Forkable Strings are Rare

Alexander Russell[1], Cristopher Moore[2], Aggelos Kiayias[3], and Saad Quader[1]

[1]University of Connecticut
[2]University of Edinburgh
[3]Santa Fe Institute

March 8, 2017

A fundamental combinatorial notion related to the dynamics of the Ouroboros proof-of-stake blockchain protocol is that of a *forkable string*. The original description and analysis of the protocol [1] established that the probability that a string of length n is forkable, when drawn from a binomial distribution with parameter $(1-\epsilon)/2$, is $\exp(-\Omega(\sqrt{n}))$. In this note we improve this estimate to $\exp(-\Omega(n))$.

Definition 1 (Generalized margin and forkable strings)**.** *Let* $\eta \in \{0,1\}^*$ *denote the empty string. For a string* $w \in \{0,1\}^*$ *we define the* generalized margin *of* w *to be the pair* $(\lambda(w), \mu(w))$ *given by the following recursive rule:* $(\lambda(\eta), \mu(\eta)) = (0,0)$ *and, for all nonempty strings* $w \in \{0,1\}^*$,

$$(\lambda(w1), \mu(w1)) = (\lambda(w)+1, \mu(w)+1)\,, \textit{and}$$
$$(\lambda(w0), \mu(w0)) = \begin{cases} (\lambda(w)-1, 0) & \textit{if } \lambda(w) > \mu(w) = 0, \\ (0, \mu(w)-1) & \textit{if } \lambda(w) = 0, \\ (\lambda(w)-1, \mu(w)-1) & \textit{otherwise.} \end{cases}$$

Observe that for all strings w*,* $\lambda(w) \geq \mu(w)$*. We say that a string* w *is* forkable *if* $\mu(w) \geq 0$*.*

Our goal is to prove the following theorem.

Theorem 1. *Let* $\epsilon > 0$ *and let* $w \in \{0,1\}$ *be chosen randomly according to the probability law that independently assigns* w_i *to the value 1 with probability* $(1-\epsilon)/2$*. Then* $\Pr[w \textit{ is forkable}] = \exp(-2\epsilon^4(1-O(\epsilon))n)$*.*

In preparation for the proof, we record a standard large deviation bound for supermartingales.

Theorem 2 (Azuma; Hoeffding. See [2, 4.16] for discussion)**.** *Let* $X_0, \ldots, X_n$ *be a sequence of real-valued random variables so that, for all* t*,* $\mathbb{E}[X_{t+1} \mid X_0, \ldots, X_t] \leq X_t$ *and* $|X_{t+1} - X_t| \leq c$ *for some constant* c*. Then for every* $\Lambda \geq 0$

$$\Pr[X_n - X_0 \geq \Lambda] \leq \exp\left(-\frac{\Lambda^2}{2nc^2}\right)\,.$$

Proof of Theorem 1. Let $w_1, w_2, \ldots$ be a sequence of independent random variables so that $\Pr[w_i = 1] = (1-\epsilon)/2$ as in the statement of the theorem. For convenience, we define the associated $\{\pm 1\}$-valued random variables $W_t = (-1)^{1+w_t}$. Observe that $\mathbb{E}[W_t] = -\epsilon$.

Define $\lambda_t = \lambda(w_1 \ldots w_t)$ and $\mu_t = \mu(w_1 \ldots w_t)$ to be the components of the generalized margin for the string $w_1 \ldots w_t$. The analysis will rely on the ancillary random variable $\overline{\mu}_t = \min(0, \mu_t)$. Observe that $\Pr[w \text{ forkable}] = \Pr[\mu(w) \geq 0] = \Pr[\overline{\mu}_n = 0]$, so we may focus on the event that $\overline{\mu}_n = 0$. As an additional preparatory step, define the constant $\alpha = (1+\epsilon)/(2\epsilon) \geq 1$ and define the random variables $\Phi_t \in \mathbb{R}$ by the inner product

$$\Phi_t = (\lambda_t, \overline{\mu}_t) \cdot \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \lambda_t + \alpha\overline{\mu}_t\,.$$

The Φ_t will act as a "potential function" in the analysis: we will establish that $\Phi_n < 0$ with high probability and note, additionally, that $\alpha\overline{\mu}_n \leq \lambda_n + \alpha\overline{\mu}_n = \Phi_n$ so that this implies $\overline{\mu}_n < 0$, as desired.

Let $\Delta_t = \Phi_t - \Phi_{t-1}$; we observe that—conditioned on any value $(\lambda_t, \mu_t) = (\lambda, \mu)$—the random variable $\Delta_{t+1} \in [-(1+\alpha), 1+\alpha]$ has expectation no more than $-\epsilon$. The analysis has four cases, depending on the various regimes of the definition of generalized margin. When $\lambda > 0$ and $\mu < 0$, $\lambda_{t+1} = \lambda_t + W_t$ and $\overline{\mu}_{t+1} = \overline{\mu}_t + W_t$ so that $\Delta_t = (1+\alpha)W_t$ and $\mathbb{E}[\Delta_t] = -(1+\alpha)\epsilon \leq -\epsilon$. When $\lambda > 0$ and $\mu \geq 0$, $\lambda_{t+1} = \lambda_t + W_t$ but $\overline{\mu}_{t+1} = \overline{\mu}_t$ so that $\Delta_t = W_t$ and $\mathbb{E}[\Delta_t] = -\epsilon$. Similarly, when $\lambda = 0$ and $\mu < 0$, $\overline{\mu}_{t+1} = \overline{\mu}_t + W_t$ while $\lambda_{t+1} = \lambda_t + \min(0, W_t)$; we may compute

$$\mathbb{E}[\Delta_t] = \frac{1-\epsilon}{2}(1+\alpha) - \frac{1+\epsilon}{2}\alpha = \frac{1-\epsilon}{2} - \epsilon\alpha = \frac{1-\epsilon}{2} - \epsilon\left(\frac{1}{\epsilon} \cdot \frac{1+\epsilon}{2}\right) = -\epsilon\,.$$

Finally, when $\lambda_t = \mu_t = 0$ exactly one of the two random variables λ_{t+1} and $\overline{\mu}_{t+1}$ changes value: if $W_t = 1$ then $(\lambda_{t+1}, \overline{\mu}_{t+1}) = (\lambda_t + 1, \overline{\mu}_t)$; likewise, if $W_t = -1$ then $(\lambda_{t+1}, \overline{\mu}_{t+1}) = (\lambda_t, \overline{\mu}_t - 1)$. It follows that

$$\mathbb{E}[\Delta_t] = \frac{1-\epsilon}{2} - \frac{1+\epsilon}{2}\alpha \leq -\epsilon\,,$$

as $\alpha \geq 1$.

Thus $\mathbb{E}[\Phi_n] = \mathbb{E}[\sum_i^n \Delta_i] \leq -\epsilon n$ and we wish to apply Azuma's inequality to conclude that $\Pr[\Phi_n \geq 0]$ is exponentially small. For simplicity, we transform the random variables Φ_t to a supermartingale by shifting them: specifically, define $\tilde{\Delta}_t = \Delta_t + \epsilon$ and $\tilde{\Phi}_t = \sum_i^t \tilde{\Delta}_t = \Phi_t + \epsilon t$. Then $\mathbb{E}[\tilde{\Phi}_{t+1} | W_1, \ldots, W_t] \leq \tilde{\Phi}_t$, $\tilde{\Delta}_t \in [-(1+\alpha)+\epsilon, 1+\alpha+\epsilon]$, and $\tilde{\Phi}_n = \Phi_n + \epsilon n$. It follows from Azuma's inequality that

$$\begin{aligned}\Pr[w \text{ forkable}] &= \Pr[\overline{\mu}_n = 0] \leq \Pr[\Phi_n \geq 0] = \Pr[\tilde{\Phi}_n \geq \epsilon n] \\ &\leq \exp\left(-\frac{\epsilon^2 n^2}{2n(1+\alpha+\epsilon)^2}\right) = \exp\left(-\left(\frac{2\epsilon^2}{1+3\epsilon+2\epsilon^2}\right)^2 \cdot \frac{n}{2}\right) \leq \exp\left(-\frac{2\epsilon^4}{1+5\epsilon} \cdot n\right)\,. \qquad \square\end{aligned}$$

References

[1] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, Report 2016/889, 2016. `http://eprint.iacr.org/2016/889`.

[2] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, New York, NY, USA, 1995.