the probability space of possible paths starting at (x,s) and going until the game ends is identical to the probability space of possible paths starting at $(x,s+1)$. For each path that ends in success, the reward to Charlie is the same in both cases, because all of the block rewards that would have been won along the way are granted when he takes the longest chain. But if the path ends in a loss for Charlie, he loses all block rewards he would have won had he pursued the null strategy. He loses one more block reward if

the path started from state $(x, s+1)$ than if the same path had started from path (x, s). The difference will be the probability of a loss, which is $1 - w(x)$. □

Exercise 5.2. Using a Bernoulli space and arguments from §2.4.2.1, offer a more rigorous proof of Claim 5.1.

Now equation (5.14) becomes

$$\begin{aligned} e(x,s) &= p\big[e(x-1,s) + w(x-1) - 1\big] + (1-p)e(x+1,s) \\ &= pe(x-1,s) + (1-p)e(x+1,s) + p\big(w(x-1) - 1\big). \end{aligned}$$

This now only involves a single value in the second state variable. So if we are interested in computing $e(x, 0)$, we may define

$$e(x) := e(x, 0),$$

which must satisfy

$$e(x) - pe(x-1) - (1-p)e(x+1) = p\big(w(x-1) - 1\big) \tag{5.16}$$

$$= p\left(c_1\left(\frac{p}{1-p}\right)^{x-1} + c_2 - 1\right) \tag{5.17}$$

for the c_1 and c_2 obtained above in (5.10). This is similar to the finite difference equation (5.7) in x, but with extra terms on the right-hand side, making this a non-homogeneous equation. As with second-order linear non-homogeneous ODEs, we first find a particular solution and then add this to the solutions w_1 and w_2 obtained previously to obtain the general solution.

Consider the non-homogeneous finite difference equation

$$y(x) - py(x-1) - (1-p)y(x+1) = p(c_2 - 1). \tag{5.18}$$

We try a very basic guess (this is similar to the method of undetermined coefficients from ODE theory)

$$y_1(x) := \beta x$$

for some constant β to be determined. Plugging y_1 into (5.18) and solving for β, we get

$$\beta = \frac{p(c_2 - 1)}{2p - 1}.$$

Thus

$$y_1 = p\frac{1 - c_2}{1 - 2p}x$$

solves (5.18). Next we solve

$$y(x) - py(x-1) - (1-p)y(x+1) = pc_1\left(\frac{p}{1-p}\right)^{x-1}. \tag{5.19}$$

For this we try a solution of the form

$$y_2(x) := ax\left(\frac{p}{1-p}\right)^{x}.$$

Plugging y_2 into (5.19) and doing some straightforward computations leads to

$$a = \frac{c_1(1-p)}{1-2p}. \tag{5.20}$$

We conclude that

$$y_2(x) = \frac{(1-p)}{(1-2p)}c_1 x\left(\frac{p}{1-p}\right)^{x}$$

is a solution to (5.19).

Thus we arrive at the general solution to (5.16):

$$y(x) = \tilde{c}_1\left(\frac{p}{(1-p)}\right)^{x} + \tilde{c}_2 + p\frac{1-c_2}{(1-2p)}x + \frac{(1-p)}{(1-2p)}c_1 x\left(\frac{p}{1-p}\right)^{x}.$$

To be clear, c_1 and c_2 are the coefficients that were previously determined by (5.10), while $\tilde{c}_1$ and $\tilde{c}_2$ are coefficients that need to be solved when finding a solution to a boundary value problem. We can now solve for the boundary conditions:

$$e(-1) = \lambda,$$
$$e(k) = 0.$$

Recall that when Charlie takes the lead, he wins the blocks he would have won, plus the extra λ times the block reward, which is the value of the transaction. If Charlie gives up mining without having won a single block, he is no better or worse off than if he mined the null strategy. This analysis is available because we have reduced the equation to one where the second state variable is 0.

Solving with the boundary conditions determines $\tilde{c}_1$ and $\tilde{c}_2$ by

$$\tilde{c}_1\left(\frac{p}{(1-p)}\right)^{-1} + \tilde{c}_2 - \frac{p(1-c_2)}{(1-2p)} - \frac{(1-p)}{(1-2p)}c_1\left(\frac{p}{1-p}\right)^{-1} = \lambda, \tag{5.21}$$

$$\tilde{c}_1\left(\frac{p}{(1-p)}\right)^{k} + \tilde{c}_2 + \frac{p(1-c_2)}{(1-2p)}k + \frac{(1-p)}{(1-2p)}c_1 k\left(\frac{p}{1-p}\right)^{k} = 0. \tag{5.22}$$

It is convenient to write this as a 2×2 system of equations,

$$\begin{pmatrix} m^{-1} & 1 \\ m^k & 1 \end{pmatrix} \begin{pmatrix} \tilde{c}_1 \\ \tilde{c}_2 \end{pmatrix} = \begin{pmatrix} \lambda + mr(1-c_2) + rc_1 m^{-1} \\ -mr(1-c_2)k - rc_1 k m^k \end{pmatrix}$$
$$= \lambda \begin{pmatrix} 1 \\ 0 \end{pmatrix} + r \begin{pmatrix} m^{-1} & m \\ -km^k & -km \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_2 \end{pmatrix},$$

once again using less cumbersome notation

$$m = \frac{p}{1-p},$$
$$r = \frac{1-p}{1-2p},$$

with

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} m^{-1} & 1 \\ m^k & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{5.23}$$

Here

$$\begin{pmatrix} m^{-1} & 1 \\ m^k & 1 \end{pmatrix}^{-1} = \frac{1}{m^{-1} - m^k} \begin{pmatrix} 1 & -1 \\ -m^k & m^{-1} \end{pmatrix}$$

is the inverse matrix from standard linear algebra. Now

$$\begin{pmatrix} \tilde{c}_1 \\ \tilde{c}_2 \end{pmatrix} = \begin{pmatrix} m^{-1} & 1 \\ m^k & 1 \end{pmatrix}^{-1} \begin{pmatrix} \lambda + mr(1-c_2) + rc_1 m^{-1} \\ -mr(1-c_2)k - rc_1 k m^k \end{pmatrix}. \tag{5.24}$$

At this point we may plug the constants into the expression to obtain the function:

$$e(x,0) = \tilde{c}_1 m^x + \tilde{c}_2 + mr(1-c_2)x + rc_1 x m^x. \tag{5.25}$$

The expansion of this expression is messy and not particularly enlightening, so we leave it as is.

Example 5.1 ($p = 0.1$, k small). Suppose a miner with 10 % of the hashrate considers a strategy to mine a reorg chain if two or less blocks behind and give up if three blocks behind. Taking $p = 0.1$, $k = 3$ gives us

$$m = \frac{1}{9},$$
$$r = \frac{9}{8},$$
$$c_1 = \frac{1}{9} \frac{1}{1 - \frac{1}{9}^4} = \frac{729}{6{,}560}, \tag{5.26}$$

$$c_2 = -\frac{1}{9}^4 \frac{1}{1-\frac{1}{9}^4} = -\frac{1}{6{,}560},$$
$$\begin{pmatrix} \tilde{c}_1 \\ \tilde{c}_2 \end{pmatrix} = \begin{pmatrix} \frac{729}{6{,}560}\lambda + \frac{1{,}554{,}957}{8{,}606{,}720} \\ -\frac{1}{6{,}560}\lambda - \frac{3{,}234{,}573}{8{,}606{,}720} \end{pmatrix},$$

and

$$e(x) = \left(\frac{729}{6{,}560}\lambda + \frac{1{,}554{,}957}{8{,}606{,}720}\right)\left(\frac{1}{9}\right)^x - \frac{1}{6{,}560}\lambda - \frac{3{,}234{,}573}{8{,}606{,}720} + \frac{1}{8}\left(1 + \frac{1}{6{,}560}\right)x + \frac{9}{8} \times \frac{729}{6{,}560}x\left(\frac{1}{9}\right)^x.$$

We can plug in the values for x:

$$\begin{aligned} e(-1) &= \lambda, \\ e(0) &= \frac{91}{820}\lambda - \frac{6{,}561}{33{,}620}, \\ e(1) &= \frac{1}{82}\lambda - \frac{729}{3{,}362}, \\ e(2) &= \frac{1}{820}\lambda - \frac{405}{3{,}362}, \\ e(3) &= 0. \end{aligned}$$

We conclude that in order to mine with these odds, a miner starting with a one-block deficit is only motivated to attempt a reorg if

$$e(1) = \frac{1}{82}\lambda - \frac{729}{3{,}362} > 0, \tag{5.27}$$

that is,

$$\lambda > \frac{729}{41} \approx 17.78,$$

and for a two-block deficit,

$$\lambda > \frac{4{,}050}{41} \approx 98.78.$$

In other words, for a pool with 10 % of the hashrate, in order for it to be prudent to attempt to perform a reorg with a “mine to three blocks behind” strategy, when starting from two blocks behind, the reward would need to be roughly 100 times the block reward.

On the other hand, if a mining pool mines a transaction, only to discover that all the other pools have discovered another block seconds earlier, in order to push forward, this pool is wise to do so if