Statistical inference of relative stake

David Rusu[1] **and Alexander Mozeika**

[1]Status.im

E-mail: `davidrusu@status.im`

Abstract. We consider statistical inference of relative stake.

1. The Model

- N nodes participate in elections (or "lottery") at times $t_1, \ldots, t_T$ (see Figure 1).
- The election process is governed by the distribution

$$
\begin{aligned}
\mathrm{P}(\mathbf{s}(t)) &= \prod_{i=1}^{N} \mathrm{P}(s_i(t)) \\
&= \prod_{i=1}^{N} \left[\phi_f(\alpha_i)\, \delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\, \delta_{0;s_i(t)}\right], \qquad (1)
\end{aligned}
$$

- The probability of node i to win the lottery is [1]

$$\phi_f(\alpha) = 1 - (1-f)^{\alpha}, \qquad (2)$$

  where $\alpha_i = w_i / D^0[\{w_i\}]$ is the *relative* stake of node i, i.e. $\sum_{i=1}^{N} \alpha_i = 1$.
- The outcome of lottery of node i can be *observed* with the probability q and this happens *independently* from the other nodes.
- We assume that the total stake $D^0[\{w_i\}]$ is *not* changing on the time interval $[t_1, t_T]$.

	t_1	t_2	t_3	$\cdots$	t_T
1	[0]	0	[1]	$\cdots$	0
$\vdots$	1	0	0	$\cdots$	0
i	0	[1]	0	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
N	1	[0]	0	$\cdots$	1

Figure 1. The leader election and observation processes. Node $i \in [N]$ participates in the leader election (or "lottery") at times $t_1, \ldots, t_T$. The (binary) outcome of this lottery is either *observed* (numbers in square brackets) or *unobserved*.

2. Maximum likelihood (ML) inference of relative stake

We would like to infer the relative stake α_i of node i from the samples $\mathbf{s}(t_1), \ldots, \mathbf{s}(t_T)$, i.e. "data", generated from the distribution (1). However, not all components of $\mathbf{s}(t) \in \{0,1\}^N$ vectors are observed and we model this by the $\eta_i(t) \in \{0,1\}$ variables, organised in to the $\boldsymbol{\eta}(t) \in \{0,1\}^N$ vectors. Here $\eta_i(t) = 1$ and $\eta_i(t) = 0$ when the election outcome $s_i(t)$ of node i is, respectively, *observed* and *unobserved*. This combination of election and observation processes gives rise to the (conditional) probability distribution

$$\mathrm{P}(\mathbf{s}(t)|\boldsymbol{\eta}(t)) = \prod_{i=1}^{N} \mathrm{P}_i^{\eta_i(t)}(s_i(t)), \tag{3}$$

where $\mathrm{P}_i(s_i(t)) = \phi_f(\alpha_i)\, \delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\, \delta_{0;s_i(t)}$, of election outcomes of *observed* nodes at time t. The inference of relative stake α_i parameters can be done by maximising the log-likelihood of data

$$\mathcal{L}[\{\mathbf{s}(t)\}|\{\boldsymbol{\eta}(t)\}] = \log \prod_{t=1}^{T} \mathrm{P}(\mathbf{s}(t)|\boldsymbol{\eta}(t)), \tag{4}$$

where we replaced the set of time labels $\{t_1, \ldots, t_T\}$ by the set $[T] = \{1, \ldots, T\}$ to lighten the notation‡, subject to the constraint $\sum_{i=1}^{N} \alpha_i = 1$. To this end, applying the method of Lagrange multipliers, we first consider the derivative

$$\begin{aligned}
&\frac{\partial}{\partial \alpha_i} \left\{ \mathcal{L}[\{\mathbf{s}(t)\}|\{\boldsymbol{\eta}(t)\}] + \lambda \left(\sum_{j=1}^{N} \alpha_j - 1 \right) \right\} \\
&= \sum_{t=1}^{T} \eta_i(t) \frac{\partial}{\partial \alpha_i} \log \left[\phi_f(\alpha_i)\, \delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\, \delta_{0;s_i(t)} \right] + \lambda \\
&= \sum_{t=1}^{T} \eta_i(t) \frac{\frac{\partial}{\partial \alpha_i} \phi_f(\alpha_i) \left[\delta_{1;s_i(t)} - \delta_{0;s_i(t)} \right]}{\phi_f(\alpha_i)\, \delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\, \delta_{0;s_i(t)}} + \lambda \\
&= (1-f)^{\alpha_i} \log \left(\frac{1}{1-f} \right) \\
&\times \sum_{t=1}^{T} \eta_i(t) \frac{\delta_{1;s_i(t)} - \delta_{0;s_i(t)}}{\phi_f(\alpha_i)\, \delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\, \delta_{0;s_i(t)}} + \lambda \\
&= (1-f)^{\alpha_i} \log \left(\frac{1}{1-f} \right) \\
&\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t) \delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t) \delta_{0;s_i(t)} \right] + \lambda.
\end{aligned} \tag{5}$$

Hence in order to find α_i we need to solve the equation

$$\begin{aligned}
&(1-f)^{\alpha_i} \log \left(\frac{1}{1-f} \right) \\
&\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t) \delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t) \delta_{0;s_i(t)} \right] + \lambda = 0.
\end{aligned} \tag{6}$$

‡ Also for a set $\{f(t)|t \in [T]\}$ we will write $\{f(t)\}$ to reduce amount of notation.

2.1. Unconstrained $\lambda = 0$ case

For $\lambda = 0$, which corresponds to *unconstrained* variation of the log-likelihood (4), solving the equation (6) for α_i is equivalent to solving

$$\frac{\sum_{t=1}^{T} \eta_i(t)\delta_{1;s_i(t)}}{\sum_{t=1}^{T} \eta_i(t)\delta_{0;s_i(t)}} = \frac{\phi_f(\alpha_i)}{1-\phi_f(\alpha_i)} \tag{7}$$

and hence in this case the ML estimator of α_i is given by

$$\hat{\alpha}_i = -\frac{\log\left(1 + \frac{\sum_{t=1}^{T} \eta_i(t)\delta_{1;s_i(t)}}{\sum_{t=1}^{T} \eta_i(t)\delta_{0;s_i(t)}}\right)}{\log(1-f)}. \tag{8}$$

for $\sum_{t=1}^{T} \eta_i(t)\,\delta_{0;s_i(t)} > 0$. We note that the ratio $\frac{\sum_{t=1}^{T} \eta_i(t)\,\delta_{1;s_i(t)}}{\sum_{t=1}^{T} \eta_i(t)\,\delta_{0;s_i(t)}} = \frac{\hat{P}_i(1)}{1-\hat{P}_i(1)}$, where

$$\hat{P}_i(1) = \frac{1}{\sum_{t=1}^{T} \eta_i(t)} \sum_{t=1}^{T} \eta_i(t)\,\delta_{1;s_i(t)} \tag{9}$$

when $\sum_{t=1}^{T} \eta_i(t) > 0$, i.e. the ML estimator of the probability $\phi_f(\alpha_i)$. Suppose that the *true* parameters are α_i^0 and the data $\mathbf{s}(1), \ldots, \mathbf{s}(T)$ is sampled from the prob. distribution (1) which uses these parameters. Then averaging the estimator $\hat{P}_i(1)$ over the data gives us

$$\begin{aligned}\left\langle \hat{P}_i\,(1) \right\rangle &= \frac{1}{\sum_{t=1}^{T} \eta_i(t)} \sum_{t=1}^{T} \eta_i(t)\,\langle \delta_{1;s_i(t)} \rangle \\ &= \frac{1}{\sum_{t=1}^{T} \eta_i(t)} \sum_{t=1}^{T} \eta_i(t)\,\phi_f(\alpha_i^0) = \phi_f(\alpha_i^0)\end{aligned} \tag{10}$$

and hence $\hat{P}_i\,(1)$ is *unbiased* estimator of the probability $\phi_f(\alpha_i^0)$.

Furthermore, using the equality $\frac{\sum_{t=1}^{T} \eta_i(t)\,\delta_{1;s_i(t)}}{\sum_{t=1}^{T} \eta_i(t)\,\delta_{0;s_i(t)}} = \frac{\hat{P}_i(1)}{1-\hat{P}_i(1)}$ in the equation (8) gives us the estimator of relative stake

$$\hat{\alpha}_i = \frac{\log\left(\frac{1}{1-\hat{P}_i(1)}\right)}{\log(\frac{1}{1-f})} = \frac{\log\left(1-\hat{P}_i(1)\right)}{\log(1-f)}. \tag{11}$$

We note that above is also solution of the equation

$$\hat{P}_i(1) = \phi_f(\alpha_i). \tag{12}$$

2.2. $\lambda > 0$ case

We note that the equation (6) is equivalent to the equation

$$\begin{aligned}&[\phi_f(\alpha_i) - 1]\log\left(\frac{1}{1-f}\right) \\ &\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t)\,\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t=1}^{T} \eta_i(t)\,\delta_{0;s_i(t)}\right] = \lambda\end{aligned} \tag{13}$$

which can be written as

$$\begin{aligned}
\phi_f(\alpha_i) &= \frac{\log\left(\frac{1}{1-f}\right)\sum_{t=1}^{T}\eta_i(t)\,\delta_{1;s_i(t)}}{\log\left(\frac{1}{1-f}\right)\sum_{t=1}^{T}\eta_i(t)\,\delta_{1;s_i(t)}+\log\left(\frac{1}{1-f}\right)\sum_{t=1}^{T}\eta_i(t)\,\delta_{0;s_i(t)}-\lambda}\\
&= \frac{\sum_{t=1}^{T}\eta_i(t)\,\delta_{1;s_i(t)}}{\sum_{t=1}^{T}\eta_i(t)-\lambda/\log\left(\frac{1}{1-f}\right)}\\
&= \hat{P}_i(1)\frac{1}{1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}}. \qquad (14)
\end{aligned}$$

We note that when $T\to\infty$ we expect that $\hat{P}_i(1)\to\phi_f(\alpha_i^0)$ in above and if $\lambda\ll T$ then $\frac{1}{1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}}\to\frac{1}{1+\frac{\lambda/T}{\log(1-f)q}}$ is vanishing and hence $\phi_f(\alpha_i)=\phi_f(\alpha_i^0)$. Furthermore, solving the equation (14) for α_i gives us the estimator

$$\hat{\alpha}_i=\frac{\log\left(1-\hat{P}_i(1)\frac{1}{1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}}\right)}{\log(1-f)}, \qquad (15)$$

where $\hat{P}_i(1)$ is defined in (9). Furthermore, for $\hat{\alpha}_i$ in above equation we have to find λ is such that $\sum_{i=1}^{N}\hat{\alpha}_i=1$, i.e. to solve

$$\sum_{i=1}^{N}\log\left(1-\hat{P}_i(1)\frac{1}{1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}}\right)=\log(1-f)\,, \qquad (16)$$

for λ, which suggests that we need to observe *all* nodes to have accurate predictions. For $\sum_{t=1}^{T}\eta_i(t)$ large§ and N finite we obtain

$$\begin{aligned}
&\sum_{i=1}^{N}\log\left(1-\hat{P}_i(1)\right)\\
&+\frac{\lambda}{\log(1-f)}\sum_{i=1}^{N}\frac{\hat{P}_i(1)}{(1-\hat{P}_i(1))\sum_{t=1}^{T}\eta_i(t)}\\
&\qquad+O\left(1/\left(\sum_{t=1}^{T}\eta_i(t)\right)^2\right)=\log(1-f)\,, \qquad (17)
\end{aligned}$$

We note that for $T\to\infty$, because of $\sum_{t=1}^{T}\eta_i(t)/T\to q$, the term linear in λ and higher order terms will vanish. The latter suggests that the "naive" estimator (12) could give very accurate estimates of α_i for *long* observation times T, but for *short* observation times this is no longer guaranteed ($\hat{\alpha}_i$ inferred using (12) can be greater than 1) and we need to compute λ in (15).

2.3. Inference of Lagrange multiplier

We would like to find λ such that the equality (16) is satisfied. The latter is equivalent to

$$1-f=\prod_{i=1}^{N}\left[1-\hat{\phi}_i(\lambda)\right], \qquad (18)$$

§ The random variable $\sum_{t=1}^{T}\eta_i(t)$, by the assumption (27), is from the binomial distribution with mode at (approx.) qT.

where we defined the function

$$\hat{\phi}_i(\lambda) = \hat{P}_i(1)\frac{1}{1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}}. \tag{19}$$

Now $1-f$ is probability and hence above equation is equivalent to

$$\mathrm{D}\left(1-f||\Pi(\lambda)\right) = 0, \tag{20}$$

where we defined the function $\Pi(\lambda) = \prod_{i=1}^{N}\left[1-\hat{\phi}_i(\lambda)\right]$. Here $\mathrm{D}\left(Q||P\right)$, where $Q, P \in (0,1)$, is the Kullback−Leibler (KL) divergence (or "distance")

$$\mathrm{D}\left(Q||P\right) = Q\log\frac{Q}{P} + (1-Q)\log\frac{1-Q}{1-P} \tag{21}$$

which is 0 iff $Q = P$ and is positive semi-definite when $Q \neq P$ [2]. These properties of KL distance can be exploited to solve for λ using the gradient descent equation

$$\frac{\mathrm{d}}{\mathrm{d}t}\lambda(t) = -\frac{\partial}{\partial\lambda}\mathrm{D}\left(1-f||\Pi(\lambda)\right)\big|_{\lambda=\lambda(t)}. \tag{22}$$

Let us consider

$$\begin{aligned}\mathrm{D}\left(1-f||\Pi(\lambda)\right) &= (1-f)\log\left(\frac{1-f}{\Pi(\lambda)}\right) + f\log\left(\frac{f}{1-\Pi(\lambda)}\right)\\ &= -H(f) - (1-f)\log\Pi(\lambda) - f\log\left(1-\Pi(\lambda)\right)\end{aligned} \tag{23}$$

and hence the derivative

$$\begin{aligned}\frac{\partial}{\partial\lambda}\mathrm{D}\left(1-f||\Pi(\lambda)\right) &= (1-f)\log\left(\frac{1-f}{\Pi(\lambda)}\right) + f\log\left(\frac{f}{1-\Pi(\lambda)}\right)\\ &= -\frac{\partial}{\partial\lambda}\left[(1-f)\log\Pi(\lambda) + f\log\left(1-\Pi(\lambda)\right)\right]\\ &= -\left[(1-f)\frac{\frac{\partial}{\partial\lambda}\Pi(\lambda)}{\Pi(\lambda)} - f\frac{\frac{\partial}{\partial\lambda}\Pi(\lambda)}{1-\Pi(\lambda)}\right]\\ &= \left[-\frac{1-f}{\Pi(\lambda)} + \frac{f}{1-\Pi(\lambda)}\right]\frac{\partial}{\partial\lambda}\Pi(\lambda).\end{aligned} \tag{24}$$

We note that if λ is such that $1-f = \Pi(\lambda)$ then above is exactly 0 and hence this λ is fixed point of the equation (22), as expected, and solution of the equation (16). Calculating the derivative $\frac{\partial}{\partial\lambda}\Pi(\lambda)$ we obtain

$$\begin{aligned}\frac{\partial}{\partial\lambda}\Pi(\lambda) = \frac{\partial}{\partial\lambda}\prod_{i=1}^{N}\left[1-\hat{\phi}_i(\lambda)\right] &= -\sum_{i=1}^{N}\prod_{j\neq i}^{N}\left[1-\hat{\phi}_j(\lambda)\right]\frac{\partial}{\partial\lambda}\hat{\phi}_i(\lambda)\\ &= -\sum_{i=1}^{N}\prod_{j=1}^{N}\left[1-\hat{\phi}_j(\lambda)\right]\frac{1}{1-\hat{\phi}_i(\lambda)}\frac{\partial}{\partial\lambda}\hat{\phi}_i(\lambda)\\ &= -\Pi(\lambda)\sum_{i=1}^{N}\frac{1}{1-\hat{\phi}_i(\lambda)}\frac{\partial}{\partial\lambda}\hat{\phi}_i(\lambda)\\ &= -\Pi(\lambda)\sum_{i=1}^{N}\frac{1}{1-\hat{\phi}_i(\lambda)}\\ &\quad\times\frac{\hat{P}_i(1)}{\left(1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}\right)^2\log(1-f)\sum_{t=1}^{T}\eta_i(t)}\end{aligned} \tag{25}$$

and hence

$$\begin{aligned}\frac{\partial}{\partial\lambda}\mathrm{D}\left(1-f||\Pi(\lambda)\right) &= \left[-\frac{1-f}{\Pi(\lambda)}+\frac{f}{1-\Pi(\lambda)}\right]\frac{\partial}{\partial\lambda}\Pi(\lambda)\\ &= \left[1-f-f\frac{\Pi(\lambda)}{1-\Pi(\lambda)}\right]\sum_{i=1}^{N}\frac{1}{1-\hat{\phi}_i(\lambda)}\\ &\quad\times\frac{\hat{P}_i(1)}{\left(1+\frac{\lambda}{\log(1-f)\sum_{t=1}^{T}\eta_i(t)}\right)^2\log(1-f)\sum_{t=1}^{T}\eta_i(t)}\end{aligned} \tag{26}$$

2.4. Analysis of the naive estimator

For the data sampled from (1) with the parameters α_i we would like to know how accurate is the "naive" estimator (12) at inferring α_i. We assume that $\boldsymbol{\eta}(1),\ldots,\boldsymbol{\eta}(T)$ are sampled from the prob. distribution

$$\mathrm{P}(\boldsymbol{\eta}(t))=\prod_{i=1}^{N}\left[q\,\delta_{1;\eta_i(t)}+(1-q)\,\delta_{0;\eta_i(t)}\right], \tag{27}$$

i.e. the outcome of election of node i is observed with probability q. To this end we consider the event $\alpha_i-\epsilon\leq\hat{\alpha}_i\leq\alpha_i+\epsilon$. The probability of this event, using (12), is equivalent to the probability

$$\begin{aligned}&\mathrm{P}\left(\phi_f(\alpha_i-\epsilon)\leq\hat{P}_i(1)\leq\phi_f(\alpha_i+\epsilon)|m>0\right)\\ &\quad=\mathrm{P}\left(\phi_f(\alpha_i-\epsilon)\,m\leq n\leq\phi_f(\alpha_i+\epsilon)\,m|m>0\right)\\ &\quad=\sum_{m=1}^{T}\sum_{n=0}^{m}\frac{\mathrm{P}\left(m|T\right)\mathrm{P}\left(n|m\right)}{1-(1-q)^T}\\ &\qquad\quad\times\mathbb{1}\left[\phi_f(\alpha_i-\epsilon)\,m\leq n\leq\phi_f(\alpha_i+\epsilon)\,m\right]\end{aligned} \tag{28}$$

where in above $\mathrm{P}\left(m|T\right)$ is the distribution of $m=\sum_{t=1}^{T}\eta_i(t)$, given by the binomial

$$\mathrm{P}\left(m|T\right)=\binom{T}{m}q^m\left[1-q\right]^{T-m} \tag{29}$$

with the parameter q such that $q\,T$ is the *average* number of observations, and

$$\mathrm{P}\left(n|m\right)=\binom{m}{n}\phi_f^n(\alpha_i)\left[1-\phi_f(\alpha_i)\right]^{m-n} \tag{30}$$

is the (binomial) distribution of $n=\sum_{t=1}^{T}\eta_i(t)s_i(t)$ with parameter $\phi_f(\alpha_i)$ such that $\phi_f(\alpha_i)\,m$ is the average number of observed lottery wins.

The function $\phi_f(\alpha)$ is monotonic increasing function of α and hence $0\leq\phi_f(\alpha)\leq f$ for $\alpha\in[0,1]$. Hence if $\hat{P}_i(1)\geq(f+\epsilon)$, where $\epsilon>0$, then $\hat{\alpha}_i>1$. The probability of the event $\hat{P}_i(1)\geq(f+\epsilon)$ is given by

$$\begin{aligned}&\mathrm{P}\left(n\geq(f+\epsilon)\,m|m>0\right)\\ &\qquad=\sum_{m=1}^{T}\sum_{n=0}^{m}\frac{\mathrm{P}\left(m|T\right)\mathrm{P}\left(n|m\right)}{1-(1-q)^T}\,\mathbb{1}\left[n\geq(f+\epsilon)\,m\right]\end{aligned} \tag{31}$$

Let us define the probability

$$
\begin{aligned}
&\mathrm{P}\left(\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor+1\le n\le \lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor\right)\\
&\quad=\sum_{n=\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor+1}^{\lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor}\binom{T}{n}\phi_f^n(\alpha_i)\left[1-\phi_f(\alpha_i)\right]^{T-n}
\end{aligned}
\tag{32}
$$

for non-integer $\phi_f(\alpha_i\pm\epsilon)\,T$, i.e. this is a special case when *all* election results of node i are observed, and consider‖

$$
\begin{aligned}
&\mathrm{P}\left(\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor+1\le n\le \lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor\right)\\
&\quad=1-\mathrm{P}\left(n\le \lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor\right)\\
&\qquad\quad-\mathrm{P}\left(n\ge \lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor+1\right)
\end{aligned}
\tag{33}
$$

Now for $\frac{\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor}{T}<\phi_f(\alpha_i)$ the probability

$$
\begin{aligned}
\mathrm{P}\left(n\le \lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor\right)&=\sum_{n=0}^{\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor}\binom{T}{n}\phi_f^n(\alpha_i)\left[1-\phi_f(\alpha_i)\right]^{T-n}\\
&\le \mathrm{e}^{-T\,\mathrm{D}\left(\frac{\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor}{T}||\phi_f(\alpha_i)\right)}\\
&\quad\le \mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i-\epsilon)||\phi_f(\alpha_i))},
\end{aligned}
\tag{34}
$$

where in above we used $\frac{\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor}{T}<\phi_f(\alpha_i-\epsilon)<\phi_f(\alpha_i)$ to obtain the last inequality, and for $\phi_f(\alpha_i)<\frac{\lfloor \phi_f(\alpha_i+\epsilon)T\rfloor+1}{T}<1$ the probability

$$
\begin{aligned}
&\mathrm{P}\left(n\ge \lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor+1\right)\\
&\quad=\sum_{n=\lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor+1}^{T}\binom{T}{n}\phi_f^n(\alpha_i)\left[1-\phi_f(\alpha_i)\right]^{T-n}\\
&\quad\le \mathrm{e}^{-T\,\mathrm{D}\left(\frac{\lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor+1}{T}||\phi_f(\alpha_i)\right)}\\
&\quad\le \mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i+\epsilon)||\phi_f(\alpha_i))},
\end{aligned}
\tag{35}
$$

where to obtain the last line in above we used that $\phi_f(\alpha_i+\epsilon)<\frac{\lfloor \phi_f(\alpha_i+\epsilon)T\rfloor+1}{T}\le \phi_f(\alpha_i+\epsilon)+1/T$ and $\mathrm{D}\left(s+\epsilon||s\right)$ is monotonic increasing function of ϵ when $2s-1<\epsilon\le 1-s$ [3]. Thus using above inequalities we obtain

$$
\begin{aligned}
&\mathrm{P}\left(\lfloor \phi_f(\alpha_i-\epsilon)\,T\rfloor+1\le n\le \lfloor \phi_f(\alpha_i+\epsilon)\,T\rfloor\right)\\
&\qquad\ge 1-\mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i-\epsilon)||\phi_f(\alpha_i))}-\mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i+\epsilon)||\phi_f(\alpha_i))}
\end{aligned}
\tag{36}
$$

and hence

$$
\begin{aligned}
&\mathrm{P}\left(\alpha_i-\epsilon\le\hat{\alpha}_i\le\alpha_i+\epsilon\right)\\
&\qquad\ge 1-\mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i-\epsilon)||\phi_f(\alpha_i))}-\mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i+\epsilon)||\phi_f(\alpha_i))}\\
&\qquad\ge 1-2\max_{\sigma\in\{-1,1\}}\mathrm{e}^{-T\,\mathrm{D}(\phi_f(\alpha_i+\sigma\epsilon)||\phi_f(\alpha_i))}
\end{aligned}
\tag{37}
$$

The function $\phi_f(\alpha)$ is monotonic increasing function of α and hence $0\le\phi_f(\alpha)\le f$ for $\alpha\in[0,1]$. Hence if $T\hat{P}_i(1)\ge T(f+\epsilon)$, where $\epsilon>0$, then $\hat{\alpha}_i>1$. The probability

‖ We note that mode of the binomial distribution in above is at $\lfloor\phi_f(\alpha_i)\,(T+1)\rfloor$ for non-integer $\phi_f(\alpha_i)\,(T+1)$. Also $\phi_f(\alpha)$ is monotonic increasing function of α and hence $\lfloor\phi_f(\alpha_i-\epsilon)\,T\rfloor+1\le\lfloor\phi_f(\alpha_i)\,(T+1)\rfloor\le\lfloor\phi_f(\alpha_i+\epsilon)\,T\rfloor$.

of the event $T\hat{P}_i(1) \geq T(f+\epsilon)$ is given by

$$\begin{aligned} &\mathrm{P}\left(n \geq \lfloor (f+\epsilon)\, T \rfloor + 1\right) \\ &\quad = \sum_{n=\lfloor (f+\epsilon)\, T\rfloor + 1}^{T} \binom{T}{n} \phi_f^n(\alpha_i)\left[1-\phi_f(\alpha_i)\right]^{T-n} \end{aligned} \tag{38}$$

for non-integer $T\,(f+\epsilon)$. We note that mode of the binomial distribution in above is at $\lfloor \phi_f(\alpha_i)\,(T+1)\rfloor$ for non-integer $\phi_f(\alpha_i)\,(T+1)$ and the latter is bounded from above by $f(T+1)$. Hence for $\epsilon \geq f/T$ we have $\lfloor \phi_f(\alpha_i)\,(T+1)\rfloor \leq \lfloor (f+\epsilon)\,T\rfloor + 1$ and

$$\mathrm{P}\left(n \geq \lfloor (f+\epsilon)\, T \rfloor + 1\right) \leq \mathrm{e}^{-T\,\mathrm{D}(f+\epsilon||\phi_f(\alpha_i))}. \tag{39}$$

Also the probability can be bounded from below

$$\mathrm{P}(n \geq \lfloor (f+\epsilon)T\rfloor + 1) \geq \frac{\mathrm{e}^{-T\mathrm{D}(f+\epsilon+1/T||\phi_f(\alpha_i))}}{\sqrt{8T\frac{\lfloor (f+\epsilon)T\rfloor+1}{T}\left(1-\frac{\lfloor (f+\epsilon)T\rfloor+1}{T}\right)}}. \tag{40}$$

2.5. Inclusion of empty slots

For the set of times $\mathcal{T} = \{t_1, \ldots, t_T\}$ and its subsets $\mathcal{T}_1 = \left\{t|\, t\in\mathcal{T}, \sum_{i=1}^N s_i(t) \geq 1\right\}$ and $\mathcal{T}_0 = \left\{t|\, t\in\mathcal{T}, \sum_{i=1}^N s_i(t) = 0\right\}$, we define the likelihood

$$\begin{aligned} \mathcal{L}[\{\mathbf{s}(t)\}|\{\boldsymbol{\eta}(t)\}] &= \log\left\{\prod_{t\in\mathcal{T}_1}\mathrm{P}(\mathbf{s}(t)|\boldsymbol{\eta}(t))\right\}\prod_{\tilde{t}\in\mathcal{T}_0}\mathrm{P}(\mathbf{0}) \\ &= \sum_{t\in\mathcal{T}_1}\log\mathrm{P}(\mathbf{s}(t)|\boldsymbol{\eta}(t)) + |\mathcal{T}_0|\log\mathrm{P}(\mathbf{0}) \\ &= \sum_{t\in\mathcal{T}_1}\sum_{i=1}^N \eta_i(t)\log\mathrm{P}_i(s_i(t)) + |\mathcal{T}_0|\sum_{i=1}^N\log\mathrm{P}_i(0) \end{aligned} \tag{41}$$

and consider the derivative

$$\begin{aligned} &\frac{\partial}{\partial\alpha_i}\left\{\mathcal{L}[\{\mathbf{s}(t)\}|\{\boldsymbol{\eta}(t)\}] + \lambda\left(\sum_{i=1}^N\alpha_i - 1\right)\right\} \\ &= \sum_{t\in\mathcal{T}_1}\eta_i(t)\frac{\partial}{\partial\alpha_i}\log\left[\phi_f(\alpha_i)\,\delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\,\delta_{0;s_i(t)}\right] \\ &+ |\mathcal{T}_0|\frac{\partial}{\partial\alpha_i}\log(1-\phi_f(\alpha_i)) + \lambda \\ &= \sum_{t\in\mathcal{T}_1}\eta_i(t)\frac{\frac{\partial}{\partial\alpha_i}\phi_f(\alpha_i)\left[\delta_{1;s_i(t)} - \delta_{0;s_i(t)}\right]}{\phi_f(\alpha_i)\,\delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\,\delta_{0;s_i(t)}} \\ &- |\mathcal{T}_0|\frac{\frac{\partial}{\partial\alpha_i}\phi_f(\alpha_i)}{1-\phi_f(\alpha_i)} + \lambda \\ &= (1-f)^{\alpha_i}\log\left(\frac{1}{1-f}\right) \\ &\times \sum_{t\in\mathcal{T}_1}\eta_i(t)\frac{\delta_{1;s_i(t)} - \delta_{0;s_i(t)}}{\phi_f(\alpha_i)\,\delta_{1;s_i(t)} + (1-\phi_f(\alpha_i))\,\delta_{0;s_i(t)}} \end{aligned}$$

$$
\begin{aligned}
&- |\mathcal{T}_0| \frac{(1-f)^{\alpha_i} \log\left(\frac{1}{1-f}\right)}{1-\phi_f(\alpha_i)} + \lambda \\
&= -(1-f)^{\alpha_i} \log(1-f) \\
&\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{0;s_i(t)} \right] \\
&- |\mathcal{T}_0| \frac{-(1-f)^{\alpha_i} \log(1-f)}{1-\phi_f(\alpha_i)} + \lambda \\
&= (\phi_f(\alpha_i) - 1) \log(1-f) \\
&\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{0;s_i(t)} \right] \\
&- |\mathcal{T}_0| \frac{(\phi_f(\alpha_i) - 1) \log(1-f)}{1-\phi_f(\alpha_i)} + \lambda \\
&= (\phi_f(\alpha_i) - 1) \log(1-f) \\
&\times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{0;s_i(t)} \right] \\
&+ |\mathcal{T}_0| \log(1-f) + \lambda
\end{aligned} \tag{42}
$$

Let us now consider the equation

$$
\begin{aligned}
&\frac{\partial}{\partial \alpha_i} \left\{ \mathcal{L}[\{\mathbf{s}(t)\}|\{\boldsymbol{\eta}(t)\}] + \lambda \left(\sum_{i=1}^{N} \alpha_i - 1 \right) \right\} \\
&= (\phi_f(\alpha_i) - 1) \log(1-f) \\
&\qquad \times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{0;s_i(t)} \right] \\
&\qquad\qquad + |\mathcal{T}_0| \log(1-f) + \lambda = 0
\end{aligned} \tag{43}
$$

Multiplying both sides in above by -1 gives us

$$
\begin{aligned}
&(\phi_f(\alpha_i) - 1) \log\left(\frac{1}{1-f}\right) \\
&\qquad \times \left[\frac{1}{\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{1;s_i(t)} - \frac{1}{1-\phi_f(\alpha_i)} \sum_{t\in\mathcal{T}_1} \eta_i(t)\delta_{0;s_i(t)} \right] \\
&\qquad = \lambda + |\mathcal{T}_0| \log(1-f)
\end{aligned} \tag{44}
$$

which can be written as

$$
\begin{aligned}
\phi_f(\alpha_i) &= \frac{\sum_{t\in\mathcal{T}_1} \eta_i(t)\, \delta_{1;s_i(t)}}{\sum_{t\in\mathcal{T}_1} \eta_i(t)\, \delta_{1;s_i(t)} + \sum_{t\in\mathcal{T}_1} \eta_i(t)\, \delta_{0;s_i(t)} + \tilde{\lambda}} \\
&= \frac{\sum_{t\in\mathcal{T}_1} \eta_i(t)\, \delta_{1;s_i(t)}}{\sum_{t\in\mathcal{T}_1} \eta_i(t) + \tilde{\lambda}} \\
&= \hat{\mathrm{P}}_i(1) \frac{1}{1 + \tilde{\lambda} / \sum_{t\in\mathcal{T}_1} \eta_i(t)},
\end{aligned} \tag{45}
$$

where $\tilde{\lambda} = \frac{\lambda}{\log(1-f)} + |\mathcal{T}_0|$ and we defined

$$\hat{\mathrm{P}}_i(1) = \frac{\sum_{t\in\mathcal{T}_1} \eta_i(t)\, \delta_{1;s_i(t)}}{\sum_{t\in\mathcal{T}_1} \eta_i(t)}. \tag{46}$$

Solving for α_i gives us the estimator of relative stake

$$\hat{\alpha}_i = \frac{\log\left(1 - \hat{\mathrm{P}}_i(1)\frac{1}{1+\tilde{\lambda}/\sum_{t\in\mathcal{T}_1}\eta_i(t)}\right)}{\log(1-f)}. \tag{47}$$

Let us consider

$$\begin{aligned}\frac{\tilde{\lambda}}{\sum_{t\in\mathcal{T}_1}\eta_i(t)} &= \frac{\lambda}{\log(1-f)\sum_{t\in\mathcal{T}_1}\eta_i(t)} + \frac{|\mathcal{T}_0|}{\sum_{t\in\mathcal{T}_1}\eta_i(t)} \\ &= \frac{\lambda/T}{\log(1-f)\sum_{t\in\mathcal{T}_1}\eta_i(t)/T} + \frac{|\mathcal{T}_0|/T}{\sum_{t\in\mathcal{T}_1}\eta_i(t)/T}\end{aligned} \tag{48}$$

We note that for $T\to\infty$ we expect $|\mathcal{T}_0|/T \to 1-f$ and $\sum_{t\in\mathcal{T}_1}\eta_i(t)/T \to fq$, where f is the probability of slot being nonempty and q is prob. of observing nodes in non-empty slots. Hence also assuming that $\hat{\mathrm{P}}_i(1) \to \phi_f(\alpha_i^0)$ in this limit we obtain

$$\phi_f(\alpha_i) = \phi_f(\alpha_i^0)\frac{1}{1+\frac{1-f}{fq}}, \tag{49}$$

where to derive above we assumed that $\frac{\lambda/T}{\log(1-f)fq} \to 0$ as $T\to\infty$. The interpretation of above result is that the estimator $\hat{\alpha}_i$, obtained from solving the equation

$$\phi_f(\alpha_i) = \hat{\mathrm{P}}_i(1)\frac{1}{1+\tilde{\lambda}/\sum_{t\in\mathcal{T}_1}\eta_i(t)}, \tag{50}$$

for α_i, is not *consistent*, unless we have $\frac{\lambda/T}{\log(1-f)\sum_{t\in\mathcal{T}_1}\eta_i(t)/T} \to \frac{1-f}{fq}$ as $T\to\infty$. However, the naive estimator obtained by setting $\lambda = 0$ and solving the equation

$$\begin{aligned}\phi_f(\alpha_i) &= \frac{\sum_{t\in\mathcal{T}_1}\eta_i(t)\,\delta_{1;s_i(t)}}{\sum_{t\in\mathcal{T}_1}\eta_i(t) + |\mathcal{T}_0|} \\ &= \hat{\mathrm{P}}_i(1)\frac{1}{1+|\mathcal{T}_0|/\sum_{t\in\mathcal{T}_1}\eta_i(t)}\end{aligned} \tag{51}$$

for α is always *inconsistent*.

References

[1] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *Cryptology ePrint Archive*, 2017.

[2] Thomas M Cover and Joy A Thomas. *Elements of information theory.* John Wiley & Sons, New York, 2012.

[3] Alexander Mozeika, Marcin P. Pawlowski, David Rusu, and Giacomo Pasini. Analysis of leader election process in proof of stake consensus model, 2022. `https://nomos-tech.notion.site/Cryptarchia-De-anonymisation-of-Relative-Stake-Analysis-1fd261aa09df8181a428f52251e173c4` [Accessed: 20 August 2025].