Probability in the Engineering and Informational Sciences (2025), 1–31
doi:10.1017/S0269964825000014

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Binomial distribution with delay in analysis and parametrization of Ouroboros Praos proof of stake blockchain protocol

Yuri Bespalov[1], Lyudmila Kovalchuk[2,3], Hanna Nelasa[4] and Roman Oliynykov[3,5]

[1]Department of Mathematical Methods in Theoretical Physics, Bogolyubov Institute for Theoretical Physics, Kyiv, 03143, Ukraine
[2]Department of Mathematical and Computer Modeling, Institute for Modelling in Energy Engineering, Kyiv, 03164, Ukraine
[3]IOG Research, IOG Singapore Pte Ltd, 049908, Singapore
[4]Department of Information Security and Nanoelectronics, Zaporizhzhia Polytechnic National University, Zaporizhzhia, 69011, Ukraine
[5]Department of Cybersecurity of Information Systems, Networks and Technologies, V. N. Karazin Kharkiv National University, Kharkiv, 61022, Ukraine
Corresponding author: Roman Oliynykov; Email: roliynykov@gmail.com

Keywords: Binomial distribution with delay; Denumerable Markov chain; Ouroboros Praos; Proof-of-Stake protocol; Rational generating function

Abstract
Decentralized consensus protocols have a variety of parameters to be set during their deployment for practical applications in blockchains. The analysis given in most research papers proves the security state of the blockchain, at the same time usually providing a range of acceptable values, thus allowing further tuning of the protocol parameters. In this paper, we investigate Ouroboros Praos, the proof-of-stake consensus protocol deployed in Cardano and other blockchains. In contrast to its predecessor, Praos allows multiple honest slot leaders that lead to fork creation and resolution, consequently decreasing the block rate per time unit. In our analysis of dependence on protocol parameters such as active slot coefficient and p2p network block propagation time, we obtain new theoretical results and explicit formulas for the expectation of the length of the longest chain created during the Praos epoch, the length of the longest unintentional fork created by honest slot leaders, the efficiency of block generation procedure (the ratio of blocks included in the final longest chain vs the total number of created blocks), and other characteristics of the blockchain throughput.

We study these parameters as stochastic characteristics of the block generation process. The model is described in terms of the two-parametric family ξ_{ij} of independent Bernoulli random variables which generate deformation of the binomial distribution by a positive integer parameter—the delay (deterministic or random). An essential part of our paper is a study of this deformation in terms of denumerable Markov chains and generating functions.

1. Introduction

The main purpose of this paper is to investigate the stochastic characteristics of the block generation process in the Ouroboros Praos Proof-of-Stake protocol. The probabilistic model that emerged in this study is a deformation of the binomial distribution with an additional positive integer parameter (interpreted as time delay), deterministic or random finitely distributed. This deformation seems interesting in itself and is also systematically studied here.

Proof-of-Work (PoW) [17] and *Proof-of-Stake (PoS)* [19] (first discussion), [12], [11] are the most wide-used approaches for reaching consensus in blockchain technology. Much research has been conducted, mainly regarding their security properties, including resistance to double-spending attacks [21], [18], [7], [13], [10] and splitting attacks [11].

PoS has undoubted advantages in comparison with PoW, but at the same time, PoS requires an advanced scheme for the fair election of block producers (which are called slot leaders). Properly selecting such a scheme is crucial for the specific protocol properties and blockchain security.

The first provably secure PoS protocol is *Ouroboros* [11] that is followed by its advanced generations—Praos [3], Genesis [1], Chronos [2], and others.

Ouroboros Praos uses a special block creation function, which helps to achieve desirable properties of the slot leader election procedure. A significant property achieved with this function is stake union/splitting resistance: stakeholders have no incentive to unite or to split their stake because these actions give them no significant influence on the probability of becoming a slot leader.

Though our paper also investigates Ouroboros Praos procedure for slot leaders' election, its objectives differ from previous articles (e.g., [10]). We are not building estimations of attack probabilities, instead we concentrate on stochastic characteristics for block creation procedure in dependence on protocol parameters: *active slot coefficient f*, introduced in [3], and *block propagation time* δ. Among the most important stochastic characteristics of such a process, we may consider the following:

- the length of the longest chain created during the epoch;
- the number of slot leaders at one timeslot;
- the *efficiency* of block generation procedure, defined as the rate of useful blocks (i.e., those that create the longest chain). Its complement to 1 is the rate of orphan blocks;
- the length of the fork.

Recommendations for Praos parametrization, including for active slot coefficient, in the environment with adversarial presence, are considered in [6]. But till this time, there were no explicit formulas that allowed us to describe or at least estimate the resulting stochastic characteristics of protocols in dependence on their initial parameters.

In this paper, we obtain explicit formulas for the average length of the longest chain, for the average number of slot leaders in one timeslot, and give estimations for these values, which are rather accurate (for sufficiently large epoch length) and do not depend on stake distribution among stakeholders. Next, using these results, we create estimates for the efficiency of the block generation process and the number of orphan blocks in an epoch.

We also did multiple numerical simulations of Ouroboros Praos operation, and they fully confirm the obtained theoretical results (see GitHub - Roman-Oliynykov/PraosForksSimulation).

The paper is organized as follows. In Section 2, we introduce main notations and designations, recall some facts about binomial distributions and their generalizations, and give a short description of Ouroboros Praos, which we use in these investigations.

Section 3 is central to our paper. Here we study the mean value of the length of the longest chain depending on the number n of timeslots in epoch, block propagation time δ, and active slot coefficient f. The whole construction is based on the infinite sequence $(\xi_j)_{j\geqslant 0}$ of independent Bernoulli random variables $\xi_j \sim B(1,f)$. In Subsection 3.1, (δ,n)-chain is defined as an increasing sequence of indexes of timeslots, such that two adjacent terms differ by at least the time delay. Then we consider a random set $\Gamma_{\delta,n}$ of suitable (δ,n)-chain depending on values of ξ_j. It can contain several longest chains. A natural formalization of the longest chain rule assumes that we choose the longest chain c with the minimum possible values of its elements c_i. To describe this precisely, we introduce on the set $C_{\delta,n}$ a total order $\succcurlyeq$, a modification of the lexicographical order. The optimal random chain $\gamma_{\delta,n}$ is the $\succcurlyeq$-minimal suitable (δ,n)-chain. We describe probability distribution of $\gamma_{\delta,n}$ and its length $\lambda_{\delta,n}$. In Subsection 3.2, the equivalent description is given in terms of the infinite Markov chain (see [15], [24]). This Markov chain is δ-periodic in the sense of (15). This allows to write recurrent relation (21) for the Green function, that is the formal series $(1-tA)^{-1} := \sum_{n\geqslant 0}(tA)^n$ of transition matrix A, and then in Subsection 3.3 the recurrent relation for the ordinary generating function $L(t)$ (see [22], [23], [14]) for expectations $\mathbf{E}\lambda_{\delta,n}$ of the lengths of random chains $\gamma_{\delta,n}$. Explicitly, $L(t)$ is a rational function with denominator $(1-t)^2\cdot p^*_{\delta,f}(t)$. Partial and complete fraction decompositions of $L(t)$ are calculated. Using the Schur–Cohen test from Appendix A, it is shown that each root of $p_{\delta,f}(z)$ belongs to the open unit

disk $|z| < 1$. This allows in Subsection 3.4 to obtain asymptotic formula for the expectation $\mathbf{E}\lambda_{\delta,n}$ for $n \to \infty$. For more refined asymptotics, it is necessary to study the dependence of the roots of $p_{\delta,f}(z)$ on δ and f. Numerical calculations show that the modules of these roots in the unit disk behave like $f^{\frac{1}{\delta-1}}$. In Subsection 3.5, alternative formula for $\mathbf{E}\lambda_{\delta,n}$ is obtained in two ways. In Subsection 3.6, we get the mixed generating function for moments $\mathbf{E}\lambda_{\delta,n}^m$ and asymptotic for the variance $\mathbf{Var}\lambda_{\delta,n}$. Note that $\mathbf{E}\lambda_{\delta,n}^2 \sim n^2$, but $\mathbf{Var}\lambda_{\delta,n} \sim n$. In Subsection 3.7, a fixed delay parameter δ is replaced by a random finitely distributed variable. The corresponding Markov chain has a tree-like transition digraph glued from repeated finite parts. We briefly describe generalizations of results from the previous section to this more general context. The random moment τ_r immediately preceding the appearance of the rth block in the chain, shifted by the total delay during the creation of this chain, has a negative binomial distribution $NB(r,f)$. Finally, we show that our construction can be applied to some wide class of stochastic digraphs.

Section 4 pays more attention to the applied aspects. So, first, we summarize the main practical results about the longest chain length from the previous section. In Subsection 4.1, we note that the expected number of slot leaders is independent of the timeslot and has a Poisson binomial distribution. It depends on stake distribution among stakeholders, but we can get rid of this dependency in the important limit cases. The function $\Phi_f(\alpha)$, given by (62), equals the expected number of slot leaders when all stakes equal α. If all stakes are uniformly small the limit value $\Phi_f(0)$, given by (63), gets a good approximation for the expected number of slot leaders. A more general case of a small number of groups with equal stake α_i for each ith group member leads to the linear combination of $\Phi_f(\alpha_i)$. The exact lower and upper bounds for the expected number of slot leaders are $\Phi_f(1)$ and $\Phi_f(1/|I|)$. In Subsection 4.2, we introduce the notion of efficiency of the block creation process as the ratio of the expected number of useful blocks to the expected number of all produced blocks during the epoch. Then, using results from Section 3 and Subsection 4.1, we obtain estimations for the efficiency, from which we can also estimate the number of orphan blocks. Under the assumption of long epoch $n \gg 1$ and uniformly small stakes, we get the approximation of efficiency (68) depending only on f and δ. Moreover, in the case of the large propagation time $\delta \gg 1$, we get the approximative conservation law: the sum of efficiency and the expected length of chain produced during the propagation time equals 1. The estimations for the length of forks are considered in Subsection 4.3. Here we emphasize the importance of the following additional rule: "among two valid equal-length branches of the fork the slot leader should choose the one that is started in the earlier timeslot." In Subsection 4.4, we conclude with an analysis of our results and set directions for further investigations.

In Appendix A following [8] (see also [20]), we briefly describe the Schur–Cohen algorithm which allows one to find the distribution of the roots of a complex polynomial with respect to the unit circle in the complex plane. In Example A.3, we apply the Schur–Cohen test for a family of polynomials $p_{\delta,f}(z)$. The fact that their roots lie in the unit disk $|z| < 1$ provides an asymptotic expression for the expectation of the maximal length of chains $L_{\delta,n}$ in Corollary 3.23 from Section 3.

In Appendix B, we show how our results can be applied during the parametrization of the consensus protocol in practical deployment, giving the numerical values calculated according to the obtained formulas and comparing the efficiency of various settings.

2. Preliminaries

In this chapter, we introduce the main notations and give a short description of the Ouroboros protocol, emphasizing its properties which we essentially use in the following results.

2.1. Notations and agreements

General notations

$\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ are rings of integers, reals, and complex numbers; $\mathbb{Z}_{\geqslant 0}$ and $\mathbb{Z}_{>0}$ are the sets of nonnegative integers and positive integers, respectively.

$d|n$ means that the integer d divides the integer n.
$\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leqslant x\}$ is the floor, $\lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geqslant x\}$ is the ceiling, for $x \in \mathbb{R}$,
$\Re z$ and $\Im z$ are the real and imaginary parts of $z \in \mathbb{C}$; and $\bar{z}$ is its complex conjugate.
$\binom{k}{k_1\ k_2\ \cdots\ k_l} := \frac{k!}{k_1!k_2!\cdots k_l!}$ is the *multinomial coefficient*, for $k_i \in \mathbb{Z}_{\geqslant 0}$, and $k = k_1 + \cdots + k_l$.
$\binom{x}{k} := \frac{x^{\underline{k}}}{k!} := \frac{x(x-1)\cdots(x-k+1)}{k!}$ is the binomial coefficient written in terms of falling factorial.
$\binom{J}{k}$ is the set of k-element subsets of the set J.

Notations for the model

$\delta, f, n, (\alpha_i)_{i\in I}$ are the main numerical parameters and $\varphi_f(\alpha)$, $\Phi_f(\alpha)$, $g = g(\delta, f)$ are functions of these parameters. $(\xi_{ij})_{i\in I, 0\leqslant j<n}$ is the system of independent Bernoulli random variables generating the whole probability space; $(\xi_j)_{0\leqslant j<n}$ and $(\nu_j)_{0\leqslant j<n}$ are function of them studied in two sections. The length $\lambda_{\delta,n}$ of the random optimal chain, its expectation $(L_n = L_{\delta,n})_{n\geqslant 0}$ depending on n and the generating function $L(t) = L^{(\delta)}(t)$ of this sequence are subject of the essential part of the investigation. Finally, the efficiency $\mathrm{Eff} = \mathrm{Eff}\,(\delta, f, n, (\alpha_i)_{i\in I})$ is considered. Other notations are used locally: $C^l_{\delta,n}$, $(C_{\delta,n}, \geqslant)$, $\Gamma_{\delta,n}$, $\gamma_{\delta,n}$, $J_0(c), J_1(c), \Delta^l_m$ for combinatorial description of a random chain; $X_\delta(k), A, S$ for Markov chain; $p_{\delta,f}(t)$, $p^*_{\delta,f}(t)$, $r_{\delta,f}(t)$, $r^*_{\delta,f}(t)$, $q_1, q_2, \ldots, q_{\delta-1}$ to characterize the rational function $L(t)$; we also consider the case of random $\boldsymbol{\delta}$, when (δ, f) is replaced by the family $(\delta_k, f_k)_{1\leqslant k\leqslant s}$.

Note that recurrent formulas involving the probability $f \in (0, 1)$ remain true for the limit cases $f = 0$ and $f = 1$, if we meet the usual in combinatorics agreement $0^0 = 1$.

2.2. Binomial distributions and beyond

The notation $\xi \sim B(n, p)$ means that the random variable ξ has binomial distribution with parameters n, p, that is $\mathbf{Pr}(\xi = k) = \binom{n}{k} p^k (1-p)^{n-k}$, $k = 0, 1, \ldots, n$. The archetypal example is the sum $\xi_1 + \xi_2 + \cdots + \xi_n$ of equidistributed Bernoulli random variables $\xi_j \sim B(1, p)$ with success parameter p.

The sum $\xi_1 + \xi_2 + \cdots + \xi_n$ of Bernoulli random variables $\xi_j \sim B(1, p_j)$ with different success parameters p_j has Poisson binomial distribution. It is used in Subsection 4.1.

So-called *Markov binomial distribution* corresponds the sum $\xi_1 + \xi_2 + \cdots + \xi_n$ where ξ_j form a Markov chain with two states 0 and 1. This idea was elaborated by A.A. Markov Sr. in his 1,907 paper, whose extended version is included in the 3rd edition of his textbook [16].

Another deformation of binomial distributions studied in Section 3 can be also described in terms of Markov chains. The additional positive integer (deterministic or random) parameter can be interpreted as a time delay.

2.3. Short description of Ouroboros Praos

We will use the next series of assumptions, which are the standard for the PoS model, in what follows. Thus, we assume that all epochs have the same duration, say T, and time interval T is divided into n equal intervals $[jT/n, (j+1)T/n]$ indexed by $j = 0, 1, \ldots, n-1$ and called timeslots. We say that some stakeholder S_i, $i \in I$ is a slot leader in jth timeslot if he was assigned for this timeslot, according to slot leader election procedure, described in Ouroboros Praos paper [3]. The desirable properties of this procedure, achieved in Praos, are the following:

- slot leaders are randomly selected, and the probability for stakeholder S_i with stake ratio α_i to become a slot leader in the jth time slot is proportional (with negligible deviation) to the ratio α_i and does not depend on j;
- if S_i is a slot leader in the jth timeslot, nobody (except S_i) knows about this till the time when he creates and propagates the block;
- after block creation, each participant can verify the validity of block creation (in particular, that the block was created by the assigned slot leader);

- the probability of becoming a slot leader is indifferent w.r.t. stake union or splitting (no sense in uniting or dividing the stake, because it gives no extra profit).

The additional properties are:

- depending on protocol parameters, some ratio of timeslots may be empty (without a slot leader), and some of them may have more than one slot leader;
- in the case of multiple slot leaders in one timeslot, we necessary have a so-called orphan block(s), because only one block from one timeslot may be included in the chain.

Following the definitions and designations, introduced in [3], we consider the function

$$\varphi_f(\alpha) = 1 - (1-f)^{\alpha}, \tag{1}$$

depending on the *active slots coefficient* $f \in (0,1)$. The exponential function $1-\varphi_f = (1-f)^{\alpha}$ is the solution of the Cauchy's characteristic identity $E(x+y) = E(x) \cdot E(y)$ (see [9, Ch. 1]), which turns into the functional equation for φ_f:

$$\varphi_f(\alpha) + \varphi_f(\beta) - \varphi_f(\alpha)\,\varphi_f(\beta) = \varphi_f(\alpha+\beta), \tag{2}$$

whence by induction for a finite set $J \subseteq I$ we get the inequality:

$$\sum_{i\in J} \varphi_f(\alpha_i) \geqslant \varphi_f\left(\sum_{i\in J} \alpha_i\right). \tag{3}$$

We assume the existence of the finite set of stakeholders $(S_i)_{i\in I}$. Each stakeholder S_i owns corresponding stake ratio α_i. For $J \subseteq I$, denote $\alpha_J := \sum_{i\in J} \alpha_i$. We assume that the total stake is taken as one:

$$\alpha_I = \sum_{i\in I} \alpha_i = 1. \tag{4}$$

We consider the blockchain during an epoch, consisting of n timeslots indexed by integers $0, 1, \ldots, n-1$. The whole slot leader election in each timeslot can be described by the family of independent Bernoulli random variables $\xi_{ij} \sim B(1, \varphi_f(\alpha_i))$ attributed to stakeholder S_i for $i \in I$ and to jth timeslot: $\xi_{ij} = 1$ iff stakeholder S_i becomes jth slot leader.

For a subset $\Lambda \subseteq I$, denote $\chi_\Lambda : I \to \{0,1\}$ its characteristic function, that is $\chi_\Lambda(i) = 1$ iff $i \in \Lambda$. So the set of slot leaders in the jth timeslot is $(S_i)_{i\in\Lambda}$ with the probability

$$\Pr\left(\bigcap_{i\in I} \xi_{ij}^{-1}(\chi_\Lambda(i))\right) = \prod_{i\in I\setminus\Lambda} (1-f)^{\alpha_i} \cdot \prod_{i\in\Lambda} \varphi_f(\alpha_i) \underset{\text{by (4)}}{=} (1-f)^{1-\alpha_\Lambda} \prod_{i\in\Lambda} \varphi_f(\alpha_i), \tag{5}$$

which does not depend on j.

Remark 2.1. Due to (2), for any two stakeholders S_i and S_j with stake ratios α_i and α_j, the probabilities that at least one of them is a slot leader in some timeslot with number l and that some stakeholder with stake $\alpha_i+\alpha_j$ is a slot leader in this slot are equal. Thus, there is no reason for stakeholders to unite/divide their stakes since the profit will be the same.

Usually, the set of stakeholders split into two classes of (H)onest and (M)alicious: $(S_i)_{i\in I} = (S_i)_{i\in I_{\mathrm{H}}} \sqcup (S_i)_{i\in I_{\mathrm{M}}}$. Here we assume that all stakeholders are honest, that is act according to block production rules:

- create blocks in each corresponding timeslot and only in them;
- in the case of a fork, support the longest chain.

In particular, they do not try to provide double spending or splitting attacks.

Note that in this case, forks may occur only due to two reasons—multiple slot leaders in one timeslot (each of them creates a block of the same height) or time delay in the network (two or more slot leaders refer to the same block).

3. The longest chain and binomial distribution with delay

In this section, we systematically study the probabilistic model related to the evolution of the longest chain. At each time slot, all generated blocks form a rooted tree with the genesis block as the root, and each other block stores the reference to its parent block. The subject of our interest is the longest chain in this tree from the root to the leaf. Note that one of the stabilized blocks (already included in the longest chain) can be considered the root of a new full subtree and its longest chain is a part of the whole longest chain.

For each timeslot j and ξ_{ij} described in Subsection 2.3, let introduce

$$\xi_j = 1 - \prod_{i \in I} (1 - \xi_{ij}).$$

Each $\xi_i \sim B(1,f)$ is a Bernoulli random variable. All $(\xi_j)_{0 \leqslant j < n}$ are independent. The event $\xi_j = 1$ means that the jth timeslot receives one or more slot leaders, and each of them extends the tree with a new block.

From now and to the end of this section, we suppose that $(\xi_j)_{j \geqslant 0}$ is an infinite sequence of independent Bernoulli random variables, and $n \geqslant 0$ will be used as a discrete-time parameter. Another parameter $\delta \in \mathbb{Z}_{>0}$ is interpreted as a *block propagation time* measured in timeslos, that is a block created in jth slot becomes visible only in timeslot with index $j + \delta$.

3.1. Random chain $\gamma_{\delta,n}$

For our probabilistic model, δ, n, l are just integers which in the context of Ouroboros Praos can be interpreted as the time delay, the epoch length, and the chain length respectively. We define a (δ, n)-chain as an increasing sequence of indexes of timeslots, such that two adjacent terms differ by at least the time delay:

Definition 3.1. *For $\delta, l \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{\geqslant 0}$, a (δ, n)-chain of length l is a sequence $c = (c_i)_{1 \leqslant i \leqslant l}$ with $c_i \in \{0, 1, \ldots, n-1\}$ such that $c_i + \delta \leqslant c_{i+1}$ for $1 \leqslant i < l$. In this case, we write $\ell(c) := l$.*

We denote $C^l_{\delta,n}$ the set of all (δ, n)-chain with fixed length l, and let $C_{\delta,n}$ be the disjoint union $\coprod_{l \geqslant 0} C^l_{\delta,n}$ over all lengths.

During a random event that fixes the values of random variables $(\xi_j)_{0 \leqslant j < n}$, for a given (δ, n)-chain $c = (c_i)_{1 \leqslant i \leqslant l}$, it is possible to construct a chain of blocks created exactly in the time intervals indexed by c_i if and only if $\xi_{c_i} = 1$ for all c_i. This explains the following definition:

Definition 3.2. *The random set $\Gamma_{\delta,n} \subseteq C_{\delta,n}$ of suitable chains is defined by the following formula:*

$$\Gamma_{\delta,n} := \{c \in C_{\delta,n} \,|\, \xi_{c_i} = 1, 1 \leqslant i \leqslant \ell(c)\}.$$

Remark 3.3. Note that multiple blocks can be generated in a timeslot but only one can be included in the longest chain. A suitable chain does not store information about a specific block but only about its timeslot index.

The random set $\Gamma_{\delta,n}$ of suitable chains can contain several longest chains. A natural formalization of the longest chain rule assumes that we choose the longest chain c with the minimum possible values of c_i. To describe this precisely, we consider a total order $\succcurlyeq$ on $C_{\delta,n}$, which is a modification of the lexicographical order:

Definition 3.4. *Let $(A, \geqslant)$ be a totally ordered set, and $(A^*, \cdot)$ be the free monoid of words $a_0a_1\cdots a_{n-1}$, $a_i \in A$, $n \geqslant 0$ in the alphabet A. One can also identify a word $a_0a_1\cdots a_{n-1}$ with a sequence $(a_i)_{0\leqslant i<n}$. The structure binary operation is concatenation:*

$$(a_0, a_1, \ldots a_{n-1}) \cdot (b_0, b_1, \ldots b_{m-1}) := (a_0, a_1, \ldots a_{n-1}, b_0, b_1, \ldots b_{m-1});$$

the neutral element is the empty string ().

(1) The lexicographical order (or dictionary order) $\succcurlyeq$ on A^* is the total order uniquely determined by the following properties:
  (1) the empty string () is the smallest element in A^*;
  (2) if $a > b$ in A, then $(a, \ldots) \succ (b, \ldots)$ in A^*;
  (3) for $\alpha, \beta, \gamma \in A^*$, if $\beta \succ \gamma$ then $\alpha \cdot \beta \succ \alpha \cdot \gamma$.

(2) The Kleene–Brouwer order (or Lusin–Sierpiński order) $\succcurlyeq$ on A^* is the total order uniquely determined by the following property
  (a) the empty string () is the greatest element in A^*;
  and the above properties (b) and (c).

Now let take the alphabet $A = \{0 < 1 < \cdots < n-1\}$ and consider the restriction $\succcurlyeq$ of the Kleene–Brouwer order to the subset of (δ, n)-chains $C_{\delta,n} \subset \{0 < 1 < \cdots < n-1\}^*$.

Example 3.5. The totally ordered set $(C_{2,5}, \succcurlyeq)$ is the following:

$$(0,2,4) \prec (0,2) \prec (0,3) \prec (0,4) \prec (0) \prec (1,3) \prec (1,4) \prec (1) \prec (2,4) \prec (2) \prec (3) \prec (4) \prec ().$$

In general, $\min_{\succcurlyeq} C_{\delta,n} = ((i-1)\delta)_{1\leqslant i\leqslant \lceil n/\delta \rceil}$.

Definition 3.6. *The optimal random chain $\gamma_{\delta,n} \in C_{\delta,n}$ is defined as the $\succcurlyeq$-minimal suitable chain:*

$$\gamma_{\delta,n} := \min_{\succcurlyeq} \Gamma_{\delta,n}.$$

Directly from the definition of the total order on $C_{\delta,n}$, we get the following lemma:

Lemma 3.7. *The elements of the optimal random chain $\gamma_{\delta,n}$ can be calculated sequentially:*

- *Let $\Xi_0 = \{i \mid \xi_i = 1\}$. If $\Xi_0 = \varnothing$, then $\gamma_{\delta,n} = ()$, otherwise $(\gamma_{\delta,n})_0 = \min \Xi_0$.*
- *Let we know first $k \geqslant 1$ elements of $\gamma_{\delta,n}$. Put $\Xi_k = \Xi_0 \cap [(\gamma_{\delta,n})_{k-1} + \delta, n)$. If $\Xi_k = \varnothing$, then $\ell(\gamma_{\delta,n}) = k$, otherwise $(\gamma_{\delta,n})_k = \min \Xi_k$.*

Corollary 3.8. *The optimal random chain $\gamma_{\delta,n}$ is one of the longest chains in $\Gamma_{\delta,n}$, that is $\ell(\gamma_{\delta,n}) \geqslant \ell(c)$ for all $c \in \Gamma_{\delta,n}$.*

For each $c \in C^l_{\delta,n}$, let consider two subsets in $\{0, 1, \dots, n-1\}$:

$$\begin{aligned} J_1(c) &:= \{c_j \,|\, 1 \leqslant j \leqslant l\}, \\ J_0(c) &:= [0, c_1) \cup [c_1 + \delta, c_2) \cup \dots \cup [c_i + \delta, c_{i+1}) \cup \dots \cup [c_\ell + \delta, n). \end{aligned} \tag{6}$$

Lemma 3.9. *For $c \in C_{\delta,n}$, $\gamma_{\delta,n} = c$ iff $\xi_j = 1$ for all $j \in J_1(c)$ and $\xi_j = 0$ for all $j \in J_0(c)$. Hence,*

$$\mathbf{Pr}\left(\gamma_{\delta,n} = c\right) = f^{\#J_1(c)}(1-f)^{\#J_0(c)} = \begin{cases} f^{\ell(c)}(1-f)^{n-\ell(c)\cdot\delta}, & \text{if } c_{\ell(c)} + \delta < n, \\ f^{\ell(c)}(1-f)^{c_{\ell(c)}}, & \text{otherwise.} \end{cases} \tag{7}$$

Proof. For $c \in C_{\delta,n}$, $c \in \Gamma_{\delta,n}$ iff $\xi_j = 1$ for all $j \in J_1(c)$. Under this assumptions, $c = \min_{\geqslant} \Gamma_{\delta,n}$ iff $\xi_j = 0$ for all $j \in J_0(c)$.

Two expressions for $\#J_0(c)$ corresponds to the cases $[c_\ell + \delta, n)$ is empty or not. □

Definition 3.10. *For $l \in \mathbb{Z}_{\geqslant 0}$ and l-tuple $k = (k_1, \dots, k_l) \in \mathbb{Z}^l_{\geqslant 0}$, we put $|k| := k_1 + \dots + k_l$, and for $m > 0$, denote*

$$\Delta^l_m := \{k \in \mathbb{Z}^l_{\geqslant 0} \,|\, |k| < m\}. \tag{8}$$

Note that the cardinality of this set is the number of weak $(l+1)$-compositions of $(m-1)$ (see [22, 1.2])

$$\#\Delta^l_m = \left(\!\!\binom{l+1}{m-1}\!\!\right) = \binom{m+l-1}{l}. \tag{9}$$

Lemma 3.11. *For each $l \geqslant 0$, there is a bijection*

$$\Delta^l_{n-(l-1)\delta} \ni k = (k_1, k_2, \dots, k_l) \mapsto c(k) \in C^l_{\delta,n}, \qquad c(k)_i = (i-1)\delta + k_1 + k_2 + \dots + k_i.$$

Proof. Both above sets are nonempty iff $n > (l-1)\delta$.

The inverse map is $C^l_{\delta,n} \ni c \mapsto \Delta_\delta c \in \Delta^l_{n-(l-1)\delta}$ with $(\Delta_\delta c)_1 = c_1$ and $(\Delta_\delta c)_{i+1} = c_{i+1} - c_i - \delta$ for $i = 1, 2 \dots, l-1$. □

Lemma 3.12. *For $k \in \Delta^l_{n-(l-1)\delta}$, (7) can be rewritten as follows*

$$\mathbf{Pr}\left(\gamma_{\delta,n} = c(k)\right) = \begin{cases} f^l(1-f)^{|k|}, & \text{if } k \in \Delta^l_{n-(l-1)\delta} \setminus \Delta^l_{n-l\delta} \\ f^l(1-f)^{n-l\delta}, & \text{if } k \in \Delta^l_{n-l\delta}. \end{cases} \tag{10}$$

In this section, we will study a random variable $\lambda_{\delta,n} := \ell\left(\gamma_{\delta,n}\right)$, the length of the random chain $\gamma_{\delta,n}$, its expectation

$$L_n = L_{\delta,n} := \mathbf{E}\lambda_{\delta,n} = \sum_{c \in C_{\delta,n}} \ell(c) \cdot \mathbf{Pr}\left(\gamma_{\delta,n} = c\right), \qquad n \geqslant 0, \tag{11}$$

and describe the sequence $(L_n)_{n \geqslant 0}$ in terms of its ordinary generating series

$$L(t) = L^{(\delta)}(t) := \sum_{n \geqslant 0} L_n t^n. \tag{12}$$

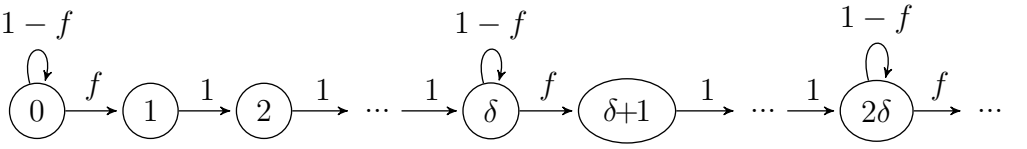

Figure 1. *Transition digraph of the Markov chain $X_\delta(n)$.*

Remark 3.13. In the case $\delta = 1$,

$$\mathbf{Pr}\left(\gamma_{1,n} = c\right) = f^{\ell(c)}(1-f)^{n-\ell(c)}, \qquad \#C^l_{1,n} = \binom{n}{l}.$$

So we obtain binomial distribution for $\lambda_{1,n} \sim B(n,f)$ with well-known expectation

$$\mathbf{E}\lambda_{1,n} = nf, \qquad L^{(1)}(t) := \sum_{n\geqslant 0} \mathbf{E}\lambda_{1,n} t^n = \frac{ft}{(1-t)^2}.$$

3.2. Markov chains $X_\delta(n)$

In this subsection, we give an equivalent description of random chains $\gamma_{\delta,n}$ in terms of a family of discrete-time and time-homogeneous Markov chains X_δ.

Definition 3.14. *For $\delta \in \mathbb{Z}_{>0}$, the Markov chain $X_\delta(n) \in \mathbb{Z}_{\geqslant 0}$, $n \geqslant 0$ is defined by a random mapping representation ([15, 1.2]):*

$$X_\delta(0) = 0, \qquad X_\delta(n+1) = X_\delta(n) + \begin{cases} \xi_{n+1}, & \text{if } \delta | n \\ 1, & \text{otherwise.} \end{cases} \tag{13}$$

Hence, the transition matrix

$$A_{ij} := \mathbf{Pr}\big(X_\delta(n+1) = i \,|\, X_\delta(n) = j\big), \qquad i,j \in \mathbb{Z}_{\geqslant 0}$$

has the following nonzero entries:

$$A_{\delta i,\delta i} = 1-f, \qquad A_{i+1,i} = \begin{cases} f, & \text{if } \delta | i \\ 1, & \text{otherwise,} \end{cases} \qquad i \in \mathbb{Z}_{\geqslant 0}. \tag{14}$$

The graph of this Markov chain is shown in Figure 1.

We adopt Dirac bra-ket notation ([4], [5]) from linear algebra. A state $i \in \mathbb{Z}_{\geqslant 0}$ is written as a *ket* $|i\rangle$. Nonnegative affine combinations of states are distributions. A *bra* $\langle f|$ is a linear form on linear combinations of states. $\langle f|x\rangle$ is a pairing, $|i\rangle\langle j|$ for $i,j \in \mathbb{Z}_{\geqslant 0}$ is the matrix element. In this term, (14) takes form

$$A = \sum_{i\in\mathbb{Z}} \big(|i+1\rangle\langle i| + (1-f)(|\delta i\rangle\langle \delta i| - |\delta i+1\rangle\langle \delta i|)\big).$$

Let S be a linear operator acting on states as a shift: $S|i\rangle = |i+1\rangle$. Note that our Markov chain is δ-periodic, that is:

$$AS^\delta = S^\delta A. \tag{15}$$

Proposition 3.15. *The random chain $\gamma_{\delta,n}$ and the family of random variables $\big(X_\delta(k)\big)_{1\leqslant k\leqslant n}$ are recovered each from other:*

$$\lambda_{\delta,n} = \lceil X_\delta(n)/\delta \rceil, \tag{16}$$

$$\big(\gamma_{\delta,n}\big)_k = \max\{m \,|\, X(m) = (k-1)\delta\}, \qquad 1 \leqslant k \leqslant \lambda_{\delta,n}$$

$$X_\delta(n) = \delta\cdot\lambda_{\delta,n} - \max\big\{((\gamma_{\delta,n})_i + \delta - n)_{1\leqslant i\leqslant \lambda_{\delta,n}}, 0\big\}.$$

Proof. For $0 \leqslant k < n$, $X_\delta(k+1) = X_\delta(k) + 1$ iff $k \in [0,n) \setminus I_0(\gamma_{\delta,n})$. □

Expectations of random variables X_δ, $\lambda^m_{\delta,n}$ can be expressed with the help of the corresponding linear forms $\langle X_\delta|$ and $\langle\lambda^m_\delta|$:

$$\mathbf{E}X_\delta(n) = \langle X_\delta|A^n|0\rangle, \qquad \langle X_\delta|i\rangle = i,$$

$$\mathbf{E}\lambda^m_{\delta,n} = \langle\lambda^m_\delta|A^n|0\rangle, \qquad \langle\lambda^m_\delta|i\rangle = \lceil i/\delta\rceil^m. \tag{17}$$

Compatibility with shift for $\langle\lambda^m_\delta|$ and for formal series in x takes the form:

$$\langle\lambda^m_\delta|S^\delta = \sum_{k=0}^{m}\binom{m}{k}\langle\lambda^k_\delta|, \tag{18}$$

$$\langle e^{\lambda_\delta x}|S^\delta = \langle e^{(\lambda_\delta+1)x}|. \tag{19}$$

Lemma 3.16. *The transition matrix A satisfies the following recurrent formula:*

$$A^n|0\rangle = (1-f)^n|0\rangle + \sum_{k=1}^{\min\{\delta,n\}} f(1-f)^{n-k}|k\rangle + \sum_{k=0}^{n-\delta-1} f(1-f)^k A^{n-\delta-k}|\delta\rangle. \tag{20}$$

Or in terms of the generating function $\frac{1}{1-tA} = \sum_{n\geqslant 0}(tA)^n$:

$$(1-tA)^{-1}|0\rangle = \frac{1}{1-(1-f)t}|0\rangle + \sum_{k=1}^{\delta-1}\frac{ft^k}{1-(1-f)t}|k\rangle + \frac{ft^\delta}{(1-(1-f)t)(1-tA)}|\delta\rangle. \tag{21}$$

Negative binomial distribution

For $r \in \mathbb{Z}_{\geqslant 0}$, let the random time $\tau_{\delta,r}$ is such that $X_\delta(\tau_{\delta,r}) = r\delta$ and $X_\delta(\tau_{\delta,r}+1) = r\delta+1$. Then $\tau_{\delta,r} - r\delta$ has the negative binomial distribution:

$$\tau_{\delta,r} - r\delta \sim NB(r,f), \qquad \mathbf{Pr}(\tau_{\delta,r} - r\delta = k) = \binom{k+r-1}{k}(1-f)^k f^r, \quad k \in \mathbb{Z}_{\geqslant 0}. \tag{22}$$

3.3. Generating functions for L_n

Lemma 3.17.

(1) The sequence $(L_n)_{n\geqslant 0}$ is determined by the following recurrent identity:

$$L_n = 1-(1-f)^n + f\sum_{0\leqslant k<n-\delta}(1-f)^k L_{n-k-\delta}, \qquad n\geqslant 0. \tag{23}$$

(2) In terms of generating function $L(t)$, the identity (23) takes the form

$$L(t) = L(t)\cdot ft^{\delta}\sum_{n\geqslant 0}(1-f)^n t^n + \sum_{n\geqslant 0}\bigl(1-(1-f)^n\bigr)t^n \tag{24}$$

$$= \frac{ft^{\delta}}{1-(1-f)t}L(t) + \frac{ft}{(1-t)(1-(1-f)t)}. \tag{25}$$

Proof. Write $L_n = \mathbf{E}\lambda_{\delta,n}$ in the form (17). Apply $\langle\lambda_\delta|$ to (20). Finally use $\langle\lambda_\delta|A^{n-\delta-k}|\delta\rangle = 1+\langle\lambda_\delta|A^{n-\delta-k}|0\rangle$, which follows from δ-shift invariance (15). □

Theorem 3.18

(1) The generating function $L(t)$ has the form:

$$\begin{aligned} L^{(\delta)}(t) &= \frac{ft}{1-(2-f)t+(1-f)t^2-ft^{\delta}+ft^{\delta+1}} \\ &= \frac{ft}{(1-t)^2\bigl(1+f(t+t^2+\cdots+t^{\delta-1})\bigr)} = \frac{L^{(1)}(t)}{1+f(t+t^2+\cdots+t^{\delta-1})}. \end{aligned} \tag{26}$$

(2) The corresponding recurrent relation for coefficients is

$$L_n = (2-f)L_{n-1}-(1-f)L_{n-2}+fL_{n-\delta}-fL_{n-\delta-1}, \qquad n>\delta \tag{27}$$

with the initial conditions

$$L_n = 1-(1-f)^n, \qquad n\leqslant\delta. \tag{28}$$

Proof. The formula (26) is an explicit solution of (25) with respect to $L(t)$.

The formula (27) follows from (26) rewritten in the form

$$(1-(2-f)t+(1-f)t^2-ft^{\delta}+ft^{\delta+1})L(t) = ft.$$

The formula (28) for initial conditions can be easily obtained if taken into attention that in this case the length of the chain $\leqslant 1$. □

Corollary 3.19. *The sequence $(L_n)_{n\geqslant 0}$ satisfies the recurrent relation:*

$$L_n + f(L_{n-1}+L_{n-2}+\cdots+L_{\max\{n-\delta+1,0\}}) = nf. \tag{29}$$

Proof. This follows from (26) rewritten in the form

$$(1 + ft + ft^2 + \cdots + ft^{\delta-1})L(t) = \sum_{n\geqslant 0} nft^n.$$

□

Theorem 3.18 and the following Theorem 3.20 agree with the scheme of usage of rational generating functions [22, Thm. 4.1.1] and partial fractions [8, Part 7].

Denote

$$g = g(\delta, f) = \frac{f}{1 + (\delta - 1)f}. \tag{30}$$

Let's also consider two pairs of *reciprocal adjoint* polynomials (see Definition A.1)

$$\begin{aligned} p_{\delta,f}(t) &= t^{\delta-1} + f(t^{\delta-2} + t^{\delta-3} + \cdots + 1), \\ p^*_{\delta,f}(t) &= 1 + f(t + t^2 + \cdots + t^{\delta-1}); \end{aligned} \tag{31}$$

$$\begin{aligned} r_{\delta,f}(t) &= \sum_{k=0}^{\delta-2} \left(\frac{(k+1)(\delta-1)(\delta-k-2)}{2} f - \binom{k+2}{2} \right) t^k, \\ r^*_{\delta,f}(t) &= \sum_{k=0}^{\delta-2} \left(\frac{k(\delta-1)(\delta-k-1)}{2} f - \binom{\delta-k}{2} \right) t^k. \end{aligned}$$

Theorem 3.20

(1) The generating function admits presentations

$$L(t) = \frac{gt + \binom{\delta}{2} g^2 (1-t)}{(1-t)^2} + \frac{g^2 r^*_{\delta,f}(t)}{1 + f(t + t^2 + \cdots + t^{\delta-1})} \tag{32}$$

$$= \frac{gt}{(1-t)^2} + \frac{\binom{\delta}{2} g^2}{1-t} + g^2 \sum_{k=1}^{\delta-1} \frac{\alpha_k}{1 - q_k t}, \tag{33}$$

where $q_1, q_2, \ldots, q_{\delta-1}$ are the roots of the polynomial $p_{\delta,f}(t)$ from (31), and

$$\alpha_k = \frac{r_{\delta,f}(q_k)}{\prod_{j\neq i}(q_k - q_j)}, \qquad k = 1, 2, \ldots, \delta - 1.$$

(2) The corresponding formula for the coefficient is

$$L_n = ng + \binom{\delta}{2} g^2 + \sum_{k=1}^{\delta-1} \alpha_k g^2 q_k^n. \tag{34}$$

Proof. We subsequently get two decompositions of (26) into partial fractions: firstly incomplete (32), and then complete (33). In both cases, we can use the indeterminant coefficients method, solving corresponding linear equations via substitutions $t = 1$ (two times) and $t = q_i$ respectively.

In the second step, the polynomial $p^*_{\delta,f}(t)$ must have no multiple roots for $f \in (0, 1)$. This follow from the fact that the polynomial $p(t) = (1-t)p^*_{\delta,f}(t) = 1 - (1-f)t - ft^\delta$ and its derivative $p'(t)$ have

no common roots. Indeed, for $\delta > 1$, the polynomial $tp'(t) - \delta p(t) = (\delta - 1)(1-f)t - \delta$ has the single root $\frac{\delta}{(\delta-1)(1-f)}$, but $p\left(\frac{\delta}{(\delta-1)(1-f)}\right) < 0$.

The equivalence of (33) and (34) becomes obvious if we represent all elementary fractions in (33) as power series. □

Example 3.21. For $\delta = 2$, $g = f/(1+f)$,

$$L_n = f\sum_{m=0}^{n-1}(n-m)(-f)^m = gn + g^2 - g^2(-f)^n.$$

Example 3.22. For $\delta = 3$, $g = f/(1+2f)$,

$$L(t) = \frac{gt}{(1-t)^2} + \frac{3g^2}{1-t} + g^2\Re\frac{\alpha}{1-tq}$$
$$L_n = ng + 3g^2 + g^2\Re(\alpha q^n),$$

where $q = -f/2 + i\sqrt{f - f^2/4}$ and $\overline{q}$ are the roots of $p_{3,f}(z) = z^2 + fz + f$, and

$$\alpha = 2\frac{r_{3,f}(q)}{q-\overline{q}} = -3 + i\frac{1-5f/2}{\sqrt{f-f^2/4}}.$$

3.4. Asymptotic for L_n

Corollary 3.23. *For each fixed $f \in (0,1)$ and $n \to \infty$,*

$$L_n = ng + \binom{\delta}{2}g^2 + o(1). \tag{35}$$

Proof. For $f \in (0,1)$, in Example A.3 from Appendix A, it is shown that all roots of polynomial $p_{\delta,f}(z)$ from (31) lie in the open unit disk $|z| < 1$. Hence from (34), we get (35). □

In Figure 2, the values of L_n/n and their approximations according (35) (up to $O(1/n)$ and $O(1/n^2)$) are shown depending on f. In Figure 2(a), we can see that even $O(1/n)$-approximation of $L(n)/n$ with only one term of (35) is very close to the value. Taking the first two terms of (35) improves this approximation and is almost undistinguished from $L(n)/n$, especially for small values of f, till 0.62, usually in practice.

Remark 3.24. Taking into account the negative binomial distribution (22) of $\tau_{\delta,r} - r\delta$ and asymptotic (35) for $\mathbf{E}\lambda$, we get the equality

$$\lim_{n\to\infty}\frac{\mathbf{E}\lambda_{\delta,n}}{n} = g = \frac{f}{1+(\delta-1)f} = \frac{r}{\mathbf{E}\tau_{\delta,r}}, \tag{36}$$

which is true for each $r \in \mathbb{Z}_{>0}$.

To pay more attention to the last member in the asymptotic (35), let's consider the behavior of roots of $p_{\delta,f}(z)$ depending on f. For $\delta \geqslant 2$, the whole set $\bigcup_{f\in(0,1)} p_{\delta,f}^{-1}(0)$ of root is described in terms of variables $x = \Re z$ and $y = \Im z$.

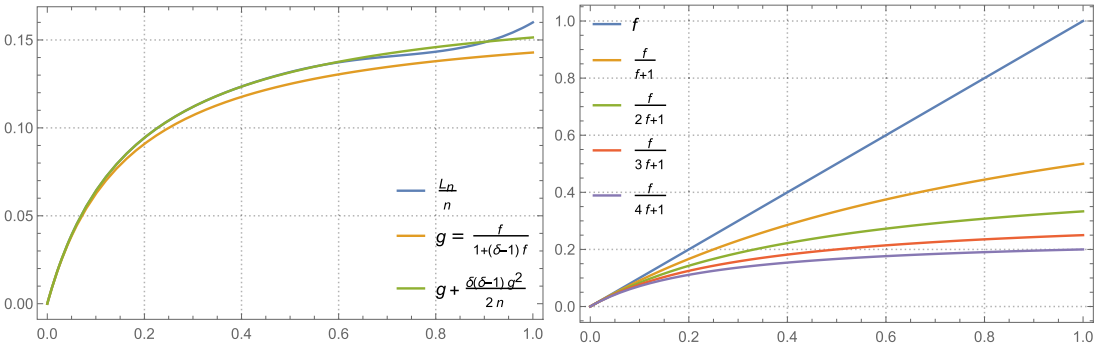

Figure 2. *The values of L_n/n and their $O(1/n)$–, $O(1/n^2)$ approximations* g, $g + \binom{\delta}{2}\frac{g^2}{n}$ *depending on* f. *(a)* $\frac{L_n}{n}$, g, *and* $g + \binom{\delta}{2}\frac{g^2}{n}$ *for* $\delta = 7$ *and* $n = 50$. *(b)* g *for* $1 \leqslant \delta \leqslant 5$.

Proposition 3.25.

(1) For $\delta \geqslant 2$, $\mathbb{R} \cap \bigcup_{f\in(0,1)} p^{-1}_{\delta,f}(0) = \begin{cases}(0,1), & \text{if } \delta \text{ is even,}\\ \varnothing, & \text{if } \delta \text{ is odd.}\end{cases}$

(2) For $\delta > 2$, *elements of* $\bigcup_{f\in(0,1)} p^{-1}_{\delta,f}(0) \setminus \mathbb{R}$ *satisfy the following polynomial equation in* $x = \Re z$ *and* $y = \Im z$ *of degree* $2(\delta-2)$

$$\Re z^{\delta-1} \cdot \sum_{m=1}^{\delta-2} \frac{\Im z^m}{y} = \frac{\Im z^{\delta-1}}{y} \cdot \sum_{m=0}^{\delta-2} \Re z^m, \tag{37}$$

where

$$\Re z^m = \sum_{k=0}^{\lfloor m/2\rfloor} \binom{m}{2k} (-y^2)^k x^{m-2k}, \qquad \frac{\Im z^m}{y} = \sum_{k=0}^{\lceil m/2\rceil-1} \binom{m}{2k+1} (-y^2)^k x^{m-2k-1}.$$

Proof. For $z = x + iy$, we write $p_{\delta,f}(z) = 0$ as a pair of equations $\begin{matrix}\Re\\ \Im\end{matrix} p_{\delta,f}(z) = 0$ and then exclude f. □

Example 3.26. For $\delta = 3$, Eq. (37) describes the circle $(x+1)^2 + y^2 = 1$ or in polar form $\rho = -2\cos(\varphi)$. According to Example 3.22 for $f \in [0,4]$, roots of the polynomial $p_{3,f}(z)$ belong to this circle, moreover in the case $f \in (0,1)$, they are on its arc in the open unit disk $|z| < 1$.

For $\delta = 4$, (37) turns into equation $x^4 + 2x^2y^2 + y^4 + 2x^3 + 2xy^2 + 3x^2 - y^2 = 0$ or in polar form $\rho^2 + 2\rho\cos(\varphi) + 4cos^2(\varphi) - 1 = 0$. So the pair of complex conjugate roots is described by the formulas

$$\rho = -\cos(\varphi) + \sqrt{1 - 3\cos^2(\varphi)}, \qquad \pi/3 < \varphi < \pi/2.$$

In Figure 3, the roots of the polynomial $p_{\delta,f}(z)$ in the unit disk for $f \in (0,1)$ are shown in two cases $\delta = 4$ and $\delta = 7$.

Note that for the roots q_k of the polynomial $p_{\delta,f}(t)$, the values $|q_k|/f^{\frac{1}{\delta-1}}$ are close to 1. Moreover, $|q_k|/f^{\frac{1}{\delta-1}} = 1$ for $\delta = 2, 3$; and for any δ,

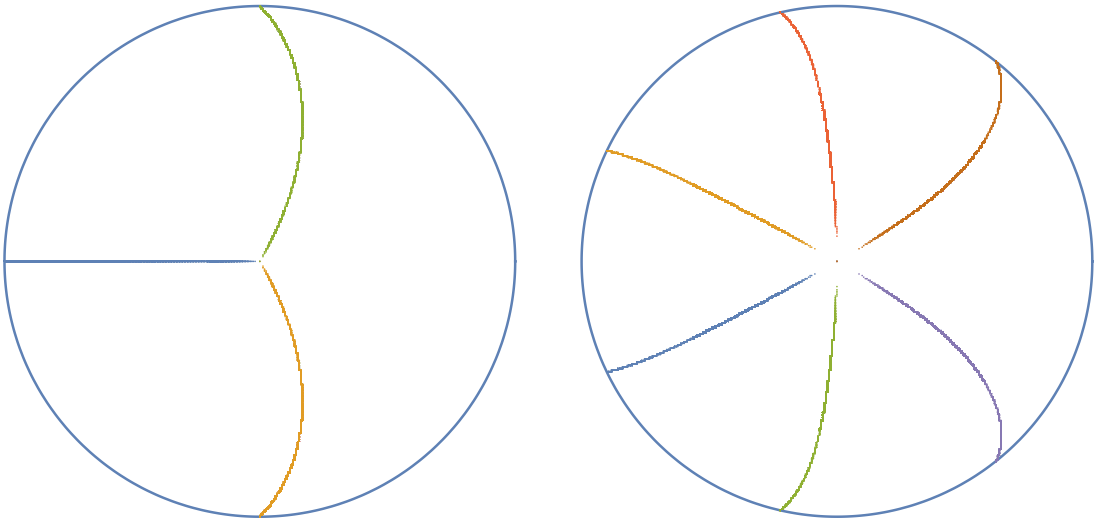

Figure 3. *The roots of $p_{\delta,f}(z)$ in the unit disk $|z| < 1$ for $f \in (0,1)$ and $\delta = 4, 7$.*

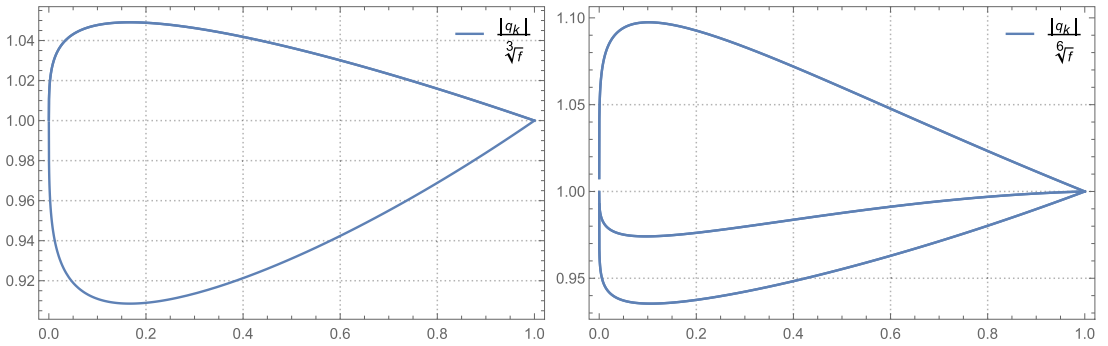

Figure 4. *The values $|q_k|/\sqrt[\delta-1]{f}$ for the roots $\mathrm{q_k}$ of $p_{\delta,f}(t)$ depending on f for $\delta = 4, 7$.*

$$|q_k|/f^{\frac{1}{\delta-1}} \to 1 \qquad \text{whenever} \qquad f \to 0 \quad \text{or} \quad f \to 1.$$

In Figure 4, the values $|q_k|/\sqrt[\delta-1]{f}$ for the roots q_k of the polynomial $p_{\delta,f}(t)$ are shown depending on f for $\delta = 4$ and $\delta = 7$.

Proposition 3.27.

(1) The generating function $L(t)$ is a product of two series

$$L(t) = \left(\sum_{n\geqslant 1} nft^n\right) \cdot \sum_{m\geqslant 0} (-f)^m (t + t^2 + \cdots + t^{\delta-1})^m$$

$$= \left(\sum_{n\geqslant 1} nft^n\right) \cdot \sum_{k=(k_1,k_2,\ldots,k_{\delta-1})\in\mathbb{Z}_{\geqslant 0}^{\delta-1}} (-f)^{|k|} \binom{|k|}{k_1, k_2, \ldots, k_{\delta-1}} t^{k_1+2k_2+\cdots+(\delta-1)k_{\delta-1}}. \tag{38}$$

(2) The corresponding expressions of L_n as polynomials in f are the following:

$$L_n = f\sum_{m=0}^{n-1} a_{nm}(-f)^m,$$
$$a_{nm} = \sum_{\substack{k_1,k_2,\dots,k_{\delta-1}\geqslant 0\\ k_1+k_2+\dots+k_{\delta-1}=m\\ k_1+2k_2+\dots+(\delta-1)k_{\delta-1}<n}} (n-k_1-2k_2-\dots-(\delta-1)k_{\delta-1})\binom{m}{k_1,k_2,\dots,k_{\delta-1}}. \tag{39}$$

In particular, $a_{n0} = n$.

Proof. The identity (38) rewrites (26) in terms of series, (39) is an equivalent form of (38). □

Proposition 3.28. *Coefficient of series (39) for L_n admits the asymptotic*

$$\frac{a_{nm}}{n} \underset{n\to\infty}{\nearrow} (\delta-1)^m. \tag{40}$$

Proof.

$$\frac{a_{nm}}{n} \underset{n\to\infty}{\nearrow} \sum_{\substack{k_1,k_2,\dots,k_{\delta-1}\geqslant 0\\ k_1+k_2+\dots+k_{\delta-1}=m}} \binom{m}{k_1,k_2,\dots,k_{\delta-1}} = (\delta-1)^m.$$

□

Remark 3.29. The asymptotic (35) for L_n and the asymptotic (40) for its coefficients at f are consistent within the circle of convergence $f < (\delta-1)^{-1}$.

Remark 3.30. For small/large f, we have the following approximations:

$$L_n \approx fn, \qquad \text{whenever} \quad f\delta \ll 1. \tag{41}$$

$$L_n \nearrow \lceil n/\delta \rceil, \quad \text{whenever} \quad f \nearrow 1. \tag{42}$$

The fastest way to get (42) is to look on (45). The last formula (42) is illustrated in Figure 5 and the values of L_n and L_n/n are shown depending on f for $\delta = 7$ and $n = 7\delta + r$, $r = 0, 1, 2, 3, 4, 5, 6$.

3.5. Alternative formula for L_n

The rest of this section is devoted to two alternative proofs of another formula for L_n (45).

Lemma 3.31. *$L(t)$ is the product of two series:*

$$L(t) = \left(\sum_{l\geqslant 0} f^l \sum_{k\in\mathbb{Z}^l_{\geqslant 0}} (1-f)^{l\delta+|k|}\cdot t^{|k|}\right)\cdot \sum_{k\geqslant 0}\bigl(1-(1-f)^k\bigr)t^k. \tag{43}$$

Proof. Note that the ring $\mathbb{R}[[t]]$ of formal series is local whose maximal ideal $\mathfrak{m}$ consists of the series $\sum_{n\geqslant 0} a_n t^n$ with $a_0 = 0$. For each $a \in \mathfrak{m}$, $(1-a)^{-1} = \sum_{l\geqslant 0} a^l$, where the infinite sum is defined because expression for each its coefficient at t^n turns into a finite sum.

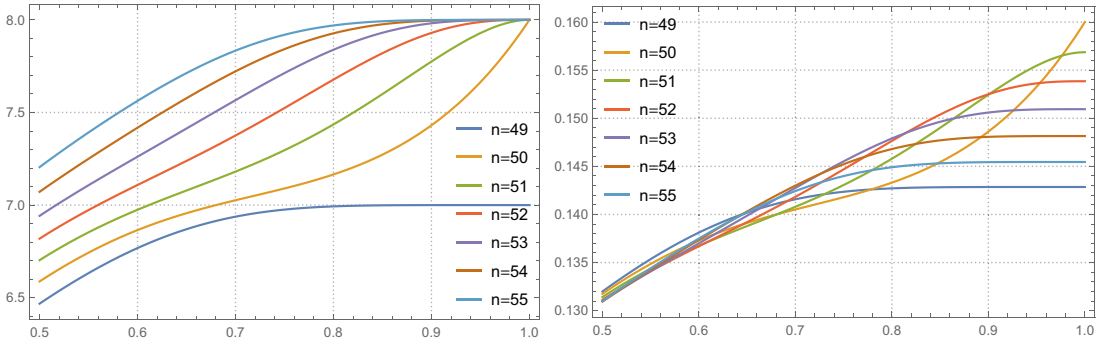

Figure 5. *The values of* $\mathrm{L_n}$ *and* L_n/n *depending on* f *for* $\delta = 7$ *and* $49 \leqslant n \leqslant 55$. *(a)* $\mathrm{L_n}$. *(b)* L_n/n.

From (24), we get

$$L(t) = \left(1 - ft^\delta \sum_{k\geqslant 0}(1-f)^k t^k\right)^{-1} \cdot \sum_{k\geqslant 0}\left(1-(1-f)^k\right)t^k$$
$$= \left(\sum_{l\geqslant 0}\left(ft^\delta \sum_{k\geqslant 0}(1-f)^k t^k\right)^l\right) \cdot \sum_{k\geqslant 0}\left(1-(1-f)^k\right)t^k.$$

□

Lemma 3.32. *For* $l \in \mathbb{Z}_{\geqslant 0}$, $n \in \mathbb{Z}_{>0}$, *the following identity between polynomials from* $\mathbb{Z}[f]$ *is true:*

$$\sum_{k\in\Delta_n^l} f^l(1-f)^{|k|} = 1-(1-f)^n \sum_{m=0}^{l-1}\binom{n+m-1}{m} f^m. \tag{44}$$

Proof. By induction on l, we have: For $l = 0$, (44) takes the from $\#\Delta_n^0 = 1$. For $l \geqslant 1$,

$$\sum_{k\in\Delta_n^l} f^l(1-f)^{|k|} = \sum_{k'\in\Delta_n^{l-1}} f^{l-1}(1-f)^{|k'|} \sum_{k''=0}^{n-|k'|-1} f(1-f)^{k''}$$
$$= \sum_{k'\in\Delta_n^{l-1}} f^{l-1}(1-f)^{|k'|}\left(1-(1-f)^{n-|k'|}\right)$$
$$= \sum_{k'\in\Delta_n^{l-1}} f^{l-1}(1-f)^{|k'|} - \binom{n+l-2}{l-1} f^{l-1}(1-f)^n.$$

□

Proposition 3.33. L_n *admits the following presentations:*

$$L_n = \lceil n/\delta\rceil - \sum_{l=0}^{\lceil n/\delta\rceil - 1}(1-f)^{n-l\delta}\sum_{m=0}^{l}\binom{n-l\delta+m-1}{m} f^m. \tag{45}$$

Proof. The first way: In terms of coefficients (43) can be rewritten as

$$\begin{aligned} L_n &= \sum_{l=0}^{\lceil n/\delta\rceil-1} \sum_{k\in\Delta^l_{n-l\delta}} f^l(1-f)^{|k|}\big(1-(1-f)^{n-l\delta-|k|}\big) \\ &= \sum_{l=0}^{\lceil n/\delta\rceil-1} \sum_{k\in\Delta^l_{n-l\delta}} f^l(1-f)^{|k|} - \sum_{l=0}^{\lceil n/\delta\rceil-1} \binom{n-l\Delta+l-1}{l} f^l(1-f)^{n-l\delta}. \end{aligned} \tag{46}$$

Then we can apply (44) to the first summand of (46).

The second way: The explicit formula for the expectation (11) together with expressions for probabilities (10) gets

$$\begin{aligned} L_n &= \sum_{l=1}^{\lceil n/\delta\rceil-1} l \sum_{k\in\Delta^l_{n-l\delta}} f^l(1-f)^{n-l\delta} + \sum_{l=1}^{\lceil n/\delta\rceil} l \sum_{k\in\Delta^l_{n-(l-1)\delta}\setminus\Delta^l_{n-l\delta}} f^l(1-f)^{|k|} \\ &= \sum_{l=1}^{\lceil n/\delta\rceil-1} l\binom{n-l\delta+l-1}{l} f^l(1-f)^{n-l\delta} \\ &\qquad + \sum_{l=1}^{\lceil n/\delta\rceil} l \sum_{k\in\Delta^l_{n-(l-1)\delta}} f^l(1-f)^{|k|} - \sum_{l=1}^{\lceil n/\delta\rceil-1} l \sum_{k\in\Delta^l_{n-l\delta}} f^l(1-f)^{|k|}. \end{aligned}$$

Again we can apply (44) to the second and third summands. □

3.6. Moments and variance

Let consider the mixed generating function for moments of $\lambda_{\delta,n}$:

$$L_\delta(t,x) := \sum_{n\geqslant 0} t^n \sum_{m\geqslant 0} \mathbf{E}\lambda^m_{\delta,n}\cdot\frac{x^m}{m!}.$$

Theorem 3.34 *The mixed generating function for moments of $\lambda_{\delta,n}$ is the following:*

$$L_\delta(t,x) = \frac{1+fe^x(t+t^2+\cdots+t^{\delta-1})}{1-(1-f)t-fe^x t^\delta}. \tag{47}$$

Proof. We describe this generating function in terms of the transition matrix A of the Markov chain.

$$\begin{aligned} L_\delta(t,x) &= \langle e^{\lambda^m_\delta}|(1-tA)^{-1}|0\rangle \\ &\underset{\text{by (21)}}{=} \frac{1}{1-(1-f)t}\langle e^{\lambda^m_\delta}|0\rangle + \sum_{k=1}^{\delta-1}\frac{ft^k}{1-(1-f)t}\langle e^{\lambda^m_\delta}|k\rangle + \frac{ft^\delta}{1-(1-f)t}\langle e^{\lambda^m_\delta}|(1-tA)^{-1}|\delta\rangle \\ &\underset{\text{by (15),(19)}}{=} \frac{1+fe^x(t+t^2+\cdots+t^{\delta-1})}{1-(1-f)t} + \frac{fe^x t^\delta}{1-(1-f)t}L_\delta(t,x). \end{aligned}$$

Finally, the obtained identity is solved with respect to $L_\delta(t,x)$. □

Lemma 3.35. *For a, b, c, d independent on x,*

$$\frac{d^m}{dx^m}\frac{ae^x+b}{ce^x+d}\bigg|_{x=0} = \sum_{k=1}^{n}\frac{k!(-c)^{k-1}(ad-bc)\cdot S(n,k)}{(c+d)^{k+1}}. \tag{48}$$

Proof. We apply Faá di Bruno's formula for mth derivative of the composition of the exponent with a fractional linear function. Stirling numbers of the second kind appear here as the values $B_{n,k}(1,\dots,1)$ of incomplete exponential Bell polynomials. □

Corollary 3.36. *For $m \in \mathbb{Z}_{>0}$, the generating function for m-th moments of $\lambda_{\delta,n}$ is the following*

$$\sum_{n\geqslant 0}\lambda_{\delta,n}^m t^n = \sum_{k=1}^{m}\frac{(-1)^{k-1}k!S(m,k)f^k t^{(k-1)\delta+1}}{(1-t)^{k+1}\big(1+f(t+t^2+\cdots+t^{\delta-1})\big)^k}. \tag{49}$$

Example 3.37. The generating function for second moments of $\lambda_{\delta,n}$ is the following

$$\sum_{n\geqslant 0}\lambda_{\delta,n}^2 t^n == \frac{ft(1-t+ft+ft^{\delta})}{(1-t)^3\big(1+f(t+t^2+\cdots+t^{\delta-1})\big)^2}. \tag{50}$$

Theorem 3.38 *The variance of $\lambda_{\delta,n}$ admits the following asymptotic for $n\to\infty$:*

$$\mathbf{Var}\lambda_{\delta,n} = n\frac{f(1-f)}{(1+(\delta-1)f)^3}+o(n). \tag{51}$$

Proof. Let's consider a partial fraction decomposition of (50) in the form

$$\frac{A}{(1-t)^3}+\frac{B}{(1-t)^2}+\frac{C}{1-t}+\frac{R(t)}{\big(1+f(t+t^2+\cdots+t^{\delta-1})\big)^2}.$$

The values $A=\frac{2f^2}{(1+(\delta-1)f)^2}$ and $B=\frac{f-4f^2+(\delta-1)(\delta-3)f^3}{(1+(\delta-1)f)^3}$ allow to obtain the asymptotic $\mathbf{E}\lambda_{\delta,n}^2 = n^2g^2 + n\frac{f-f^2+\delta(\delta-1)f^3}{(1+(\delta-1)f)^3}+o(n)$. From (35), we get $(\mathbf{E}\lambda_{\delta,n})^2 = n^2g^2+n\delta(\delta-1)g^3+o(n)$. Finally, $\mathbf{Var}\lambda_{\delta,n} = \mathbf{E}\lambda_{\delta,n}^2-(\mathbf{E}\lambda_{\delta,n})^2$. □

3.7. Binomial distribution with random delay

In this subsection, we generalize the longest chain distribution to the case of random delay.

Let Γ be a transition digraph of a finite Markov chain. We assume that Γ is a tree with additional loops at the root and leaves. First, we will consider a special case of such a digraph, shown in Figure 6, where the root has $s\geqslant 1$ children with weights $f_i>0$, $i=1,\dots,s$ and a loop with the weight $f_0 = 1-f_1-\cdots-f_s>0$. Each other internal vertex has a single child with the weight 1 and the maximal subchains have lengths $\delta_i\in\mathbb{Z}_{>0}$, $i=1,\dots,s$.

Let T_s be the infinite s-ary tree considered as a digraph with all edges oriented from the root as shown in Figure 7. Vertexes of this tree are labeled by elements of the free monoid $\{1,2\dots,s\}^*$, that is by strings in the alphabet $\{1,2\dots,s\}$. The monoid $\{1,2\dots,s\}^*$ acts on T_s by endomorphisms: $\{1,2\dots,s\}^*\ni w\mapsto S_w\in\mathrm{End}(T_s)$. Restricted to the vertexes, this action is isomorphic to the left regular action: $S_w(w')=ww'$.

Let $\widetilde{\Gamma}$ be an infinite transition digraph obtained if substitute each vertex in the infinite tree T_s by the digraph Γ as shown in Figure 8. The vertices of $\widetilde{\Gamma}$ are labeled by tuples $i_1,\dots,i_k;j$, where $i_1,\dots,i_k$ are elements of $\{1,2,\dots,s\}$ and $j\in\mathbb{Z}/\delta_{i_k}\mathbb{Z}$. So $|i_1,\dots,i_k;\delta_{i_k}\rangle = |i_1,\dots,i_k;0\rangle$.

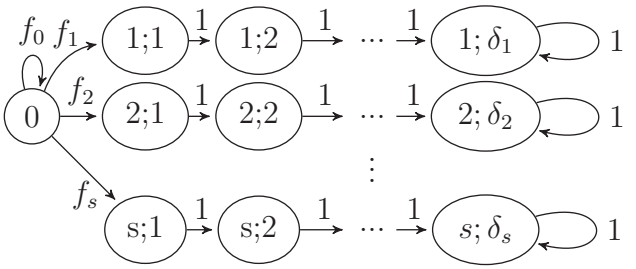

Figure 6. *Finite transition digraph* Γ.

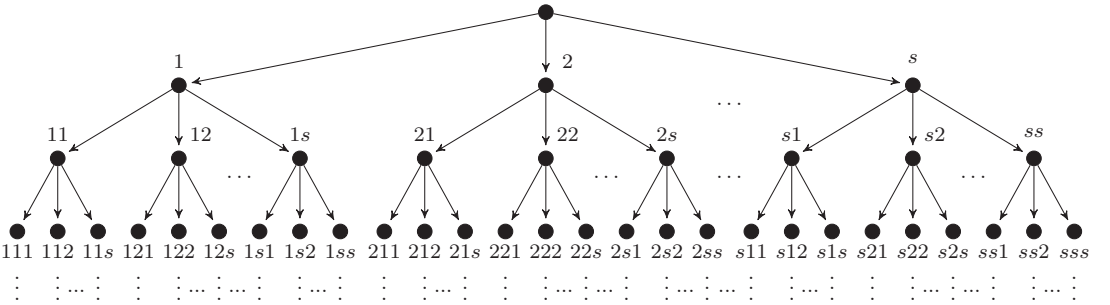

Figure 7. *The infinite* s*-ary tree* T_s.

Let $(\boldsymbol{\iota}_n)_{n\geqslant 0}$ be the sequence of independent random variables taking values $0, 1, 2, \ldots, s$, respectively, with probabilities $f_0, f_1, \ldots, f_s$. The following random mapping representation generalizes Definition 3.14 and describes the Markov chain $(X(n))_{\geqslant 0}$ corresponding to stochastic digraph $\widetilde{\Gamma}$.

Definition 3.39. *$X(0) = |;0\rangle$, and if $X(n) = |i_1, \ldots, i_k; j\rangle$, then*

$$X(n+1) = \begin{cases} X(n), & \text{if } j = 0 \wedge \boldsymbol{\iota}_n = 0, \\ |i_1, \ldots, i_k, \boldsymbol{\iota}_n; 1\rangle, & \text{if } j = 0 \wedge \boldsymbol{\iota}_n \neq 0, \\ |i_1, \ldots, i_k; j+1\rangle, & \text{if } j \neq 0. \end{cases}$$

Negative binomial distribution

One can generalize (22): For $r \in \mathbb{Z}_{\geqslant 0}$, let the random time τ_r is such that $X_\delta(\tau_r) = |i_1, \ldots, i_r; 0\rangle$ and $X_\delta(\tau_r + 1) = |i_1, \ldots, i_r, \boldsymbol{\iota}_{\tau_r}; 1\rangle$. Then $\tau_r - \sum_{r'=0}^{r-1} \delta_{\boldsymbol{\iota}_{\tau_{r'}}}$ has the negative binomial distribution $NB(r, 1-f_0)$.

Let A be the transition matrix corresponding to the stochastic digraph $\widetilde{\Gamma}$. The following generalization of (21) is true.

Lemma 3.40. *The Green function $(1-tA)^{-1} := \sum_{n\geqslant 0}(tA)^n$ satisfies the following recurrent relation:*

$$(1-tA)^{-1}|0\rangle = \frac{1}{1-f_0 t}|0\rangle + \sum_{i=1}^{s}\sum_{k=1}^{\delta_i - 1}\frac{f_i t^k}{1-f_0 t}|i;k\rangle + \sum_{i=1}^{s}\frac{f_i t^{\delta_i}}{(1-f_0 t)}(1-tA)^{-1}|i;\delta_i\rangle. \tag{52}$$

The action of the free monoid $\{1, 2, \ldots, s\}^*$ on T_s is carried over to $\widetilde{\Gamma}$: In terms of generators, for each $i = 1, 2, \ldots, s$, there exists weight preserving endomorphism of the stochastic digraph $\widetilde{\Gamma}$

$$S_i : \widetilde{\Gamma} \to \widetilde{\Gamma}, \qquad |i_1, \ldots, i_k; j\rangle \mapsto |i, i_1, \ldots, i_k; j\rangle.$$

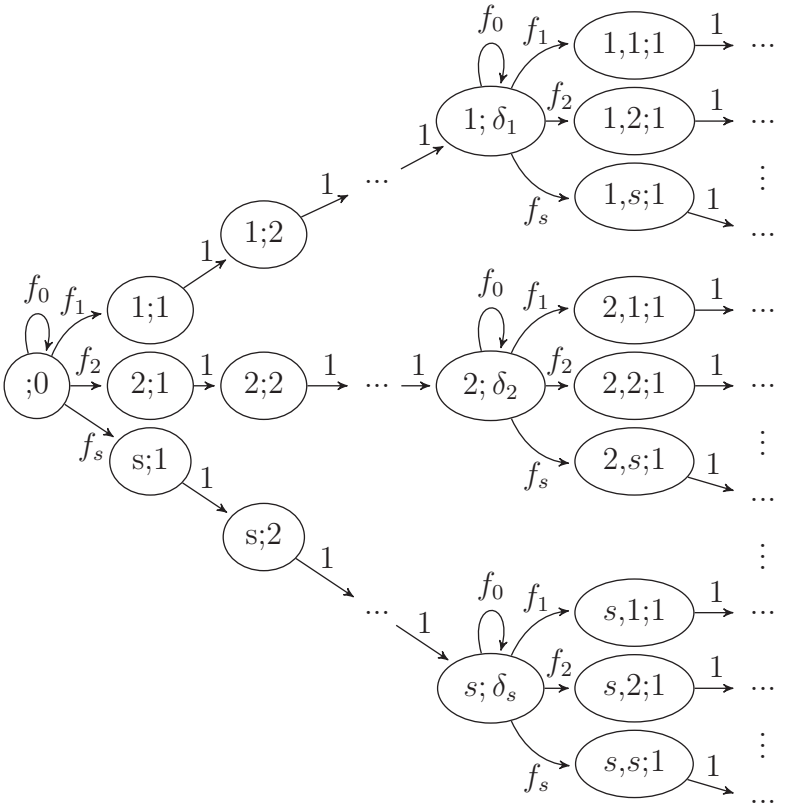

Figure 8. *Transition digraph of the infinite Markov chain with random delay.*

Hence, the corresponding linear operators commute with the transition matrix:

$$AS_i = S_i A. \tag{53}$$

Let us consider a function on edges of $\widetilde{\Gamma}$, which extends to linear functional, given by the formula

$$\langle \lambda | i_1, \dots, i_k; j \rangle = k. \tag{54}$$

The subject of our interest is the random variables

$$\lambda_n := \langle \lambda | A^n | ; 0 \rangle. \tag{55}$$

For $\langle e^{\lambda x}| := \sum_{m \geqslant 0} \frac{x^m}{m!} \langle \lambda^m |$, generalization of (19) is true:

$$\langle e^{\lambda x} | S_i = \langle e^{(\lambda+1)x} |. \tag{56}$$

Theorem 3.41 *The mixed generating function* $L_(t,x) := \sum_{n \geqslant 0} t^n \sum_{m \geqslant 0} \mathbf{E} \lambda_n^m \cdot \frac{x^m}{m!}$ *is given by the identity*

$$L(t,x) = \frac{1 + e^x \sum_{i=1}^{s} f_i (t + t^2 + \dots + t^{\delta_i - 1})}{1 - f_0 t - e^x \sum_{i=1}^{s} f_i t^{\delta_i}}.$$

Proof.

$$\begin{aligned} L(t,x) &= \langle e^{\lambda x}|(1-tA)^{-1}|0\rangle \\ &\underset{\text{by (52)}}{=} \frac{1}{1-f_0 t}\langle e^{\lambda x}|0\rangle + \sum_{i=1}^{s}\sum_{k=1}^{\delta-1}\frac{f_i t^k}{1-f_0 t}\langle e^{\lambda x}|i;k\rangle + \sum_{i=1}^{s}\frac{f_i t^{\delta}}{1-f_0 t}\langle e^{\lambda x}|(1-tA)^{-1}|i;\delta_i\rangle. \\ &\underset{\text{by (53), (19)}}{=} \frac{1+e^x\sum_{i=1}^{s} f_i(t+t^2+\cdots+t^{\delta_i-1})}{1-f_0 t} + \frac{e^x\sum_{i=1}^{s} f_i t^{\delta_i}}{1-f_0 t}L(t,x). \end{aligned}$$

□

Like in the proof of the special case, one can use the corollary (48) of Faá di Bruno formula to obtain expressions for generating function for mth moments of λ_n very close to (49).

Theorem 3.42 *The generating function* $L(t) = \sum_{n\geqslant 0}\mathbf{E}\lambda_n t^n$ *is*

$$L(t) = \frac{d}{dx}L(t,x)|_{x=0} = \frac{t\sum_{i=1}^{s} f_i}{(1-t)^2(1+\sum_{i=1}^{s} f_i(t+t^2+\cdots+t^{\delta_i-1}))}.$$

Its partial fraction decomposition takes the form

$$\begin{aligned} L(t) = &\frac{t\sum_{i=1}^{s} f_i}{\left(1+\sum_{i=1}^{s} f_i(\delta_i-1)\right)(1-t)^2} + \frac{\left(\sum_{i=1}^{s} f_i\right)\left(\sum_{i=1}^{s}\binom{\delta_i}{2}f_i\right)}{\left(1+\sum_{i=1}^{s} f_i(\delta_i-1)\right)^2(1-t)} \\ &+ \frac{R(t)}{1+\sum_{i=1}^{s} f_i(t+t^2+\cdots+t^{\delta_i-1})}, \end{aligned}$$

where

$$R(t) = \frac{\left(\sum_{i=1}^{s} f_i\right)\left(\sum_{i=1}^{s}\binom{\delta_i}{2}f_i\right)\sum_{i=1}^{s} f_i\sum_{k=0}^{\delta_i-2}(\delta_i-k-1)t^k}{\left(1+\sum_{i=1}^{s} f_i(\delta_i-1)\right)^2} - \frac{\left(\sum_{i=1}^{s} f_i\right)\sum_{i=1}^{s} f_i\sum_{k=0}^{\delta_i-2}\binom{\delta_i-k}{2}t^k}{\left(1+\sum_{i=1}^{s} f_i(\delta_i-1)\right)}.$$

Similarly to (33), one can get the full fraction decomposition of $L(t)$ and generalization of (34) for expectations $\mathbf{E}\lambda_n$. According to Example A.3, all roots of the denominator $1+\sum_{i=1}^{s} f_i(t+t^2+\cdots+t^{\delta_i-1})$ are out of the closed unit disc $|t|>1$. So finally we get the asymptotic formula generalizing (35).

Theorem 3.43 *For each fixed* $f\in(0,1)$ *and* $n\to\infty$,

$$\mathbf{E}\lambda_n = \frac{n\sum_{i=1}^{s} f_i}{1+\sum_{i=1}^{s} f_i(\delta_i-1)} + \frac{\left(\sum_{i=1}^{s} f_i\right)\left(\sum_{i=1}^{s}\binom{\delta_i}{2}f_i\right)}{\left(1+\sum_{i=1}^{s} f_i(\delta_i-1)\right)^2} + o(1). \tag{57}$$

Let $\boldsymbol{\delta}$ be a random variable taking values δ_i with probabilities f_i/f for $i=1,2,\ldots,s$, where $f=f_1+f_2+\cdots+f_s$. Then the expression (57) can be rewritten in the form very close to (35)

$$L_n = ng + g^2\mathbf{E}\binom{\boldsymbol{\delta}}{2} + o(1), \qquad g=\frac{f}{1+f\mathbf{E}(\boldsymbol{\delta}-1)}. \tag{58}$$

Remark 3.44. We consider special stochastic digraphs: finite trees with loops allowed only at the root and leaves, and where all edges are oriented from the root to the leaves. We say that two such stochastic digraphs Γ and Γ' are equivalent if

- the bijection between leaves of Γ and leaves of Γ' is given;
- for each path π in Γ from the root to a leaf and the path π' in Γ' from the root to the corresponding leaf
  - π and π' have the same length,
  - the products of the weights of all edges in π and π' are equal.

For each such stochastic digraph Γ, there exists a unique equivalent stochastic digraph Γ' where each internal vertex has a single child with the weight 1 (i.e., similar to the one described at the beginning of this section and shown in Figure 6).

If we apply the construction from this subsection to such a stochastic digraph Γ, then the distributions of the resulting random variables λ_n will be independent of the representative Γ of the equivalence class.

4. Stochastic characteristics of block generation process

Let us summarize the main practical results of the previous section: two descriptions (7) and (10) of the probability distribution of the longest chain $\gamma_{\delta,n}$; explicit formulas for expectation of the length $\lambda_{\delta,n}$ of the longest chain: (34) (exponential form) and (45), (39) (polynomial on f); asymptotic formulas for $\mathbf{E}\lambda_{\delta,n}$ when $n \to \infty$: (35) (fixed delay δ) and (57), (58) (random delay) and (51) for $\mathbf{Var}\lambda_{\delta,n}$.

In this section, we find the average value of blocks created in one timeslot, depending on the active slot parameter f. Using this result and results about the average length of the longest chain, obtained in Section 3, we can estimate the efficiency of the block creation process.

4.1. The expected number of slot leaders in a timeslot

The random number of slot leaders in the fixed jth timeslot is the sum $\nu_j = \sum_{i\in I} \xi_{ij}$ of independent Bernoulli random variables $\xi_{ij} \sim B(1, \varphi_f(\alpha_i))$. Thus, all ν_j are independent, and regardless of the slot index j, have the same Poisson binomial distribution:

$$\mathbf{Pr}(\nu_j = k) = \sum_{I' \in \binom{I}{k}} (1-f)^{1-\sum_{i\in I'} \alpha_i} \prod_{i\in I'} \varphi_{\alpha_i}(f), \tag{59}$$

and (as the expected value of the sum of independent random variables)

$$\mathbf{E}\nu_j = \sum_{i\in I} \mathbf{E}\xi_{ij} = \sum_{i\in I} \varphi_f(\alpha_i). \tag{60}$$

Lemma 4.1. *For the above random variables ν_j with Poisson binomial distribution (59), the expectation is represented by the polynomial series*

$$\mathbf{E}\nu_j = f + \sum_{k\geqslant 2} a_k f^k, \qquad a_k = \sum_{i\in I} \frac{\alpha_i}{k} \cdot \frac{(1-\alpha_i)(2-\alpha_i)\cdots(k-1-\alpha_i)}{(k-1)!} \tag{61}$$

convergent for $|f| < 1$.

Proof. We rewrite each summand in (60) using binomial series $(1-f)^{\alpha_i} = \sum_{k\geqslant 0} \binom{\alpha_i}{k} (-f)^k$. □

For $\alpha \in (0, 1]$, let consider the function:

$$\Phi_f(\alpha) := \frac{\varphi_f(\alpha)}{\alpha} = \frac{1-(1-f)^\alpha}{\alpha}. \tag{62}$$

It can be continued continuously:

$$\Phi_f(0) := \lim_{\alpha \searrow 0} \Phi_f(\alpha) = -\log(1-f). \tag{63}$$

One can rewrite (60) as

$$\mathbf{E}\nu_j = \sum_{i \in I} \alpha_i \Phi_f(\alpha_i). \tag{64}$$

In the case when all stakeholders have the stake ratio $\alpha_j = 1/|I|$ and each ν_j has the binomial distribution $B(|I|, \varphi_f(1/|I|))$,

$$\mathbf{E}\nu_j = \Phi_f(1/|I|). \tag{65}$$

More generally, one can group stakeholders in (64) by its stake ratios:

Proposition 4.2. *Suppose that I is the disjoint union $\coprod_{k \in K} I_k$ and for each $i \in I_k$ the stake ratio $\alpha_i = \beta_k/|I_k|$ depends only on k, with $\sum_k \beta_k = 1$. In this case:*

$$\mathbf{E}\nu_j = \sum_{k \in K} \beta_k \Phi_f(\beta_k/|I_k|). \tag{66}$$

Proposition 4.3. *For the above random variables ν_j with Poisson binomial distribution (59), the following inequalities hold:*

$$\Phi_f(1) = f \leqslant \mathbf{E}\nu_j \leqslant \Phi_f(1/|I|). \tag{67}$$

The lower bound is reached when a single stakeholder owns the whole stake. The upper bound is reached in the case (65) of equal stake ratios.

Proof. The first inequality follows from (60) using (3) and (4). The upper bound is found by the Lagrange multipliers method. □

Proposition 4.4. *The expected values $\mathbf{E}\nu_j$ admit the following limit cases:*

(1) for fixed $(\alpha_i)_{i \in I}$ and $f \searrow 0$,

$$\mathbf{E}\nu_j = f + a_2 f^2 + O(f^3),$$

where $a_2 = \frac{1-\sum_{i \in I} \alpha_i^2}{2}$ and, in particular when all α_i are the same, $a_2 = \frac{1-1/|I|}{2}$;

(2) for fixed $(\alpha_i)_{i \in I}$ and $f \nearrow 1$,

$$\mathbf{E}\nu_j \nearrow |I|;$$

(3) for fixed f and $\max_{i \in I} \alpha_i \to 0$,

$$\mathbf{E}\nu_j \to \Phi_f(0) = -\ln(1-f) = \sum_{k \geqslant 1} \frac{f^k}{k}.$$

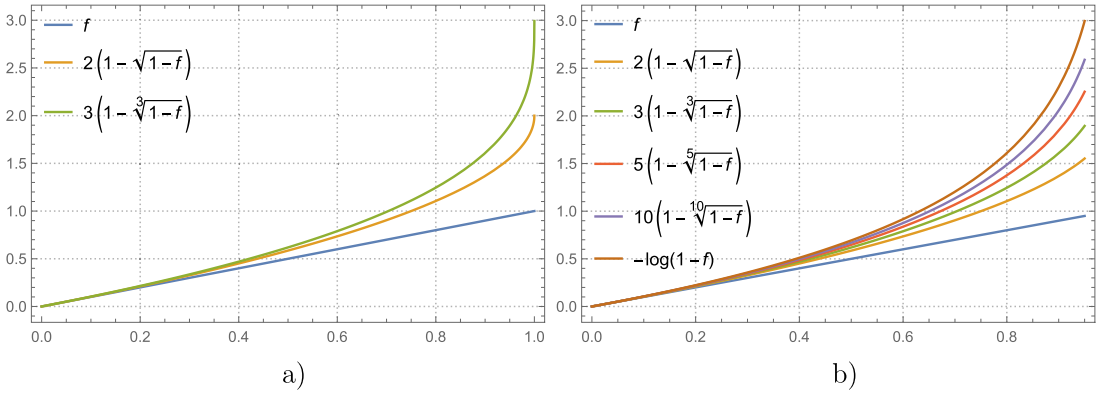

Figure 9. *The values of* $\mathbf{E}\nu_j = \Phi_f(1/|I|)$ *depending on* f *for equal stakes* $\alpha_j = 1/|I|$. *(a)* $|I| = 1, 2, 3$; $f \in [0, 1]$. *(b)* $|I| = 1, 2, 3, 5, 10, \infty$; $f \in [0, .95]$.

Proof. Items (1) and (2) follow directly from (61) and (60) respectively.

To prove (3) put $\alpha = \max_{i\in I} \alpha_i$. Then by (64) $\Phi_f(0) - \mathbf{E}\nu_j \leqslant \Phi_f(0) - \Phi_f(\alpha)$. □

On Figure 9, the values of $\mathbf{E}\nu_j = \Phi_f(1/|I|)$ are shown depending on f in the case of equal stakes $\alpha_j = 1/|I|$ for $|I| = 1, 2, 3, 5, 10, \infty$. Here we can see that, in the case of equally distributed stake, the average number of slot leaders in a timeslot for small f (less than 0.2) does not depend on the number of stakeholders. But the difference between charts increases dramatically when f tends to 1.

4.2. Efficiency

Definition 4.5. *The efficiency is the ratio of the expected number of useful blocks to the expected number of all produced blocks during the epoch:*

$$\mathrm{Eff} := \frac{\mathbf{E}\lambda_{\delta,n}}{\sum_{0\leqslant j<n} \mathbf{E}\nu_j} = \frac{L_{\delta,n}}{n \cdot \sum_{i\in I} \varphi(\alpha_i)}.$$

Note that the number of orphan blocks is $\sum_{0\leqslant j<n} \mathbf{E}\nu_j - \mathbf{E}\lambda_{\delta,n}$ and so the rate of orphan blocks is $1 - \mathrm{Eff}$.

If $n \gg 1$, one can use the asymptotic $\mathbf{E}\lambda_{\delta,n} \approx ng$ from (35) or (58); for the case of small stakes $\max_{i\in I} \alpha_i \ll 1$, we have $\mathbf{E}\nu_j \approx \Phi_f(0) = -\log(1-f)$. So in this case, one can use the approximation

$$\mathrm{Eff} \approx \frac{g}{\Phi_f(0)} = \frac{-f/\log(1-f)}{1 + (\delta - 1)f}. \tag{68}$$

If additionally $f \ll 1$, one can replace the numerator in (68) by 1:

$$\mathrm{Eff} \approx \frac{1}{1 + (\delta - 1)f}.$$

In both cases for the random delay presented by the data $(\delta_i, f_i)_{i=1,2,\ldots,s}$, one should put $f = f_1 + f_2 + \cdots + f_s$ and $\delta = \mathbf{E}\boldsymbol{\delta} = \frac{f_1\delta_1 + f_2\delta_2 + \cdots + f_s\delta_s}{f}$. As was expected, the large δ causes the smaller efficiency, but for all δ efficiency tends to 0 when f tends to 1.

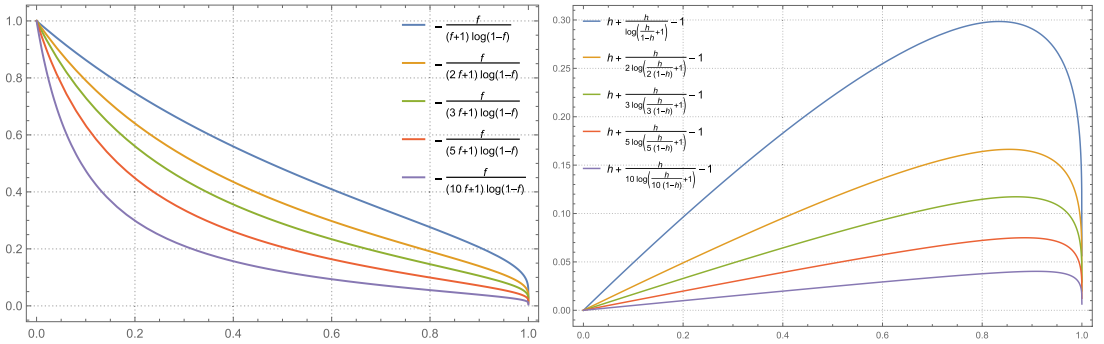

Figure 10. *The asymptotic of efficiency. (a)* $\mathrm{Eff}(f)$ *for* $\delta = 1, 2, 3, 5, 10$. *(b)* $\mathrm{Eff}_\delta(h) - \mathrm{Eff}_\infty(h)$ *for* $\delta = 1, 2, 3, 5, 10$.

One can inverse the identity (30) as

$$f = \frac{g}{1-(\delta-1)g}, \qquad g \in [0, 1/\delta],$$

and substituting this value in (68), we express the efficiency depending on the new dimensionless quantity $h = \delta \cdot g$, the expected length of chain produced during the propagation time δ

$$\mathrm{Eff} \approx \mathrm{Eff}_\delta(h) := \frac{h}{\delta \log\left(1 + \frac{h}{\delta(1-h)}\right)}. \tag{69}$$

Note that $\mathrm{Eff}_\infty(h) := \lim_{\delta\to\infty} \mathrm{Eff}_\delta(h) \to 1-h$. So we get an approximative conservation law:

$$\mathrm{Eff} + h \approx 1 \qquad \text{for } \delta \gg 1. \tag{70}$$

The deviation $\mathrm{Eff}_\delta(h) - \mathrm{Eff}_\infty(h)$ from the linear law admits the following series expansion at $h=0$

$$\mathrm{Eff}_\delta(h) - \mathrm{Eff}_\infty(h) = \frac{h}{\delta \log\left(1 + \frac{h}{\delta(1-h)}\right)} + h - 1 = \frac{h}{2\delta} - \frac{h^2}{12\delta^2} + \frac{(1-2\delta)h^3}{24\delta^3} + O(h^4).$$

On Figure 10 for $\delta = 1, 2, 3, 5, 10$ is shown (a) the asymptotic of Eff according to (68) depending on f, (b) the deviation $\mathrm{Eff}_\delta(h) - \mathrm{Eff}_\infty(h)$.

4.3. About length of forks

Forks are much more dangerous in the PoS consensus protocol than in PoW. It is connected with the procedure of slot leader election, which is strictly bound to the epoch. In this case, if the fork occurs with a length more than epoch length, there will be many problems not only with canceled transactions but also with protocol operation. So the probability distribution of fork length is also of significant importance.

The notion of a fork is widely used but still lacks formalization, though intuitively one understands its meaning. It causes additional difficulties in fork length estimation.

In our model, a fork may occur because of two reasons:

(1) two (or more) blocks were created by different slot leaders in different timeslots during the time which is less than block propagation time;
(2) there are two (or more) slot leaders at the same timeslot.

Note that the influence of the first reason may be reduced, if we add the new rule for choosing a valid branch:

Among two valid equal-length branches of the fork the slot leader should choose the one that is started in the earlier timeslot.

In this case, the forks that occur for the first reason may have only the length 1. If we consider the second reason, we note that the length of the current fork may increase only in the case when the next nonempty timeslot has more than 1 slot leader. In other words, the timeslot with only one slot leader stops the fork.

For a fixed timeslot, let $\Lambda \subseteq I$ be the random set such that $(S_i)_{i\in\Lambda}$ is the set of slot leaders in the fixed timeslot. As the special cases of (5), we get:

$$\mathbf{Pr}(\Lambda = \varnothing) = 1 - f, \tag{71}$$

and for each $i \in I$,

$$\mathbf{Pr}(\Lambda = \{i\}) = (1-f)^{1-\alpha_i}\varphi_f(\alpha_i) \gtrapprox (1-f)\varphi_f(\alpha_i). \tag{72}$$

The symbol "$\gtrapprox$" in (72) means inequality "$\geqslant$" and approximation "$\approx$" whenever all $\alpha_i \ll 1$. From (71) and (72), we get

$$\mathbf{Pr}(\Lambda \neq \varnothing) = f,$$
$$\Pr(\#\Lambda = 1) = \sum_{i\in I} \mathbf{Pr}(\Lambda = \{i\}) \gtrapprox (1-f)\sum_{i\in I}\varphi_f(\alpha_i) \underset{\text{by (3)}}{\geqslant} (1-f)\varphi_f(\alpha_I) = f(1-f).$$

Finally, we get the inequality for the conditional probability

$$\Pr(\#\Lambda > 1 \mid \Lambda \neq \varnothing) = \frac{\Pr(\Lambda \neq \varnothing) - \Pr(\#\Lambda = 1)}{\Pr(\Lambda \neq \varnothing)} \leqslant f.$$

Lemma 4.6. *The conditional probability that r fixed subsequent timeslots from the random chain $\gamma_{\delta,n}$ obtain more than 1 slot leaders is majorized by f^r.*

The value f^r from the lemma above can be considered an upper bound on the probability that a new fork of length r will begin in a fixed habitable timeslot.

Remark 4.7. Because the probability that a fixed timeslot obtains k slot leaders is $\approx f^k$ (for small k), with good approximation, we can assume that each of r slots has exactly two leaders. In each of r time slots, slot leaders with probabilities $1/2$ continue either two different branches or both the same branch. So the value $(f/2)^r$ is a more closed approximation for the probability that a new fork of length r will begin in a fixed habitable timeslot

4.4. Conclusion

The paper's results allow us to estimate different important parameters, connected with the operation of Ouroboros-based blockchains. Within the framework of our mathematical model, explicit analytical expressions for the quantities of interest to us are obtained, allowing convenient approximation. They were nevertheless obtained under the following simplified assumptions:

- all slot leaders in the current epoch are honest and act according to the consensus protocol;
- block propagation time is either a constant or random variable with finite support;
- epoch length is sufficiently large to use the asymptotics.

Deviations from at least one of these assumptions cause additional analytical problems, which, in turn, essentially complicate research. The most interesting and promising direction of the next research may be an estimation of the longest chain length under the presence of an adversary, which tries to split the blockchain. Note that this problem can't be solved by simply reducing the value of the active slot coefficient proportionally to the stake of honest slot leaders, because Adversary may try to use honest stakeholders' potential for splitting, by supporting the creation of chains of equal length. We also have a conjecture that the presence of an adversary cannot decrease the speed of chain growing by honest participants, though adversarial activity increases the length of forks and block stabilization time together with the share of orphan blocks, as well as decreases chain quality.

Note that results characterizing blockchain behavior in a model without adversary are also of great interest. In reality, most of the time the blockchain operates without any visible attacks. For example, during Cardano's work (since 2018), no double spending or splitting attacks were fixed—maybe because of protocol security, which makes such attacks impractical. Moreover, knowing the expected characteristics of the chain parameters (length of the longest fork, growth of the chain, number of lost blocks, etc.) allows an observer to distinguish some deviations in the behavior of the chain that may be caused by the activity of an attacker, and to be aware of his malicious actions.

The obtained results may also be used by developers to choose blockchain parameters, first of all, active slot coefficient f, according to their preferences, such as to increase the speed of chain growing or to minimize the orphan block ratio.

Acknowledgments. We thank the Horizen Lab team for the statistical data and fruitful discussions. The first author is partially supported by the Simons Foundation. Reviewers' comments helped us improve the presentation. Figures in this article were made using TikZ/PGF TeX packages and Wolfam Mathematica.

Competing interest. The authors declare no conflict of interest.

Appendix A. Schur–Cohn test

Definition A.1. *For a complex polynomial p of degree n, its reciprocal adjoint polynomial p^* is defined by $p^*(z) := z^n\overline{p(\bar{z}^{-1})}$ and its Schur transform Tp by $Tp := \overline{p(0)}p - \overline{p^*(0)}p^*$.*

Let consider the sequence $Tp, T^2p, \dots, T^np$ of iterated Schur transforms $T^kp := T(T^{k-1}p)$, where $T^{k-1}p$ is to be regarded as a polynomial of degree $n - k + 1$ even if its leading coefficient is zero

The next theorem describes the Schur–Cohn test in its simplest form sufficient for our purposes:

Theorem A.2 [8, Thm. 6.8b] *Let $p \neq 0$ be a polynomial of degree n. All zeros of p lie outside of the closed unit disk $|z| \leqslant 1$ iff*

$$T^kp(0) > 0, \qquad k = 1, 2, \dots, n. \tag{A.1}$$

Table A1. $L_n/n \approx g = f/(1-(\delta-1)f)$.

δ \ f	0.050	0.100	0.250	0.333	0.500	0.632	0.667
1	0.050	0.100	0.250	0.333	0.500	0.632	0.667
2	0.048	0.091	0.200	0.250	0.333	0.387	0.400
3	0.045	0.083	0.167	0.200	0.250	0.279	0.286
4	0.043	0.077	0.143	0.167	0.200	0.218	0.222
5	0.042	0.071	0.125	0.143	0.167	0.179	0.182
8	0.037	0.059	0.091	0.100	0.111	0.117	0.118
10	0.034	0.053	0.077	0.083	0.091	0.094	0.095
15	0.029	0.042	0.056	0.059	0.063	0.064	0.065
20	0.026	0.034	0.043	0.045	0.048	0.049	0.049

Table A2. $\mathbf{E}\nu_j = \Phi_f(1/|I|) = |I|\left(1 - \sqrt[|I|]{1-f}\right)$.

I \ f	0.050	0.100	0.250	0.333	0.500	0.632	0.667
1	0.050	0.100	0.250	0.333	0.500	0.632	0.667
2	0.051	0.103	0.268	0.367	0.586	0.787	0.846
3	0.051	0.104	0.274	0.379	0.619	0.850	0.921
4	0.051	0.104	0.278	0.385	0.636	0.885	0.961
10	0.051	0.105	0.284	0.397	0.670	0.951	1.041
∞	0.051	0.105	0.288	0.405	0.693	1.000	1.100

Note that the sign test in (A.1) for each k is based on the application of Rouché's theorem [8, Thm. 4.10b].

Example A.3. Let $p^*(z) = a_n z^n + \cdots + a_1 z + a_0 \neq 0$ be a polynomial with real coefficients satisfying the following inequalities

$$a_0 > a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n > 0. \tag{A.2}$$

Then coefficients of Tp^* (and hence also $T^k p^*$, $k = 1, 2, \ldots, n$) satisfy the same inequalities, that is

$$a_0 a_0 - a_n a_n > a_0 a_1 - a_n a_{n-1} \geqslant \cdots \geqslant a_0 a_{n-1} - a_n a_1 > 0.$$

So $T^k p^*(0)$ for $k = 1, 2, \ldots, n$, all zeros of p^* lie outside of the closed unit disk, and all roots of its reciprocal adjoint $p(z)$ are the images under inversion in the unit circle and lie in the open unit disk $|z| < 1$.

Appendix B. Numerical results

In this subsection, we give numerical values calculated according to the obtained formulas, to show how our results may be used during parametrization of the consensus protocol.

Table A1 shows the ratio between the longest chain and the number of timeslots in this epoch $L_n/n \approx g = f/(1-(\delta-1)f)$ defined by (30), Figure 2(b), thus showing the practically achievable active slot coefficient g. As can be seen from the table, this value drops with the increased network delivery delay. For example, suppose $f = 0.05$, the timeslot duration is set to 1 second, and the network propagation time is 8 seconds (i.e., $\delta = 8$). Then the practical average block time is $1/0.037 = 27$ seconds, which is 7 seconds greater than the assumed value for the expected average block time of $1/f = 20$ seconds.

Table B1. Eff $\approx -f/\log(1-f)/(1+(\delta-1)f)$.

δ \ f	0.050	0.100	0.250	0.333	0.500	0.632	0.667
1	0.975	0.949	0.869	0.822	0.721	0.632	0.607
2	0.928	0.863	0.695	0.617	0.481	0.387	0.364
3	0.886	0.791	0.579	0.494	0.361	0.279	0.260
4	0.848	0.730	0.497	0.411	0.289	0.218	0.202
5	0.812	0.678	0.435	0.353	0.240	0.179	0.165
8	0.722	0.558	0.316	0.247	0.160	0.117	0.107
10	0.672	0.500	0.267	0.206	0.131	0.095	0.087
15	0.573	0.395	0.193	0.145	0.090	0.064	0.059
20	0.500	0.327	0.151	0.112	0.069	0.049	0.044

Table A2 shows the average number of slot leaders per timeslot depending on the number of stakeholders $\mathbf{E}\nu_j = \Phi_f(1/|I|) = |I|\left(1 - \sqrt[|I|]{1-f}\right)$ (65), Figure 9, keeping the assumption that stake is equally distributed among all stakeholders. It can be seen that relatively big values of f lead to the increased number of stakeholders per timeslot with respect to the increased number of consensus participants (i.e., this gives more active timeslots than are expected with the given f).

Finally, Table B1 shows the efficiency—the ratio of blocks included in the longest chain to all blocks generated during the epoch Eff $\approx -f/\log(1-f)/(1+(\delta-1)f)$ (68), Figure 10(a). As expected, the orphan block ratio increases with network delivery delay. For example, for $\delta = 1$ and $f = 0.1$, the ratio of orphan blocks is 1–0.949 = 0.051; when delivery delay increases to $\delta = 5$, the orphan block ratio reaches 0.322—thus, almost 1/3 of all generated blocks are lost.

Table B1 allows the selection of more optimal combinations of f, δ, and timeslot duration. Let us have block propagation time over the network as 5 seconds, and we expect the average block generation time of 20 seconds. In this case, we can select a timeslot duration of 1 second, so $f = 1/20 = 0.05$, and $\delta = 5$. The orphan block ratio is 1–0.812 = 0.188. At the same time, the timeslot duration can be set to 5 seconds, so $f = 1/4 = 0.25$, and $\delta = 1$. The latter gives us the orphan block ratio of $1 - 0.869 = 0.131$. Thus, having the same p2p network characteristics, we increased the longest chain density by 5% just having other numerical parameters.

Let us remember that we consider the model with 100% honest participation, so all cells in the tables are filled, even with impractical combinations where values in the table for delivery delays δ greatly exceed $1/f$. For example, $f = 1/2 = 0.5$ and $\delta = 20$ mean that during one block propagation time, on average, there will be generated nine more blocks not seen by the next slot leaders. At the same time, with only honest participation, eventually, there will be reached the longest chain view, and for this set of parameters, the ratio of orphan blocks reaches $1 - 0.069 = 0.931$.

References

[1] Badertscher, C., Gaži, P., Kiayias, A., Russell, A. & Zikas, V. (2018). Ouroboros Genesis: Composable proof-of-stake blockchains with dynamic availability. New York, NY, USA. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, pp. 913–930. https://doi.org/10.1145/3243734.3243848.

[2] Badertscher, C., Gaži, P., Kiayias, A., Russell, A., Zikas, V. (2019). Ouroboros Chronos: Permissionless clock synchronization via proof-of-stake, Cryptology ePrint Archive, Report 2019/838, https://ia.cr/2019/838.

[3] David, B., Gaži, P., Kiayias, A. & Russell, A. (2018). Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, pp. 66–98. https://ia.cr/2017/573, https://doi.org/10.1007/978-3-319-78375-8_3.

[4] Dirac, P.A.M. (1939). A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society* **35**(3): 416–418, https://doi.org/10.1017/S0305004100021162.

[5] Dirac, P.A.M. (1958). *The principles of quantum mechanics*, 4th ed. International Series of Monographs on Physics, Oxford: Clarendon Press.
[6] Gaži, P., Ren, L., Russell, A. (2022). Practical settlement bounds for longest-chain consensus, Cryptology ePrint Archive, Report 2022/1571, https://ia.cr/2022/1571.
[7] Grunspan, C. & Pérez-Marco, R. (2018). Double spend races. *International Journal of Theoretical and Applied Finance* **21**(8): 1850053. https://doi.org/10.1142/S021902491850053X arXiv:1702.02867.
[8] Henrici, P. (1974). *Applied and computational complex analysis - vol 1: Power series, integration, conformal mapping, location of zeros*. Pure and Applied Mathematics, John Wiley & Sons.
[9] Kannappan, P. (2009). *Functional equations and inequalities with applications*. Springer Monographs in Mathematics, Springer, https://doi.org/10.1007/978-0-387-89492-8.
[10] Karpinski, M., Kovalchuk, L., Kochan, R., Oliynykov, R., Rodinko, M. & Wieclaw, L. (2021). Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus. *Sensors* **121**(19): 75–81. https://www.mdpi.com/1424-8220/21/19/6408 https://doi.org/10.3390/s21196408.
[11] Kiayias, A., Russell, A., David, B. & Oliynykov, R. *Ouroboros: A provably secure proof-of-stake blockchain protocol*. CRYPTO 2017, Part I - Lecture Notes in Computer Science, vol. 10401. Springer, pp. 357–388, https://doi.org/10.1007/978-3-319-63688-7_12.
[12] King, S. & Nadal, S. (2012). PPCoin: Peer-to-peer crypto-currency with proof-of-stake. https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf.
[13] Kovalchuk, L., Kaidalov, D., Nastenko, A., Rodinko, M., Shevtsov, O. & Oliynykov, R. (2020). Decreasing security threshold against double spend attack in networks with slow synchronization. *Computer Communications* **154**(15): 75–81, https://doi.org/10.1016/j.comcom.2020.01.079.
[14] Lando, S.K. (2003). Lectures on generating functions. *Student Mathematical Library,* **23** AMS https://dx.doi.org/10.1090/stml/023.
[15] Levin, D.A., Peres, Y. & Wilmer, E.L. (2017). *Markov chains and mixing times*, 2nd ed. AMS. https://doi.org/10.1090/mbk/107.
[16] Markov, A.A. (2022). *Calculus of probabilities*, Printing House of the Imperial Academy of Sciences, St. Petersburg, 1900. https://digital.fandm.edu/calculusofprobabilities Translated by Alan Levine.
[17] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*, https://www.bitcoin.org.
[18] Pinzón, C. & Rocha, C. (2016). Double-spend attack models with time advantage for bitcoin. *Electronic Notes in Theoretical Computer Science* **329**(9): 79–103, https://doi.org/10.1016/j.entcs.2016.12.006.
[19] QuantumMechanic, *Proof of stake instead of proof of work*, https://bitcointalk.org/index.php?topic=27787.0;all.
[20] Rahman, Q.I. & Schmeisser, G. (2002). *Analytic theory of polynomials: Critical points, zeros and extremal properties*. London Mathematical Society Monographs, USA: Oxford University Press, https://doi.org/10.1093/oso/9780198534938.001.0001.
[21] Rosenfeld, M. (2014). *Analysis of hashrate-based double spending*, arXiv:1402.2009.
[22] Stanley, R.P. (2011). *Enumerative combinatorics*, 2nd ed. Cambridge Studies in Advanced Mathematics 49, vol. 1. Cambridge University Press, https://doi.org/10.1017/CBO9781139058520.
[23] Wilf, H.S. (2006). *Generating functionology*, 3rd ed. Taylor & Francis, https://doi.org/10.1201/b10576.
[24] Woess, W. (2009). *Denumerable Markov chains: Generating functions, boundary theory, random walks on trees*. EMS Textbooks in Mathematics, European Mathematical Society, https://doi.org/10.4171/071.

Cite this article: Bespalov Y., Kovalchuk L., Nelasa H. and Oliynykov R. (2025). Binomial distribution with delay in analysis and parametrization of Ouroboros Praos proof of stake blockchain protocol. *Probability in the Engineering and Informational Sciences* 1–31. https://doi.org/10.1017/S0269964825000014