



HAL
open science

A method for designing asynchronous probabilistic processes

Samy Abbas

► **To cite this version:**

| Samy Abbas. A method for designing asynchronous probabilistic processes. 2013. hal-00878114v1

HAL Id: hal-00878114

<https://hal.science/hal-00878114v1>

Preprint submitted on 29 Oct 2013 (v1), last revised 9 Jan 2014 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Method for Designing Asynchronous Probabilistic Processes

Samy Abbes

University Paris Diderot - Paris 7 (France)

Laboratory PPS

<http://www.pps.univ-paris-diderot.fr/abbes>

October 2013

Abstract

We present a method for constructing asynchronous probabilistic processes. The asynchronous probabilistic processes thus obtained are called invariant. They generalize the familiar independent and identically distributed sequences of random variables to an asynchronous framework. Invariant processes are shown to be characterised by a finite family of real numbers, their characteristic numbers. Our method provides first a way to obtaining necessary and sufficient normalization conditions for a finite family of real numbers to be the characteristic numbers of some invariant asynchronous probabilistic process; and second, a procedure for constructing new asynchronous probabilistic processes.

1 Introduction

Probability has become a widely used tool in about every scientific field, from the most theoretical fields such as Quantum Mechanics to the most applied fields, where probability is often used as an auxiliary device for the generation of samples “to be trusted”. Computer Science has not escaped the probability wave: random algorithms were introduced where deterministic algorithms were stumped, and the emerging of network systems has opened yet another application field to probability, since network systems are “the” place where uncertainty dominates.

However, when it comes to the very practice of probability, not all researchers are aware of the whole machinery from Measure theory that sustains modern Probability theory. Probability basically means: “toss a coin”, or maybe “roll a dice” with an integer number n of possible outcomes, which amounts in considering a finite family of non negative real numbers $(p_i)_{1 \leq i \leq n}$ such that $p_1 + \dots + p_n = 1$. Independence of event is most of time understood, hence rolling the dice k times is equivalent to rolling a bigger dice with n^k possible outcomes, and each sequence $(o_i, \dots, o_k) \in \{1, \dots, n\}^k$ of outcomes is given the

probability $p_{o_1} \times \dots \times p_{o_k}$. This paradigm is called an iid sequence, that is to say, independent and identically distributed.

Would we want to make the game a bit more complicated, one could consider Markov chains, either in discrete or in continuous time, instead of iid sequences. And again, basic algebraic manipulations are enough to compute basic probabilities, even with the more involved model of Markov chains. No need of Measure theory so far. Of course, obtaining fine results on the asymptotic behaviour of the process could not be done by hand; but the point to underline here is that, without serious reasons, one usually does not bother with Measure theory to do probability because most of the time, it comes down to the simple equation $p_1 + \dots + p_n = 1$.

All of this is fine as long as we stay in the sequential world. The world of asynchronous processes is entirely different. Indeed, considering a causal model with finitely many possible events, what is a probability is not even easy to define. In the sequential world, each experience has n different and mutually exclusive outcomes; whence the equation $p_1 + \dots + p_n = 1$. On the contrary, in the asynchronous world, some events can be concurrent and thus not exclusive with each other. Hence the sum $p_1 + \dots + p_n$ cannot be equal to 1 anymore, when it is extended to all possible events. Furthermore, because of asynchrony, one event can occur in parallel with an arbitrary number of other concurrent events; how would probability take care of this feature is not obvious either.

Although in the sequential world it is possible to deal with finite probabilities only—at least until a certain point—, the understanding of probability in the asynchronous world requires some theoretical material from Measure theory. We will also see that some notions borrowed from classical probabilistic process theory prove to be useful as well.

In this paper, our goal is to finally re-obtain the comfortable feeling of a simple equation for attaching a probabilistic behavior, but this time to an asynchronous system. The point is that the equation in question is not trivial to obtain. The paper explains a method to obtain the corresponding equation, which replaces the familiar $p_1 + \dots + p_n = 1$.

The model we adopt is a concrete representation of a trace model. We call it a multi-sites model. It matches with several message passing models or shared-memory models, and is nothing but a kind of asynchronous system in the sense of [8], that is to say, a trace semi-group acting on a set of states. Its mathematical treatment is specially convenient for our purpose.

After having exposed our asynchronous model, we will consider the probabilistic elements that can be attached to it, defining by this way a probabilistic behavior of the system. This amounts to defining a class of asynchronous probabilistic process that we call invariant. They are the analogues, in the asynchronous world, of iid sequences in the synchronous world. Obviously, they deserve much interest, just as iid sequences deserve much interest since they are basic tools in probability. It turns out that until today, it was not known how to design such basic processes in the asynchronous world—because of the inherent difficulties related to the mixing of probability with asynchrony.

Invariant processes are characterised by a finite collection of non negative

real numbers, that we call the characteristic numbers of the process. On the practical side, the characteristic numbers are the p_i that we are seeking. The main issue is to obtain necessary and sufficient normalization conditions for these numbers to define indeed an invariant process. In the sequential world, the condition is the usual $p_1 + \dots + p_n = 1$ equation.

We expose our new method for desiging such asynchronous probabilistic processes on an example. Our exposition is decomposed in two parts. A first part is devoted to the analysis of the model, and provides necessary conditions by means of a normalization equation on the characteric numbers. The second part is more technical: it shows that the conditions thus obtained are sufficient for the construction of such a process with the assigned characteristic numbers.

From the practical side, a researcher interested in the design of an invariant probabilistic asynchronous process should simply follow the method that we introduce. Doing so, she will obtain a normalization constraint and a series of inequations. The obtained equation and inequations depend on the topology of the system, and cannot be given a general analytical form. The remaining work for the researcher consists then in solving both the equation and the inequations. The theory guarantees the existence and uniqueness of an invariant asynchronous probabilistic process with the associated charactersitic numbers.

Organization of the paper Section 2 describes the algebraic part of the multi-sites model. Section 3 adds a probabilistic layer. It introduces invariant asynchronous probabilistic processes and their characteristic numbers. Section 4 explains on a non trivial example our method to obtain a normalization equation for the characteristic numbers. Section 5 shows the sufficiency of the normalization condition by constructing an invariant process with specified characteristic numbers obeying the normalization condition. Section 6 discusses the amount of generality of the method, and the computational meaning of invariance for asynchronous probabilistic processes. Finally, the concluding Section 7 presents perspectives for further work.

Related work The topic of this work departs from probabilistic process algebra or probabilistic automata, which all rely on variants of Markov chains models either in discrete or in continuous time. The closest models are probabilistic event structures, studied by the same author and co-authors [3] and by others authors [13, 14], and probabilistic Petri nets [4, 5]. All these models have severe limitations however: confusion-freeness for [13], and more generally local finiteness for [3, 4]. On the one hand, the Markov hypothesis of [4] is more general than the invariance hypothesis that we adopt here. But on the other hand, and much more importantly, the range of models that we cover in the present work is much richer than the confusion-free event structures or the locally finite event structures. To the extent of our knowledge, this work is the first exhaustive presentation of a natural class of non trivial asynchronous probabilistic processes.

2 The multi-sites model

Let $n \geq 1$ be an integer, that represents a number of *sites*. To each site $i \in \{1, \dots, n\}$ is attached a finite and non empty set S^i . Elements of S^i are the *local states* of site i . It is understood that the S^i may have arbitrary intersections, corresponding to shared states. By definition, the family (S^1, \dots, S^n) constitutes a *n-sites system*.

To each local state $x \in \bigcup_i S^i$ we associate a *transition* t defined as a n -tuple $t = (t^1, \dots, t^n)$ such that, for all $i \in \{1, \dots, n\}$:

$$t^i = \begin{cases} x, & \text{if } x \in S^i, \\ \emptyset, & \text{the empty word, otherwise.} \end{cases} \quad (1)$$

So for instance, if x belongs to S^1 and to S^2 only, the associated transition is $t = (x, x, \emptyset, \dots, \emptyset)$. We denote by \mathcal{T} the set of transitions. The *resources* of the transition t defined by (1) are those indices $i \in \{1, \dots, n\}$ such that $t^i \neq \emptyset$. We denote by $\rho(t)$ the set of resources of t . A transition t is said to be *private* if $\rho(t)$ is a singleton; it is said to be *shared* otherwise.

Two transitions $t, t' \in \mathcal{T}$ are said to be *independent*, denoted by $t \parallel t'$, if $\rho(t) \cap \rho(t') = \emptyset$.

Transitions are concatenated component by component, with the concatenation of words on each component. We call *finite trajectory* the result of any finite concatenation of transitions. A finite trajectory is thus given as a n -tuple, where the i^{th} component is a word on the alphabet S^i . We denote by \mathcal{S} the set of finite trajectories. The concatenation of trajectories gives a structure of semi-group to \mathcal{S} . Observe that \mathcal{S} is isomorphic to the semi-group with the elements of \mathcal{T} as generators and with the commutation relations $t \cdot t' = t' \cdot t \iff t \parallel t'$.

Let us examine two examples. The first example consists of a single 1-site system (S^1). The associated independence relation is empty. Transitions merely identify with local states of S^1 . And finite trajectories are given by finite sequences of states.

Our second example is a 4-sites system with a ring structure. Let x_1, x_2, x_3, x_4 be 4 distinct symbols, and put $S^i = \{x_{i-1}, x_i\}$ for $i \in \{1, 2, 3, 4\}$ with the convention $0 = 4$. The 4-sites system (S^1, S^2, S^3, S^4) has 4 transitions that we depict as vertical vectors for a better readability:

$$t_1 = \begin{pmatrix} x_1 \\ x_1 \\ \emptyset \\ \emptyset \end{pmatrix} \quad t_2 = \begin{pmatrix} \emptyset \\ x_2 \\ x_2 \\ \emptyset \end{pmatrix} \quad t_3 = \begin{pmatrix} \emptyset \\ \emptyset \\ x_3 \\ x_3 \end{pmatrix} \quad t_4 = \begin{pmatrix} x_4 \\ \emptyset \\ \emptyset \\ x_4 \end{pmatrix}$$

The associated independence relation is given by $t_1 \parallel t_3$ and $t_2 \parallel t_4$. An example of a finite trajectory is $s = t_2 \cdot t_1 \cdot t_3 \cdot t_4$, given by the following vector:

$$s = \begin{pmatrix} \emptyset \\ x_2 \\ x_2 \\ \emptyset \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_1 \\ \emptyset \\ \emptyset \end{pmatrix} \cdot \begin{pmatrix} \emptyset \\ \emptyset \\ x_3 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} x_4 \\ \emptyset \\ \emptyset \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \cdot x_4 \\ x_2 \cdot x_1 \\ x_2 \cdot x_3 \\ x_3 \cdot x_4 \end{pmatrix}.$$

Observe that, since $t_1 \parallel t_3$, we may switch the two adjacent transitions t_1 and t_3 : indeed, $s = t_2 \cdot t_3 \cdot t_1 \cdot t_4$.

In passing, we observe on this example that *not* any tuple of finite sequences is a trajectory! For share states might not be correctly distributed over the adequate components in general. For instance, (x_1, x_2, x_3, x_4) is not a finite trajectory in our example.

Resuming the study of the general case, recall that as for any semi-group, the left divisibility relation defined on \mathcal{S} by:

$$\forall s, s' \in \mathcal{S} \quad s \leq s' \iff \exists r \in \mathcal{S} \quad s' = s \cdot r,$$

is a preorder on \mathcal{S} , compatible with concatenation on the left ($s \leq s' \Rightarrow u \cdot s \leq u \cdot s'$). In our case, the preorder is actually a partial ordering relation on \mathcal{S} , making thus \mathcal{S} a partially ordered semi-group.

Denote by $(S^i)^*$ the free semi-group generated by S^i . There are n natural projections $\theta^i : \mathcal{S} \rightarrow (S^i)^*$ which are semi-group homomorphisms, and thus also homomorphisms of partial orders, equipping $(S^i)^*$ with the prefix ordering on words—yet another name for the left divisibility relation on $(S^i)^*$.

We say that $s' \in \mathcal{S}$ is a *sub-trajectory* of $s \in \mathcal{S}$ is $s' \leq s$. We denote by \mathcal{S}_s the set of sub-trajectories of s . Observe that not any prefix of s is a sub-trajectory, since it might not be a trajectory itself.

Proposition 2.1. *Let s be a finite trajectory. Then \mathcal{S}_s is a lattice, with least upper bound (lub) and greatest lower bound (glb) obtained component by component.*

Now is the time for a parenthesis in probability for motivating what follows. Even when considering simple independent and identically distributed (iid) sequences of discrete random variables, one has to consider that the dice is thrown potentially infinitely many times. Indeed, if one considers random outcomes such as “the first time the dice is even”, there is no bound on the number of needed outcomes. It is therefore necessary to consider infinite sequences of possible outcomes. Let us briefly review the usual notions for dealing with infinite sequences before embarking to the asynchronous model.

Let $\overline{(S^i)^*}$ denote the set of sequences, either finite or infinite, of elements in S^i , and let Ω^i denote the set of infinite sequences of elements in S^i . The elements of Ω^i are just the missing elements for $(S^i)^*$ to be complete with respect to lub of increasing countable chains (no advanced Domain theory is needed here, hence we will refrain from introducing any language elements from Domain theory). On the one hand, the ordering relation of $(S^i)^*$ extends in an obvious way on its completion $\overline{(S^i)^*}$; on the other hand, the semi-group structure on S^i does not extend to a semi-group structure on $\overline{(S^i)^*}$. Instead, one only has a left semi-group action of S^i on its completion $S^i \times \overline{(S^i)^*} \rightarrow \overline{(S^i)^*}$, $(s, w) \mapsto s \cdot w$ corresponding to the concatenation of a finite word s on the left with an infinite word w on the right.

These trivialities were recalled for free semi-groups in order to underline the analogy with the more involved situation of our trace semi-group \mathcal{S} . Since it is

not the core of our subject, we will just briefly mention the construction of the order completion of \mathcal{S} , referring for instance to [1] for the details. The canonical completion of \mathcal{S} , with respect to the lub of increasing countable chains, is a partial order that we denote $\overline{\mathcal{S}}$. There is a natural embedding of partial orders $\mathcal{S} \rightarrow \overline{\mathcal{S}}$. Every element of $\overline{\mathcal{S}}$ is obtained as the lub of an increasing sequence $(x_k)_{k \geq 0}$ in \mathcal{S} . Furthermore, if $x = \sup_{k \geq 0} x_k$ and $y = \sup_{k \geq 0} y_k$ with $(x_k)_{k \geq 0}$ and $(y_k)_{k \geq 0}$ two increasing sequences in \mathcal{S} , then $x \leq y$ in $\overline{\mathcal{S}}$ if and only if:

$$\forall k \geq 0 \quad \exists k' \geq 0 \quad x_k \leq y_{k'}. \quad (2)$$

In particular, the equality $x = y$ holds if and only if (2) holds, together with the same relation with the roles of x and y inverted.

The projection mappings $\theta^i : \mathcal{S} \rightarrow (S^i)^*$ have natural extensions $\theta^i : \overline{\mathcal{S}} \rightarrow \overline{(S^i)^*}$, which gives us a concrete representation for the elements of $\overline{\mathcal{S}}$: any element w of $\overline{\mathcal{S}}$ is a n -tuple (s^1, \dots, s^n) , where each s^i is itself an element of $\overline{(S^i)^*}$. In particular, there is a natural embedding of \mathcal{S} in the infinite product:

$$\overline{\mathcal{S}} \subseteq (S^1)^{\mathbb{N}} \times \dots \times (S^n)^{\mathbb{N}} \simeq (S^1 \times \dots \times S^n)^{\mathbb{N}}. \quad (3)$$

For example, in the framework of our previous example with $n = 4$ sites, the regular pattern consisting of infinitely many occurrences of transition t_1 in parallel with infinitely many occurrences of transition t_3 is represented by the following vector of sequences (the order of appearance of t_1 and t_3 is irrelevant since $t_1 \parallel t_3$):

$$\sup_{k \rightarrow \infty} \underbrace{t_1 \cdot \dots \cdot t_1}_{k \text{ times}} \cdot \underbrace{t_3 \cdot \dots \cdot t_3}_{k \text{ times}} = \begin{pmatrix} x_1 \cdot x_1 \cdot \dots \\ x_1 \cdot x_1 \cdot \dots \\ x_3 \cdot x_3 \cdot \dots \\ x_3 \cdot x_3 \cdot \dots \end{pmatrix}.$$

We call *trajectories* the elements of $\overline{\mathcal{S}}$. They contain the finite trajectories. The same observation than we did for finite trajectories holds for trajectories in general: *not* any n -tuple of sequences is a trajectory (see the example above).

The notion of sub-trajectory naturally extends to arbitrary trajectories. And Prop. 2.1 extends then as follows: the set $\overline{\mathcal{S}}_v$ of sub-trajectories of an arbitrary trajectory $v \in \overline{\mathcal{S}}$ is a complete lattice, with lub and glb taken component by component.

Just as for free semi-groups, the completion $\overline{\mathcal{S}}$ comes equipped with a left semi-group action $\mathcal{S} \times \overline{\mathcal{S}} \rightarrow \overline{\mathcal{S}}$, which extends the semi-group concatenation $\mathcal{S} \times \mathcal{S} \rightarrow \mathcal{S}$. This action consists in the concatenation of a finite trajectory on the left with a possibly infinite trajectory on the right. The concatenation can be characterized as follows: for $s \in \mathcal{S}$ and $w \in \overline{\mathcal{S}}$, the element $s \cdot w$ is the only element of $\overline{\mathcal{S}}$ such that:

$$\forall i \in \{1, \dots, n\}, \quad \theta^i(s \cdot w) = \theta^i(s) \cdot \theta^i(w).$$

Note that the right member of the above equation refers to the semi-group action of $(S^i)^*$ on $\overline{(S^i)^*}$.

3 Invariant asynchronous processes

Adding a probabilistic layer to a model classically consists in defining a measurable space of samples, which will support a probability measure to be constructed. A sample should describe an entire history of the system. In our case, the natural candidates for samples are infinite trajectories. But, since trajectories have several components, we need to be more specific.

We say that a trajectory $s \in \overline{\mathcal{S}}$ is a *sample* if all components of s are infinite. Accepting some components to be finite would be possible without fundamental changes; but sticking to our definition of samples brings appreciable simplifications.

Referring to the usual notation from Probability theory, we denote by Ω the set of samples. Since all S^i are supposed to be non empty, note that Ω itself is non empty as well. Since $\Omega \subseteq \overline{\mathcal{S}}$, the embedding noted in (3) induces an embedding of Ω into an infinite product of finite sets. Each finite set being equipped with its discrete σ -algebra, the infinite product carries a product σ -algebra, which induces by restriction a σ -algebra \mathfrak{F} on Ω . The σ -algebra \mathfrak{F} is generated by the subsets of the form:

$$\forall s \in \mathcal{S}, \quad \uparrow s = \{\omega \in \Omega : s \leq \omega\}. \quad (4)$$

In reference to the analogous concept in Measure theory or in Topology, we call the subsets of the form (4) the *elementary cylinders* of Ω .

Alternatively, the σ -algebra \mathfrak{F} on Ω can be defined as the restriction to Ω of the Borel σ -algebra associated with the Scott topology on $\overline{\mathcal{S}}$: both definitions are equivalent (since the compact elements of $\overline{\mathcal{S}}$ are precisely the elements of \mathcal{S}).

We define an *asynchronous probabilistic process* (APP) as a probability measure \mathbb{P} defined on the space (Ω, \mathfrak{F}) of samples associated with some n -sites system. We derive from classical theorems the following:

Proposition 3.1. *Two APP that coincide on elementary cylinders are equal.*

Hence, constructing an APP consists in defining an adequate countable collection of non negative real numbers for the probability $\mathbb{P}(\uparrow s)$ of all elementary cylinders.

Just as in sequential systems, we pay a special attention to certain probability measures, not to arbitrary ones, we will restrict the class of APP that we plan to deal with. For this, let us introduce the notion of probabilistic future, which is a sort of local shift in the sample space Ω .

Let s be a finite trajectory. The concatenation of s with arbitrary trajectories (see § 2) defines a mapping $\Phi_s : \Omega \rightarrow \uparrow s$ given by $\Phi_s(\omega) = s \cdot \omega$ which is a bimeasurable bijection. Assume furthermore that $\mathbb{P}(\uparrow s) > 0$. The elementary cylinder $\uparrow s$ is then equipped with the conditional probability $\mathbb{P}(\cdot | \uparrow s) = \frac{1}{\mathbb{P}(\uparrow s)} \mathbb{P}(\cdot)$. The image of this conditional probability by the measurable mapping Φ_s^{-1} defines a probability measure \mathbb{P}_s on Ω , which we call the *probabilistic future of s with respect to \mathbb{P}* . The APP \mathbb{P}_s is characterized by its values on elementary

cylinders:

$$\forall s' \in \mathcal{S} \quad \mathbb{P}_s(\uparrow s') = \frac{1}{\mathbb{P}(\uparrow s)} \mathbb{P}(\uparrow(s \cdot s')).$$

Definition 3.2. An APP \mathbb{P} is said to be invariant whenever the two following conditions are fulfilled:

$$\forall s \in \mathcal{S} \quad \mathbb{P}(\uparrow s) > 0, \tag{5}$$

$$\forall s \in \mathcal{S} \quad \mathbb{P}_s = \mathbb{P}. \tag{6}$$

Condition (5) will bring appreciable technical simplifications without restricting the generality; see the comment after Lemma 3.7.

We claim that invariant APP are the analogous, in the asynchronous framework, of iid sequences in the sequential framework. The following proposition supports this claim; recall that if $n = 1$ the transitions of (S^1) are given by the local states of S^1 .

Proposition 3.3. An APP \mathbb{P} defined on a 1-site system (S^1) is invariant if and only if \mathbb{P} is the law of a sequence of iid random variables with values in S^1 , and assigning a positive probability to every state.

Our target is now twofold: firstly, effectively construct invariant APP; and secondly, characterize invariant APP defined on a given multi-sites system through a finite family of real numbers, very much as the finite family of individual probabilities $(p_i)_i$ characterize a whole sequence of iid random variables distributed according to the family $(p_i)_i$. Observe that we proceed backward compared to the usual way in the sequential framework: instead of starting from the finite family $(p_i)_i$, and then constructing the associated probability measure on the space of samples, we start from the probability measure on the space of samples, and then we derive the finite family of numbers.

Characterizing invariant APP is the job of characteristic numbers that we introduce now.

Definition 3.4. The characteristic numbers associated with an invariant APP \mathbb{P} are defined as follows:

$$\forall t \in \mathcal{T}, \quad p_t = \mathbb{P}(\uparrow t), \tag{7}$$

where transitions are identified in the obvious way with finite trajectories.

The next definition follows naturally:

Definition 3.5. An invariant APP is said to be symmetric if all its characteristic numbers are equal.

Although (7) makes sense for any APP, the family $(p_t)_{t \in \mathcal{T}}$ really characterizes the process only in case it is invariant. Indeed:

Proposition 3.6. Two invariant APP with the same characteristic numbers are equal.

The proposition is based on the following lemma, which is of interest *per se*:

Lemma 3.7. *If \mathbb{P} is an invariant APP, then we have for any transitions t_1, \dots, t_k :*

$$\mathbb{P}(\uparrow(t_1 \cdot \dots \cdot t_k)) = p_{t_1} \cdot \dots \cdot p_{t_k}.$$

In view of Lemma 3.7, the condition (5) that appears in Def. 3.2 implies no loss of generality. Indeed, if some $s \in \mathcal{S}$ satisfies $\mathbb{P}(\uparrow s) = 0$, then it means that $p_t = 0$ for some $t \in \mathcal{T}$. Removing all transitions t with $p_t = 0$ defines an isomorphic process, now complying with Def. 3.2.

What really matters next is to find adequate conditions for a given collection $(q_t)_{t \in \mathcal{T}}$ of non negative real numbers to coincide with the collection of characteristic numbers of some invariant APP.

Before that, we briefly examine the case where there is $n = 1$ site only. In that case, the characteristic numbers are just the individual probabilities p_x attached to the local states $x \in S^1$. The normalization condition is well known: $\sum_{x \in S^1} p_x = 1$. In particular, *symmetric* invariant APP correspond to *uniformly* distributed iid sequences of random variables.

4 Analysis of the ring example

In this section we thoroughly analyze the example with $n = 4$ sites on a ring structure introduced above, and derive a necessary normalization condition for the characteristic numbers of associated invariant APP. Showing the sufficiency of the normalization condition for the existence of an invariant APP with the specified characteristic numbers is the topic of next section. The amount of generality of our method is discussed in § 6.

We assume thus given some invariant APP \mathbb{P} on the 4-sites system (S^1, S^2, S^3, S^4) with 4 transitions t_1, t_2, t_3, t_4 described above. For $i \in \{1, 2, 3, 4\}$, let $p_i = \mathbb{P}(\uparrow t_i)$ be the characteristic number of \mathbb{P} corresponding to transition t_i .

Our analysis involves the notion of asynchronous stopping time, that we introduce in all generality:

Definition 4.1. *An asynchronous stopping time, or stopping time for short, is a mapping $T : \Omega \rightarrow \overline{\mathcal{S}}$, denoted $\omega \mapsto \omega_T$, such that $\omega_T \leq \omega$ for all $\omega \in \Omega$, and satisfying furthermore the following property:*

$$\forall \omega, \omega' \in \Omega \quad \omega' \geq \omega_T \Rightarrow \omega'_T = \omega_T. \quad (8)$$

Stopping times are a fundamental notion in classical probabilistic processes theory introduced in the 1950's [9]. For a sequential process, a typical example of stopping time is the first instant the process hits a given state. Clearly, it has the property that, at each instant, an observer can determine whether the given state has been hit or not, *only* based on the history of the process.

Our definition of asynchronous stopping times has the same meaning. Indeed, the trajectory ω_T is a sub-trajectory of the sample ω . In the asynchronous framework, we believe that sub-trajectories can be seen as time instants; whence

the temporal interpretation of $\omega_T \leq \omega$ in Def. 4.1. Property (8) expresses that the value ω_T does not depend on the queue of ω after ω_T , and expresses it without reference to any time index, which was the challenging point. We let the interested reader refer to the definitions found in classical textbooks and check that, in case of $n = 1$ site, asynchronous stopping times correspond exactly to the usual stopping times (associated to the canonical filtration).

One stopping time in particular will have our attention. We define it in all generality as follows. For any $\omega \in \Omega$, let $N(\omega)$ be the following set of subtrajectories of ω :

$$N(\omega) = \{s \in \overline{\mathcal{S}}_\omega : \theta^1(\omega) \neq \emptyset\}.$$

$N(\omega)$ is non empty since, by definition, all components of the sample ω are infinite, and in particular the first component. Furthermore, $N(\omega)$ contains finite trajectories. Since we have seen that $\overline{\mathcal{S}}_\omega$ is a complete lattice, it is legitimate to put:

$$\omega_U = \inf N(\omega). \quad (9)$$

This defines a finite subtrajectory ω_U of ω , with the property that $\theta^1(\omega_U)$ has exactly one element. The fact that ω_U satisfies (8) is the matter of a simple verification. And since $\omega_U \leq \omega$ by construction, ω_U is indeed a stopping time, corresponding to the “first instant” where the first coordinate has been put in motion.

If $n = 1$, ω_U identifies with the prefix of length 1 of ω . It correspond thus to the constant time 1. As soon as $n > 1$ however, ω_U is of unbounded size in general. For an example on the ring structure with $n = 4$ sites, consider some sample $\omega \in \uparrow s$, where $s = t_2 \cdot t_1 \cdot t_3 \cdot t_4$ is the finite trajectory defined earlier. Then it is easy to check that $\omega_U = t_2 \cdot t_1 = (x_1, x_2 \cdot x_1, x_2, \emptyset)$. Observe that, by property (8) of Def. 4.1, the remaining part of ω is not needed to determine ω_U . Actually, for any $\omega \in \uparrow(t_2 \cdot t_1)$ one has $\omega_U = t_2 \cdot t_1$.

We now generalize this example in order to obtain a general form for ω_U for the ring structure with 4 sites. Let X^1 denote the first element of the first coordinate of ω , which is thus a random variable with values in $\{x_1, x_4\}$. Assume that $X^1 = x_1$. The first coordinate of ω_U is then necessarily x_1 . The second coordinate of ω_U ends thus with x_1 , but carries an arbitrary number K of x_2 's. We keep turning and arrive now at the third coordinate of ω_U , which must carry the same number K of occurrences of x_2 . Between two occurrences of x_2 , and prior to the first occurrence of x_2 , the third coordinate of ω_U is free to carry an arbitrary number of occurrences of x_3 ; whence J_1, \dots, J_K arbitrary integers corresponding to the successive numbers of occurrences of x_3 in the third coordinate. The last coordinate must carry as many occurrences of x_3 as the third coordinate, which is $J_1 + \dots + J_K$. But it cannot carry any occurrence of x_4 , otherwise the first coordinate should have as many occurrences of x_4 as well, which is not. We arrive to the following form for ω_U :

$$\omega_U = \left(\begin{array}{c} x_1 \\ (x_2)^K \cdot x_1 \\ (x_3)^{J_1} \cdot x_2 \cdot \dots \cdot (x_3)^{J_K} \cdot x_2 \\ (x_3)^{J_1 + \dots + J_K} \end{array} \right). \quad (10)$$

In the previous example with $\omega \in \uparrow(t_2 \cdot t_1)$, we had $K = 1$ and $J_1 = 0$.

This concerned the case where $X^1 = x_1$. In the case where $X^1 = x_4$, a similar analysis turning in the other way around yields the following form for ω_U :

$$\omega_U = \begin{pmatrix} x_4 \\ (x_2)^{J'_1 + \dots + J'_{K'}} \\ (x_2)^{J'_1} \cdot x_3 \cdot \dots \cdot (x_2)^{J'_{K'}} \cdot x_3 \\ (x_3)^{K'} \cdot x_4 \end{pmatrix}, \quad (11)$$

where K' and $J'_1, \dots, J'_{K'}$ are arbitrary integers.

The above analysis allows us to derive precise informations on the probabilistic side, which we gather in the following result.

Proposition 4.2. *In the framework of the 4-sites system with a ring structure, we put $r_1 = \mathbb{P}(X^1 = x_1)$ and $r_4 = \mathbb{P}(X^1 = x_4)$. Then:*

1. *The following inequalities hold:*

$$p_2 + p_3 < 1 \quad p_1, p_2, p_3, p_4 < 1. \quad (12)$$

2. *The law of X^1 is given by:*

$$r_1 = \frac{p_1(1-p_3)}{1-p_2-p_3}, \quad r_4 = \frac{p_4(1-p_2)}{1-p_2-p_3}. \quad (13)$$

3. *Conditionally on $X^1 = x_1$, the integer K follows a geometric distribution:*

$$\mathbb{P}(K = k | X^1 = x_1) = \frac{1-p_2-p_3}{1-p_3} \left(\frac{p_2}{1-p_3} \right)^k.$$

4. *Conditionally on $X^1 = x_4$, the integer K' follows a geometric distribution:*

$$\mathbb{P}(K' = k | X^1 = x_4) = \frac{1-p_2-p_3}{1-p_2} \left(\frac{p_3}{1-p_2} \right)^k.$$

5. *For all integers $k \geq 1$, conditionally on $X^1 = x_1$ and on $K = k$, the integers J_1, \dots, J_k are iid with a geometric distribution:*

$$\mathbb{P}(J_1 = m | X^1 = x_1 \wedge K = k) = (1-p_3)p_3^m.$$

6. *For all integers $k \geq 1$, conditionally on $X^1 = x_4$ and on $K' = k$, the integers J'_1, \dots, J'_k are iid with a geometric distribution:*

$$\mathbb{P}(J'_1 = m | X^1 = x_4 \wedge K' = k) = (1-p_2)p_2^m.$$

Note that the inequalities (12) stated in the very first point of Prop. 4.2 justify the existence of all quotients occurring in Prop. 4.2 and the existence of the geometric laws involved.

To establish Prop. 4.2, there are three basic ingredients: firstly, the decompositions (10)(11) established above for ω_U ; secondly, the property that ω_U is a stopping time; and finally Lemma 3.7 for the computation of probabilities.

Our efforts are rewarded by the sought normalization relation, necessarily satisfied by the characteristic numbers of \mathbb{P} :

$$p_1 + p_2 + p_3 + p_4 = 1 + p_1p_3 + p_2p_4. \quad (14)$$

To establish (14), just write down the equation $\mathbb{P}(X^1 = x_1) + \mathbb{P}(X^1 = x_4) = 1$ and replace the probabilities with the results obtained in Prop. 4.2, point 2.

Our forthcoming task is now to establish a converse result, by showing the existence and uniqueness of an invariant APP with characteristic numbers given by arbitrary numbers $p_i \in (0, 1)$ satisfying (14).

5 Construction of an invariant process

We keep our 4-sites example on a ring structure to expose the construction of invariant APP. We gather both the already obtained necessary condition and the positive construction result in the following theorem.

Theorem 5.1. *Let \mathbb{P} be an invariant APP on the 4-sites ring structure (S^1, S^2, S^3, S^4) . Then the characteristic numbers p_1, p_2, p_3, p_4 of \mathbb{P} satisfy the following conditions:*

$$\forall i \in \{1, 2, 3, 4\} \quad p_i \in (0, 1) \quad (15)$$

$$p_1 + p_2 + p_3 + p_4 = 1 + p_1p_3 + p_2p_4. \quad (16)$$

Conversely, for any tuple (p_1, p_2, p_3, p_4) of real numbers satisfying (15)(16), there is a unique APP on the 4-sites ring structure with p_1, p_2, p_3, p_4 as characteristic numbers.

In particular, there is a unique symmetric invariant APP on the 4-sites ring structure, and its characteristic number is $p = 1 - \frac{1}{2}\sqrt{2} \simeq 0.293$.

The remaining of this section is devoted to the proof of Th. 5.1. The necessity of (15)(16) has already been seen in Prop. 4.2, point 1, and in (14). The last statement about symmetric APP is a consequence of the previous statement in the theorem, since $p = 1 - \frac{\sqrt{2}}{2}$ is the only non negative root of the polynomial $4p = 1 + 2p^2$, obtained from (16) with $p_i = p$ for all i . What remains to be proved is the second paragraph on the existence and uniqueness of invariant APP with assigned characteristic numbers. Uniqueness is a consequence of Prop. 3.6, hence the sole existence remains to be proved.

We decompose the existence proof in three steps. The first step exposes the construction. The second step states a general result that guarantees that our construction is invariant. The last step shows that it has the expected characteristic numbers.

5.1 First step: construction of \mathbb{P}

Let p_1, p_2, p_3, p_4 be real numbers satisfying (15)(16). The idea is to simulate the probabilistic behaviour of ω_U , based on the results of Prop. 4.2. Simple algebraic manipulations based on (16) first yield the following relation:

$$p_1 + p_2 + p_3 < 1 + p_1 p_3, \quad (17)$$

implying in particular:

$$p_2 + p_3 < 1. \quad (18)$$

It is thus legitimate to define, in view of (13):

$$\rho_1 = \frac{p_1(1-p_3)}{1-p_2-p_3}. \quad (19)$$

Based on (16), it is then readily seen that:

$$1 - \rho_1 = \frac{p_4(1-p_2)}{1-p_2-p_3}. \quad (20)$$

Furthermore, (17) implies that $\rho_1 \in (0, 1)$. It is thus legitimate to consider a random variable X defined on some external probability space (Ξ, \mathfrak{G}, Q) with values in $\{x_1, x_4\}$, and such that:

$$Q(X = x_1) = \rho_1, \quad Q(X = x_4) = 1 - \rho_1. \quad (21)$$

We will freely use the usual technique of defining as many fresh random variables as we want, extending the probability space (Ξ, \mathfrak{G}, Q) as needed.

We start by considering an integer random variable K such that, conditionally on $\{X = x_1\}$, K has the geometric distribution given in point 3 of Prop. 4.2. This is legitimate, thanks to (18) and since $p_2 > 0$. In the same fashion, we introduce an integer random variable K' such that, conditionally on $\{X = x_4\}$, K' has the geometric distribution stated in point 4 of Prop. 4.2. Again, this is legitimate, thanks to (18) and $p_3 > 0$. Finally, we introduce the iid random variables J_1, \dots, J_k and J'_1, \dots, J'_k , conditionally on $\{X = x_1 \wedge K = k\}$ and on $\{X = x_4 \wedge K' = k\}$ respectively, and with the conditional laws given in points 5 and 6 of Prop. 4.2 respectively. This is legitimate since $p_3 \in (0, 1)$ and since $p_2 \in (0, 1)$, respectively.

All these random variables being properly defined, we now consider a random finite trajectory S which mimics ω_U : we define S as the right member of (10) if $X = x_1$, and as the right member of (11) if $X = x_4$.

Finally, we define a probability measure \mathbb{P} on (Ω, \mathfrak{F}) as follows. Consider an infinite iid sequence $(S_i)_{i \geq 0}$ of finite trajectories, all with the same distribution as S just constructed. We claim that the concatenation $S_0 \cdot S_1 \cdots$, which always exists in $\bar{\mathcal{S}}$, is actually an element of Ω with Q -probability 1. Indeed, since each S_n has a positive Q -probability of having all its components non empty, and since $(S_i)_{i \geq 0}$ is an iid sequence, the Borel-Cantelli lemma implies our claim. Hence the mapping $\Phi : \Xi \rightarrow \bar{\mathcal{S}}$ defined by the infinite concatenation of the S_i 's,

can actually be considered up to a set of zero probability as a mapping $\Phi : \Xi \rightarrow \Omega$.

Let \mathbb{P} be the probability law of the infinite concatenation $S_0 \cdot S_1 \cdot \dots$. It is formally given as the image

$$\mathbb{P} = \Phi_* Q. \quad (22)$$

As a probability measure on (Ω, \mathfrak{F}) , \mathbb{P} defines an APP. We claim that: 1) \mathbb{P} is an invariant APP, and 2) the characteristic numbers of \mathbb{P} are the p_i 's. These two points are the topic of the next two steps of the proof.

5.2 Second step: using an invariance result

We state below a result that should be used when dealing with other examples than the specific 4-sites ring structure. The 4-sites ring structure will serve as an example of its application.

Let us first introduce some notations and another definition. If U is a stopping time and u is a finite trajectory, we conventionnaly write $u < U$ if there exists $\omega \in \Omega$ such that $u < \omega_U$. We also write $u \in U$ if there exists $\omega \in \Omega$ such that $u = \omega_U$. Definition 5.2 and Th. 5.3 below apply to general multi-sites systems. In the first point of Def. 5.2 below, we recognize a repetition of the trick used in (22) to define a probability measure on (Ω, \mathfrak{F}) .

Definition 5.2. *Let U be a stopping time with values in \mathcal{S} . We assume that ω_U is equipped with a probability law Q , which defines the pair (U, Q) as a randomized stopping time.*

1. *The pair (U, Q) is said to be exhaustive if: a) $Q(U = u) > 0$ for every $u \in U$, and b) for every $s \in \mathcal{S}$, there exists $u_1, \dots, u_k \in U$ such that $s \leq u_1 \cdot \dots \cdot u_k$, and c) the infinite concatenation of an iid sequence $(U_i)_{i \geq 0}$, each U_i being distributed according to Q , belongs to Ω with probability 1, which defines a probability law P on (Ω, \mathfrak{F}) induced by the pair (U, Q) .*
2. *The pair (U, Q) is said to be invariant if the following property is satisfied for all $u, v \in \mathcal{S}$:*

$$(u < U) \wedge (v \in U) \Rightarrow \begin{cases} u \cdot v \in U, & \text{and} \\ Q(\omega_U = u \cdot v) = \\ Q(\omega_U \geq u) \cdot Q(\omega_U = v). \end{cases}$$

Our general result is then the following.

Theorem 5.3. *Let (U, Q) be an exhaustive randomized stopping time, and let \mathbb{P} be the probability measure on (Ω, \mathfrak{F}) induced by (U, Q) . If (U, Q) is invariant, then \mathbb{P} is an invariant APP.*

We now come back to the study of the 4-sites ring structure, and we exploit Th. 5.3 in this framework. If U denotes as in § 4 the stopping time defined by (9), it is readily seen that $\omega_U = S_0$, an obvious consequence of the construction of S .

The probability law Q defined in the first step of the proof (§ 5.1) is thus also a probability law for ω_U . With the language of Def. 5.2, the pair (U, Q) is exhaustive, and the probability \mathbb{P} defined by (22) is the APP induced by the pair (U, Q) .

The well known memoryless property of the geometric distributions involved in the construction of Q is the key to invariance, stated in the following result.

Lemma 5.4. *The pair (U, Q) constructed in § 5.1 is an exhaustive and invariant randomized stopping time.*

In view of Th. 5.3, Lemma 5.4 has the following consequence.

Corollary 5.5. *The APP \mathbb{P} is invariant.*

5.3 Last step: computation of the characteristic numbers

Now that we know by Corollary 5.5 that \mathbb{P} is indeed an invariant APP, it remains to compute its characteristic numbers. For $i \in \{1, 2, 3, 4\}$, let p'_i be the characteristic number of \mathbb{P} associated with transition t_i . Our proof of Th. 5.1 will be complete if we show that $p'_i = p_i$ for all i .

We base our analysis on the forms (10)(11) that we found for ω_U . Recall that, by construction, $\omega_U = S_0$.

Let us start with $p'_1 = \mathbb{P}(\uparrow t_1)$. A single look at (10) shows that:

$$\uparrow t_1 = \{X = x_1 \wedge K = 0\}. \quad (23)$$

The probabilistic event (23) is thus entirely determined by the sole value of S_0 . Its probability is computed accordingly:

$$p'_1 = Q(X = x_1) \cdot Q(K = 0|X = x_1).$$

By construction of the random variables X and K , we have thus, using (19):

$$p'_1 = \rho_1 \frac{1 - p_2 - p_3}{1 - p_3} = p_1, \text{ as expected.}$$

The computation of p'_4 is analogous: $p'_4 = \mathbb{P}(\uparrow t_4)$ and $\uparrow t_4 = \{X = x_4 \wedge K' = 0\}$, referring to (11) this time. Again, $\uparrow t_4$ is entirely determined by the value of S_0 , and its probability is computed accordingly:

$$\begin{aligned} p'_4 &= Q(X = x_4) \cdot Q(K' = 0|X = x_4) \\ &= (1 - \rho_1) \frac{1 - p_2 - p_3}{1 - p_2}. \end{aligned}$$

Thanks to (20), we obtain $p'_4 = p_4$, as expected.

The computation of $p'_2 = \mathbb{P}(\uparrow t_2)$ is more involved, since the probabilistic event $\uparrow t_2$ may depend on an arbitrary number of S_i 's. Let us introduce a game interpretation: the goal is to detect Success, where Success means that at stage i , the event $\uparrow t_2$ has been detected. Both forms (10)(11) are involved. The

probabilistic event **Success** is equivalent to the following disjunction of disjoint probabilistic events:

$$\begin{cases} (X = x_1) \wedge (K \geq 1) \wedge (J_1 = 0), & \text{or} \\ (X = x_4) \wedge (K' \geq 1) \wedge (J'_1 \geq 1), & \text{or} \\ (X = x_4) \wedge (K' = 0) \wedge (\text{Success at next stage}). \end{cases} \quad (24)$$

By invariance, the probability of **Success** at next stage is the same than the probability of **Success**, that is p'_2 . Referring to the specified distributions of the various random variables involved in (24), we obtain that p'_2 satisfies the following equation:

$$\begin{aligned} p'_2 &= \frac{p_1(1-p_2)}{1-p_2-p_3} \left(1 - \frac{1-p_2-p_3}{1-p_3}\right) (1-p_3) \\ &\quad + \frac{p_4(1-p_3)}{1-p_2-p_3} \left(1 - \frac{1-p_2-p_3}{1-p_2}\right) p_2 \\ &\quad + \frac{p_4(1-p_3)}{1-p_2-p_3} \frac{1-p_2-p_3}{1-p_2} p'_2. \end{aligned}$$

Regrouping the different terms yields:

$$p'_2(1-p_4) = \frac{p_2}{1-p_2-p_3} (p_1 - p_1p_3 + p_3p_4). \quad (25)$$

It is readily checked that (16) is equivalent to:

$$1-p_4 = \frac{p_1 - p_1p_3 + p_3p_4}{1-p_2-p_3}. \quad (26)$$

Comparing (25)(26) we obtain $p'_2 = p_2$, as expected.

The computation of p'_3 follows a pattern similar to the computation of p'_2 , and yields indeed $p'_3 = p_3$, which completes the proof of Th. 5.1.

6 Discussion

Range of application Our method applies to any multi-sites system. However, the construction step must still be done on a case-by-case basis. In particular, the inequalities that legitimate the construction of random variables should be properly checked. The 4-sites ring structure is specially pleasant since all the needed inequalities already derive from the basic normalization condition, but this is not the case in general. For instance, the case of a invariant and symmetric 5-sites ring structure yields the normalization condition $5p = 1 + 5p^2$, with two roots $p = \frac{1}{2} \pm \frac{\sqrt{5}}{10}$, both in $(0, 1)$. But only $\frac{5-\sqrt{5}}{10}$ satisfies the additional inequalities gathered on the analysis part. For the record, the n -sites ring structure, even in the symmetric case, yields as normalization condition a polynomial of degree $\lfloor \frac{n}{2} \rfloor$, which does not seem to have a simple analytical form but is rather obtained by induction.

Legitimacy of the invariance hypothesis The invariance hypothesis (Def. 3.2) makes full sense from the distributed systems point of view, since it implies a *modular* property which takes on two forms.

Firstly, the probability of executing a transition t with $\rho(t)$ as resources, is not affected by the parallel execution of transitions depending on resources disjoint from $\rho(t)$; since the probability remains equal to the characteristic number p_t .

And secondly, consider the following graph associated with a n -sites system: the vertices are the sites $\{1, \dots, n\}$, and two sites are connected if they share a common state. Assume that this graph has several connected components, corresponding to non communicating sub-systems. Then the global asynchronous process decomposes in a natural way as a free product of sub-processes defined on each connected components of the graph and that do not synchronize with each other. The invariance hypothesis implies that the sub-processes are independent in the probabilistic sense, a rather natural and expected property.

7 Conclusion

We have introduced and characterized invariant asynchronous probabilistic processes. In a nutshell, they are *asynchronous versions of the geometric probability distribution*. Invariance is indeed a memoryless property, expressed in an asynchronous framework.

Further analysis of the method presented here should provide thorougher understanding of invariant APP. A simple question such as “Is there always a unique symmetric and invariant APP on a multi-sites system?” could then be answered. Although the answer seems intuitively to be “Yes”, it is not obvious based on the present work only.

Studying additional structures on the class of invariant APP is worth considering: restriction of an APP to a sub-system, and composition of APP.

Candidates for more general classes of processes than invariant APP are Markov asynchronous processes, introduced in [2] but for which the construction step was restricted to $n = 2$ sites only.

We expect that this work might have applications in the field of random distributed algorithms, since it introduces new paradigms for the construction of asynchronous probabilistic processes. References [6, 7, 12] are examples showing the diversity of this field; hence it is hard to be more specific at this stage. What can be noted though, is that the topology of the asynchronous process is directly taken into account in our method. Although simple topologies will obviously lead to simpler results, we make no restrictive assumption that would narrow the application range to particular structures, such as tree structures for instance [10].

Applications in the analysis of network systems, such as network dimensioning, are distant targets that might become reachable once further work on the asymptotic analysis of invariant APP is done. In this respect, comparison with other methods for obtaining asymptotics related to trace semi-groups [11] might

be of interest.

A Omitted proofs

A.1 Proofs for Sections 3 and 4

Proofs of the results of § 3 depend on Lemma 3.7, which we prove first.

Proof of Lemma 3.7. By induction on the integer $k \geq 0$. The result is trivial for $k = 0$ with the convention that an empty product is 1, and for $k = 1$ this is just the definition of characteristic numbers. Assume the result is true for any $k \geq 1$. Let t_1, \dots, t_{k+1} be any transitions. Put $s = t_1 \cdot \dots \cdot t_k$ and $s' = t_1 \cdot \dots \cdot t_{k+1}$. On the one hand, we have $\uparrow s' \subseteq \uparrow s$ since $s \leq s'$. On the other hand, we have $\mathbb{P}(\uparrow s) > 0$ by (5), and therefore:

$$\begin{aligned} \mathbb{P}(\uparrow s') &= \mathbb{P}(\uparrow s) \cdot \mathbb{P}(\uparrow(s \cdot t_{k+1}) \mid \uparrow s) \\ &= \mathbb{P}(\uparrow s) \cdot \mathbb{P}_s(\uparrow t_{k+1}). \end{aligned}$$

By the induction hypothesis, $\mathbb{P}(\uparrow s) = p_{t_1} \cdot \dots \cdot p_{t_k}$. Since \mathbb{P} is assumed to be invariant, $\mathbb{P}_s = \mathbb{P}$ and therefore $\mathbb{P}_s(\uparrow t_{k+1}) = \mathbb{P}(\uparrow t_{k+1}) = p_{t_{k+1}}$. Finally, $\mathbb{P}(\uparrow s') = p_{t_1} \cdot \dots \cdot p_{t_{k+1}}$, which was to be proved. \square

Proof of Prop. 3.3. Let \mathbb{P} be an invariant APP defined on the 1-site system (S^1) . Then for any $x_1, \dots, x_k \in S^1$, we have according to Lemma 3.7:

$$\mathbb{P}(\uparrow x_1 \cdot \dots \cdot x_k) = p_{x_1} \cdot \dots \cdot p_{x_k}. \quad (27)$$

This implies that the sequence $(x_k)_{k \geq 0}$ that constitutes a sample $\omega = (x_0, x_1, \dots)$ is an iid sequence where each stat $x \in S^1$ is assigned probability p_x . Since the members of (27) are positive by (5), all p_x are positive.

Conversally, assume that $(X_k)_{k \geq 0}$ is an iid sequence of random variables with values in S^1 , distributed according to $\mathbb{P}(X_0 = x) = p_x$, with all $p_x > 0$. Then \mathbb{P} is an APP on the canonical sample space Ω . Let us show that \mathbb{P} is invariant. Let $s, s' \in \mathcal{S}$. Then $s = x_1 \cdot \dots \cdot x_k$ and $s' = y_1 \cdot \dots \cdot y_{k'}$. Therefore $\mathbb{P}(\uparrow s) = p_{x_1} \cdot \dots \cdot p_{x_k} > 0$, and:

$$\begin{aligned} \mathbb{P}_s(\uparrow s') &= \frac{p_{x_1} \cdot \dots \cdot p_{x_k} \cdot p_{y_1} \cdot \dots \cdot p_{y_{k'}}}{p_{x_1} \cdot \dots \cdot p_{x_k}} \\ &= \mathbb{P}(\uparrow s'). \end{aligned}$$

Hence \mathbb{P} and \mathbb{P}_s coincide on all elementary cylinders, and therefore they are equal by Prop. 3.1. \square

Proof of Prop. 3.6. By Lemma 3.7, two invariant APP with the same characteristic numbers coincide on all elementary cylinders, and thus they are equal by Prop. 3.1. \square

Proof of Prop. 4.2. A proof is given for each point.

Proofs of points 1 and 2 The probabilistic event $\{X = x_1\}$ decomposes as the disjoint union of the different values (10) for ω_U . Hence:

$$r_1 = \sum_{k \geq 0} \sum_{j_1, \dots, j_k \geq 0} \mathbb{P}(\omega_U = u), \quad (28)$$

where u is the finite trajectory given by the right member of (10). Since U is a stopping times, and since u is a value taken by U , it is straightforward to check that we have:

$$\mathbb{P}(\omega_U = u) = \mathbb{P}(\uparrow u). \quad (29)$$

By Lemma 3.7, and since u can be written as:

$$u = (t_3)^{j_1} \cdot t_2 \cdot \dots \cdot (t_3)^{j_k} \cdot t_2 \cdot t_1, \quad (30)$$

we deduce from (29):

$$\mathbb{P}(\omega_U = u) = p_1 \cdot p_2^k \cdot p_3^{j_1 + \dots + j_k}.$$

Replacing in (28), we get:

$$r_1 = p_1 \sum_{k \geq 0} p_2^k \sum_{j_1, \dots, j_k \geq 0} p_3^{j_1 + \dots + j_k}.$$

Since $r_1 < \infty$ on the one hand, and since $p_1 > 0$ and $p_2 > 0$ on the other hand, it follows that $p_3 < 1$. Since the argumnet could be repeated after a circular permutation of $\{1, \dots, 4\}$, we actually obtain: $p_1, p_2, p_3, p_4 < 1$. Calculating first the k geometric sums, we get:

$$r_1 = p_1 \sum_{k \geq 0} \left(\frac{p_2}{1 - p_3} \right)^k.$$

Since $r_1 < \infty$ and $p_1 > 0$ by assumption, we deduce that $\frac{p_2}{1 - p_3} < 1$, that is to say $p_2 + p_3 < 1$. This completes the proof of point 1 of Prop. 4.2. We complete the computation of r_1 as follows:

$$\begin{aligned} r_1 &= p_1 \frac{1}{1 - \frac{p_2}{1 - p_3}} \\ &= \frac{p_1(1 - p_3)}{1 - p_2 - p_3}. \end{aligned}$$

The computation of r_4 is analogous, starting from:

$$r_4 = \sum_{\substack{k \geq 0 \\ j_1, \dots, j_k \geq 0}} p_4 p_3^k p_2^{j_1 + \dots + j_k},$$

which derives from (11). This completes the proof of point 2.

Proof of point 3 The probabilistic event $\{X^1 = x_1 \wedge K = k\}$ decomposes as the following disjoint union:

$$\{X^1 = x_1 \wedge K = k\} = \bigcup_{j_1, \dots, j_k \geq 0} \{\omega_U = u\}$$

where u has the form given in (10), or equivalently in (30). Using again (29) and the definition of the conditional probability, we calculate as follows:

$$\begin{aligned} \mathbb{P}(K = k | X^1 = x_1) &= \frac{\mathbb{P}(X^1 = x_1 \wedge K = k)}{\mathbb{P}(X^1 = x_1)} \\ &= \frac{1}{r_1} \sum_{j_1, \dots, j_k \geq 0} p_1 p_2^k p_3^{j_1 + \dots + j_k} \\ &= \frac{p_1 p_2^k}{r_1} \left(\frac{1}{1 - p_3} \right)^k. \end{aligned}$$

Using the value of r_1 obtained above, we get:

$$\mathbb{P}(K = k | X^1 = x_1) = \frac{1 - p_2 - p_3}{1 - p_3} \left(\frac{p_2}{1 - p_3} \right)^k,$$

which was to be proved.

Proof of point 4 Analogous to the previous point.

Proof of point 5 We have the equality of probabilistic events:

$$\begin{aligned} \{X^1 = x_1 \wedge K = k \wedge (J_1, \dots, J_k) = (j_1, \dots, j_k)\} \\ = \{\omega_U = (t_3)^{j_1} \cdot t_2 \cdot \dots \cdot (t_3)^{j_k} \cdot t_2 \cdot t_1\}. \end{aligned}$$

Using (29) again and the definition of conditional probability, we obtain thus:

$$\begin{aligned} \mathbb{P}(J_1 = j_1, \dots, J_k = j_k | X^1 = x_1 \wedge K = k) \\ = \frac{p_1 p_2^k p_3^{j_1} \cdots p_3^{j_k}}{p_1 p_2^k} (1 - p_3)^k \\ = p_3^{j_1} (1 - p_3) \cdots p_3^{j_k} (1 - p_3). \end{aligned}$$

We recognize thus the product of k independent geometric laws $p_3^j (1 - p_3)$, as expected.

Proof of point 6 Analogous to the previous point. □

A.2 Proofs for Section 5

Proof of Lemma 5.4. We first claim that, for any $u \leq U$, $Q(\omega_U \geq u)$ is given by the following function:

$$\lambda(u) = p_1^{k_1} p_2^{k_2} p_3^{k_3} p_4^{k_4}, \quad (31)$$

where k_1, k_2, k_3, k_4 are the numbers of occurrences of transitions t_1, t_2, t_3, t_4 respectively that appear in u (note that k_2, k_3 are arbitrary, while $k_1, k_4 \leq 1$ and $k_1 + k_4 = 1$).

To prove this claim, assume first that $u \in U$, and the first coordinate of u is x_1 . Then u has the following form:

$$u = t_3^{j_1} \cdot t_2 \cdot \dots \cdot t_3^{j_k} \cdot t_2 \cdot t_1,$$

so that $k_1 = 1$, $k_2 = k$, $k_3 = j_1 + \dots + j_k$, $k_4 = 0$. By construction of Q , we have:

$$\begin{aligned} Q(\omega_U = u) &= \rho_1 \frac{1 - p_2 - p_3}{1 - p_3} \left(\frac{p_2}{1 - p_3} \right)^{k_2} \\ &\quad (1 - p_3) p_3^{j_1} \cdots (1 - p_3) p_3^{j_k} \\ &= p_1 \frac{p_2^{k_2} (1 - p_3)^{k_2} p_3^{j_1 + \dots + j_k}}{(1 - p_3)^{k_2}} \\ &= \lambda(u). \end{aligned}$$

The same holds in the case where the first coordinate of u is x_4 , so that $Q(\omega_U \geq u) = \lambda(u)$ is true if $u \in U$.

Now for the general case where $u \leq U$, we have by the property that U is a stopping time:

$$\begin{aligned} Q(\omega_U \geq u) &= \sum_{\substack{v \in U \\ u \leq v}} Q(\omega_U = v) \\ &= \sum_{\substack{v \in U \\ u \leq v}} \lambda(v). \end{aligned}$$

Assume that $u < U$, since we have already treated the case where $u \in U$. Then the $v \in U$ such that $u \leq v$ are in bijection with the $r \in U$, and the correspondance is given by $v = u \cdot r$. Hence:

$$Q(\omega_U \geq u) = \sum_{r \in U} \lambda(u \cdot r).$$

It is obvious on (31) that $\lambda(u \cdot r) = \lambda(u)\lambda(r)$. Hence:

$$\begin{aligned} Q(\omega_U \geq u) &= \lambda(u) \sum_{r \in U} \lambda(r) \\ &= \lambda(u) \sum_{r \in U} Q(\omega_U = r) \\ &= \lambda(u). \end{aligned}$$

We have thus, as claimed, that $Q(\omega_U \geq u) = \lambda(u)$ for all $u \leq U$.

The invariance of the pair (U, Q) is now obvious. \square

From now on, all the proofs and results presented here apply in whole generality, not to the 4-sites ring structure only.

In view of the proof of Th. 5.3, we need some preliminary results. We start with some combinatorial lemmas, which might be found elsewhere in the literature.

Lemma A.1. *Let $a, b, c, d \in \mathcal{S}$ such that $a \cdot b = c \cdot d$. Then there are $a_1, a_2, b_1, b_2 \in \mathcal{S}$ such that:*

$$\begin{aligned} a &= a_1 \cdot a_2, & b &= b_1 \cdot b_2, \\ c &= a_1 \cdot b_1, & d &= a_2 \cdot b_2. \end{aligned}$$

Proof. If $s \leq s'$ are two finite trajectories, we denote by $s' - s$ the unique finite trajectory r such that $s \cdot r = s'$. Assuming a, b, c, d given as in the statement, we put:

$$\begin{aligned} a_1 &= a \wedge c, & a_2 &= (a - a_1) \wedge d, \\ b_1 &= b \wedge (c - a_1), & b_2 &= (b - b_1) \wedge (d - a_2), \end{aligned}$$

to obtain the result. \square

Lemma A.2. *Let $a, c, d \in \mathcal{S}$ such that $a \leq c \cdot d$. Then there exist $a_1, a_2 \in \mathcal{S}$ such that:*

$$a = a_1 \cdot a_2, \quad a_1 \leq c, \quad a_2 \leq d.$$

Proof. Since $a \leq c \cdot d$, there is $b \in \mathcal{S}$ such that $a \cdot b = c \cdot d$. Let thus $a_1, a_2, b_1, b_2 \in \mathcal{S}$ be as in the conclusion of Lemma A.1. From $a_1 \cdot b_1 = c$ and $a_2 \cdot b_2 = d$, we deduce: $a_1 \leq c$ and $a_2 \leq d$. \square

Lemma A.3. *Let $k \geq 0$ be an integer, and let u, u_1, \dots, u_k be finite trajectories such that $u \leq u_1 \cdot \dots \cdot u_k$. Then there are finite trajectories v_1, \dots, v_k such that $v_i \leq u_i$ for all $i \in \{1, \dots, k\}$, and $u = v_1 \cdot \dots \cdot v_k$.*

Proof. By induction on the integer $k \geq 0$. The result is obvious for $k = 0$ and for $k = 1$. Assume it is true for $k \geq 1$, and let $u \leq u_1 \cdot \dots \cdot u_{k+1}$. Put $c = u_1 \cdot \dots \cdot u_k$. Then $u \leq c \cdot u_{k+1}$. According to Lemma A.2, there are $a_1, a_2 \in \mathcal{S}$ such that $u = a_1 \cdot a_2$ and $a_1 \leq c$ and $a_2 \leq u_{k+1}$. Applying the induction hypothesis to $a_1 \leq u_1 \cdot \dots \cdot u_k$, we find $v_1, \dots, v_k \in \mathcal{S}$ such that $a_1 = v_1 \cdot \dots \cdot v_k$ and $v_i \leq u_i$ for all $i \in \{1, \dots, k\}$. Putting $v_{k+1} = a_2$, we are done. \square

Lemma A.4. *Let (U, Q) be an exhaustive randomized stopping time. Then for all $u \in \mathcal{S}$, there exists $v_1, \dots, v_k \in \mathcal{S}$ such that $u = v_1 \cdot \dots \cdot v_k$ and $v_i \leq U$ for all $i \in \{1, \dots, k\}$.*

Proof. Let $u \in \mathcal{S}$. In order to prove the existence of the v_1, \dots, v_k , and in view of Lemma A.3, it is enough to have the existence of u_1, \dots, u_k such that $u_i \in U$ for all $i \in \{1, \dots, k\}$, and $u \leq u_1 \cdot \dots \cdot u_k$. But this is part of the definition of an exhaustive stopping time, hence we are done. \square

Lemma A.5. *Let (U, Q) be an invariant and exhaustive stopping time, and let \mathbb{P} be the probability on (Ω, \mathfrak{F}) induced by (U, Q) . Then we have:*

$$\forall u \in \mathcal{S} \quad u \leq U \Rightarrow \mathbb{P}_u = \mathbb{P}. \quad (32)$$

Proof. The equality in (32) is clear if $u \in U$ since the sequence $(U_i)_{i \geq 0}$ is iid. Hence, without loss of generality, we assume $u < U$. The invariance assumption on (U, Q) implies then:

$$\forall v \in U \quad \mathbb{P}_u(\uparrow v) = \mathbb{P}(\uparrow v).$$

Since the sequence $(U_i)_{i \geq 0}$ is iid, it follows that, for any sequence $v_1, \dots, v_k \in U$, one has:

$$\mathbb{P}_u(\uparrow(v_1 \cdot \dots \cdot v_k)) = \mathbb{P}(\uparrow(v_1 \cdot \dots \cdot v_k)) \quad (33)$$

We now prove that $\mathbb{P}_u(\uparrow v) = \mathbb{P}(\uparrow v)$ for all $v \in \mathcal{S}$, which will complete the proof of the lemma. For this, we introduce the following stopping time V : for $\omega \in \Omega$, considering the chain:

$$\emptyset \leq U_0(\omega) \leq U_0(\omega) \cdot U_1(\omega) \leq \dots$$

which goes to ω with probability 1 since (U, Q) is exhaustive, we put:

$$V(\omega) = \inf\{U_0 \cdot \dots \cdot U_k \geq v\}. \quad (34)$$

It is readily checked that V is indeed a stopping time, which is finite on $\uparrow v$. This implies the following decomposition of $\uparrow v$ as a countable disjoint union:

$$\uparrow v = \bigcup_{\substack{w \in V \\ w \geq v}} \uparrow w. \quad (35)$$

Taking the \mathbb{P}_u -probabilities of both members of (35), we get:

$$\begin{aligned} \mathbb{P}_u(\uparrow v) &= \sum_{\substack{w \in V \\ w \geq v}} \mathbb{P}_u(\uparrow w) \\ &= \sum_{\substack{w \in V \\ w \geq v}} \mathbb{P}(\uparrow w) && \text{by (33)} \\ &= \mathbb{P}(\uparrow v) && \text{by (34)}. \end{aligned}$$

The proof of the lemma is complete. \square

Lemma A.6. *Let (U, Q) be an invariant and exhaustive stopping time, and let \mathbb{P} be the probability on (Ω, \mathfrak{F}) induced by (U, Q) . Then we have, for any $u_1, \dots, u_k \in \mathcal{S}$ such that $u_i \leq U$ for all $i \in \{1, \dots, k\}$:*

$$\mathbb{P}(\uparrow(u_1 \cdot \dots \cdot u_k)) = \mathbb{P}(\uparrow u_1) \cdot \dots \cdot \mathbb{P}(\uparrow u_k). \quad (36)$$

Proof. By induction on the integer $k \geq 0$. The relation (36) is obvious if $k = 0$ or $k = 1$. Assume it is true until $k - 1 \geq 0$. By definition of \mathbb{P}_{u_1} , one has:

$$\mathbb{P}(\uparrow(u_1 \cdot \dots \cdot u_k)) = \mathbb{P}(\uparrow u_1) \mathbb{P}_{u_1}(\uparrow(u_2 \cdot \dots \cdot u_k))$$

Since $u_1 \leq U$, we have $\mathbb{P}_{u_1} = \mathbb{P}$ according to Lemma A.5, and therefore the induction hypothesis yields $\mathbb{P}(\uparrow(u_2 \cdot \dots \cdot u_k)) = \mathbb{P}(\uparrow u_2) \cdot \dots \cdot \mathbb{P}(\uparrow u_k)$ which brings the result. \square

Proof of Theorem 5.3. We have to show that $\mathbb{P}_u = \mathbb{P}$ for all $u \in \mathcal{S}$. This equivalent to showing that $\mathbb{P}(\uparrow(u \cdot v)) = \mathbb{P}(\uparrow u) \cdot \mathbb{P}(\uparrow v)$ for all $u, v \in \mathcal{S}$. According to Lemma A.6, this is true if u has the form $u = u_1 \cdot \dots \cdot u_k$ with $u_i \leq U$ for all $i \in \{1, \dots, k\}$, and if v is of the same form. But any u and v have this form according to Lemma A.4, so the proof is complete. \square

References

- [1] S. Abbes. On countable completions of quotient ordered semigroups. *Semigroup Forum*, 3(77):482–499, December 2008.
- [2] S. Abbes. Markov two-components processes. *Logical Methods in Computer Science*, 9(2:14):1–34, 2013.
- [3] S. Abbes and A. Benveniste. Probabilistic true-concurrency models: branching cells and distributed probabilities for event structures. *Information & Computation*, 204(2):231–274, 2006.
- [4] S. Abbes and A. Benveniste. Probabilistic true-concurrency models: Markov nets and a law of large numbers. *Theoretical Computer Science*, 390(2-3):129–170, 2008.
- [5] S. Abbes and A. Benveniste. Concurrency, sigma-algebras and probabilistic fairness. In L. de Alfaro, editor, *FOSSACS 2009*, volume 5504 of *LNCS*, pages 380–394, 2009.
- [6] S. Alpern and S. Gal. *The theory of search game and rendezvous*. Kluwer, 2002.
- [7] J. Aspnes and M. Herlihy. Fast randomized consensus using shared memory. *Journal of Algorithms*, 11(3):441–460, 1990.

- [8] M. A. Bednarczyk, L. Bernardinello, B. Caillaud, W. Pawlowski, and L. Pomello. Modular system development with pullbacks. In W. van der Aalst and E. Best, editors, *ATPN 2003*, volume 2679 of *LNCS*, pages 140–160. Springer, 2003.
- [9] J.L. Doob. *Stochastic processes*. Wiley, 1953, reprinted 1990.
- [10] B. Genest, H. Gimbert, A. Muscholl, and I. Walukiewicz. Asynchronous games over tree architectures. In F.V. Fomin, R. Freivalds, M. Kwiatkowska, and D. Peleg, editors, *ICALP 2013, Part II*, volume 7966 of *LNCS*, pages 275–286. Springer, 2013.
- [11] D. Krob, J. Mairesse, and I. Michos. On the average parallelism in trace monoids. In H. Alt and A. Ferreira, editors, *STACS 2002*, volume 2285 of *LNCS*, pages 477–488, 2002.
- [12] G. Norman. Analyzing randomized distributed algorithms. In C. Baier, B. Haverkort, H. Hermanns, J.-P. Katoen, and M. Siegle, editors, *Validation of stochastic systems 2004*, volume 2925 of *LNCS*, pages 384–418. Springer, 2004.
- [13] D. Varacca, H. Völzer, and G. Winskel. Probabilistic event structures and domains. *Theoretical Computer Science*, 358(2–3):173–199, 2006.
- [14] G. Winskel. Distributed probabilistic strategies. In *MFPS XXVII*, 2013.