mathematics

Article

Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains

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

[1] Bogolyubov Institute for Theoretical Physics, 03143 Kiev, Ukraine
[2] Horizen, 20121 Milan, Italy; alberto@horizen.global
[3] IOHK Research, Hong Kong; lusi.kovalchuk@gmail.com
[4] Department of Information Security, Zaporizhzhia Polytechnic National University, 69063 Zaporizhzhia, Ukraine; annanelasa@gmail.com
* Correspondence: yu.n.bespalov@gmail.com (Y.B.), roliynykov@gmail.com (R.O.)

Abstract: The paper is devoted to the investigation of the distributed proof generation process, which makes use of recursive zk-SNARKs. Such distributed proof generation, where recursive zk-SNARK-proofs are organized in perfect Mercle trees, was for the first time proposed in Latus consensus protocol for zk-SNARKs-based sidechains. We consider two models of a such proof generation process: the simplified one, where all proofs are independent (like one level of tree), and its natural generation, where proofs are organized in partially ordered set (poset), according to tree structure. Using discrete Markov chains for modeling of corresponding proof generation process, we obtained the recurrent formulas for the expectation and variance of the number of steps needed to generate a certain number of independent proofs by a given number of provers. We asymptotically represent the expectation as a function of the one variable n/m, where n is the number of provers m is the number of proofs (leaves of tree). Using results obtained, we give numerical recommendation about the number of transactions, which should be included in the current block, idepending on the network parameters, such as time slot duration, number of provers, time needed for proof generation, etc.

Keywords: blockchain; perfect binary tree; lumping/factorization of Markov chains; product of Markov chains; Stirling numbers of the second kind; asymptotic of Stirling numbers; coupon collector's problem; classical occupancy distribution; probability on posets; Birkhoff duality

MSC: 60J10; 60J20; 05A18; 06A07

check for updates

Citation: Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains. *Mathematics* **2021**, *9*, 3016. https://doi.org/10.3390/math9233016

Academic Editor: Jan Lansky

Received: 26 October 2021
Accepted: 18 November 2021
Published: 24 November 2021

1. Introduction

Sidechains (SCs) [1–4], and also some similar tools, such as [5,6] are very suitable and prospective instrument in modern blockchains. They may be considered as some adjunct to the blockchain which allows one to obtain some additional features that are not implemented in initial blockchain (which is also called mainchain, not to be confused with sidechain).

Generally speaking, SCs may use an arbitrary consensus protocol with proved security—taking into account conditions in which its security was proved [7–10]. In what follows we will consider only SCs based on Latus Consensus Protocol [11], which isa hybrid PoS based on Ouroboros Praos [12], with additional binding to a PoW mainchain (MC). Binding to MC is a necessary requirement for SCs [1–4,11], to guarantee such blockchain properties as liveness and persistence [13]. To ensure security level of transactions in SC, some information should be regularly sent from SC to MC. One MC may have a plethora of SCs, so we need to reduce the volume of information sent, but in a such way that will not increase different risks for SC. In Latus consensus, this information contains a series of recursive zk-SNARK-proofs [14,15] that establish decentralized and verifiable cross-chain data transfers.

The abbreviation "zk-SNARK" means "zero-knowledge Succinct Non-interactive ARgument of Knowledge" [16]. This is a really ingenious technique for proving that somebody knows some information without revealing anything about this information, or for proving that some statement is true, without revealing its details. zk-SNARK may be considered as some kind of non-interactive zero-knowledge proof system, which was introduced about 40 years ago in [17] and has been intensively developing since then. For the first time term "zk-SNARK" itself was introduced in [18], based on [19]. In [20,21] the Pinoccio protocol was introduced, making zk-SNARKs more convenient and applicable for general purposes.

As it was mentioned, zk-SNARK is succinct argument, which means that the proof length is sufficiently small. For example, it may be constant, as in [22], i.e., its length depends only on the desirable security level and does not depend on the size of data which we prove to be true. That is why zk-SNARKs are a very attractive tool to be used in blockchains, where the problem of block size reduction is imminent. They are used, for example, in blockchains such as zCash [23], MINA [24], and Horizen [11], and even some special cryptographic primitives, like block ciphers and hash-functions, are created for using in zk-SNARKs [25,26].

Each blockchain choses variant of zk-SNARK, which is most suitable for it. Latus Consensus uses Darlin [27], which is advanced composition of Marlin [28] and Halo [29].

This work does not deal with developing of zk-SNARK topic, and, actually, for our investigations it does not matter what exactly zk-SNARK is used for in Latus. Similar to [1–4], it is devoted to providing of stable and correct functioning of SCs. However, unlike these works, we investigate these issues within each separate block, because block creation in Latus is a rather cumbersome procedure. In Latus, decentralized proofs generation use a special dispatching scheme, which allows all interested parties, or provers, to create a randomly chosen proof and then to submit it to the blockchain, getting some reward (incentive) for each accepted proof. If two or more provers created the same proof, block-forger (the entity who creates block) chooses one of them. In other words, Latus Consensus allows all interested parties to participate simultaneously in one-block generation. From the one hand, it increases decentralization; the need to create more complicated protocols of interaction between blockforger and provers, as well as the choice parameters of these protocols and justification of their correctness and robustness. The article is devoted just to these questions.

In Latus, decentralized proofs generation use a special dispatching scheme, which allows all interested parties, or provers, to create a randomly chosen proof and to then submit it to the blockchain, getting some reward (incentive) for each accepted proof. If two or more provers created the same proof, blockforger (the entity who creates block) chooses one of them.

The main feature of the Latus consensus is to reduce the volume of information sent to MC from SC, using a recursive composition of zk-SNARKs, which allows to construct a succinct proof of the correctness for sidechain state transitions for the period of a withdrawal epoch. At the end of an epoch, a zk-SNARK for a withdrawal certificate is constructed to prove correctness of sidechain state transitions for the whole epoch and validates backward transfers. Such a procedure allows the MC to efficiently verify the sidechain's activity, without using any intermediary—such as certifiers [4]—and without delving into the details of the processes inside SC.

In SC, a blockforger collects the transactions he intends to include in his block, orders them and forms correspondent proposals for provers. Each block contains some totally ordered set of transactions (its size is the power of 2) and perfect binary tree, which nodes are zk-SNARK-proofs. In what follows we will call this tree "proof tree". Each proof of the bottom of the tree proves some assertion about the correctness of transition from some state of UTXO (unspent transaction output) to its next state, which is the state after corresponding transaction. Such assertions we will call "base assertions", and proofs of the bottom level, which are the leaves of the proof tree, we will call "base proofs".

Other, internal nodes of the proof tree are so-called "merge" proofs [4], which prove the correctness of two proofs in child nodes. Therefore proof in the root node proves correctness of transitions between UTXO states corresponding to the whole block.

All zk-SNARK-proofs for the proof tree are distributively constructed by proovers. Each prover, who creates zk-SNARK-proof, assigns the prices for his proofs within some interval or set, defined at the end of the previous epoch. If there is more than one proof for some node of the proof tree, the blockforger chooses the cheapest one. Under these conditions, the mutual activity of blockforger and provers should provide efficient and stable functioning of sidechain.

This work is a revised, corrected, and extended version of the conference thesis [30]. It contains the results which describe and explain the functioning of SCs, and first of all the blockforger's and prover's behavior, using probability theory and combinatorial apparatus. We use Markov chains for modeling distributed proof generation process in zk-SNARKs-based blockchains. The main purposes of our researches are:

- To estimate the number of steps (or to find its expectation and variance) needed to build a complete set of zk-SNARK-proofs for base assertions corresponding to the transactions, which the blockforger includes in the block he creates;
- Using these results, to recommend the maximal number of transactions that the blockforger should include in the block, to guarantee that the corresponding proof tree will be created with high probability during one time slot.

We consider two different models, which corresponds to two types of proof construction. The first model describes the the simpler case when all the proofs are built independently (like one level of the proof tree). The second model investigates a more complicated problem, when the proofs are located at nodes from the different levels of the proof tree. Such a set of proofs has the natural partial order, because the proofs from the upper level of the tree may be constructed only when the proofs from the previous levels are constructed.

The paper is organized as follows. At the beginning of the Section 2 we give some preliminary information from combinatorics, probability theory, and Markov chains technique, which is necessary for further researches. The notion of lumping for Markov chains is a special case regarding the general idea of factorization for mathematical structures. Unfortunately only a small part of textbooks pay attention to this concept. Our point of view here is that a problem can be described by several Markov chains with different level of factorization, depending on how many details we want to know at the moment. In Section 2.3 we illustrate this idea on the sample of coupon collector's problem.

Then, in Section 3 we analyse the number of steps needed to construct a complete set of proofs, which are the leaves of the unproved part of the proof tree. In this case they may be generated independently and simultaneously. We give a series of examples of different stochastic models, which are helpful in our researches. We prove that two models, described in Examples 5 and 6, are stochastically equivalent, although the first one was initially formulated as non-Markovian, and the second one was formulated in terms of the Markov chain. We study the lumped form of this model in Example 7. Using this technique we obtained the recurrent formulas for the expectation and variance of the number of steps, depending on the number of provers n and the number of leaves m, and then asymptotically reduce the expectation to a function h of single parameter n/m and describe its behavior.

Finally in Section 4 we research the process of proof creation for the entire perfect binary tree and show that this construction is convenient to generalize the previously investigated models for the case of a partially ordered set. Some useful insights emerged from this generalization, such as a more appropriate probability distribution on poset items. We conclude our article with Section 4.6 which contains numerical results regarding the number of transactions, which the blockforger should include in the current block. Such a number depends on the network parameters, such as time slot duration, number of active provers, time needed for prove generation, and so on. We present a few tables with these recommended numbers of transactions for the different preset probabilities of successful block generation.

2. Preliminaries

Here we provide the necessary facts about lumping for Markov chains and describe the Markov chain corresponding to the coupon collector problem as a result of two subsequent lumping constructions. These technique and examples are important for our main models.

Notation 1. *For cardinality of finite set S, we use two notations (depending on convenience):*

$$\#S = |S|.$$

Notation 2. *For non-negative integer m, by the corresponding boldface letter* $\mathbf{m}$ *we denote (depending on context) the totally ordered poset $\{1 < 2 < \cdots < m\}$ or its underlying set $\{1, 2, \ldots, m\}$.*

Notation 3. Iverson bracket *for statement P turns boolean value into the corresponding number:*

$$[\![P]\!] := \begin{cases} 1, & \text{if } P \text{ is true,} \\ 0, & \text{if } P \text{ is false.} \end{cases} \tag{1}$$

Notation 4. *We use the generally accepted notations for*

- falling factorials*:*
$$n^{\underline{r}} = (n)_r = n(n-1)\cdots(n-r+1);$$
- binomial *and* multinomial coefficients*:*
$$\binom{m}{k} := \frac{m!}{k!(m-k)!}; \qquad \binom{m}{m_1, \ldots, m_n} := \frac{m!}{m_1! \cdots m_n!}, \quad \textit{where} \quad m_1 + \cdots + m_n = m.$$

2.1. Stirling Numbers of the Second Kind

The "twelve-fold way" of combinatorics ([31], 1.9) counts the number of mappings (injections, surjections, or all possible) between two finite sets, distinguishing or not distinguishing elements in each of them. For example, the symmetric groups S_m and S_n act on the set $\mathrm{Sur}(\mathbf{m}, \mathbf{n})$ of surjections $\mathbf{m} \twoheadrightarrow \mathbf{n}$ via pre- and post- composition, respectively. The *Stirling partition numbers* (or *Stirling numbers of the second kind*) can be defined as a number of orbits:

$$S(m, n) = \left\{ {m \atop n} \right\} := |S_n \backslash \mathrm{Sur}(\mathbf{m}, \mathbf{n})|,$$

i.e., this is the number of partitions of the m labeled elements into n non-empty non-labelled blocks, or the number of ways to nest m Matryoshka dolls so you can still see n (matryoshkas are linear, ordered by size).

The action S_n on $\mathrm{Sur}(\mathbf{m}, \mathbf{n})$ is free, so

$$|\,\mathrm{Sur}(\mathbf{m}, \mathbf{n})| = n! \left\{ {m \atop n} \right\}.$$

On the other hand, given a surjection $\pi : \mathbf{m} \twoheadrightarrow \mathbf{n}$, elements of the orbit $\pi \circ S_m$ are identified with cosets from $S_m / \mathrm{St}_\pi = S_m / (S_{m_1} \times \cdots \times S_{m_n})$, where $m_i = \#\pi^{-1}(i)$. All surjections can be calculated via the sum over n-compositions of m:

$$n! \left\{ {m \atop n} \right\} = |\,\mathrm{Sur}(\mathbf{m}, \mathbf{n})| = \sum_{\substack{m_1 + \cdots + m_n = m \\ m_1, \ldots, m_n \geqslant 1}} \left| \frac{S_m}{S_{m_1} \times \cdots \times S_{m_n}} \right| = \sum_{\substack{m_1 + \cdots + m_n = m \\ m_1, \ldots, m_n \geqslant 1}} \binom{m}{m_1, \ldots, m_n}. \tag{2}$$

Multiplying both parts of (2) by $z^m/m!$ and taking the sum over m one can obtain the exponential generating function for $n!\{{m \atop n}\}$

$$\sum_{m=0}^{\infty} n! \left\{ {m \atop n} \right\} \frac{z^m}{m!} = (e^z - 1)^n. \tag{3}$$

Each map $f : \mathbf{m} \to \mathbf{n}$ is factorised as $f = (\mathbf{m} \twoheadrightarrow \operatorname{Im} f \hookrightarrow \mathbf{n})$. Then the total number of functions $\mathbf{m} \to \mathbf{n}$

$$n^m = \sum_{S \subseteq \mathbf{n}} |S|! \left\{ {m \atop |S|} \right\} = \sum_{r=0}^{n} \left\{ {m \atop r} \right\} (n)_r. \tag{4}$$

One can consider (4) as an identity between integer polynomial in a free variable n. So we get an alternative definition of Stirling numbers as coefficients of the transition matrix between two polynomial bases.

Möbius inversion [31] (3.7) in the case of power-set $\mathcal{P}\mathbf{m}$ admits a simpler formulation as the inclusion-exclusion principle [31] (2.1). It allows, on the contrary to (4), to express the number of surjections in terms of the numbers of all functions:

$$n! \left\{ {m \atop n} \right\} = \sum_{S \subseteq \mathbf{n}} (-1)^{n-|S|} |S|^m = \sum_{r=0}^{n} (-1)^r \binom{n}{r} (n-r)^m. \tag{5}$$

The (forward) difference operator acts on numerical sequences (x_k) as $\Delta : x_k \mapsto x_{k+1} - x_k$. Its powers are expressed by binomial formula $\Delta^n x_k = \sum_{r=0}^{n} (-1)^r \binom{n}{r} x_{k+n-r}$. It allows to rewrite the previous formula (5) as:

$$n! \left\{ {m \atop n} \right\} = \Delta^n 0^m = \Delta^n k^m |_{k=0}.$$

Stirling numbers of the second kind appear in [32] as a double sequence A008277, where one can find some additional information, references, and links.

2.2. Factorisation of Markov Chains

In what follows, we assume that Markov chains are discrete-time, time-homogeneous and with finite or countable state-space S. Elements of transition matrix p are written as

$$p_{ij} = p(i,j) = \mathbf{Pr}(X(n+1) = j \mid X(n) = i), \qquad i,j \in S.$$

A such position of indexes corresponds to the right action of p on the row vector of states. This is a right stochastic matrix, i.e., with $\sum_{j \in S} p_{ij} = 1$.

Here we consider the notion of lumping for Markov chains; see, for example [33] (§6.3). The general mathematical idea of transferring a structure from a set to a factor-set also works in the case of Markov chains. Given a surjection $\pi : S \twoheadrightarrow T$, consider the corresponding logical matrix v_π and its Moore–Penrose inverse $v_\pi^\dagger$ (see [34]).

$$v_\pi := (\delta_{\pi(s),t})_{s \in S, t \in T}, \qquad v_\pi^\dagger := (v_\pi^t v_\pi)^{-1} v_\pi^t.$$

In our special case: the logical matrix corresponding to surjection isa projection and, hence, Moore–Penrose inverse $v_\pi^\dagger$ is a real one-side inverse: $v_\pi^\dagger v_\pi = 1$.

Lemma 1. *Let $p = (p_{ss'})_{s,s' \in S}$ be a right stochastic matrix over a state-space S. For surjection $\pi : S \twoheadrightarrow T$ the following conditions are equivalent:*

1. *for any $t' \in T$ the sum $\sum_{s' \in \pi^{-1}(t')} p_{ss'}$ is locally constant on $s \in \pi^{-1}(t)$ for each $t \in T$;*
2. $v_\pi v_\pi^\dagger p v_\pi = p v_\pi$.

Definition 1. *Let $p = (p_{ss'})_{s,s' \in S}$ be a right stochastic matrix over a state-space S. A surjection $\pi : S \twoheadrightarrow T$ satisfying the conditions of the previous lemma is called a* lumping map *(and the corresponding partition $S = \coprod_{t \in T} \pi^{-1}(t)$ is called* lumpable*).*

Proposition 1. *Let $p = (p_{ss'})_{s,s' \in S}$ be a stochastic matrix and $\pi : S \twoheadrightarrow T$ a lumping map.*

1. *Then, one can define a new stochastic matrix p^{π} over a state-space T with entries*

$$p^{\pi}_{tt'} := \sum_{s' \in \pi^{-1}(t')} p_{ss'}, \qquad s \in \pi^{-1}(t). \tag{6}$$

2. *The lumped k-fold transition matrix can be written as*

$$(p^{\pi})^k = (v^{\dagger}_{\pi} p v_{\pi})^k = v^{\dagger}_{\pi} p^k v_{\pi}. \tag{7}$$

We believe that the following statement is a kind of "folkloric" result.

Proposition 2. *Suppose that a finite group G acts on the set of states S by the rule $S \times G \ni (s, g) \mapsto s^g \in S$ and the stochastic matrix $p = (p(s, s'))_{s,s' \in S}$ is G-invariant, i.e.,*

$$p(s_1^g, s_2^g) = p(s_1, s_2), \qquad s_1, s_2 \in S, \quad g \in G.$$

Then, the canonical projection $\pi : S \twoheadrightarrow S/G$ to the set of orbits is a lumping map.

Proof. Denote $\mathrm{St}_s := \{g \in G \mid s^g = s\}$ the stabilizer subgroup of state s. For an orbit $s^G := \{s^g \mid g \in G\}$ the sum from Lemma 1 takes the form

$$\sum_{s'' \in \pi^{-1}(s^G)} p(s_1, s'') = \frac{1}{|\,\mathrm{St}_s\,|} \sum_{g \in G} p(s_1, s^g).$$

Then, the standard argument shows that the last sum is G-invariant as a function on s_1:

$$\sum_{g \in G} p_{(}s_1^h, s^g) = \sum_{g \in G} p_{(}s_1, s^{gh^{-1}}) = \sum_{g' \in G} p(s_1, s^{g'}). \qquad \square$$

2.3. Coupon Collector Model via Products and Factorizations

The classical coupon collector problem can be described as follows.

Example 1. *There are n distinct coupons in the urn. A collector draws with return one random coupon in a step. The subjects of interest are the following random variables:*

- *The number of distinct coupons selected after m steps;*
- *The number of steps required to obtain exactly r distinct coupons.*

Crossed products of Markov chains (and their generalizations) are described in [35]. We obtain a version of the coupon collector model as the crossed power of a simple deterministic process. The other two versions are results of its subsequent factorizations. It leads to the classical occupancy distribution described via Stirling partition numbers. This context is closely related to our further models.

Example 2 (Hyperoctant-full information)**.** *Consider a fully deterministic Markov chain that counts natural numbers: $X_0 = 0, X_1 = 1, X_2 = 2, \ldots$ Its transition matrix is a semi-infinite Jordan cell:*

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

The n-th crossed power of the above Markov chain has the set of states $\mathbb{Z}^n_{\geqslant 0}$ and transition matrix

$$p = \frac{1}{n}\sum_{i=1}^{n} \underbrace{1_{\mathbb{Z}_{\geqslant 0}} \otimes \cdots \otimes 1_{\mathbb{Z}_{\geqslant 0}}}_{i-1} \otimes J \otimes \underbrace{1_{\mathbb{Z}_{\geqslant 0}} \otimes \cdots \otimes 1_{\mathbb{Z}_{\geqslant 0}}}_{n-i},$$

where $1_{\mathbb{Z}_{\geqslant 0}}$ is the identity matrix on the basis $\mathbb{Z}_{\geqslant 0}$.

This is a random walk over the n-dimensional hyperoctant $\mathbb{Z}^n_{\geqslant 0}$ with nonzero transition probabilities

$$p(a, a + e_i) = 1/n, \qquad a \in \mathbb{Z}^n_{\geqslant 0}, \qquad e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i}).$$

Then nonzero entries of m-fold transition matrix are

$$p^m(a, a + h) = n^{-m}\binom{m}{h_1, \ldots, h_n}, \qquad \text{where} \quad h_i \geqslant 0 \quad \text{and} \quad h_1 + \cdots + h_n = m.$$

So each row of this matrix represents a multinomial distribution on vectors h.

The next step is when a collector wants to remember whether each fixed coupon was drawn, no matter how many times.

Notation 5. *For $a \in \mathbb{Z}^N_{\geqslant 0}$ or $a \in \{0.1\}^N$ the support of a is defined as follows.*

$$\operatorname{supp} a := \{i \in N \mid a_i \neq 0\}.$$

Example 3 (Hypercube-partial information)**.** *Iverson bracket* (1) *applied to each coordinate $(a_i)_{i\in\mathbf{n}} \mapsto ([\![a_i > 0]\!])_{i\in\mathbf{n}}$ gets a lumping map $\mathbb{Z}^n_{\geqslant 0} \to \{0,1\}^n$ for the previous Markov chain. According to* (7) *for the obtained Markov chain on the hypercube $\{0,1\}^n$ m-step transition matrix p^m is the following: if $p^m(a,b) > 0$ then $a_i \leqslant b_i$ for all i; and by inclusion-exclusion principle*

$$p^m(a,b) = n^{-m} \sum_{\substack{m_1+\cdots+m_n=m \\ m_1,\ldots,m_n \geqslant 0 \\ m_i>0 \Rightarrow i\in\operatorname{supp}\ b \\ i\notin\operatorname{supp} a \Rightarrow m_i>0}} \binom{m}{m_1, \ldots, m_n} = n^{-m} \sum_{r=|\operatorname{supp} a|}^{|\operatorname{supp} b|} (-1)^{\operatorname{supp}|b|-r} \binom{|\operatorname{supp}(b-a)|}{r - |\operatorname{supp} a|} r^m.$$

In particular,

$$p^m(a,a) = (|\operatorname{supp} a|/n)^m, \qquad p^m(0,b) = n^{-m}|\operatorname{supp} b|!\left\{ {m \atop |\operatorname{supp} b|} \right\}.$$

If the collector is able to keep only one number in memory, we continue the lumping.

Example 4 (Only number of samples)**.** *The projection of hypercube to the main diagonal*

$$\{0,1\}^n \to \{0,1,\ldots,n\}, \qquad (a_i)_{1\leqslant i\leqslant n} \mapsto \sum_i a_i$$

is a lumping map. Combining the states, we get so called coupon collecting Markov chain [36] *(2.2), where nonzero m-step transition probabilities are the following:*

$$p^m(k, k+r) = n^{-m}\binom{n-k}{r}\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}(k+s)^m.$$

The number $\xi_m = \xi_0 p^m$ of distinct coupons selected after m steps has the classical occupancy distribution [37]*:*

$$\mathbf{Pr}(\xi_m = r) = p^m(0,r) = \frac{(n)_r}{n^m}\left\{ {m \atop r} \right\}. \tag{8}$$

The expectation of number ζ_r^n of steps required to obtain exactly r distinct coupons is described via harmonic numbers $H_n = 1 + 1/2 + \cdots + 1/n$:

$$\mathbf{E}\,\zeta_r^n = n(H_n - H_{n-r}). \tag{9}$$

3. Distributed Generation of Sets of Proofs

This section presents the main results about the distributed generation of sets of separate independent proofs. This is the simplified model, where all proofs may be generated simultaneously and independently. This model corresponds, in particular, to the case of the generation of proofs which are on the same level as proof tree.

3.1. Models of Distributed Generation of Sets of Proofs

The further two examples show two possible approaches to the description of this model, which then appear equivalent.

Example 5 (States are subsets)**.** *Let provers be special nodes in the peer-to-peer network. They need to construct zk-SNARK-proofs for finite set N of so called* proof-candidates.

We describe this process as a Markov chain, whose states are subsets of $N' \subseteq N$ of proof-candidates not yet proved. The number of provers $m > 0$ is fixed. On each step, beginning in the state N', each prover independently and with equal probabilities selects a single proof-candidate from N' and construct its proof, so the selection is given by a function $g : \mathbf{m} \to N'$ uniformly distributed among all functions $\mathbf{m} \to N'$. The resulting state is the difference $N'' := N' \smallsetminus \operatorname{Im} g$ obtained by removing just the proved elements. Nonzero transition probabilities $p(N', N'')$ equal the part of all functions $\mathbf{m} \to N'$ which come from surjections to $N' \smallsetminus N''$ i.e., $g = (\mathbf{m} \twoheadrightarrow N' \smallsetminus N'' \hookrightarrow N')$.

$$p(N', N'') = \frac{|\operatorname{Sur}(\mathbf{m}, N' \smallsetminus N'')|}{|N'|^m} = \frac{|N' \smallsetminus N''|!}{|N'|^m} \left\{ \begin{matrix} m \\ |N' \smallsetminus N''| \end{matrix} \right\}, \qquad N'' \subseteq N'. \tag{10}$$

An alternative way is to define a probability measure on trajectories:

Notation 6. *A* linear ordering *of a set N is a bijection $\sigma : N \xrightarrow{\cong} \{1, 2, \ldots, |N|\}$. Denote* Ord N *the set of linear orderings on N.*

Example 6 (Non-Markovian model)**.** *Let at the beginning each prover for $1 \leqslant i \leqslant m$ independently select its own so-called priority ordering $\sigma_i \in \operatorname{Ord} N$ with equal probability $1/|\operatorname{Ord} N| = 1/|N|!$. This determines the chain of states, i.e., the subsets together with linear orderings:*

$$N = N_0 \supset N_1 \supset \cdots \supset N_{k-1} \supset N_k = \varnothing,$$
$$\sigma_i^{(j)} \in \operatorname{Ord}(N_j), \qquad \sigma_i^{(0)} = \sigma_i, \qquad 1 \leqslant i \leqslant m, \qquad 0 \leqslant j \leqslant k.$$

In jth step, $1 \leqslant j \leqslant k$, being in the state N_{j-1} ith prover select proof-candidate according to the function $g_j : \mathbf{m} \to N_{j-1}$ given by $g_j(i) := \left(\sigma_i^{(j-1)}\right)^{-1}(1)$. The next state is $N_j = N_{j-1} \smallsetminus \operatorname{Im}(g_j)$. There is the natural projection $\rho^N_{N'} : \operatorname{Ord}(N) \to \operatorname{Ord}(N')$, which removes elements of $N \smallsetminus N'$ from an ordering. Then, we put

$$\sigma_i^{(j)} = \rho^N_{N_j}(\sigma_i). \tag{11}$$

Proposition 3. *The models from Examples 5 and 6 are stochastically equivalent.*

Proof. We give a sketch of the proof. A more general situation is described in Example 12. Selections of $(\sigma_i)_{1 \leqslant i \leqslant m}$ are uniformly distributed on $(\operatorname{Ord} N)^m$. This implies

1. uniform distribution of g_j in the set of functions $\mathbf{m} \to N_{j-1}$, and
2. uniform distribution of $\sigma_i^{(j)} \in \operatorname{Ord}(N_j)$.

The second item follows from the definition (11) and from the fact that the fiber of $\rho^N_{N'}$ over each point has the same cardinality $|\operatorname{Ord} N|/|\operatorname{Ord} N'| = |N|!/|N'|!$. □

Example 7 (States are numbers)**.** *The cardinality function $N' \mapsto |N'|$ is a lumping map for the Markov chain from Example 5. The states of the factorized Markov chain are $\{0, 1, \dots, |N|\}$, the only nonzero elements of transition matrix are the following:*

$$\begin{aligned} p(0,0) &= 1, \\ p(n, n-r) &= \frac{1}{n^m}\binom{n}{r} r! \left\{ {m \atop r} \right\} = \frac{(n)_r}{n^m} \left\{ {m \atop r} \right\}, \quad n > 0,\ 1 \leqslant r \leqslant m. \end{aligned} \tag{12}$$

Note that each row this matrix coincides with the classical occupancy distribution from Example 4.

Let the initial state be $\xi^{mn}_0 \equiv n$. The evolution is described via powers of transition matrix:

$$\xi^{mn}_k = \xi^{mn}_0 p^k.$$

The absorbing state is 0. All trajectories are strictly decreasing and $\xi^{mn}_k \equiv 0$ for $k \geqslant n$.

The absorption time *τ^{mn} is a random variable which measures the exact number of steps m provers needs to generate all n proofs. i.e., $\tau^{mn} = k + 1$ iff $\xi^{mn}_{k+1} = 0$ and $\xi^{mn}_k \neq 0$.*

Taking into account the lower triangular form of our transition matrix, we get recurrent and explicit formulas for probabilities:

$$\begin{aligned} \mathbf{Pr}(\tau^{mn} = 0) &= \delta_{n0}, \\ \mathbf{Pr}(\tau^{mn} = k+1) &= \sum_{r=1}^{\min(m,n)} p_{n\,n-r}\, \mathbf{Pr}(\tau^{m\,n-r} = k) = \sum_{r=0}^{\min(m,n)} \frac{(n)_r}{n^m} \left\{ {m \atop r} \right\} \mathbf{Pr}(\tau^{m\,n-r} = k) \end{aligned} \tag{13}$$

$$\begin{aligned} \mathbf{Pr}(\tau^{mn} = k) &= \sum_{0 < n_k < \cdots < n_2 < n_1 = n} p_{n_1 n_2} \cdots p_{n_{k-1} n_k} p_{n_k 0} \\ &= \sum_{0 < n_k < \cdots < n_2 < n_1 = n} \frac{n!}{(n_1 n_2 \cdots n_k)^m} \left\{ {m \atop n_1 - n_2} \right\} \cdots \left\{ {m \atop n_{k-1} - n_k} \right\} \left\{ {m \atop n_k} \right\} \\ &= \sum_{\substack{r_1 + \cdots + r_k = n \\ r_1, \dots, r_k > 0}} \frac{n!}{(r_1(r_1 + r_2) \cdots n)^m} \left\{ {m \atop r_1} \right\} \cdots \left\{ {m \atop r_k} \right\} \\ &= \sum_{\substack{s_1 + \cdots , s_{2k} = n \\ s_1, s_3, \dots, s_{2k-1} \geqslant 0 \\ s_2, s_4, \dots, s_{2k} > 0}} \binom{n}{s_1, \dots, s_{2k}} \frac{(-1)^{s_1 + s_3 + \cdots + s_{2k-1}} (s_2 s_4 \cdots s_{2k})^m}{((s_1 + s_2)(s_1 + s_2 + s_3 + s_4) \cdots n)^m}. \end{aligned} \tag{14}$$

Multiplying (13) by k^ℓ and taking a sum over k we get the recurrent formula for ℓth moment:

$$\mathbf{E}(\tau^{mn} - 1)^\ell = \sum_{r=1}^{\min(n,m)} p_{m\,n-r}\, \mathbf{E}(\tau^{m\,n-r})^\ell.$$

In particular, this allows one to get the next formulas for calculating expectation and variance.

Proposition 4. *Let $m > 0$. Then $\tau^{m0} \equiv 0$ and for $n > 0$*

$$
\begin{aligned}
\mathbf{E}\,\tau^{mn} &= 1 + \sum_{r=1}^{\min(n,m)} \frac{(n)_r}{n^m} \left\{ {m \atop r} \right\} \mathbf{E}\,\tau^{m\,n-r}, \\
\mathbf{E}(\tau^{mn})^2 &= -1 + 2\,\mathbf{E}\,\tau^{mn} + \sum_{r=1}^{\min(n,m)} \frac{(n)_r}{n^m} \left\{ {m \atop r} \right\} \mathbf{E}(\tau^{m\,n-r})^2, \\
\mathbf{Var}\,\tau^{mn} &= \mathbf{E}(\tau^{mn})^2 - (\mathbf{E}\,\tau^{mn})^2.
\end{aligned}
\tag{15}
$$

In Table 1 at the end of the paper we present probability distributions of τ^{mn} accurate to 10^{-6} (except of the last column). A cell contains the list of pairs $k; p_k^{mn}$ of value k and the corresponding probability p_k^{mn} (nonzero up to accuracy). The number of proofs n runs through powers of 2, which corresponds to the number of leaves of a perfect binary tree.

We compare the values of $\mathbf{E}\,\tau^{mn}$ as results of infinite-precision calculations according (15) using Wolfram Mathematica and of 10^5 random tests written on C++ of model from Example 6. For $m, n \in \{10, 20, 30, 40, 50, 100, 200, 300\}$ the numerical results obtained by these two different ways match up to 2 digits after the dot.

Remark 1. *For fixed positive integer m we consider two modifications of the coupon collector model from Example 4:*

1. *After m, $2m$, $3m, \ldots$ steps all coupons drown, during the last m steps, which are removed from the urn permanently.*
2. *Each time when collector drown m new distinct coupons, these m coupons are removed from the urn permanently.*

Note that if for the first modification we apply time scaling i.e., consider a subprocess at moment $0, m, 2m, \ldots$, we obtain the proofs generation model from Example 7. The second modification is slightly slower than the first, i.e., the expectation of the number of steps to obtain exactly the r distinct coupons in the second modification is no less than in the first modification. These observations show that the expectation of the time τ^{mn} of proof generation from Example 7 can be majorized by the expectation of the time ζ_r^n from coupon collector model from Example 4:

$$
\begin{aligned}
\mathbf{E}\,\tau^{m\,bm} - \mathbf{E}\,\tau^{m\,m} &\leqslant (\mathbf{E}\,\zeta_m^{bm} + \mathbf{E}\,\zeta_m^{(b-1)m} + \cdots + \mathbf{E}\,\zeta_m^{2m})/m \\
&= b(H_{bm} - H_{(b-1)m}) + (b-1)(H_{(b-1)m} - H_{(b-2)m}) + \cdots + 2(H_{2m} - H_m) \\
&= bH_{bm} - (H_{(b-1)m} + H_{(b-2)m} + \cdots + H_{2m} + 2H_m) \\
&\approx \ln \frac{b^b}{(b-1)!} \underset{b\gg 1}{\approx} b + \frac{1}{2} \ln \frac{b}{2\pi}.
\end{aligned}
\tag{16}
$$

3.2. Asymptotics of τ^{mn}

For the general Formula (14) for the probabilities $\mathbf{Pr}(\tau^{mn} = k)$ it seems very difficult to obtain approximation in an explicit form. However, $\mathbf{Pr}(\tau^{mn} = 1)$ is just a fraction of surjective maps $\mathbf{m} \to \mathbf{n}$ among all such maps:

$$
\mathbf{Pr}(\tau^{mn} = 1) = \frac{n!S(m,n)}{n^m}.
$$

3.2.1. Large Number of Provers

Firstly we consider the case of large number of provers, i.e., $m \gg n$. Equivalently this means $\mathbf{Pr}(\tau^{mn} = 1) \approx 1$ or $\mathbf{E}\,\tau^{mn} \approx 1$. Note that $\tau^{mn} = 1$ iff on the first step the corresponding map $\mathbf{m} \to \mathbf{n}$ from provers to proof-candidates is surjective.

Proposition 5. *For fixed number $n > 0$ of proof-candidates the next asymptotic hold:*

$$\mathbf{Pr}(\tau^{mn} = 1) \underset{m\to\infty}{\sim} 1 - n\left(\frac{n-1}{n}\right)^m + o\left(\left(\frac{n-1}{n}\right)^m\right). \tag{17}$$

$$\mathbf{E}\,\tau^{mn} \underset{m\to\infty}{\sim} 1 + n\left(\frac{n-1}{n}\right)^m + o\left(\left(\frac{n-1}{n}\right)^m\right). \tag{18}$$

Table 1. Probability distributions for τ^{mn} accurate to ppm (10^{-6}) and probabilities of tree creation for 9 tics.

$m\backslash n$	**2**	**4**	**8**	**16**	**32**	**64**	**128**	**256**	**9 tics**
3	1; 0.750000 2; 0.250000	2; 0.810764 3; 0.187500 4; 0.001736	3; 0.346759 4; 0.598575 5; 0.054020 6; 0.000643 7; 0.000003						$\ell = 4$ 0.948934
4	1; 0.875000 2; 0.125000	1; 0.093750 2; 0.856554 3; 0.049624	2; 0.038452 3; 0.791998 4; 0.167602 5; 0.001946 6; 0.000002						$\ell = 4$ 0.998582
9	1; 0.996094 2; 0.003906	1; 0.711365 2; 0.288588 3; 0.000047	1; 0.010815 2; 0.928031 3; 0.061145 4; 0.000009	2; 0.006789 3; 0.824258 4; 0.168743 5; 0.000210					$\ell = 5$ 0.892535
10	1; 0.998047 2; 0.001953	1; 0.780602 2; 0.219387 3; 0.000011	1; 0.028163 2; 0.944047 3; 0.027789 4; 0.000001	2; 0.036465 3; 0.901558 4; 0.061960 5; 0.000017					$\ell = 5$ 0.951990
16	1; 0.999969 2; 0.000031	1; 0.960000 2; 0.040000	1; 0.306798 2; 0.693034 3; 0.000168	1; 0.000001 2; 0.720767 3; 0.279205 4; 0.000027	3; 0.323989 4; 0.673970 5; 0.002041				
32	1; 1.000000	1; 0.999598 2; 0.000402	1; 0.891278 2; 0.108722	1; 0.073443 2; 0.926430 3; 0.000127	2; 0.490645 3; 0.509350 4; 0.000005				$\ell = 6$ 0.948374
33	1; 1.000000	1; 0.999699 2; 0.000301	1; 0.904520 2; 0.095480	1; 0.089692 2; 0.910235 3; 0.000073	2; 0.561396 3; 0.438602 4; 0.000002				$\ell = 6$ 0.961682
64	1; 1.000000	1; 1.000000	1; 0.998446 2; 0.001554	1; 0.765182 2; 0.234818	1; 0.004182 2; 0.995734 3; 0.000084	2; 0.226404 3; 0.773595 4; 0.000001			
94	1; 1.000000	1; 1.000000	1; 0.999972 2; 0.000028	1; 0.963319 2; 0.036681	1; 0.163487 2; 0.836513	2; 0.969308 3; 0.030692			$\ell = 7$ 0.944377
95	1; 1.000000	1; 1.000000	1; 0.999975 2; 0.000025	1; 0.965585 2; 0.034415	1; 0.173944 2; 0.826056	2; 0.973714 3; 0.026286			$\ell = 7$ 0.950428
128	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.995870 2; 0.004130	1; 0.562887 2; 0.437113	1; 0.000013 2; 0.999930 3; 0.000057	2; 0.048095 3; 0.951905		
256	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999999 2; 0.000001	1; 0.990585 2; 0.009415	1; 0.304309 2; 0.695691	2; 0.999956 3; 0.000044		
451	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999981 2; 0.000019	1; 0.948528 2; 0.051472	1; 0.018313 2; 0.981687		$\ell = 8$ 0.949452

Table 1. *Cont.*

$m\backslash n$	2	4	8	16	32	64	128	256	9 tics
452	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 0.999981$ $2; 0.000019$	$1; 0.949314$ $2; 0.050686$	$1; 0.018930$ $2; 0.981070$		$\ell = 8$ 0.950256
512	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 0.999997$ $2; 0.000003$	$1; 0.980019$ $2; 0.019981$	$1; 0.088899$ $2; 0.911101$		
1024	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 0.999994$ $2; 0.000006$	$1; 0.959185$ $2; 0.040815$		
2175	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 0.999995$ $2; 0.000005$	$1; 0.949825$ $2; 0.050175$	$\ell = 9$ 0.949820
2176	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 1.000000$	$1; 0.999995$ $2; 0.000005$	$1; 0.950016$ $2; 0.049984$	$\ell = 9$ 0.950011

Proof. For each proof-candidate i let A_i be the event that i is not proved on the first step, $\mathbf{Pr}\,A_i = \left(\frac{n-1}{n}\right)^m$, with complement $\overline{A_i}$. From the inclusion-exclusion principle:

$$\mathbf{Pr}(\tau^{mn} = 1) = \mathbf{Pr} \bigcup_i \overline{A_i} = 1 - \sum_i \mathbf{Pr}\,A_i + \sum_{i<j} \mathbf{Pr}\,A_i \cap A_j - \cdots,$$

where the next sums are small with respect to the first. To calculate expectation $\mathbf{E}\,\tau^{mn}$ we can take into account only values $\tau = 1, 2$; the contribution of other values is asymptotically small. □

Remark 2. *In blog post [38] it is observed that the upper bound*

$$\mathbf{Pr}(\tau^{mn} = 1) \leqslant (1 - (1 - 1/n)^m)^n \tag{19}$$

can be derived from the inequality between usual and conditional probabilities.

$$\mathbf{Pr} \bigcap_i \overline{A_i} = \prod_i \mathbf{Pr}\left(\overline{A_i} \,\middle|\, \bigcap_{j<i} \overline{A_j}\right) \leqslant \prod_i \mathbf{Pr}\,\overline{A_i}$$

Note that the right hand side of (17) has the same asymptotic as $\mathbf{Pr}(\tau^{mn} = 1)$ *in (19), so one can consider it as asymptotical upper bound for* $\mathbf{Pr}(\tau^{mn} = 1)$.

3.2.2. Asymptotics of the Stirling Numbers and Probabilities $\mathbf{Pr}(\tau^{mn} = 1)$

The asymptotics of the Stirling numbers of the second kind have been studied since Laplace (1814). From a long list of publications we consider only results related with our context.

A usual way is to apply Cauchy's integration formula to the generating function (3):

$$n!S(m,n) = m![z^m](e^z - 1)^n = \frac{m!}{2\pi i} \oint_C (e^z - 1)^n z^{-(m+1)}\, dz = \frac{m!}{2\pi i} \oint_C e^{\phi(z)} \frac{dz}{z},$$

where C is a suitable contour around the origin and $\phi(z) = n \ln(e^z - 1) - m \ln(z)$. The saddle point ρ solves the equation $\phi'(\rho) = 0$ or $\frac{\rho}{1-e^{-\rho}} = \frac{m}{n}$, or, finally,

$$\rho = \frac{m}{n} + W_0\Big(-\frac{m}{n} e^{-m/n}\Big).$$

Lambert W function or *product logarithm* is a multivalued function inverse to $w \mapsto we^w$, and W_0 is its principal branch; see [39].

The following expression coincides with the first term of [40] (5.1) or with [41] (5.9) derived in the context local limit theorem or with [42] (2.9):

$$S(m,n) \sim \frac{m!(e^{\rho}-1)^{n+1}}{n!\rho^{m+1}e^{\rho}\sigma\sqrt{2\pi m}},$$

where $\sigma^2 = \left(\frac{n}{m}\right)^2\left(1-\frac{\rho}{e^{\rho}-1}\right)$ is a variance of the limiting normal distribution. This approximation is uniform for n/m in each closed subinterval of $(0,1)$.

Using Stirling formula for $m!$ we can obtain asymptotic probability as a function of two parameters n/m and m:

$$\mathbf{Pr}(\tau^{mn}=1) = \frac{n!S(m,n)}{n^m} \sim \alpha\gamma^m, \tag{20}$$

where α and γ depends only on the ratio n/m:

$$\alpha = \frac{1}{\left(1-\frac{\rho}{e^{\rho}-1}\right)^{1/2}}, \qquad \gamma = \frac{e^{\rho-1}}{(e^{\rho}-1)^{1-n/m}}.$$

This dependencies are shown on Figures 1 and 2. One can see that when n/m run from 0 to 1, the functions $\alpha(n/m)$ and $\gamma(n/m)$ change respectively from 1 to ∞ and from 1 to $1/e$.

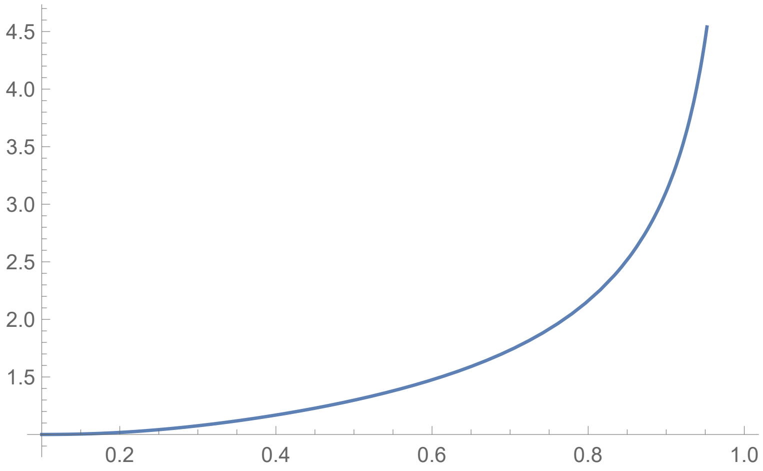

Figure 1. $\alpha(n/m)$.

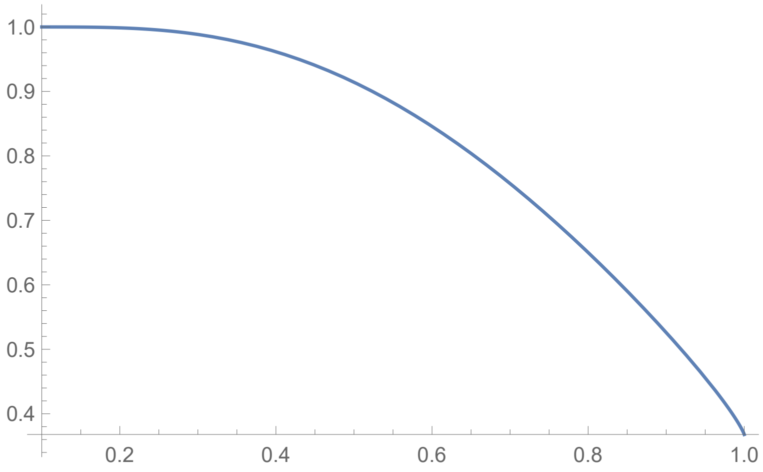

Figure 2. $\gamma(n/m)$.

3.2.3. Dependence on the Ratio n/m

Next we research asymptotical behaviour of τ^{mn} depending on m and n, and formulate related results as conjectures. At the moment we can prove only some transitions, as others comes from infinite-precision calculations. Note that $\mathbf{E}\,\tau^{mn}$ for large m and n asymptotically depends only on the ratio n/m and we study the character of this dependence.

A series of calculations with infinite precision allows one to formulate the following sequence of hypotheses.

Hypothesis 1. *For each fixed $m, n \in \mathbb{Z}_{>0}$ the sequence $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\,\tau^{km\,kn}$ is increasing and upper bounded.*

Remark 3. *Recall that Remark 1 states a connection between coupon collector and proof generation models. Taking into account (16) and that for ζ_r^n from Example 4 the sequence $k \mapsto \zeta_{kr}^{kn}$ is increasing and upper bounded, we can prove the following. If the sequence $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\,\tau^{k\,k}$ is increasing and upper bounded, then for each fixed $m, n \in \mathbb{Z}_{>0}$ with $n > m$ the sequence $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\,\tau^{km\,kn}$ is increasing and upper bounded.*

So under assumptions of Hypothesis 1 there exists a function $h : \mathbb{Q}_{\geqslant 0} \to \mathbb{R}_{\geqslant 1}$ defined by the limit

$$h(n/m) = \lim_{k\to\infty} \mathbf{E}\,\tau^{km\,kn}, \qquad \text{in particular,} \quad h(0) = 1.$$

The function $h(x)$ is non-decreasing because $\mathbf{E}\,\tau^{mn}$ strictly increases by n and strictly decreases by m.

For the case of $m = 750$ provers, points $(\frac{n}{750}, \mathbf{E}\,\tau^{750\,n})$ of graph on Figure 3 approximate the corresponding points of the imaging graph of function $h(x)$. For small x it looks like a flight of stairs with steps of height 1 starting at point $(0, 1)$.

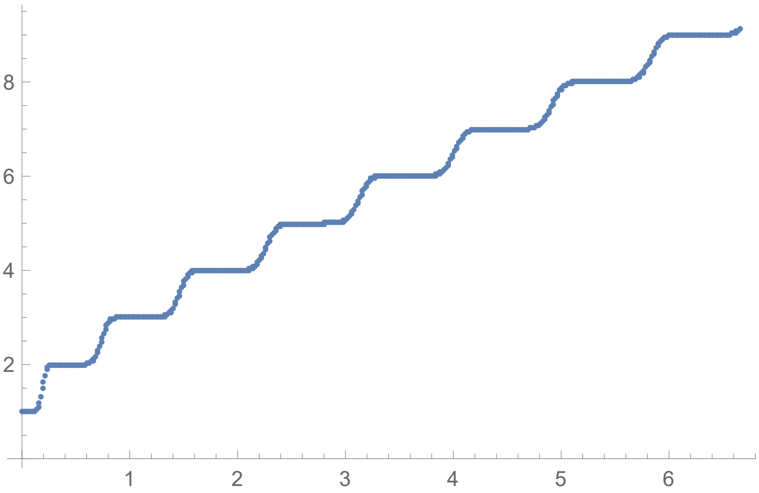

Figure 3. Graph of the function $\frac{n}{750} \mapsto \mathbf{E}\,\tau^{750\,n}$ as an approximation for $h(x)$.

Asymptotic (20) for $\mathbf{Pr}(\tau^{mn} = k)$, $k = 1$ implies that $h(x)$ cannot be (right) continuous at 0: $\lim\limits_{q\searrow 0} h(q) > h(0)$. Our further calculations of asymptotics for $k \geqslant 2$ indicate the occurrence of a break point for each k. One would hope that the function $h(x)$ is left-continuous.

Hypothesis 2. *There exists a left-continuous non-decreasing function $h : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 1}$ defined by the limit*

$$h(x) := \lim_{\substack{m\to\infty \\ n/m \nearrow x}} \mathbf{E}\,\tau^{mn} = \sup_{m/n \leqslant x} \lim_{k\to\infty} \mathbf{E}\,\tau^{km\,kn}. \tag{21}$$

Hypothesis 3. *There exists an increasing sequence of real numbers* $0 = \zeta_1 < \zeta_2 < \cdots$ *with* $\zeta_k < k$*, such that the following two equivalent statements are true:*

1. $h(x)$ *is a sum of Iverson brackets*

$$h(x) = 1 + \sum_{k=1}^{\infty} [\![x > \zeta_k]\!] = \begin{cases} 1, & \text{if } x = 0, \\ k, & \text{if } \zeta_{k-1} < x \leqslant \zeta_k \text{ for } k \geqslant 2. \end{cases} \tag{22}$$

2.

$$\lim_{\substack{m\to\infty \\ n/m \nearrow x}} \mathbf{Pr}(\tau^{mn} = k) = 1 \quad \text{iff} \quad (k = 1 \land x = 0) \lor (k \geqslant 2 \land x \in (\zeta_{k-1}, \zeta_k]) \tag{23}$$

Hypothesis 4. *The function* $h(x)$ *admits the asymptotic for* $x \to +\infty$*:*

$$h(x) = x + \frac{1}{2}\ln(x) + o(\ln(x)), \tag{24}$$

or equivalently:

$$\zeta_k = k - \frac{1}{2}\ln(k) + o(\ln(k)).$$

Moreover,

$$\zeta_1 = 0, \qquad \zeta_2 = 1/3, \qquad \zeta_3 = 1. \tag{25}$$

Remark 4. *For the case of* $m = 50$ *provers, points* $(\frac{n}{50}, \mathbf{E}\,\tau^{50\,n} - \frac{n}{50} - \frac{1}{2}\ln(\frac{n}{50}))$ *of graph on Figure 4 approximate the corresponding points of the imaging graph of function* $h(x) - x - \frac{1}{2}\ln(x)$*.*

The approximation (24) for $h(x)$ *agrees with estimation (16).*

To approve (25) one can calculate:

$$\mathbf{Pr}(\tau^{3n\,n} \neq 2)|_{n=2000} \approx 3.5 \cdot 10^{-21}, \qquad \mathbf{E}\,\tau^{900\,300} \approx 1.99999994;$$
$$\mathbf{Pr}(\tau^{n\,n} \neq 3)|_{n=900} \approx 3.7 \cdot 10^{-10}, \qquad \mathbf{E}\,\tau^{500\,500} \approx 2.999994.$$

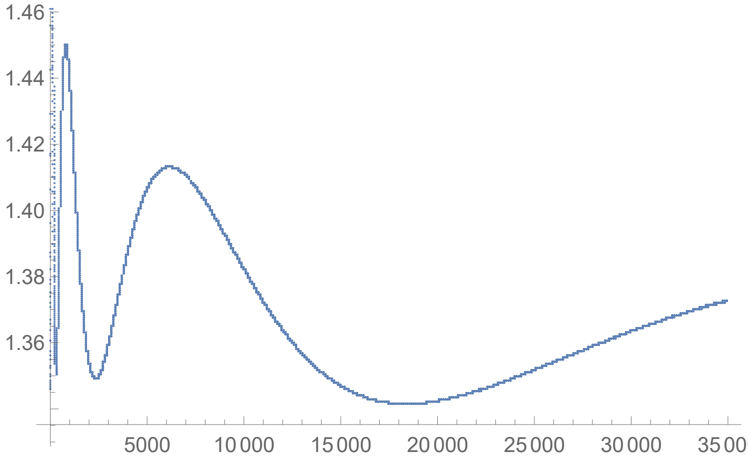

Figure 4. Graph of the function $\frac{n}{50} \mapsto \mathbf{E}\,\tau^{50\,n} - \frac{n}{50} - \frac{1}{2}\ln(\frac{n}{50})$ as an approximation for $h(x) - x - \frac{1}{2}\ln(x)$.

We would like to obtain asymptotics for all probabilities $\mathbf{Pr}(\tau^{mn} = k)$ similar to the case $k = 1$. Note that $\mathbf{Pr}(\tau^{mn} = k) \neq 0$ when $n/m \in (0, k]$, and according to Hypothesis 3 the limit of this probability is either 1 or 0. Our calculations show that in both cases one can expect asymptotics in the form similar to (20).

Hypothesis 5. *For $n, m \to \infty$ and $n/m \nearrow x$*

$$\mathbf{Pr}(\tau^{mn} = k) \asymp \gamma_k(x)^m, \qquad x \in h^{-1}(k),$$
$$1 - \mathbf{Pr}(\tau^{mn} = k) \asymp \lambda_k(x)^m, \qquad x \in (0, k] \setminus h^{-1}(k),$$

for some $\gamma_k, \lambda_k \in (0, 1)$.

Results of calculations are presented as graphs of $\gamma_k(x), \lambda_k(x)$ on Figures 5 and 6 for $k = 2$ and on Figures 7–9 for $k = 3$.

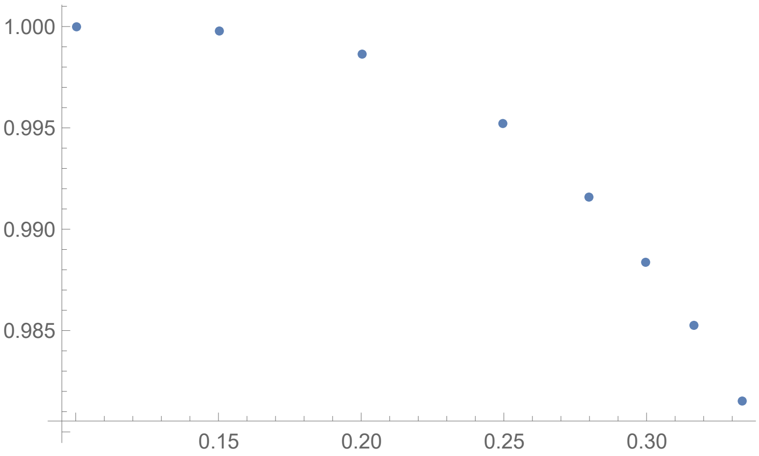

Figure 5. $\lambda_2(n/m)$.

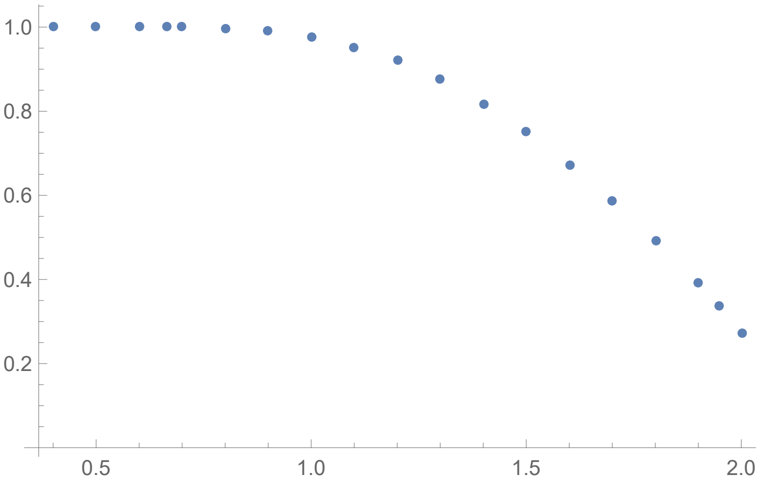

Figure 6. $\gamma_2(n/m)$.

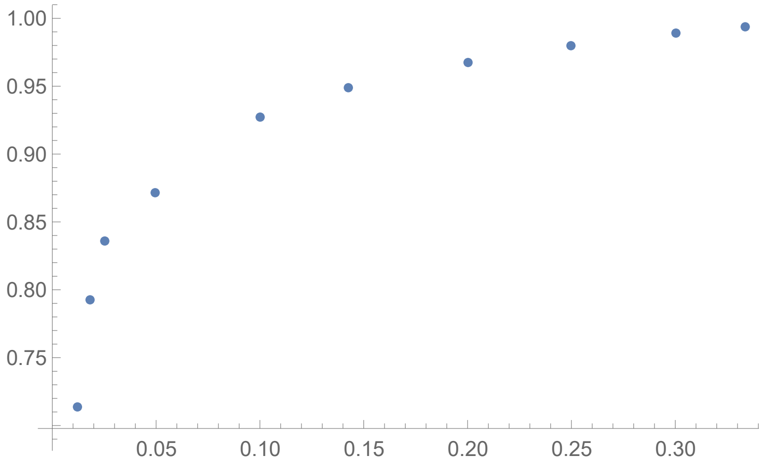

Figure 7. $\gamma_3(n/m)$.

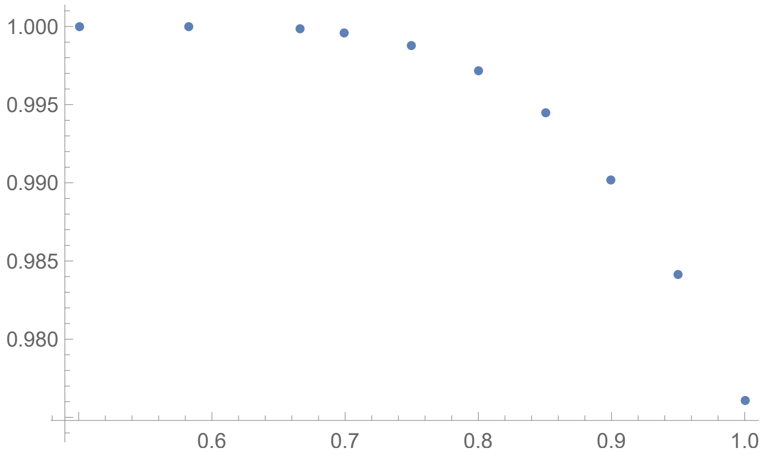

Figure 8. $\lambda_3(n/m)$.

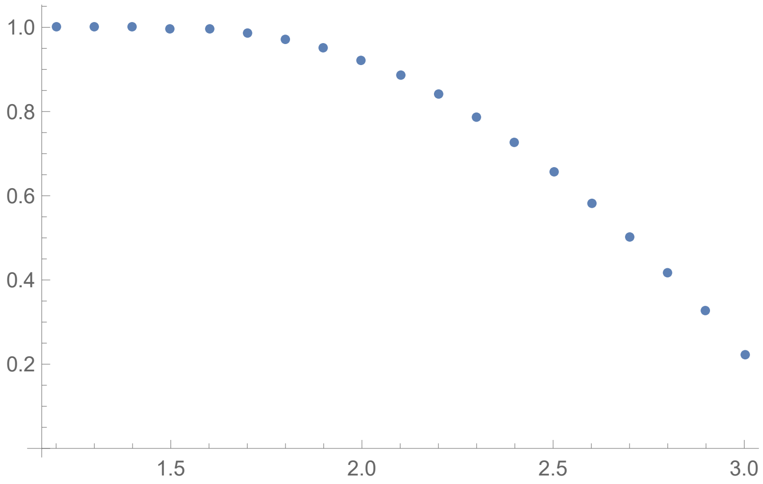

Figure 9. $\gamma_3(n/m)$.

Hypothesis 6. *For $k \geqslant 2$*

$$\lambda_k(x) = \gamma_{k-1}(x) > \gamma_{k'}(x), \quad \textit{for} \quad k' \neq \{k-1, k\}, \quad x \in (\zeta_{k-1}, \zeta_k). \tag{26}$$

Remark 5. *The inequalities (26) mean that for m large enough and $n/m \to x \in (\zeta_{k-1}, \zeta_k)$ the distribution of τ^{mn} tends to Bernoulli distribution with values $k-1, k$. One can see this in Table 1,* *where for large numbers of provers m and proof-candidates n lists of values and probabilities contain at most two items (i.e., for other values probabilities are very small).*

Moreover, the variance of τ^{mn} *tends to the variance of Bernoulli distribution:*

$$\mathbf{Var}\,\tau^{mn} \to \mathbf{Pr}(\tau^{mn} = k-1)\cdot\mathbf{Pr}(\tau^{mn} = k) \leqslant 1/4.$$

Indeed, our numerical calculations allow to suppose that $\mathbf{Var}\,\tau^{mn} < 1$ *if* $m \geqslant 10$, $n/m < 10^4$.

4. Distributed Generation of Proof Trees

This subsection deals with more complicated and, at the same time, more useful real application models of proof generation. In Latus consensus, zk-SNARK-proofs form perfect binary trees (proof trees), like the hashes of transactions form similar trees in the mainchain. The nodes of the tree form a partially ordered set (poset) whose Hasse diagram is the tree itself. So it is natural to formulate a part of our results in terms of general posets.

4.1. Ordered Sets and Lattices

Basic facts about posets mentioned below can be found in [31,43] (ch.3).

A *poset* is a set equipped with a partial order, i.e., a binary relation which is transitive, reflexive, and antisymmetric.

Let P be a poset. A *chain* in P is a subset with total induced order. An *antichain* in P is a subset where any two distinct elements are incomparable. The *height* $\mathrm{ht}(P)$ of finite poset P is the maximum cardinality of a chain in P. The *width* $\mathrm{wd}(P)$ of finite poset P is the maximum cardinality of a antichain in P.

A subset $I \subseteq P$ in a poset P is called a *down-set* (resp. *up-set*) if for each $x \in I$ and $y \in P$ with $y \leqslant x$ (resp. $y \geqslant x$) we have $y \in I$. Note that down-sets in P are up-sets in the opposite poset P^{op} and vice versa.

Denote $\mathcal{O}_d(P)$ (resp. $\mathcal{O}_u(P)$) the lattice of down-sets (resp. up-sets). A subset $I \subseteq P$ is a down-set if its complement $P \smallsetminus I$ is an up-set. The set of up-sets in P form a distributive lattice ordered by inclusion. The map $\mathcal{O}_d(P) \to \mathcal{O}_u(P)$, $I \mapsto P \smallsetminus I$ is an anti-isomorphism of lattices.

Denote $\mathrm{Min}\, I$ (resp. $\mathrm{Max}\, I$) the set of minimal (resp. maximal) elements in $I \subseteq P$. Note that $\mathrm{Min}\, I$ and $\mathrm{Max}\, I$ are antichains. For an arbitrary subset $X \subseteq P$, we denote $X^{\downarrow}$ (resp. $X^{\uparrow}$) the *down closure* (resp. (*up closure*), i.e., the smallest down-set (resp. greatest up-set) containing X. In the case of a singleton the down-set $\{x\}^{\downarrow}$ is called *principle*.

$$I = (\mathrm{Min}\, I)^{\uparrow} \quad \text{for } I \in \mathcal{O}_u(P), \qquad J = (\mathrm{Max}\, J)^{\downarrow} \quad \text{for } J \in \mathcal{O}_d(P). \tag{27}$$

In this way up-sets (resp. down-sets) are in one-to-one correspondence with antichains.

Note that the above correspondence $P \mapsto \mathcal{O}_u(P), \mathcal{O}_d(P)$ is a part of Birkhoff's representation theorem, which in modern formulation states the antiequivalence of categories of finite posets and finite distributive lattices.

A direct corollary of Birkhoff's theorem states that the symmetry group $\mathrm{Aut}\, P$ of a finite poset P is naturally isomorphic to the symmetry group $\mathrm{Aut}\, \mathcal{O}(P)$ of the corresponding lattice $\mathcal{O}(P) = \mathcal{O}_d(P)$ or $\mathcal{O}_u(P)$.

Corollary 1. *The canonical map* $\alpha : \mathrm{Aut}\, P \to \mathrm{Aut}\, \mathcal{O}(P)$, $Q^{\alpha(g)} = \{p^g \mid p \in Q\}$, $g \in \mathrm{Aut}\, P$, $Q \in \mathcal{O}(P)$ *is a group isomorphism.*

For two posets P and Q there exist new posets

- the product $P \times Q$, where $(p,q) \leqslant (p',q')$ iff $p \leqslant p'$ in P and $q \leqslant q'$ in Q. The product of distributive latices is a distributive lattice;
- the co-product $P \sqcup Q$ which is the disjoint union, orders restricted on P and Q coincide with the initial, the elements from different sets are incomparable;

- linear sum $P+Q$ which is disjoint union where, orders restricted on P and Q coincide with initial and $p<q$ for each $p\in P, q\in Q$. The linear sum of distributive latices is a distributive lattice;

  For two posets P and Q there exist the following natural isomorphisms of lattices:

$$\mathcal{O}_d(P\sqcup Q)\simeq\mathcal{O}_d(P)\times\mathcal{O}_d(Q),\qquad \mathcal{O}_u(P\sqcup Q)\simeq\mathcal{O}_u(P)\times\mathcal{O}_u(Q),\tag{28}$$

$$\mathcal{O}_d(P+Q)\simeq\frac{\mathcal{O}_d(P)+\mathcal{O}_d(Q)}{\top_{\mathcal{O}_d(P)}\sim\bot_{\mathcal{O}_d(Q)}},\qquad \mathcal{O}_u(P+Q)\simeq\frac{\mathcal{O}_u(Q)+\mathcal{O}_u(P)}{\top_{\mathcal{O}_u(Q)}\sim\bot_{\mathcal{O}_u(P)}},\tag{29}$$

where the top element of one sublattice is glued with the bottom element of another.

Definition 2. *Let P be a finite poset. A* compatible total ordering *of P is a monotone bijection to finite ordinal $\sigma : P \xrightarrow{\cong} \{1<2<\cdots<|P|\}$. Denote* $\mathrm{Ord}(P)$ *the set of all compatible total orderings of P.*

For finite posets P and Q there exist natural bijections

$$\begin{aligned}\mathrm{Ord}(P+Q)&\simeq\mathrm{Ord}(P)\times\mathrm{Ord}(Q),\\ \mathrm{Ord}(P\sqcup Q)&\simeq\mathrm{Ord}(P)\times\mathrm{Ord}(Q)\times\mathrm{Ord}(\mathbf{p}\sqcup\mathbf{q}),\qquad p=|P|,\ q=|Q|.\end{aligned}\tag{30}$$

Compatible total orderings $\mathrm{Ord}(\mathbf{p}\sqcup\mathbf{q})$, $p,q\in\mathbb{Z}_{\geqslant 0}$ for a coproduct of two chains are in one-to-one correspondence with shuffle permutations $\sigma\in S_{p,q}\subseteq S_{p+q}$, i.e., such that $\sigma(i)<\sigma(j)$ for $i<j\leqslant p$ or $p<i<j$. The number of such a permutation is given by binomial coefficient $\frac{(p+q)!}{p!q!}$.

Definition 3. *For a poset P and a subset $Q\subseteq P$ with induced order there exists the natural restriction map $\mathrm{Ord}(P)\to\mathrm{Ord}(Q)$, $\sigma\mapsto\sigma|_Q$, where a pair of monotone bijection $\sigma|_Q$ and monotone injection ι is uniquely determined from the following commutative diagram*

$$\begin{tikzcd}
Q \arrow[r, "\sigma|_Q", "\cong"'] \arrow[d, hook] & \{1<2<\cdots<|Q|\} \arrow[d, hook, "\iota"] \\
P \arrow[r, "\sigma", "\cong"'] & \{1<2<\cdots<|P|\}
\end{tikzcd}\tag{31}$$

Proposition 6. *Let P be a finite poset. Then $\mathrm{Ord}(Q)$ for $Q\subset P$ with a natural restriction maps form a presheaf on subsets of P ordered by inclusion.*

Proof. One can directly check that for a chain of subsets $Q''\subseteq Q'\subseteq Q\subseteq P$ and $\sigma\in\mathrm{Ord}(Q)$ we have $\sigma|_{Q'}|_{Q''}=\sigma|_{Q''}$. □

Note that very similar constructions around Birkhoff's duality describe shapes of cells of higher categories in [44].

4.2. Poset Version of Coupon Collector Model

Coupon Collector's Process on Posets was considered in the PhD thesis [45]. Here we describe generalisations of Markov chains from Examples 2–4 to the case of poset N.

Notation 7. *For $a\in\mathbb{Z}^N_{\geqslant 0}$ or $a\in\{0.1\}^N$ the set of elements accessible from a is defined as follows:*

$$\mathrm{acc}(a):=\mathrm{supp}(a)\cup\mathrm{Min}(N\smallsetminus\mathrm{supp}(a)).$$

Example 8 (Hyperoctant with forbidden dimensions). *Consider the asymmetric random walk on the $|N|$-dimensional integer hyperoctant $\mathbb{Z}^N_{\geqslant 0}$ with nonzero transition probabilities*

$$p(a, a+e_i) = \frac{1}{|\operatorname{acc}(a)|}, \qquad a \in \mathbb{Z}^N_{\geqslant 0}, \qquad e_i = (\underbrace{0,\ldots,0}_{i-1}, 1, \underbrace{0,\ldots,0}_{|N|-i}) \quad \textit{for} \quad i \in \operatorname{acc}(a).$$

Example 9 (Hypercube with forbidden dimensions). *Iverson bracket (1) applied to each coordinate $(a_i)_{i\in\mathbf{n}} \mapsto ([\![a_i > 0]\!])_{i\in\mathbf{n}}$ gets a lumping map $\mathbb{Z}^n_{\geqslant 0} \to \{0,1\}^n$ for the previous Markov chain. For the obtained Markov chain on the hypercube $\{0,1\}^N$ nonzero transition probabilities are the following:*

$$p(a, a+e_i) = 1/|\operatorname{acc}(a)|, \qquad a, a+e_i \in \{0,1\}^N, \quad i \in \operatorname{Min}(N \setminus \operatorname{supp}(a))$$
$$p(a,a) = \frac{|\operatorname{supp}(a)|}{|\operatorname{acc}(a)|} = \frac{\sum_i a_i}{|\operatorname{acc}(a)|}.$$

Note that the vertex $a \in \{0,1\}^N$ is accessible from 0 iff $\operatorname{supp}(a)$ is a down-set. So we can reduce a graph of Markov chain (without loops) to the corresponding subgraph of the hypercube, which coincides with the Hasse diagram of the lattice of down-sets.

Example 10 (Factorization by symmetries). *Consider the symmetry group $\operatorname{Aut}\mathcal{O}_d(N) \simeq \operatorname{Aut}N$ of the down-set lattice $\mathcal{O}_d(N)$. By Proposition 2, the canonical projection $\pi : \mathcal{O}_d(N) \to \mathcal{O}_d(N)/\operatorname{Aut}\mathcal{O}_d(N)$ to the orbit set is a lumping map.*

The special cases:

- *If N is a discrete poset (where any two distinct elements are incomparable), then elements of $\mathcal{O}_d(N)$ are arbitrary subsets of N. The symmetry group $\operatorname{Aut}\mathcal{O}_d(N)$ is isomorphic to a full permutation group of N and acts transitive on subsets of fixed cardinality, and orbits are identified with cardinalities $0, 1, \ldots, |N|$. So this is the Coupon collector's model from Example 4.*
- *Consider the cases when $N = \mathbb{N}$ are natural numbers with the usual linear order. The lattice $\mathcal{O}_d(\mathbb{N})$ can be naturally identified with $\mathbb{N}$ via cardinality. The symmetry group $\operatorname{Aut}\mathcal{O}_d(N)$ is trivial, all orbits are singletons. The non-zero transition probabilities are:*

$$p(k,k) = k/(k+1), \qquad p(k,k+1) = 1/(k+1).$$

$$p^m(k,k) = k^m/(k+1)^m, \qquad p^m(k,k+m) = 1/(k+m)_m.$$

$$p^m(k,k+1) = \sum_{i=0}^{m-1} \frac{k^i}{(k+1)^{i+1}} \frac{(k+1)^{m-i-1}}{(k+2)^{m-i-1}} = \frac{(k+1)^{2m} - k^m(k+2)^m}{(k+1)^m(k+2)^{m-1}}$$

4.3. Around Perfect Binary Trees

Definition 4. *A rooted binary tree is called* perfect *if all its interior nodes have two children and all leaves have the same depth or same level.*

A perfect binary tree is completely determined by the number of its leaves. To produce a perfect binary tree with ℓ levels we need to create $2^\ell - 1$ proofs.

A perfect binary tree M_ℓ with $2^\ell - 1$ nodes as a poset consists of words of length $< \ell$ in an alphabet of two letters, say $\{0,1\}$; and $w \geqslant w'$ iff w' begins with w. So the empty word ϵ corresponds to the greatest element, the root. Figure 10 illustrates the case of M_4 .

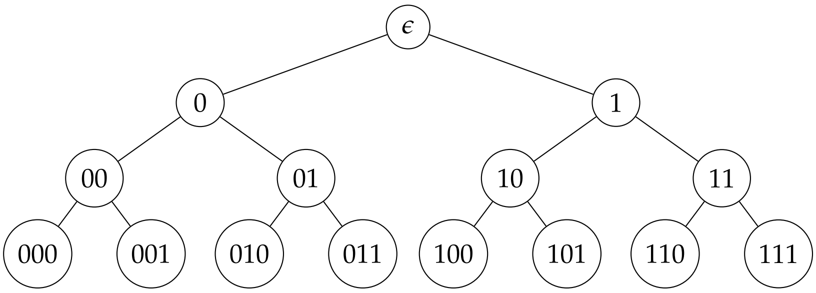

Figure 10. Labeling of nodes for the perfect binary tree M_4.

Each perfect binary tree $M_{\ell+1}$ with $\ell+1$ levels as a poset is the disjoint sum of two copies of one level smaller trees with the greatest element added

$$M_{\ell+1} \simeq (M_\ell \sqcup M_\ell) + \{\epsilon\}. \tag{32}$$

The last identity together with (28) and (29) implies

$$\begin{aligned}\mathcal{O}_u(M_{\ell+1}) &\cong \{\varnothing\} + (\mathcal{O}_u(M_\ell) \times \mathcal{O}_u(M_\ell)),\\ \mathcal{O}_d(M_{\ell+1}) &\cong (\mathcal{O}_d(M_\ell) \times \mathcal{O}_d(M_\ell)) + \{M_\ell\},\end{aligned}$$

i.e., up-set in ether empty or consists of ϵ and any up-sets in left and right subtrees. Note that for two incomparable nodes x and y the corresponding subtrees are disjoint: $\{x\}^\downarrow \cap \{y\}^\downarrow = \varnothing$. So down-sets in a tree are forests, i.e., disjoint unions of subtrees.

Proposition 7. *The following sequences are described recursively.*

1. *The number $u_\ell = |\mathcal{O}_u(M_\ell)|$ of up-sets in the perfect binary tree M_ℓ:*

$$u_{-1} = 0, \qquad u_{\ell+1} = u_\ell^2 + 1$$

This is the sequence A003095 in [32]: $0, 1, 2, 5, 26, 677, 458330, \ldots$.

2. *The number $v_\ell = |\mathcal{O}_u(M_\ell) / \operatorname{Aut} M_\ell|$ of the orbits of such up-sets:*

$$v_0 = 1, \qquad v_{\ell+1} = \binom{v_\ell + 1}{2} + 1.$$

This is the sequence A006894 in [32]: $1, 2, 4, 11, 67, 2279, \ldots$.

Proposition 8. *Each compatible total ordering on $M_{\ell+1}$ given by (32), according to (30) can be obtained as a shuffle of two orderings on M_ℓ. So the number of compatible total orderings of a perfect binary tree satisfies the recurrent relations*

$$|\operatorname{Ord}(M_{\ell+1})| = |\operatorname{Ord}(M_\ell)|^2 \binom{2^\ell - 2}{2^{\ell-1} - 1}$$

and, hence, admits the explicit formula

$$|\operatorname{Ord}(M_{\ell+1})| = (2^\ell - 1)! / \prod_{k=1}^{\ell} (2^k - 1)^{2^{\ell-k}},$$

which can be interpreted as the number of all permutations on nodes of the tree multiplied the probability that the random permutation of nodes is compatible order on tree. This is the sequence A056972 in [32]: $1, 2, 80, 21964800, 74836825861835980800000, \ldots$.

Proposition 9. *The symmetry group of a perfect binary tree can be described recursively as a wreath product i.e., a semidirect product:*

$$\operatorname{Aut}(M_{\ell+1}) \simeq S_2 \ltimes (\operatorname{Aut}(M_\ell) \times \operatorname{Aut}(M_\ell)),$$

where the symmetric group $S_2 = \{e, \tau\}$ acts from the right by permutation on factors $\operatorname{Aut}(M_\ell)$. So

$$M_\ell \simeq S_2 \ltimes \Big((S_2 \ltimes ((S_2 \ltimes \cdots) \times (S_2 \ltimes \cdots))) \times (S_2 \ltimes ((S_2 \ltimes \cdots) \times (S_2 \ltimes \cdots))) \Big), \quad (33)$$

where copies of S_2 are indexed by internal nodes of M_ℓ, i.e., by words $w \in \{0,1\}^*$ of length $< \ell - 1$. Denote τ_w the transposition from the corresponding copy of S_2, the 'symmetry in w'. It swaps between left and right subtrees at w (i.e. $(w0v)^{\tau_w} = w1v$ and $(w1v)^{\tau_w} = w0v$ for $v \in \{0,1\}^*$) and leaves the rest immobile.

The symmetry group $\operatorname{Aut} M_\ell$ admits a presentation with all of the above symmetries τ_w as generators and relations are:

- $\tau_w^2 = e$;
- $\tau_w \tau_{w'} = \tau_{w'} \tau_w$ *whenever w and w' are incomparable in M_ℓ (in this case τ_w and $\tau_{w'}$ lives in two different factors of a direct product in (33));*
- $\tau_{wv} \tau_w = \tau_w \tau_{(wv)^{\tau_w}}$ *(this is the multiplication rule for semidirect product in (33)).*

The presentation (33) of elements of $\operatorname{Aut} M_\ell$ means that in each position corresponding to the internal node labeled by a word w one can put either transposition τ or the neutral element e. So $\operatorname{Aut} M_\ell$ has $2^{2^{\ell-1}-1}$ elements τ_W which are in one-to-one correspondence with subsets W on internal nodes (where transpositions τ are located). For any compatible total ordering $\sigma \in \operatorname{Ord}(W)$,

$$\tau_W := \tau_{\sigma^{-1}(|W|)} \tau_{\sigma^{-1}(|W|-1)} \cdots \tau_{\sigma^{-1}(1)}.$$

4.4. Distributed Generation of Posets

First we consider models from Examples 11–13 which are generalizations of models from Examples 5–7. We switch from sets to posets.

Notation 8. *Given finite poset N, denote $\boldsymbol{\mathcal{M}}(N) = \prod_{\varnothing \neq N' \in \mathcal{O}_u(N)} \mathcal{M}(\operatorname{Min} N')$ the Cartesian product of sets of probabilities distributions on all nonempty anti-chains $\operatorname{Min} N'$.*

Example 11. *Let N be a poset and $\boldsymbol{\mu} = (\mathbf{Pr}_{\operatorname{Min}(N')})_{\varnothing \neq N' \in \mathcal{O}_u(N)} \in \boldsymbol{\mathcal{M}}(N)$ are fixed probability distributions. We consider a Markov chain, where states are up-sets in N. Non-zero elements of transition matrix are*

$$p(N', N'') = \sum_{g \in \operatorname{Sur}(\mathbf{m}, N' \setminus N'')} \prod_{i=1}^{m} \mathbf{Pr}_{\operatorname{Min}(N')}(g(i)), \qquad N' \setminus \operatorname{Min} N' \subseteq N'' \subseteq N', \quad (34)$$

and existence of surjection $\mathbf{m} \twoheadrightarrow N' \setminus N''$ implies $|N' \setminus N''| \leqslant m$.

In the case of uniform distributions non-zero elements of transition matrix are

$$p(N', N'') = |N' \setminus N''|! \cdot \genfrac{\{}{\}}{0pt}{}{m}{|N' \setminus N''|} \cdot |\operatorname{Min} N'|^{-m}.$$

If N is a discrete poset then $\operatorname{Min} N' = N'$ are arbitrary subsets and we obtain a Markov chain from Example 5.

For this Markov chain the empty set $\varnothing$ is the absorbing state and all trajectories are strictly decreasing by inclusion. The subject of our interest is the absorption time $\tau^{m\,N'} = \tau_{\boldsymbol{\mu}}^{m\,N'}$, a random variable which is equal to the number of steps it takes m provers to create all the proofs in up-set N'. Note that $\tau^{m\,N} = k$ iff $p^{k-1}_{N\varnothing} = 0$ and $p^{k}_{N\varnothing} = 1$ The random variable $\tau^{m\,N}$ takes values in the *interval* $[\mathrm{ht}(N), |N|]$, *i.e.,* $p^n_{N\varnothing} = 0$ *for* $n < \mathrm{ht}(N)$ *and* $p^n_{N\varnothing} = 1$ *for* $n \geqslant |N|$. *S,o one can express the expectation of the absorption time via elements of powers of the transition matrix:*

$$\mathbf{E}\,\tau^{m\,N} = \sum_{k=\ell}^{|N|} k(p^k_{N\varnothing} - p^{k-1}_{N\varnothing}) = |N| - 1 - \sum_{k=\ell}^{|N|-1} p^k_{N\varnothing}. \tag{35}$$

From the other hand we have a recurrent formula involving matrix elements of the top raw of p *as coefficients:*

$$\mathbf{E}\,\tau^{m\,N} = 1 + \sum_{\varnothing \neq M \subseteq \mathrm{Min}\,N} p_{N\,N\smallsetminus M}\,\mathbf{E}\,\tau^{m\,N\smallsetminus M}. \tag{36}$$

Now we can extend Example 6 and Proposition 3 about stochastic equivalence of two models to the case of posets. To do this, we need to go from a uniform distribution of probabilities to an arbitrary one.

Example 12 (Non-Markovian model)**.** *Let a probability distribution* $\mathbf{Pr}_{\mathrm{Ord}(N)}$ *on the set of compatible total orderings* $\mathrm{Ord}(N)$ *be given. Then, for each up-set* $N' \in \mathcal{O}_u(N)$ *the probability distributions on* $\mathrm{Ord}(N')$ *and on* $\mathrm{Min}\,N'$

$$\mathbf{Pr}_{\mathrm{Ord}(N')}(\sigma') := \sum_{\substack{\sigma \in \mathrm{Ord}(N) \\ \sigma|_{N'} = \sigma'}} \mathbf{Pr}_{\mathrm{Ord}(N)}(\sigma), \qquad \mathbf{Pr}_{\mathrm{Min}\,N'}(a) := \sum_{\substack{\sigma' \in \mathrm{Ord}(N') \\ \sigma'(a) = 1}} \mathbf{Pr}_{\mathrm{Ord}(N')}(\sigma'), \tag{37}$$

are unique, turning the maps $N \xrightarrow{\sigma \mapsto \sigma|_{N'}} N' \xrightarrow{\sigma' \mapsto (\sigma')^{-1}(1)} \mathrm{Min}\,N'$ *into morphisms of probability spaces. (Here the restriction* $\sigma|_{N'}$ *is defined by* (31)*.) Then we can consider the Markov chain from the previous Example 11 with probability distributions on anti-chains* $\mathrm{Min}\,N'$ *obtained by composing of* (37)

$$\mathbf{Pr}_{\mathrm{Min}\,N'}(a) := \sum_{\substack{\sigma \in \mathrm{Ord}(N) \\ \sigma|_{N'}(a) = 1}} \mathbf{Pr}_{\mathrm{Ord}(N)}(\sigma). \tag{38}$$

An element of Cartesian degree $(\mathrm{Ord}\,N)^m$ *corresponds to the choice of a ranging* $\sigma_i \in \mathrm{Ord}(N)$ *by each prover* $1 \leqslant i \leqslant m$*. It completely determines a trajectory for this Markov chain, i.e., strongly decreasing sequence of up-sets of not yet proven candidates*

$$N = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = \varnothing, \qquad N_{j+1} = N_j \smallsetminus \left\{ \left(\sigma_i|_{N_j}\right)^{-1}(1) \,\middle|\, 1 \leqslant i \leqslant m \right\},$$

together with selection in each moment $0 \leqslant j < k$ *by each prover* $1 \leqslant i \leqslant m$ *the first possible proof-candidate* $\left(\sigma_i|_{N_j}\right)^{-1}(1) \in \mathrm{Min}\,N_j$ *according to its own ranging. Directly from the definition one can see that conditional probabilities of such selections are given by* (38)*.*

Consider the case when N *is a discrete poset and, hence,* $\mathrm{Min}\,N' = N'$ *are arbitrary subsets. If we additionally suppose that the initial distribution* $\mathbf{Pr}_{\mathrm{Ord}\,N}$ *is uniform, then for each* N' *the matched distributions* $\mathbf{Pr}_{\mathrm{Ord}\,N'}$ *and* $\mathbf{Pr}_{\mathrm{Min}\,N'}$ *are also uniform because the numbers of summands in* (37) *are independent on* $\sigma' \in N'$ *and* $a \in \mathrm{Min}\,N'$ *respectively. They are naturally indexed in the first case by* $|N|!/|N'|!$ *permutations of* N *preserving order between elements of* N' *and in the second case by* $(|N'| - 1)!$ *permutations preserving* a*. So, this covers the case of Example 6 and Proposition 3.*

It should be emphasized that the construction in this example is less universal than the general case of Example 11. For instance in the case of $N = \{a\} \sqcup \{b < c\}$ *from* (38) *we obtain* $\mathbf{Pr}_{\{a,b\}}(a) = \mathbf{Pr}_N(a < b < c)$, $\mathbf{Pr}_{\{a,c\}}(a) = \mathbf{Pr}_N(a < b < c, b < a < c)$ *and the restriction* $\mathbf{Pr}_{\{a,b\}}(a) \leqslant \mathbf{Pr}_{\{a,c\}}(a)$*. In particular, the probability distributions* $\boldsymbol{\mu} = (\mathbf{Pr}_{\mathrm{Min}\,N'})_{\varnothing \neq N' \in \mathcal{O}_u(N)}$ *minimizing* $\mathbf{E}\,\tau^{m\,N}_{\boldsymbol{\mu}}$ *do not come from this example.*

Example 13 (Factorization by the symmetry group)**.** *Consider the data from Example 11 in the case when all probability measures* $(\mathbf{Pr}_{\mathrm{Min}\,N'})_{\varnothing\neq N'\in\mathcal{O}_u(N)}$ *are* Aut N*-invariant, i.e.*

$$\mathbf{Pr}_{\mathrm{Min}\,N'}\circ\sigma=\mathbf{Pr}_{\mathrm{Min}\,N'},\qquad \sigma\in\mathrm{Aut}\,N.$$

By Proposition 2, the canonical projection $\pi:\mathcal{O}_u(N)\to\mathcal{O}_d(N)/\,\mathrm{Aut}\,\mathcal{O}_u(N)$ *to the orbit set is a lumping map.*

So we obtain a Markov chain with the set of states $\mathcal{O}_u(N)/\,\mathrm{Aut}\,N$ *the transition probabilities between orbits are given by sums* (6) *applied to* (34)

$$p([N'],[N''])=\sum_{N'''\in[N'']}p(N',N''')=\sum_{\substack{N'''\in[N'']\\ N'\smallsetminus\mathrm{Min}\,N'\subseteq N'''\subseteq N'}}\ \sum_{g:\mathbf{m}\twoheadrightarrow N'\smallsetminus N'''}\ \prod_{i=1}^{m}\mathbf{Pr}_{\mathrm{Min}(N')}(g(i))\qquad(39)$$

- In the case of discrete poset N, elements of $\mathcal{O}_u(N)$ are all subsets of N, the symmetry group Aut N consists of all permutations and orbits $\mathcal{O}_u(N)/\,\mathrm{Aut}\,N$ are just integers $0,1,\ldots,|N|$ identified with cardinalities of subsets. So we obtain a Markov chain from Example 7.
- In the case $N=M_\ell$ of perfect binary tree with ℓ levels the states of the Markov chain from Example 11 (resp. from Example 13) are up-sets in M_ℓ (res. orbits of such up-sets under action of Aut M_ℓ). According to Proposition 7 the numbers of such up-sets N' or orbits of up-sets grow rapidly depending on ℓ. Moreover, if we decide to consider not only uniform probability distributions on anti-chains Min N' we obtain a lot of additional parameters.
  For the case $\ell=3$, the oriented graph of the Markov chain from Example 13 for M_3 is presented on Figure 11. It has 11 states, has no cycles including loops (except of the loop for the final state $\varnothing$); the transition matrix is triangular; Aut M_3-invariant probability measures on different Min N' depends totally on 3 parameters.

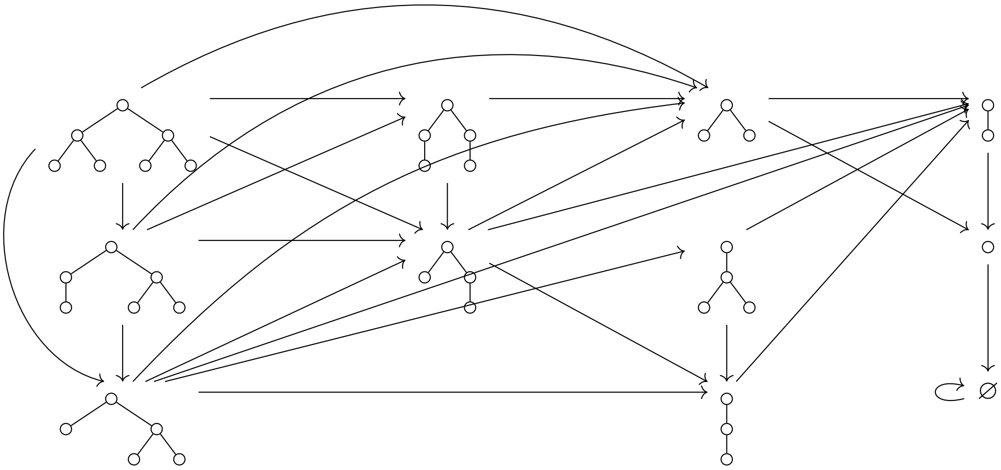

Figure 11. Markov chain for M_3 generation (factorized by Aut M_3).

4.5. Some Asymptotics for $\tau^{m\,N}$

For fixed finite poset $N\neq\varnothing$ and a fixed number of provers $m\geqslant 2$ the subject of our interest is to find minimum of $\mathbf{E}\,\tau_{\mu}^{m\,N}$ over all possible (Aut N-invariant) measures $\mu=(\mathbf{Pr}_{\mathrm{Min}\,N'})_{\varnothing\neq N'\subseteq N}$, and their limits when $m\to\infty$. We describe this asymptotic behavior in terms of heights of up-sets.

Next we show that expectation $\mathbf{E}\,\tau^{m\,N}$ tends to its minimal possible value (equal the height $\operatorname{ht}(N)$) when the number of provers m rise. Note that each finite poset N can represented as disjoint union

$$N = \bigcup_{k=0}^{\operatorname{ht}(N)-1} \operatorname{Min} N_{/k}, \qquad N_{/0} := N, \quad N_{/(k+1)} = N_{/k} \smallsetminus \operatorname{Min} N_{/k}. \tag{40}$$

Proposition 10. *Let* $\mathbf{Pr}_{\operatorname{Min} N_{/k}}(a) > 0$ *for all integers* $k \in [0, \operatorname{ht}(N) - 1]$ *and for all* $a \in \operatorname{Min} N_k$*. Then*

$$\lim_{m\to\infty} \mathbf{E}\,\tau^{m\,N} = \operatorname{ht}(N).$$

Proof. For each $\varepsilon > 0$ there exists $m_0 \in \mathbb{N}$ such that for all $m \geqslant m_0$ for all k from $[0..\operatorname{ht} N)$ all elements of $\operatorname{Min} N_{/k}$ will be proved on $(k+1)$th step with probability $> 1 - \varepsilon$. □

Some types of posets N we will obtain asymptotic in the form

$$\min_{\mu\in\boldsymbol{\mathcal{M}}(N)} \mathbf{E}\,\tau_{\mu}^{m\,N} \underset{m\to\infty}{\sim} \operatorname{ht}(N) + \alpha_N \gamma_N^m + o(\gamma_N^m), \qquad 0 \leqslant \gamma_N < 1. \tag{41}$$

The case is suitable when N admits a rich symmetry enough.

Proposition 11. *Let N be a finite poset such that in notations of* (40) *for each* $N_{/k}$*,* $k = 0, 1, \ldots, \operatorname{ht} N - 1$ *its symmetry group* $\operatorname{Aut} N_{/k}$ *acts transitive on* $\operatorname{Min} N_{/k}$*. In this case for large number of provers m accurate to* $o((1 - 1/\operatorname{wd} N)^m)$ *we have*

$$\min_{\mu\in\boldsymbol{\mathcal{M}}(N)} \mathbf{E}\,\tau_{\mu}^{m\,N} \underset{m\to\infty}{\sim} \operatorname{ht} N + \kappa_N \cdot \operatorname{wd} N \cdot (1 - 1/\operatorname{wd} N)^m, \tag{42}$$

where κ_N *is a number of such k that* $\#\operatorname{Min} N_{/k} = \operatorname{wd} N$*.*

Proof. Transitivity of the action of $\operatorname{Aut} N_{/k}$ on $\operatorname{Min} N_{/k}$ implies that uniform probability distribution on $\operatorname{Min} N_{/k}$ is optimal. Denote the right hand side of (42) by $\Phi(N)$ and $n_k = |\operatorname{Min} N_{/k}|$. By induction, we can write $\min_{\mu\in\boldsymbol{\mathcal{M}}(N_{/k})} \mathbf{E}\,\tau_{\mu}^{m\,N_{/k}}$ as a sum

$$1 + \frac{n_k!\left\{{m \atop n_k}\right\}}{n_k^m} \min_{\mu\in\boldsymbol{\mathcal{M}}(N_{/(k+1)})} \mathbf{E}\,\tau_{\mu}^{m\,N_{/(k+1)}} + n_k \frac{(n_k-1)!\left\{{m \atop n_k-1}\right\}}{n_k^m} \min_{\mu\in\boldsymbol{\mathcal{M}}(N^+_{/(k+1)})} \mathbf{E}\,\tau_{\mu}^{m\,N^+_{/(k+1)}} + \cdots,$$

where $N^+_{/(k+1)}$ is $N_{/(k+1)}$ with one additional element from $\operatorname{Min} N_{/k}$ (in all cases we obtain isomorphic posets); and "$\cdots$" means summands which are small with respect to $(1 - 1/\operatorname{wd} N)^m$. Next we remove small terms from inclusion-exclusion formula (5) for Striling numbers:

$$\begin{aligned}\min_{\mu\in\boldsymbol{\mathcal{M}}(N_{/k})} \mathbf{E}\,\tau_{\mu}^{m\,N_{/k}} &\underset{m\to\infty}{\sim} 1 + (1 - n_k(1 - 1/n_k)^m)\Phi(N_{/(k+1)}) + n_k(1 - 1/n_k)^m \cdot \operatorname{ht} N^+_{/k} \\ &\underset{m\to\infty}{\sim} \Phi(N_{/(k+1)}) + \Phi(\operatorname{Min} N_{/k}).\end{aligned}$$

Then, in all three possible cases $\operatorname{wd} N_{/(k+1)} = \operatorname{wd} N_{/k}, n_k = \operatorname{wd} N_{/k}$ or $\operatorname{wd} N_{/(k+1)} < \operatorname{wd} N_{/k}, n_k = \operatorname{wd} N_{/k}$ or $\operatorname{wd} N_{/(k+1)} = \operatorname{wd} N_{/k}, n_k < \operatorname{wd} N_{/k}$ we have $\Phi(N_{/(k+1)}) + \Phi(\operatorname{Min} N_{/k}) \sim \Phi(N_{/k})$ accurate to $o((1 - 1/\operatorname{wd} N)^m)$. □

The perfect binary tree M_ℓ satisfies assumptions of Proposition 11; we have $\operatorname{ht} M_\ell = \ell$, $\operatorname{wd} M_\ell = 2^{\ell-1}$ and $\kappa_{M_\ell} = 1$.

Corollary 2. *For perfect binary tree M_ℓ and for a large number of provers m:*

$$\min_{\mu \in \mathcal{M}(M_\ell)} \mathbf{E}\, \tau_{\mu}^{m\, M_\ell} \underset{m\to\infty}{\sim} \ell + 2^{\ell-1} \left(\frac{2^{\ell-1}-1}{2^{\ell-1}} \right)^m, \tag{43}$$

and the corresponding probability

$$\mathbf{Pr}(\tau^{m\, M_\ell} = \ell) \underset{m\to\infty}{\sim} 1 - 2^{\ell-1} \left(\frac{2^{\ell-1}-1}{2^{\ell-1}} \right)^m. \tag{44}$$

Next we consider the case of coproducts of chains

$$N = \coprod_{1\leqslant i\leqslant k} \mathbf{n}_i = \{(i,j) | 1 \leqslant i \leqslant k \wedge 1 \leqslant j \leqslant n_i\}, \qquad n_i > 0. \tag{45}$$

A kth copower $N = \coprod_{1\leqslant i\leqslant k} \mathbf{n}$ of a chain $\mathbf{n}$ satisfies assumptions of Proposition 11. We have $\operatorname{ht} N = \kappa_N = n$ and $\operatorname{wd} N = k$.

Corollary 3. *For positive integer k and n*

$$\min_{\mu \in \mathcal{M}(\coprod_{1\leqslant i\leqslant k} \mathbf{n})} \mathbf{E}\, \tau_{\mu}^{m\, \coprod_{1\leqslant i\leqslant k} \mathbf{n}} \underset{m\to\infty}{\sim} n + kn(1-1/k)^m + o((1-1/k)^m). \tag{46}$$

If assumptions of Proposition 11 about symmetry of poset N are violated, asymptotic formulas (41) become more complicated. We can obtain explicit formula for the simplest such case.

Proposition 12. *For positive integers n_1, n_2 with accuracy $o((|n_2 - n_1| + 2)^{-m})$*

$$\min_{\mu \in \mathcal{M}(\mathbf{n}_1 \sqcup \mathbf{n}_2)} \mathbf{E}\, \tau_{\mu}^{m\, \mathbf{n}_1 \sqcup \mathbf{n}_2} \underset{m\to\infty}{\sim} n_1 \vee n_2 + \left(\binom{n_1 \vee n_2}{n_1 \wedge n_2} \frac{n_1+n_2+1}{|n_1-n_2|+1} - 1 \right) \left(\frac{1}{|n_2-n_1|+2} \right)^m,$$

where $n_1 \vee n_2 = \max\{n_1, n_2\}$ *and* $n_1 \wedge n_2 = \min\{n_1, n_2\}$

Proof. Firstly we show that if $n_2 > n_1 > 0$, then numbers $\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1$ satisfy Pascal recursive rule and boundary conditions

$$\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1 = (\alpha_{(\mathbf{n}_1 - \mathbf{1}) \sqcup (\mathbf{n}_2 - \mathbf{1})} + 1) + (\alpha_{\mathbf{n}_1 \sqcup (\mathbf{n}_2 - 1)} + 1), \tag{47}$$

$$\alpha_{\mathbf{0} \sqcup \mathbf{n}} = \alpha_{\mathbf{n}} = 0, \qquad \alpha_{\mathbf{n} \sqcup \mathbf{n}} = 2n. \tag{48}$$

(The second boundary condition comes from (46).)

Suppose that $n_2 > n_1$ and probability distribution $\mathbf{Pr}_{\operatorname{Min} \mathbf{n}_1 \sqcup \mathbf{n}_2}$ on $\operatorname{Min} \mathbf{n}_1 \sqcup \mathbf{n}_2 = \{(1,1),(1,2)\}$ is given by $\mathbf{Pr}_{\operatorname{Min} \mathbf{n}_1 \sqcup \mathbf{n}_2}(1,j) = p_j$, $j = 1,2$ and $p_1 + p_2 = 1$. Then by induction $\mathbf{E}\, \tau^{m\, \mathbf{n}_1 \sqcup \mathbf{n}_2}$ can be written as

$$1 + p_1^m \min \mathbf{E}\, \tau^{m\, \mathbf{n}_1 - \mathbf{1} \sqcup \mathbf{n}_2} + p_2^m \min \mathbf{E}\, \tau^{m\, \mathbf{n}_1 \sqcup \mathbf{n}_2 - \mathbf{1}} + (1 - p_1^m - p_2^m) \min \mathbf{E}\, \tau^{m\, \mathbf{n}_1 - \mathbf{1} \sqcup \mathbf{n}_2 - \mathbf{1}}.$$

Removing a priori small terms, one rewrite this expression as

$$\sim n_2 + \alpha_{n_1 - 1\, n_2 - 1} \left(\frac{1}{n_2 - n_1 + 2} \right)^m + p_1^m + \alpha_{n_1\, n_2 - 1} \left(\frac{1}{n_2 - n_1 + 1} \right)^m p_2^m.$$

The method of Lagrange multipliers for $m \to \infty$ gets $p_1 = 1/(n_2 - n_1 + 2)$ and

$$\min \mathbf{E}\, \tau^{m\, \mathbf{n}_1 \sqcup \mathbf{n}_2} \sim n_2 + (1 + \alpha_{n_1 - 1\, n_2 - 1} + \alpha_{n_1\, n_2 - 1}) \left(\frac{1}{n_2 - n_1 + 2} \right)^m.$$

And so we obtain Pascal rule (47).

Next we find the generating function for the double sequence $\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1$:

$$f(x,y) = \sum_{k=0}^{\infty} \sum_{n=k}^{\infty} (\alpha_{\mathbf{k} \sqcup \mathbf{n}} + 1) x^k y^{n-k} = \frac{1+x}{(1-x)(1-x-y)}.$$

This explicit expression can be obtained from simplification of $(1-x-y)f(x,y)$ using recurrent relation (47) and boundary conditions (48).

Finally we extract coefficients $\alpha_{\mathbf{k} \sqcup \mathbf{n}} + 1 = [x^k y^{n-k}] f(x,y)$ from

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} (\alpha_{\mathbf{k} \sqcup \mathbf{n}} + 1) x^k y^{n-k} = (1+x)(1+x+x^2+\cdots)\Big(1+(x+y)+(x+y)^2+\cdots\Big). \qquad \square$$

The next step would be:

Problem 1. *Find asymptotic formula* (41) *for arbitrary finite coproduct* (45) *of finite chains.*

For each fixed finite poset N one can consider its nth copowers $\coprod_{i \in \mathbf{n}} N$ and then study the dependence of absorption time $\tau^{m \coprod_{i \in \mathbf{n}} N}$ on the number of copies n and number of provers m. If N is a singleton we obtain a random variable τ^{mn} from Example 7.

Hypothesis 7. *For finite poset N, there exists a generalization of function $h(x)$ from Hypothesis 2, given by the limit*

$$h_N(x) := \lim_{\substack{m,n \to \infty \\ n/m \nearrow x}} \min \mathbf{E}\, \tau^{m \coprod_{i \in \mathbf{n}} N}.$$

This function has a number of properties that generalize the properties of $h(x)$.

4.6. Practical Realization of Proof Trees Generation

For the stable and efficient functioning of the sidechain, it is necessary that the following conditions are met:

1. All transactions that the blockforger plans to include in the issued block must be processed within the time slot, i.e., the time allotted for the creation of this block, and the correspondent proof tree must be completely built;
2. The number of these transactions should be the maximum possible, for which the probability of constructing the corresponding proof tree is close to 1.

The first condition is necessary in order to minimize or reduce to zero the number of proofs that will be created but not used, i.e., so that the work of the provers is not done in vain. The second condition is necessary to maximize the sidechain throughput.

Therefore, it is necessary to define, given the network parameters (such as the length of the time slot and the number of active provers), such a maximum number of leaves so that the corresponding proof tree is completely built in a time slot with a probability of at least $1-\varepsilon$ for sufficiently small $\varepsilon > 0$.

We assume that the time slot length is fixed throughout the life of the sidechain. We also assume that the time required to form one proof is the same throughout the lifetime of the sidechain for all miners. This time will be called a tick. The whole part of dividing the time slot duration by the tick duration is equal to the number of proofs that each active miner can build in one time slot. Since the lengths of the time slot and tick are fixed, the number of such proofs during the time slot is also fixed. However, the number of provers may vary.

The task is to determine the maximum number of transactions in a block for a given numbers k of ticks in a time slot, m of provers, for which the corresponding proof tree will be built with a probability of at least $1-\varepsilon$.

To solve this problem, we will use the results of Section 3, and also make the following assumptions.

We will assume that provers build all levels of the proof tree sequentially, from leaves to root. First probabilities are calculated so that the corresponding level will be completely built in $1, 2, 3$, etc., ticks (for a given number of proofs and provers). Then, using these probabilities we find the number of levels that will be built with probability $\geqslant 1 - \varepsilon$ in $\leqslant k$ tics:

$$\mathbf{Pr}(\tau^{m\,M_\ell} \leqslant k) \approx \sum_{\substack{k_1+\cdots+k_\ell \leqslant k \\ k_1,\ldots,k_\ell \geqslant 1}} \prod_{1 \leqslant r \leqslant \ell} \mathbf{Pr}(\tau^{m\,2^{r-1}} = k_r).$$

If $\mathbf{Pr}(\tau^{m\,2^{\ell'-1}} = 1) \approx 1$, we can reduce the previous formula as

$$\mathbf{Pr}(\tau^{m\,M_\ell} \leqslant k) \approx \sum_{\substack{k_{\ell'+1}+\cdots+k_\ell \leqslant k-\ell' \\ k_{\ell'+1},\ldots,k_\ell \geqslant 1}} \prod_{\ell' < r \leqslant \ell} \mathbf{Pr}(\tau^{m\,2^{r-1}} = k_r).$$

Table 1, which indicates the probabilities of constructing a given number of proofs for a given number of provers for a given number of ticks, is auxiliary for solving our problem.

Each row in Table 1 corresponds to a certain fixed number of provers. The columns correspond to the levels of the proof tree, starting from the second from the root. For example, in a cell with coordinates 512 provers, 32 proofs there is a list of two pairs of numbers: $\substack{1;0:999997 \\ 2;0.000003}$. This means that 512 provers will build 32 proofs in exactly 1 tick with a probability of 0.999997 and in exactly 2 ticks with a probability of 0.000003. Therefore, the probability of building 32 proofs in no more than 2 ticks is non-distinguished from 1.

Let us calculate the maximum number of transactions in a block that 512 provers can process with a probability of at least 0.95 in 9 ticks.

The first 5 levels (including the root) will be processed each in 1 tick with a probability almost equal to 1. Therefore, we have at most 4 ticks for building the remaining levels. Note that the eighth level can be built in 1 tick with a very small probability of 0.088899, so this level requires two ticks. The probability of building it in no more than two ticks will be $0.088899 + 0.911101$, which is practically equal to 1. That is, if there are 8 levels in the tree, then 2 ticks remain for the 6th and 7th levels, 1 tick for each level. According to the results in Table 1, the probability of building these two levels in 2 ticks is $0.999997 \cdot 0.980019 = 0.980016$, which is more than 0.95, therefore, a block with 128 transactions will be released with a probability of at least 0.95, which satisfies our requirements.

Similarly, it can be shown that the probability of a block with 256 transactions being released is significantly less than 0.95. Therefore, if there are 512 active provers, it is recommended to issue a block with 128 transactions.

Based on Table 1, Table 2 was built, which shows the recommended number of transactions in a block for a different number of provers. All possible values of the number of provers are divided here into intervals, in accordance with the number of transactions in the block. For example, 2176 provers will build a block with 512 transactions with a probability of 0.95001, and 2175 provers with a probability of 0.949825. Therefore, if the number of provers is at least 2176, then the recommended number of transactions in a block is 512, and if the number of provers is from 998 to 2175, then the recommended number of transactions is 256.

Table 2. Recommended number of transactions in a block $2^{\ell-1}$, corresponding to the probability of block creation $1 - \varepsilon = 0.95$ (for a different numbers of provers)

m	**[1..3]**	**[4..9]**	**[10..32]**	**[33..94]**	**[95..451]**	**[452..2175]**	**⩾2176**
$2^{\ell-1}$	4	8	16	32	64	128	256

Remark 6. *One can solve* (44) *as equation with respect to the number of provers:*

$$m \approx \frac{\ln n - \ln \varepsilon}{-\ln(1 - 1/n)}, \qquad n = 2^{\ell-1}, \quad \varepsilon = 1 - \mathbf{Pr}(\tau^{m\,M_\ell} = \ell).$$

In our case $n = 256$ *and* $\varepsilon = 0.05$ *and we have* $m \approx 2182$. *This coincides with the last boundary* 2176 *in Table* 2 *with accuracy* $(2182 - 2176)/2176 \approx 0.3\%$.

5. Conclusions

This paper is a part of series of works concerning the sidechains with Latus consensus and zk-SNARKs. The previous works were [30], which may be considered as a restricted preimage of this one, and [46], which researches some game theoretical aspects, occurring when provers set prices for their proofs. All articles from the series are devoted to some concrete practical problems, which may be formulated, in general, as conditions of fully decentralized sidechains based on the Latus consensus protocol. We partially solved these problems analyzing existed mathematical models and methods and creating our specific ones, like probability distributions on partially ordered sets, which are the most suitable for existing purposes. The specific characteristics of this work is some numbers of hypothesis, which were formulated based on a large amount of numerical results obtained using infinite-precision calculations. For our opinion, the task to prove all them seems to be rather non-trivial. The numerical results, obtained at the end of the article, allows to chose correct values of some parameters to achieve stability and high throughput in sidechains. The further researches, which continue the series, are planned to be devoted to a more general, more efficient, and more complicated approach, when a series of blocks are built simultaneously, allowing provers to create proofs for several sequential blocks. Note that this approach allows one to increase essentially without losing stability in the sidechain, and it is therefore useful and interesting.

Author Contributions: Conceptualization, R.O.; Data curation, A.G.; Formal analysis, Y.B. and L.K.; Software, H.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thanks Ulrich Haboeck for the fruitful discussion and comments.

Conflicts of Interest: The authors declare that they have no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

zk-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
SC	Sidechain
MC	Mainchain
PoW	Proof of work
PoS	Proof of stake
UTXO	Unspent transaction output
iff	if and only if
poset	partially ordered set
ppm	parts per million

References

1. Rootstock: Smart Contracts on Bitcoin Network. 2018. Available online: https://www.rsk.co/ (accessed on 10 October 2021).
2. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. 2014. Available online: https://blockstream.com/sidechains.pdf (accessed on 10 October 2021).
3. Kiayias, A.; Zindros, D. Proof-of-Work Sidechains. 2018. Available online: https://ia.cr/2018/1048 (accessed on 11 October 2021).

4. Garoffolo, A.; Kaidalov, D.; Oliynykov, R. Zendoo: A zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. *arXiv* **2020**, arXiv:2002.01847.
5. Pass, R.; Shi, E. FruitChains: A Fair Blockchain. Cryptology ePrint Archive, Report 2016/916. 2016. Available online: https://ia.cr/2016/916 (accessed on 11 October 2021).
6. VeriBlock Inc.. Proof-of-Proof and VeriBlock Blockchain Protocol Consensus Algorithm and Economic Incentivization Specifications. 2019. Available online: http://bit.ly/vbk-wp-pop (accessed on 12 October 2021).
7. Gaži, P.; Kiayias, A.; Russell, A. Tight consistency bounds for bitcoin. In Proceedings of the 2020 ACM SIGSAC Conference on Compute and Communications Security, Virtual Event, 9–13 November 2020; pp. 819–838.
8. Karpinski, M.; Kovalchuk, L.; Kochan, R.; Oliynykov, R.; Rodinko, M.; Wieclaw, L. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. *Sensors* **2021**, *121*, 75–81.
9. Kovalchuk, L.; Kaidalov, D.; Nastenko, A.; Rodinko, M.; Oliynykov, R. Probability of double spend attack for network with non-zero synchronization time. In Proceedings of the 21th Central European Conference on Cryptology (CECC 2021), Budapest, Hungary, 23–25 June 2021; pp. 52–54.
10. Kovalchuk, L.; Kaidalov, D.; Nastenko, A.; Rodinko, M.; Shevtsov, O.; Oliynykov, R. Decreasing security threshold against double spend attack in networks with slow synchronization. *Comput. Commun.* **2020**, *154*, 75–81.
11. Garoffolo, A.; Viglione, R. Sidechains: Decoupled Consensus Between Chains. *arXiv* **2018**, arXiv:1812.05441.
12. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *CRYPTO 2017, Part I*; Lecture Notes in Computer Science; Springer: Heidelberg, Germany, 2017; Volume 10401, pp. 357–388.
13. Garay, J.; Kiayias, A.; Leonardos, N. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology-EUROCRYPT 2015, Part II*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9057, pp. 281–310.
14. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. 2013. Available online: https://ia.cr/2013/879 (accessed on 10 October 2021).
15. Bowe, S.; Gabizon, A. Making Groth's zk-SNARK Simulation Extractable in the Random Oracle Model. 2018. Available online: https://ia.cr/2018/187 (accessed on 10 October 2021).
16. Reitwiessner, C. zkSNARKs in a Nutshell. 2016. Available online: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/ (accessed on 17 October 2021).
17. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proofs. *SIAM J. Comput.* **1989**, *18*, 186–208.
18. Bitansky, N.; Canetti, R.; Chiesa, A.; Tromer, E. From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again. Cryptology ePrint Archive, Report 2011/443. 2011. Available online: https://ia.cr/2011/443 (accessed on 10 October 2021).
19. Groth, J. Short pairing-based non-interactive zero-knowledge arguments. In *ASIACRYPT 2010*; Abe, M., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6477, pp. 321–340.
20. Gennaro, R.; Gentry, C.; Parno, B.; Raykova, M. Quadratic Span Programs and Succinct NIZKs without PCPs. Cryptology ePrint Archive, Report 2012/215. 2012. Available online: https://ia.cr/2012/215 (accessed on 12 October 2021).
21. Parno, B.; Gentry, C.; Howell, J.; Raykova, M. Pinocchio: Nearly Practical Verifiable Computation. Cryptology ePrint Archive, Report 2013/279. 2013. Available online: https://ia.cr/2013/279 (accessed on 12 October 2021).
22. Groth, J. On the Size of Pairing-Based Non-interactive Arguments. In *Advances in Cryptology–EUROCRYPT 2016*; Fischlin, M., Coron, J.S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9666, pp. 305–326.
23. Hopwood, D.; Bowe, S.; Hornby, T.; Wilcox, N. Zcash Protocol Specification: Version 2021.2.16 [NU5 Proposal]. 2021. Available online: https://zips.z.cash/protocol/protocol.pdf (accessed on 12 October 2021).
24. Mina. Started by $O(1)$ Labs. 2021. Available online: https://minaprotocol.com (accessed on 17 October 2021).
25. Grassi, L.; Khovratovich, D.; Rechberger, C.; Roy, A.; Schofnegger, M. Poseidon: New Hash Functions for Zero Knowledge Proof Systems. Cryptology ePrint Archive, Report 2019/458. 2019. Available online: https://ia.cr/2019/458 (accessed on 12 October 2021).
26. Kovalchuk, L.; Oliynykov, R.; Rodinko, M. Security of the Poseidon Hash Function Against Non-Binary Differential and Linear Attacks. *Cybern Syst. Anal.* **2021**, *57*, 268–278.
27. Haböck, U.; Garoffolo, A.; Benedetto, D.D. Darlin: Recursive Proofs using Marlin. Cryptology ePrint Archive, Report 2021/930. 2021. Available online: https://ia.cr/2021/930 (accessed on 12 October 2021).
28. Chiesa, A.; Hu, Y.; Maller, M.; Mishra, P.; Vesely, N.; Ward, N. Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS. In Proceedings of the Advances in Cryptology-EUROCRYPT 2020-39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I, Zagreb, Croatia, 10–14 May 2020; Canteaut, A., Ishai, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12105, pp. 738–768.
29. Boneh, D.; Drake, J.; Fisch, B.; Gabizon, A. Halo Infinite: Recursive zk-SNARKs from Any Additive Polynomial Commitment Scheme. Cryptology ePrint Archive, Report 2020/1536. 2020. Available online: https://ia.cr/2020/1536 (accessed on 12 October 2021).
30. Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Models of distributed proof generation for zk-SNARK-based blockchains. In *Theoretical and Applied Cryptography*; Belarusian State University: Minsk, Belarus, 2020; pp. 112–120.

31. Stanley, R.P. *Enumerative Combinatorics*, 2nd ed.; Cambridge Studies in Advanced Mathematics, 49; Cambridge University Press: Cambridge, UK, 2011; Volume 1.
32. The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Available online: https://oeis.org (accessed on 17 October 2021).
33. Kemeny, J.G.; Snell, J.L. *Finite Markov Chains*; Undergraduate Texts in Mathematics; Springer: Berlin/Heidelberg, Germany, 1976.
34. Ben-Israel, A.; Greville, T.N. *Generalized Inverses: Theory and Applications*, 2nd ed.; CMS Books in Mathematics; Springer: Berlin/Heidelberg, Germany, 2003.
35. D'Angeli, D.; Donno, A. Crested products of Markov chains. *Ann. Appl. Probab.* **2009**, *19*, 414–453.
36. Levin, D.A.; Peres, Y.; Wilmer, E.L. *Markov Chains and Mixing Times*, 2nd ed.; AMS: Providence, RI, USA, 2017.
37. O'Neill, B. The Classical Occupancy Distribution: Computation and Approximation. *Am. Stat.* **2021**, *75*, 364–375.
38. Jiang, Z. An Upper Bound on Stirling Number of the Second Kind. 2015. Available online: https://blog.zilin.one/2015/02/25/an-upper-bound-on-stirling-number-of-the-second-kind/ (accessed on 12 October 2021).
39. Corless, R.; Gonnet, G.; Hare, D.; Jeffrey, D.; Knuth, D. On the Lambert W function. *Adv. Comput. Math.* **1996**, *5*, 329–359.
40. Moser, L.; Wyman, M. Stirling numbers of the second kind. *Duke Math. J.* **1958**, *25*, 29–48.
41. Bender, E.A. Central and local limit theorems applied to asymptotic enumeration. *J. Combin. Theory Ser. A* **1973**, *15*, 91–111.
42. Temme, N.M. Asymptotic estimates of Stirling numbers. *Stud. Appl. Math.* **1993**, *89*, 233–243.
43. Roman, S. *Lattices and Ordered Sets*; Springer: Berlin/Heidelberg, Germany, 2008.
44. Bespalov, Y. Categories: Between Cubes and Globes. Sketch I. *Ukr. J. Phys.* **2019**, *64*, 1125–1128.
45. Sidenko, S. Kac's Random Walk and Coupon Collector's Process on Posets. Ph.D. Thesis, MIT, Cambridge, MA, USA, 2008.
46. Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Game-Theoretic View on Decentralized Proof Generation in zk-SNARK Based Sidechains. In Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), CEUR Workshop Proceedings 2021, Online, 7–8 January 2021; Volume 2923, pp. 47–59.