A method for designing asynchronous probabilistic processes

Samy Abbes

A Method for Designing Asynchronous Probabilistic Processes

Samy Abbes
University Paris Diderot - Paris 7 (France)
Laboratory PPS – CNRS UMR 7126
http://www.pps.univ-paris-diderot.fr/~abbes

Abstract

We introduce a method for constructing asynchronous probabilistic processes. The asynchronous probabilistic processes thus obtained are called invariant. They generalize to the asynchronous framework the familiar sequences of independent and identically distributed random variables by showing a memoryless behavior. Invariant processes are characterized by a finite family of real numbers, their characteristic numbers. Our method provides: firstly, a way to obtain necessary and sufficient normalization conditions for a finite family of real numbers to be the characteristic numbers of some invariant process; and secondly, a procedure to effectively construct the specified process.

1. Introduction

It is common knowledge that, given a finite set of states S equipped with a probability distribution $(p_x)_{x\in S}$, there is a unique probability measure on the space of samples (infinite sequences of states) that corresponds to a series of infinitely many independent random outcomes with values in S, each one being distributed according to $(p_x)_{x\in S}$. Since independent and identically distributed (*iid*) sequences correspond to memoryless processes, this can be rephrased by saying that memoryless sequential processes on S are in bijective correspondence with finite families of non negative real numbers bound to the normalization condition $\sum_{x\in S} p_x = 1$.

In this paper, we explore an extension of this textbook result to asynchronous systems. Our aim is thus to establish a correspondence between some probabilistic parameters and memoryless probabilistic processes on an asynchronous system.

Sequential processes (discrete time Markov chains or *iid* sequences for instance) are usually presented in terms of their probabilistic parameters, before any reference to Measure theoretical aspects. This has the advantage of simplicity, and still allows for the computation of basic probabilities related to Probabilistic Logic for instance. But unlike sequential systems, the mere definition of an asynchronous probabilistic system challenges the probabilistic intuition since there, runs consist of partially ordered sets of events, not of sequences of actions or states. Basic notions from Measure theory provide a way for properly setting up a probabilistic layer for asynchronous systems. Probabilistic parameters shall then be defined *afterward*, fulfilling their role by allowing for the computation of probabilities without referring to the foundational background.

The asynchronous systems that we study, and that we call *multi-sites systems*, match usual and well-known models based on trace monoids [1], [2]. A multi-sites system has several finite sets of local states, whence synchronization and concurrency paradigms through a shared resources mechanism. In this framework, we introduce a class of asynchronous probabilistic processes that we call *invariant*. We argue that the probabilistic behavior of an invariant process transposes to multi-sites systems the behavior performed by an *iid* sequence of random variables defined on a *single* set of states. Invariance is indeed a memoryless property expressed in a framework featuring *several asynchronous* sets of local states. Although invariant processes may appear as basic processes, just as *iid* sequences are basic tools in probability, it was not known so far how to design such basic processes.

An invariant asynchronous process is characterized 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 probabilistic parameters that we are seeking to define an invariant process. However, unlike sequential processes, their normalization conditions are non trivial to obtain. This issue is central throughout the paper. We propose a method combining probability with partial orders techniques to obtain the adequate normalization conditions.

Of course, sequential processes are subsumed as a particular case. In the absence of concurrency features, the invariance hypothesis is equivalent to the *iid* hypothesis. Nothing fancy in that case: our method yields indeed the usual normalization equation $\sum_{x\in S} p_x = 1$.

We explain our new method for designing asynchronous probabilistic processes on a simple and yet non trivial example. The example illustrates the use of general results which are also stated. Following the traditional "analysis and synthesis" approach, we first seek a normalization condition necessarily fulfilled by the characteristic numbers. Then we show the existence and uniqueness of an invariant process with specified characteristic numbers obeying the normalization condition. Our proof is based on a combination of probability tools with combinatorial properties of trace monoids, sum up in a general theorem which provides a versatile tool for the construction of asynchronous probabilistic processes.

It turns out that the normalization condition that we obtain for the characteristic numbers of invariant processes is closely related to the Möbius polynomial associated to the trace monoid in play. This suggests that our work brings new contributions to the combinatorial study of trace monoids. This aspect is discussed at the end of the paper (§ 6).

On the practical side, a researcher willing to design an invariant probabilistic asynchronous process could simply adapt the method that we describe to his or her own system. Doing so, the researcher will obtain a normalization constraint and a series of inequalities for characteristic numbers, which depend on the topology of the system. The remaining work for the researcher consists in solving both the equation and the inequalities. The theory that we develop provides the tools for showing the existence and uniqueness of an invariant asynchronous probabilistic process with the associated characteristic 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, corresponding to the analysis part, shows the method to obtain a normalization equation. Section 5 tackles the effective construction of invariant processes, corresponding to the synthesis part. 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.

Related work. The topic of this work departs from probabilistic process algebra, probabilistic automata or stochastic Petri nets, which all rely on variants of labeled or unlabeled Markov chains models either in discrete or in continuous time. We quickly explain in § 6 that random walks on trace monoids do not give a hint in the study of invariant processes. The closest probabilistic models are probabilistic event structures [3], [4] and probabilistic Petri nets [5], [6]. But all these models have severe limitations: only "confusion-free" [3] or "locally finite" event structures [4], [5] are handled. All non trivial examples of multi-sites systems are out of their range. The probabilistic event structures of [7] are more general but not concerned with the memoryless property, and hence cannot be specified by a *finite* family of parameters, which is precisely the role of characteristic numbers in the present work. To the extend of our knowledge, this work is the first to allow for natural and non trivial examples of probabilistic finite-state machines under a partial order semantics.

2. The multi-sites model

Let $n \geq 1$ be an integer, that represents a number of *sites*. To each site $i \in \{1, \ldots, n\}$ 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 $(S^1, \ldots, S^n)$ constitutes a *n-sites system.*

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

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

So for instance, if x belongs to S^1 and to S^2 only, the associated transition is $t = (x, x, \emptyset, \ldots, \emptyset)$. We denote by $\mathscr{T}$ the set of transitions.

The *resources* of the transition t defined by (1) are those indices $i \in \{1, \ldots, n\}$ such that $t^i \neq \emptyset$. We denote by $\rho(t)$ the set of resources of t. Two transitions $t, t' \in \mathscr{T}$ are said to be *independent*, denoted by $t \,\|\, t'$, 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 finite trajectories gives a structure of monoid to $\mathcal{S}$, that is to say, a semi-group with identity; here, the identity is the vector of empty words. Observe that $\mathcal{S}$ is isomorphic to the monoid with the elements of $\mathscr{T}$ as generators, subject to the commutation relations $t \cdot t' = t' \cdot t \iff t \,\|\, t'$. This is not obvious; one way to proceed is to use a *heap monoid* interpretation of $\mathcal{S}$ [2], and then to apply [2, Prop. 3.4]. It follows in particular that $\mathcal{S}$ is a cancellative monoid: $\forall a, b, u, u' \in \mathcal{S}$ $a \cdot u \cdot b = a \cdot u' \cdot b \Rightarrow u = u'$.

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. Put $S^1 = \{x_4, x_1\}$ and $S^i = \{x_{i-1}, x_i\}$ for $i \in \{2, 3, 4\}$. The 4-sites system (S^1, S^2, S^3, S^4) has 4 transitions $\tau_1, \tau_2, \tau_3, \tau_4$ that we depict vertically:

$$\tau_1 = \begin{pmatrix} x_1 \\ x_1 \\ \emptyset \\ \emptyset \end{pmatrix} \quad \tau_2 = \begin{pmatrix} \emptyset \\ x_2 \\ x_2 \\ \emptyset \end{pmatrix} \quad \tau_3 = \begin{pmatrix} \emptyset \\ \emptyset \\ x_3 \\ x_3 \end{pmatrix} \quad \tau_4 = \begin{pmatrix} x_4 \\ \emptyset \\ \emptyset \\ x_4 \end{pmatrix}$$

The associated independence relation is given by $\tau_1 \,\|\, \tau_3$ and $\tau_2 \,\|\, \tau_4$. An example of a finite trajectory is $u = \tau_2 \cdot \tau_1 \cdot \tau_3 \cdot \tau_4$, given by the following vector:

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

Observe that we may switch the two adjacent transitions τ_1 and τ_3 since $\tau_1 \,\|\, \tau_3$: indeed, $u = \tau_2 \cdot \tau_3 \cdot \tau_1 \cdot \tau_4$.

In passing, we observe on this example that *not* any tuple of finite sequences is a trajectory! 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 monoid, the left divisibility relation $\leq$ defined on $\mathcal{S}$ by:

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

is a preorder on $\mathcal{S}$, compatible with concatenation on the left ($u \leq u' \Rightarrow v \cdot u \leq v \cdot u'$). In our case, the preorder is actually a partial ordering relation on $\mathcal{S}$.

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

We say that $u' \in \mathcal{S}$ is a *sub-trajectory* of $u \in \mathcal{S}$ if $u' \leq u$. We denote by $\mathcal{S}_u$ the set of sub-trajectories of u.

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

In probability, considering infinitely many outcomes of a random experiment is natural. In the sequential framework, outcomes of infinite length correspond to infinite sequences. Let us review some notions for dealing with infinite sequences before embarking on 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 the *lub* of countable chains. On the one hand, the ordering relation of $(S^i)^*$ extends in an obvious way to its completion $\overline{(S^i)^*}$; on the other hand, the monoid structure on $(S^i)^*$ does not extend to a monoid structure on $\overline{(S^i)^*}$. Instead, one only has a left monoid action of $(S^i)^*$ on its completion $(S^i)^* \times \overline{(S^i)^*} \to \overline{(S^i)^*}$, $(u, w) \mapsto u \cdot w$ corresponding to the concatenation of a finite word u on the left with a possibly infinite word w on the right.

These trivialities were recalled for free monoids in order to underline the analogy with the more involved situation of our monoid $\mathcal{S}$. Since it is not the core of our subject, we will just briefly mention the properties of the order completion of $\mathcal{S}$, referring for instance to [8] for the details of its construction. The canonical completion of $\mathcal{S}$, with respect to the *lub* of countable chains, is a partial order that we denote $\overline{\mathcal{S}}$. There is a natural embedding of partial orders $\mathcal{S} \to \overline{\mathcal{S}}$. Every element of $\overline{\mathcal{S}}$ is obtained as the *lub* of an increasing sequence $(u_k)_{k \geq 0}$ in $\mathcal{S}$. Furthermore, if $u = \bigvee_{k \geq 0} u_k$ and $v = \bigvee_{k \geq 0} v_k$ with $(u_k)_{k \geq 0}$ and $(v_k)_{k \geq 0}$ two increasing sequences in $\mathcal{S}$, then $u \leq v$ in $\overline{\mathcal{S}}$ if and only if: $\forall k \geq 0 \quad \exists k' \geq 0 \quad u_k \leq v_{k'}$.

The projection mappings $\theta^i : \mathcal{S} \to (S^i)^*$ have natural extensions $\theta^i : \overline{\mathcal{S}} \to \overline{(S^i)^*}$, which gives us a concrete representation for the elements of $\overline{\mathcal{S}}$: any element w of $\overline{\mathcal{S}}$ is a n-tuple $(w^1, \ldots, w^n)$, where each $w^i = \theta^i(w)$ is an element of $\overline{(S^i)^*}$. In other words, $\overline{\mathcal{S}}$ is embedded into the following product:

$$\overline{\mathcal{S}} \subseteq \overline{(S^1)^*} \times \cdots \times \overline{(S^n)^*} . \tag{2}$$

For example, in the framework of our previous example with $n = 4$ sites, the regular pattern consisting of one occurrence of transition τ_1 in parallel with infinitely many occurrences of transition τ_3 is represented by the following vector of sequences:

$$\bigvee_{k\geq 0} \tau_1 \cdot \underbrace{\tau_3 \cdot \ldots \cdot \tau_3}_{k \text{ times}} = \begin{pmatrix} x_1 \\ x_1 \\ x_3 \cdot x_3 \cdot \ldots \\ x_3 \cdot x_3 \cdot \ldots \end{pmatrix}$$

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.

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 monoids, the completion $\overline{\mathcal{S}}$ comes equipped with a left monoid action $\mathcal{S} \times \overline{\mathcal{S}} \to \overline{\mathcal{S}}$, which extends the monoid concatenation $\mathcal{S} \times \mathcal{S} \to \mathcal{S}$. 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 $u \in \mathcal{S}$ and $w \in \overline{\mathcal{S}}$, the element $u \cdot w$ is the only element of $\overline{\mathcal{S}}$ such that:

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

Note that the right member of the above equation refers to the monoid 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 $w \in \overline{\mathcal{S}}$ is a *sample* if all components of w are infinite. As it is standard in Probability theory, we denote by Ω the set of samples, and by ω generic samples. Since all S^i are supposed to be non empty, note that Ω is non empty as well.

The embedding (2) induces an embedding of Ω into an infinite product of finite sets:

$$\Omega \subseteq (S^1)^{\mathbb{N}} \times \cdots \times (S^n)^{\mathbb{N}} \simeq (S^1 \times \cdots \times S^n)^{\mathbb{N}}\,.$$

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:

$$\forall u \in \mathcal{S} \qquad \uparrow u = \{\omega \in \Omega \;:\; u \leq \omega\}. \tag{3}$$

In reference to the analogous concept in Measure theory or in Topology, we call the subsets of the form (3) 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 $\overline{\mathcal{S}}$ in the Domain theoretic sense are just the elements of $\mathcal{S}$).

Definition 3.1: An *asynchronous probabilistic process* (APP) is defined as a probability measure $\mathbb{P}$ on the space $(\Omega, \mathfrak{F})$ of samples associated with some n-sites system.

The following result derives from classical theorems.

Proposition 3.2: 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 $\mathbb{P}(\uparrow u)$ of all elementary cylinders.

Just as, in the sequential framework, one pays a special attention to certain probability measures, corresponding to memoryless or to Markovian processes for instance, we will restrict the class of APP that we plan to deal with. For this, we introduce a "local shift" in the sample space Ω as follows.

Let $\mathbb{P}$ be an invariant APP, and let u be a finite trajectory. The concatenation of u with samples (see § 2) defines a mapping $\Phi_u : \Omega \to \uparrow u$ given by $\Phi_u(\omega) = u \cdot \omega$ which is a bi-measurable bijection. Assume furthermore that $\mathbb{P}(\uparrow u) > 0$. The elementary cylinder $\uparrow u$ is then equipped with the normalized probability $\mathbb{P}(\,\cdot \mid \uparrow u) = \frac{1}{\mathbb{P}(\uparrow u)}\mathbb{P}(\,\cdot\,)$. The image of this probability by the measurable mapping Φ_u^{-1} defines a probability $\mathbb{P}_u(\,\cdot\,) = (\Phi_u^{-1})_* \mathbb{P}(\cdot \mid \uparrow u)$ on Ω (recall the covariant action of measurable mappings on probability measures, given by $f_* P(A) = P\big(f^{-1}(A)\big)$ for P a probability on X, $f : X \to Y$ and $A \subseteq Y$ measurable).

According to Prop. 3.2, the APP $\mathbb{P}_u$ is entirely characterized by its values on elementary cylinders. By definition of the image probability, these are given by:

$$\forall u' \in \mathcal{S} \quad \mathbb{P}_u(\uparrow u') = \frac{1}{\mathbb{P}(\uparrow u)} \mathbb{P}\big(\uparrow (u \cdot u')\big)\,. \tag{4}$$

Definition 3.3: An APP $\mathbb{P}$ is said to be *invariant* whenever the two following conditions are fulfilled:

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

$$\forall u \in \mathcal{S} \qquad \mathbb{P}_u = \mathbb{P}\,. \tag{6}$$

Condition (5) brings technical simplifications, but does not actually restrict generality: see the comment after Lemma 3.7. In view of (4), condition (6) can be seen as a multiplicative property: if $\mathbb{P}(\uparrow u) > 0$

for all $u \in \mathcal{S}$, then $\mathbb{P}$ is invariant if and only if $\mathbb{P}\big(\uparrow(u \cdot u')\big) = \mathbb{P}(\uparrow u) \cdot \mathbb{P}(\uparrow u')$ for all $u, u' \in \mathcal{S}$ (the "if" part uses Prop. 3.2).

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 3.4: 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 by a finite family of real numbers, very much as the finite family of individual probabilities $(p_x)_x$ characterizes a whole sequence of *iid* random variables distributed according to the family $(p_x)_x$. Observe that we proceed backward compared to the usual way in the sequential framework: instead of starting from the finite family $(p_x)_x$, 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 family of probabilistic parameters.

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

Definition 3.5: The *characteristic numbers* associated with an invariant APP $\mathbb{P}$ are defined as follows:

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

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

Although (7) makes sense for any APP, the family $(p_t)_{t\in\mathscr{T}}$ 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* since it shows how to compute the probability of basic probabilistic events by means of the characteristic numbers.

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

$$\mathbb{P}\big(\uparrow(t_1 \cdot \ldots \cdot t_k)\big) = p_{t_1} \cdot \ldots \cdot p_{t_k}\,.$$

In particular, $p_t > 0$ for all $t \in \mathscr{T}$.

In view of Lemma 3.7, the condition (5) that appears in Def. 3.3 implies no loss of generality. Indeed, if some $u \in \mathcal{S}$ satisfies $\mathbb{P}(\uparrow u) = 0$, then it means that $p_t = 0$ for some $t \in \mathscr{T}$. Removing all transitions t with $p_t = 0$ defines a process complying with Def. 3.3.

Note that, for the case $n = 1$, the characteristic numbers coincide with the individual probabilities p_x attached to the local states $x \in S^1$. Their normalization condition is obvious: $\sum_{x\in S^1} p_x = 1$. If $n > 1$ however, finding a normalization condition for $(p_t)_{t\in\mathscr{T}}$ becomes non trivial, as we shall see. In particular, the sum $\sum_{t\in\mathscr{T}} p_t$ exceeds 1 in general, since the $\uparrow t$ are not disjoint, for t ranging over $\mathscr{T}$.

4. Analysis of the ring example

In this section we develop a method to obtain a normalization condition for the characteristic numbers of an invariant APP defined on a multi-sites system. We explain the method on the example with $n = 4$ sites on a ring structure introduced above. 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 $\tau_1, \tau_2, \tau_3, \tau_4$ described above (§ 2). For $i \in \{1, 2, 3, 4\}$, let $p_i = \mathbb{P}(\uparrow \tau_i)$ be the characteristic number of $\mathbb{P}$ corresponding to transition τ_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 $T : \Omega \to \overline{\mathcal{S}}$, denoted $\omega \mapsto \omega_T$, such that $\omega_T \leq \omega$ for all $\omega \in \Omega$, and satisfying furthermore the following property:

$$\forall \omega, \omega' \in \Omega \quad \omega' \geq \omega_T \Rightarrow \omega'_T = \omega_T\,. \tag{8}$$

Stopping times are a fundamental notion in classical stochastic processes theory introduced in the 1950's. For a sequential process, a typical example of stopping time is the first instant the process hits a given state. Clearly, is 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 of samples 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 usual stopping times (associated to the canonical filtration). The author has previously introduced and used a similar notion in [5], [9].

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 sub-trajectories of ω: $N(\omega) = \{u \in \overline{\mathcal{S}}_\omega \;:\; \theta^1(u) \neq \emptyset\}$. Since we have seen that $\overline{\mathcal{S}}_\omega$ is a complete lattice, it is legitimate to consider the following *glb*:

$$\omega_U = \bigwedge N(\omega)\,. \tag{9}$$

It is easy to realize that $N(\omega)$ is non empty, and contains finite trajectories. Hence ω_U is actually a finite sub-trajectory 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, the mapping $U : \omega \in \Omega \mapsto \omega_U$ is indeed a stopping time, corresponding to the "first instant" where the first coordinate has been put in motion. This seemingly gives a special role to the first site, which is thus our *base* site. See the comment in § 6, part *Combinatorial aspects*, if the base site is changed.

If $n = 1$, ω_U identifies with the prefix of length 1 of ω. It corresponds thus to the constant time 1. As soon as $n > 1$ however, the trajectories ω_U with ω ranging over Ω, although they are finite, are of unbounded size in general. For an example on the ring structure with $n = 4$ sites, consider some sample $\omega \in \uparrow u$, where $u = \tau_2 \cdot \tau_1 \cdot \tau_3 \cdot \tau_4$ is the finite trajectory defined earlier. Then it is easy to check that $\omega_U = \tau_2 \cdot \tau_1 = (x_1, x_2 \cdot x_1, x_2, \emptyset)$. Observe that, by the stopping time property (8), the remaining part of ω is not needed to determine ω_U. Actually, for any $\omega \in \uparrow(\tau_2 \cdot \tau_1)$ one has $\omega_U = \tau_2 \cdot \tau_1$.

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 $S^1 = \{x_1, x_4\}$. 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 prior to x_1 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 $J_1, \ldots, J_K$ 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 $J_1 + \cdots + J_K$. But it cannot carry any occurrence of x_4, since the first coordinate doesn't have any. We arrive thus at the following form for ω_U:

$$\omega_U = \begin{pmatrix} x_1 \\ (x_2)^K \cdot x_1 \\ (x_3)^{J_1} \cdot x_2 \cdot \ldots \cdot (x_3)^{J_K} \cdot x_2 \\ (x_3)^{J_1 + \cdots + J_K} \end{pmatrix}. \tag{10}$$

In the previous example with $\omega \in \uparrow(\tau_2 \cdot \tau_1)$, 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:

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

where K' and $J'_1, \ldots, J'_{K'}$ 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) $p_i < 1$ for $i \in \{1, \ldots, 4\}$.
2) The law of X^1 is given by:

$$r_1 = \frac{p_1(1 - p_3)}{1 - p_2 - p_3}\,, \quad r_4 = \frac{p_4(1 - p_2)}{1 - p_2 - p_3}\,. \tag{12}$$

3) Conditionally on $X^1 = x_1$, the integer K has a geometric distribution:

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

4) Conditionally on $X^1 = x_4$, the integer K' has a geometric distribution:

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

5) For all integers $k \geq 1$, conditionally on $X^1 = x_1$ and on $K = k$, the integers $J_1, \ldots, J_k$ 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 $J'_1, \ldots, J'_k$ 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 it is part of the proposition that all quotients and geometric laws involved are well defined: $\frac{p_2}{1-p_3}, \frac{p_3}{1-p_2} \in (0, 1)$ in particular, so that $p_2 + p_3 < 1$, which was not obvious *a priori*.

Point 2 of Prop. 4.2 is enough to establish a normalization relation for the characteristic numbers of $\mathbb{P}$. We write down the total probabilities equation $\mathbb{P}(X^1 = x_1) + \mathbb{P}(X^1 = x_4) = 1$, and then we replace the probabilities with the values obtained above, to get after regrouping the terms:

$$p_1 + p_2 + p_3 + p_4 = 1 + p_1 p_3 + p_2 p_4 \,. \qquad (13)$$

Our method for obtaining a necessary condition like (13) *consists in applying the total probability law to the first coordinate of the stopping time* ω_U (9)*.*

5. Construction of invariant processes

In this section, our aim is to state a general construction result for invariant APPs (Th. 5.7 in § 5.2). We first give the consequences for our running example to underline the concrete applications that we are seeking.

Theorem 5.1: For any tuple (p_1, p_2, p_3, p_4) *of real numbers satisfying the following two conditions:*

$$\forall i \in \{1, 2, 3, 4\} \quad p_i \in (0, 1) \qquad (14)$$

$$p_1 + p_2 + p_3 + p_4 = 1 + p_1 p_3 + p_2 p_4 \,, \qquad (15)$$

there is a unique invariant APP *on the* 4*-sites ring structure with* (p_1, p_2, p_3, p_4) *as characteristic numbers associated with transitions* $(\tau_1, \tau_2, \tau_3, \tau_4)$.

Note that Th. 5.1 implies the mere existence of an invariant APP on the 4-sites ring structure, which is not obvious *a priori*. Indeed, let $p = 1 - \frac{\sqrt{2}}{2} \in (0, 1)$ be the unique non negative root of the polynomial $4p = 1 + 2p^2$ obtained from (15) with $p_i = p$ for $i \in \{1, \ldots, 4\}$. Then (p, p, p, p) is a correct tuple.

Uniqueness in Th. 5.1 is a consequence of Prop. 3.6, hence the sole existence remains to be proved. We decompose the proof in two steps. The first step (§ 5.1) demonstrates the construction of an APP. The second step (§ 5.2) consists in showing that our construction yields the expected object, by using the key technical result Th. 5.7.

5.1. First step: construction of $\mathbb{P}$

Let (p_1, p_2, p_3, p_4) be a tuple of real numbers satisfying (14)(15). The idea is to simulate the probabilistic behavior of ω_U, based on the results of Prop. 4.2. Simple algebraic manipulations based on (15) first yield the following relation:

$$p_1 + p_2 + p_3 < 1 + p_1 p_3 \,, \qquad (16)$$

which implies in particular $p_2 + p_3 < 1$. It is thus legitimate to define, inspired by (12):

$$\rho_1 = \frac{p_1(1 - p_3)}{1 - p_2 - p_3} \,. \qquad (17)$$

Furthermore, (16) implies that $\rho_1 \in (0, 1)$. It is thus legitimate to consider a random variable X defined on some external probability space $(\Xi, \mathfrak{G}, \mathbb{Q})$ with values in $S^1 = \{x_1, x_4\}$, and such that:

$$\mathbb{Q}(X = x_1) = \rho_1 \,, \quad \mathbb{Q}(X = x_4) = 1 - \rho_1 \,. \qquad (18)$$

We will freely use the usual technique of defining as many fresh random variables as we want, extending the probability space $(\Xi, \mathfrak{G}, \mathbb{Q})$ 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: indeed, we have seen that $p_2 + p_3 < 1$, and we also have $p_2 > 0$; thus $\frac{p_2}{1 - p_3} \in (0, 1)$. 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.

Finally, we introduce the *iid* integer random variables $J_1, \ldots, J_k$ and $J'_1, \ldots, J'_k$, 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 $(\Omega, \mathfrak{F})$ 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 $\bigvee_{i \geq 0}(S_0 \cdot \ldots \cdot S_i)$, which always exists in $\overline{\mathcal{S}}$, is actually an element of Ω with $\mathbb{Q}$-probability 1. Indeed, since each S_i has a positive $\mathbb{Q}$-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 $\Phi : \Xi \to \overline{\mathcal{S}}$ defined by the infinite concatenation of the S_i's, can actually be considered up to a set of zero probability as a mapping $\Phi : \Xi \to \Omega$.

Let $\mathbb{P}$ be the probability law of the infinite concatenation $\Phi = \bigvee_{i \geq 0}(S_0 \cdot \ldots \cdot S_i)$, given by the image probability $\mathbb{P} = \Phi_* \mathbb{Q}$. 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 step of the proof.

5.2. Second step: using an invariance result

Theorem 5.7 stated below is a general result for constructing invariant APPs. The 4-sites ring structure will serve as an example of its application.

Let us first introduce some notations and definitions that apply to general multi-sites systems. If $u, v \in \overline{\mathcal{S}}$ are such that $u \leq v$, we denote by $v - u$ the unique $v' \in \overline{\mathcal{S}}$ such that $v = u \cdot v'$.

Let U be a stopping time. If u is a finite trajectory, we conventionally write $u \in U$ if there exists $\omega \in \Omega$ such that $u = \omega_U$. Assume that U only takes finite values. We introduce the sequences $(U_k)_{k\geq 0}$ and $(W_k)_{k\geq 0}$, with $U_k, W_k : \Omega \to \mathcal{S}$, as follows: $U_0 = U$, $W_k = U_0 \cdot \ldots \cdot U_k$, and:

$$\forall \omega \in \Omega \quad U_{k+1}(\omega) = U\big(\omega - W_k(\omega)\big)\,. \tag{19}$$

Lemma 5.2: All W_k are stopping times, for $k \geq 0$.

Finally, we put:

$$Z_0 = \Big\{\omega \in \Omega \;:\; \bigvee_{k\geq 0} W_k(\omega) \neq \omega\Big\}\,. \tag{20}$$

Definition 5.3: A *randomized stopping time* (*r.s.t.*) is a pair (U, Q) where U is a stopping time with values in $\mathcal{S}$, and Q is a probability law for U, that is to say: Q is a probability distribution on the at most countable set of values of U.

Definition 5.4: A *r.s.t.* (U, Q) is *exhaustive* if the infinite concatenation $\bigvee_{k\geq 0}(S_0 \cdot \ldots \cdot S_k)$ of an *iid* sequence $(S_k)_{k\geq 0}$ of finite trajectories, each S_k being distributed according to Q, belongs to Ω with probability 1. In that case, the law of $\bigvee_{k\geq 0}(S_0 \cdot \ldots \cdot S_k)$ on $(\Omega, \mathfrak{F})$ is the probability *induced* by the pair (U, Q).

Of course, in Def. 5.4, the induced probability law does not depend on the particular *iid* sequence $(S_k)_{k\geq 0}$. Nevertheless, the following result states that, if (U, Q) is an exhaustive *r.s.t.*, then the sequence $(U_k)_{k\geq 0}$ introduced in (19) is a canonical choice for the *iid* sequence of Def. 5.4. This will be instrumental.

Proposition 5.5: Let (U, Q) be an exhaustive *r.s.t.*, and let $\mathbb{P}$ be the probability on $(\Omega, \mathfrak{F})$ it induces. Then, with respect to $\mathbb{P}$, the sequence $(U_k)_{k\geq 0}$ defined by (19) is *iid*, each U_k is distributed according to Q, and $\mathbb{P}(Z_0) = 0$.

Definition 5.6: A *r.s.t.* (U, Q) is *invariant* if:

1) For all $u, v \in \mathcal{S}$:

$$(v \in U \wedge u \leq v) \Rightarrow (v - u = \emptyset \vee v - u \in U)\,.$$

2) For all $u \in \mathcal{S}$ and for all $\omega \in \Omega$: $\omega \notin Z_0 \Rightarrow u \cdot \omega \notin Z_0$, where Z_0 is defined by (20).
3) There exists a family $(q_t)_{t\in\mathscr{T}}$ of positive real numbers such that for every $u \in U$, if $t_1, \ldots, t_k \in \mathscr{T}$ are such that $u = t_1 \cdot \ldots \cdot t_k$, then:

$$Q(\omega_U = u) = q_{t_1} \cdot \ldots \cdot q_{t_k}\,. \tag{21}$$

Our general result is then the following.

Theorem 5.7: The APP *induced by an exhaustive and invariant r.s.t. is invariant, and its characteristic numbers are the $(q_t)_{t\in\mathscr{T}}$ of Def. 5.6.*

Proof: Preliminaries. Let $\mathbb{P}$ be the probability on $(\Omega, \mathfrak{F})$ induced by a *r.s.t.* (U, Q), exhaustive and invariant. Recall that an equality is said to hold $\mathbb{P}$-almost surely, abbreviated $\mathbb{P}$-a.s., if it holds everywhere but maybe on a set of $\mathbb{P}$-probability 0.

Using the notations introduced above for Z_0, $(U_k)_{k\geq 0}$ and $(W_k)_{k\geq 0}$, we also denote by $W \subseteq \mathcal{S}$ the set of values taken by any of the W_k's.

For any $u \in \mathcal{S}$, we define $V_u : \Omega \to \overline{\mathcal{S}}$ as follows, for $\omega \in \Omega$:

$$V_u(\omega) = \bigwedge\big\{W_k(\omega) \;:\; W_k(\omega) \geq u\big\}\,,\ \text{if } \omega \in \uparrow u \setminus Z_0\,,$$

and by $V_u(\omega) = \omega$ otherwise. Note that $V_u(\omega) \in \mathcal{S}$ if $\omega \in \uparrow u \setminus Z_0$. We leave to the reader to check that V_u is a stopping time, using that all W_k are stopping times by Lemma 5.2.

Let $\lambda : \mathcal{S} \to \mathbb{R}$ be the real-valued function defined by $\lambda(u) = q_{t_1} \cdot \ldots \cdot q_{t_k}$ whenever $u = t_1 \cdot \ldots \cdot t_k$ with $t_1, \ldots, t_k \in \mathscr{T}$. Clearly, λ is well defined and is multiplicative: $\lambda(u \cdot v) = \lambda(u) \cdot \lambda(v)$ for all $u, v \in \mathcal{S}$. Note also that λ is positive on $\mathcal{S}$ since $q_t > 0$ for all $t \in \mathscr{T}$ by point 3 of Def. 5.6.

By (21), one has $\mathbb{P}(\omega_U = u) = Q(\omega_U = u) = \lambda(u)$ for all $u \in U$. Since U is a stopping time, it follows thus from Lemma 5.8 below, point 1: $\mathbb{P}(\uparrow u) = \mathbb{P}(\omega_U = u) = \lambda(u)$ for all $u \in U$. Since the $(U_i)_{i\geq 0}$ are *iid* by Prop. 5.5, and since λ is multiplicative, $\mathbb{P}(\uparrow u) = \lambda(u)$ also holds if $u \in W$.

Now, we claim that $\mathbb{P}(\uparrow u) = \lambda(u)$ for all $u \in \mathcal{S}$. Since λ is positive and multiplicative on $\mathcal{S}$, this will prove that $\mathbb{P}$ is invariant: see the remark after Def. 3.3. It will also prove that $\mathbb{P}(\uparrow t) = q_t$ for all $t \in \mathscr{T}$, completing the proof of the theorem.

Let us prove the claim. Let $u \in \mathcal{S}$. Observe that V_u is $\mathbb{P}$-a.s. finite on $\uparrow u$ since $\mathbb{P}(Z_0) = 0$ by Prop. 5.5. Whence, putting $K_u = \{v \in \mathcal{S} \,:\, v \in V_u \wedge v \geq u\}$ and thanks to point 1 of Lemma 5.8:

$$\uparrow u = \bigcup_{v\in K_u} \uparrow v \quad \mathbb{P}\text{-a.s.} \tag{22}$$

Since V_u is a stopping time, it follows from point 2 of Lemma 5.8 that the countable union (22) is disjoint. Since $K_u \subseteq W$, we have $\mathbb{P}(\uparrow v) = \lambda(v)$ for all $v \in K_u$. And since λ is multiplicative, we get from (22):

$$\mathbb{P}(\uparrow u) = \lambda(u) \cdot C, \quad \text{with } \ C = \sum_{v\in K_u} \lambda(v - u)\,.$$

Lemma 5.9 below implies that $v - u \in W$ for any $v \in K_u$, hence $\lambda(v-u) = \mathbb{P}\big(\uparrow(v-u)\big)$. The $\uparrow(v-u)$

are disjoint for v ranging over K_u, since the $\uparrow v$ are disjoint. Therefore, if we put: $H_u = \bigcup_{v \in K_u} \uparrow(v-u)$, we have $C = \mathbb{P}(H_u)$.

Showing that $\Omega \subseteq H_u$ $\mathbb{P}$-a.s. will complete the proof of our claim, since it yields $C = \mathbb{P}(H_u) = 1$ and thus $\mathbb{P}(\uparrow u) = \lambda(u)$. And indeed, for $\mathbb{P}$-a.s. every $\omega \in \Omega$, we have that $\omega \notin Z_0$ since $\mathbb{P}(Z_0) = 0$. By point 2 of Def. 5.6, it implies that $u \cdot \omega \notin Z_0$. Therefore $u \cdot \omega \geq v$ for some $v \in K_u$, namely for $v = V_u(u \cdot \omega)$, hence $\omega \geq v - u$, and thus $\omega \in H_u$, *qed*. □

The above proof used Lemma 5.8, elementary, and Lemma 5.9, combinatorial, below.

Lemma 5.8: Let V be a stopping time. Then:

1) For any $v \in V$: $\uparrow v = V^{-1}\big(\{v\}\big)$.
2) If $v, v' \in V$ and if $v \neq v'$, then $\uparrow v \cap \uparrow v' = \emptyset$.

Lemma 5.9: Let U be a stopping time satisfying point 1 of Def. 5.6. Let $u, v \in \mathcal{S}$ be such that $u \leq v$ and $v = v_1 \cdot \ldots \cdot v_k$ with $v_i \in U$ for all i. Then there are $v'_1, \ldots, v'_{k'} \in U$ such that $v - u = v'_1 \cdot \ldots \cdot v'_{k'}$ for some integer k'.

Thanks to Th. 5.7, we can now complete the construction for the 4-sites system with a ring structure started in § 5.1. Let U be the stopping time (9). The probability $\mathbb{Q}$ constructed in § 5.1 induces through $\mathbb{P}$ a probability law Q for ω_U, which is nothing but the law of the random trajectory S. With the language of Def. 5.3–5.4, the pair (U, Q) is thus an exhaustive randomized stopping time, and $\mathbb{P}$ is indeed the APP induced by (U, Q). Furthermore, the normalization condition (15) connects the construction of $\mathbb{Q}$ given in § 5.1 with formula (21) to yield the following result.

Proposition 5.10: In the framework of the 4-sites system with a ring structure: the pair (U, Q) is an exhaustive and invariant randomized stopping time with $q_{\tau_i} = p_i$ for $1 \leq i \leq 4$ in Def. 5.6.

In view of Th. 5.7, Prop. 5.10 implies that the APP $\mathbb{P}$ constructed in § 5.1 is invariant with $(p_i)_{1 \leq i \leq 4}$ as characteristic numbers. This completes the proof of Th. 5.1.

6. Discussion

On the invariance hypothesis. Invariance first has a temporal *stationary* interpretation: the probabilistic behavior of the system remains invariant in time.

Invariance also implies a spatial *modular* property. Indeed, consider the following graph associated with a n-sites system equipped with an invariant APP: the vertices are the sites $\{1, \ldots, n\}$, and two sites are connected if they share a common state. Assume that this graph has several connected components: these correspond to non communicating sub-systems. Then the invariant APP decomposes as the superposition of sub-APP associated to the sub-systems, and such that: 1) each sub-APP is itself invariant, and 2) the sub-APPs are independent with each other in the probabilistic sense. From the distributed systems point of view, this is a very natural and expected property.

Range of application. Our analysis method applies to any multi-sites system, without restriction on the topology of the system, although the calculations become difficult to handle by hand when the number of transitions increase. The crucial point is to determine a general form for ω_U, as we did in (10)(11), § 4. It amounts to solving for each site an enumeration problem of the form: enumerating all words w which restriction to a sub-alphabet is a given word w'. Continuing with the method implies to compute chained geometric summations. Hence the method always succeeds.

Random walks. Several other probabilistic models related to trace monoids have been studied, among which random walks, uniform distribution on traces of given length, uniform distribution on traces of given height [10]–[12]. We argue below that invariant APPs are *not* redundant with respect to random walks; neither are they with respect to the uniform distributions constructions, according to other arguments not reproduced here by lack of room. Invariant APPs are thus new, original mathematical objects.

Regarding random walks: let μ be a probability distribution on $\mathscr{T}$. The associated random walk on $\mathcal{S}$ is defined for $k \geq 1$ by $U_k = T_1 \cdot \ldots \cdot T_k$, where $(T_i)_{i \geq 1}$ is an *iid* sequence of transitions defined on some probability space $(\Xi, \mathfrak{G}, \mathbb{Q})$, and $\mathbb{Q}(T_i = \cdot) = \mu(\cdot)$ for all $i \geq 1$. Let $\Psi = \bigvee_{k \geq 1} U_k$. If $\mu(\cdot) > 0$, then $\Psi(\xi) \in \Omega$ for $\mathbb{Q}$-a.s. every $\xi \in \Xi$. The law of Ψ determines thus an APP given by $\mathbb{P} = \Psi_* \mathbb{Q}$. For the family of n-sites systems with a ring structure (generalizing our running example), our results allow to show that $\mathbb{P}$ is never invariant for $n \geq 4$.

Here is a sketch of proof for our running example with $n = 4$ sites. Assume that $\mathbb{P}' = \Psi_* \mathbb{Q}'$ is invariant for some random walk $\mathbb{Q}'$ as above. The sub-group of permutations generated by the cycle $\sigma = (1, 2, 3, 4)$ acts naturally on random walks, and also on invariant APPs. Moreover, both actions are conjugated through Ψ. Hence, putting $\mathbb{Q} = \frac{1}{4}(1 + \sigma + \sigma^2 + \sigma^3)\mathbb{Q}'$, which is the symmetric random walk, and $\mathbb{P} = \Psi_* \mathbb{Q}$, we have that $\mathbb{P} = \frac{1}{4}(1 + \sigma + \sigma^2 + \sigma^3)\mathbb{P}'$ is an invariant APP satisfying $\sigma\mathbb{P} = \mathbb{P}$. Therefore the 4 characteristic numbers of $\mathbb{P}$ are equal, and their value is necessarily

$p = 1 - \frac{\sqrt{2}}{2}$, by (13). But we also have:

$$\mathbb{P}(\uparrow\tau_1) = \sum_{k\geq 0} \mathbb{Q}\big(T_1 = \ldots = T_k = \tau_4\,,\ T_{k+1} = \tau_1\big)\,,$$

which yields $\mathbb{P}(\uparrow\tau_1) = \frac{1}{3}$, using that $\mathbb{Q}$ is symmetric. This contradicts $p = 1 - \frac{\sqrt{2}}{2}$. As a consequence, no random walk yields an invariant APP.

Combinatorial aspects. Consider for simplicity the case where all characteristic numbers of an invariant process share the same value p—call this case the *uniform case*. If f is the Möbius polynomial [13] associated with the monoid $\mathcal{S}$, we can prove that $f(p) = 0$ (I am grateful to J. Mairesse for pointing this out to me). It is the topic of an ongoing work to show that: 1) the condition $f(p) = 0$ is equivalent to the condition we obtain through our method, and 2) only the root of smallest modulus of f is suitable.

Still in the uniform case, the probability that we construct has the remarkable property of assigning an equal probability to all cylinders $\uparrow u$ such that u has a given length. No probability proposed in the literature [10]–[12] has this property. Instead, in order to "emulate" such a behavior, sequences of finite uniform and *non* coherent probability measures on traces of given length were considered. In this respect, our construction fills a theoretical gap and suggests to review results from [10]–[12] under a new light.

7. Conclusion

We have introduced and characterized invariant asynchronous probabilistic processes. In a nutshell, they are an *asynchronous version of iid sequences of random variables*. Invariance is indeed a memoryless property, expressed in an asynchronous framework.

Candidates for more general classes of processes than invariant APP are Markov asynchronous processes, introduced in [9] but for which the construction step was restricted to $n = 2$ sites only.

The theory of invariant asynchronous processes might have applications in the field of random distributed algorithms, since it introduces new paradigms for the construction of asynchronous probabilistic processes. References [14]–[16] are examples showing the diversity of this field; hence it is hard to be more specific at this stage. The similarity of the ring structure with the dining philosophers structure for instance suggests further analysis.

Applications in the analysis of network systems, such as network dimensioning, are a distant target that might become reachable once further work on the asymptotic analysis of invariant APP is done.

References

[1] B. Rozoy and P. Thiagarajan, "Event structures and trace monoids," *Theoretical Computer Science*, vol. 91, pp. 285–313, 1991.

[2] X. Viennot, "Heaps of pieces, I : basic definitions and combinatorial lemmas," in *Combinatoire énumérative*, ser. Lecture Notes in Mathematics. Springer, 1986, vol. 1234, pp. 321–350.

[3] D. Varacca, H. Völzer, and G. Winskel, "Probabilistic event structures and domains," *Theoretical Computer Science*, vol. 358, no. 2–3, pp. 173–199, 2006.

[4] S. Abbes and A. Benveniste, "Probabilistic true-concurrency models: branching cells and distributed probabilities for event structures," *Information & Computation*, vol. 204, no. 2, pp. 231–274, 2006.

[5] ——, "Probabilistic true-concurrency models: Markov nets and a law of large numbers," *Theoretical Computer Science*, vol. 390, no. 2-3, pp. 129–170, 2008.

[6] ——, "Concurrency, sigma-algebras and probabilistic fairness," in *FOSSACS*, ser. LNCS, vol. 5504, 2009, pp. 380–394.

[7] G. Winskel, "Distributed probabilistic strategies," in *Mathematical Foundations of Programming Semantics* XXIX, ser. ENTCS, 2013, pp. 379–392.

[8] S. Abbes, "On countable completions of quotient ordered semigroups," *Semigroup Forum*, vol. 3, no. 77, pp. 482–499, 2008.

[9] ——, "Markov two-components processes," *Logical Metods in Computer Science*, vol. 9(2:14), pp. 1–34, 2013.

[10] N. Saheb, "Concurrency measure in commutation monoids," *Discrete Applied Mathematics*, vol. 24, pp. 223–236, 1989.

[11] D. Krob, J. Mairesse, and I. Michos, "Computing the average parallelism in trace monoids," *Discrete Mathematics*, vol. 273, pp. 131–162, 2003.

[12] A. Bertoni and R. Radicioni, "Approximating the mean speedup in trace monoids," *International Journal of Foundations of Computer Science*, vol. 19, 2008.

[13] P. Cartier and D. Foata, *Problèmes combinatoires de commutation et réarrangements*, ser. Lecture Notes in Mathematics. Springer, 1969, vol. 85.

[14] J. Aspnes and M. Herlihy, "Fast randomized consensus using shared memory," *Journal of Algorithms*, vol. 11, no. 3, pp. 441–460, 1990.

[15] S. Alpern and S. Gal, *The theory of search game and rendezvous*. Kluwer, 2002.

[16] G. Norman, "Analyzing randomized distributed algorithms," in *Validation of stochastic systems*, ser. LNCS. Springer, 2004, vol. 2925, pp. 384–418.

Appendix

1. Proofs for Sections 3 and 4

Proof of Proposition 3.2: See the textbooks, since the family of elementary cylinders generates $\mathfrak{F}$ and is closed under finite intersections. □

For next proofs, we start with the proof of Lemma 3.7.

Proof of Lemma 3.7: Since we have observed that $u \in \mathcal{S} \mapsto \mathbb{P}(\uparrow u)$ is a multiplicative function, an induction shows that one has for all $t_1, \dots, t_k \in \mathcal{S}$:

$$\mathbb{P}\big(\uparrow(t_1 \cdot \ldots \cdot t_k)\big) = \mathbb{P}(\uparrow t_1) \cdot \ldots \cdot \mathbb{P}(\uparrow t_k)\,.$$

Since $\mathbb{P}(\uparrow t_i) = p_{t_i}$ for all $i \in \{1, \dots, k\}$ by definition of characteristic numbers, the proof of the lemma is complete. □

Proof of Prop. 3.4: 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:

$$\mathbb{P}\big(\uparrow(x_1 \cdot \ldots \cdot x_k)\big) = p_{x_1} \cdot \ldots \cdot p_{x_k}\,. \qquad (23)$$

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 state $x \in S^1$ is assigned probability p_x. Since the members of (23) are positive by (5), all p_x are positive.

Conversely, 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 it is obvious that $\mathbb{P}(\uparrow u) > 0$ for all $u \in \mathcal{S}$, and that $u \mapsto \mathbb{P}(\uparrow u)$ is multiplicative on $\mathcal{S}$. According to the remark following Def. 3.3, it implies that $\mathbb{P}$ is invariant. □

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. 3.2. □

Proof of Prop. 4.2.:

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:

$$r_1 = \sum_{K \geq 0} \sum_{J_1, \dots, J_K \geq 0} \mathbb{P}(\omega_U = u)\,, \qquad (24)$$

where u is the finite trajectory given by the right member of (10). Since U is a stopping time, and since u is a value taken by U, it follows from Lemma 5.8, point 1 (proved below):

$$\mathbb{P}(\omega_U = u) = \mathbb{P}(\uparrow u). \qquad (25)$$

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

$$u = (\tau_3)^{J_1} \cdot \tau_2 \cdot \ldots \cdot (\tau_3)^{J_K} \cdot \tau_2 \cdot \tau_1\,, \qquad (26)$$

we deduce from (25):

$$\mathbb{P}(\omega_U = u) = p_1 \cdot p_2^K \cdot p_3^{J_1 + \cdots + J_K}\,.$$

Replacing in (24), we get:

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

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 argument could be repeated after a circular permutation of $\{1, \dots, 4\}$, we actually obtain: $p_1, p_2, p_3, p_4 < 1$, which completes the proof of point 1. Calculating first the k geometric sums, we get:

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

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

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

The computation of r_4 is analogous, starting from:

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

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 (26). Using again (25) and the definition of the conditional probability, we calculate as follows:

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

Using the value of r_1 obtained above, we get:

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

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:

$$\begin{aligned}&\{X^1 = x_1 \wedge K = k \wedge (J_1,\dots,J_k) = (j_1,\dots,j_k)\}\\ &\quad= \{\omega_U = (\tau_3)^{j_1}\cdot\tau_2\cdot\ldots\cdot(\tau_3)^{j_k}\cdot\tau_2\cdot\tau_1\}\,.\end{aligned}$$

Using (25) again and the definition of conditional probability, we obtain thus:

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

We recognize thus the product of k independent geometric laws of parameter p_3 , as expected.

Proof of point 6. Analogous to the previous point. □

2. Proofs of Lemma 5.2 and 5.8 and of Propositions 5.5 and 5.10

Proof of Lemma 5.2: We prove by induction on $k \geq 0$ that W_k are stopping times. For $k = 0$, this is true since $W_k = U_0 = U$ and U is a stopping time. Assume that W_k is a stopping time, and let us prove that W_{k+1} is a stopping time. Obviously, $W_{k+1}(\omega) \leq \omega$ for all $\omega \in \Omega$. Let $\omega, \omega' \in \Omega$ such that $\omega' \geq W_{k+1}(\omega)$. By construction of W_{k+1} , we have $W_{k+1}(\omega) = W_k(\omega)\cdot u$, where $u = U\big(\omega - W_k(\omega)\big)$. Hence $\omega' \geq W_k(\omega)$. By the induction hypothesis, W_k is a stopping time. It follows thus from the stopping time property that $W_k(\omega') = W_k(\omega)$. Put $\omega'' = \omega' - W_k(\omega)$. Then $\omega'' \geq u$, and thus $U(\omega'') = u$ by the stopping time property of U. Since $W_k(\omega') = W_k(\omega)$, it follows thus: $U\big(\omega' - W_k(\omega')\big) = U\big(\omega - W_k(\omega)\big)$, and finally $W_{k+1}(\omega') = W_{k+1}(\omega)$, completing the induction. □

Proof of Proposition 5.5: Let $(S_i)_{i\geq 0}$ be an *iid* sequence defined on a probability space $(\Xi, \mathfrak{G}, \mathbb{Q})$, such that each S_i is distributed according to Q. Define $W'_i : \Xi \to \mathcal{S}$ by $W'_i = S_0 \cdot \ldots \cdot S_i$ for $i \geq 0$. Finally, let $\Phi : \Xi \to \Omega$ defined $\mathbb{Q}$-a.s. on Ξ by $\Phi(\xi) = \bigvee_{i\geq 0} W'_i(\xi)$. We prove by induction on $k \geq 0$:

$$U_k \circ \Phi = S_k \ \mathbb{Q}\text{-a.s.} \qquad W_k \circ \Phi = W'_k \ \mathbb{Q}\text{-a.s.} \qquad (27)$$

For $k = 0$, (27) is equivalent to $U \circ \Phi = S_0$ $\mathbb{Q}$-a.s., since $W'_0 = S_0$ and $W_0 = U_0 = U$ by definition. For $\mathbb{Q}$-a.s. $\xi \in \Xi$, let $\omega = \Phi(\xi) \in \Omega$. Then $\omega \geq S_0(\xi)$ since $\omega = \bigvee_{i\geq 0}\big(S_0(\xi)\cdot\ldots\cdot S_i(\xi)\big)$. Since $S_0(\xi) \in U$, it follows from the stopping time property (8) that $U(\omega) = S_0(\xi)$. Since this holds for $\mathbb{Q}$-a.s. every $\xi \in \Xi$, one has $U \circ \Phi = S_0$ $\mathbb{Q}$-a.s., as expected.

The induction step follows a similar reasoning using that W_k are stopping times (Lemma 5.2), hence we omit it. Since the indices $k \geq 0$ for which (27) hold $\mathbb{Q}$-a.s. are countably many, the equalities (27) also hold $\mathbb{Q}$-a.s. and for all $k \geq 0$.

Since $\mathbb{P} = \Phi_*\mathbb{Q}$, and since $(S_k)_{k\geq 0}$ is *iid* with S_k distributed according to Q, it follows from $U_k \circ \Phi = S_k$ that $(U_k)_{k\geq 0}$ is *iid* with U_k distributed according to Q.

From $W_k \circ \Phi = W'_k$ for all $k \geq 0$ and $\mathbb{Q}$-a.s., it follows that $\Phi^{-1}(Z_0) = \{\xi \in \Xi \ : \ \bigvee_{k\geq 0} W'_k(\xi) \notin \Omega\}$. We have $\mathbb{Q}(\bigvee_{k\geq 0} W'_k \notin \Omega) = 0$ by definition of (U, Q) being exhaustive. Hence $\mathbb{P}(Z_0) = 0$ by definition of the image probability $\mathbb{P}$. □

Proof of Lemma 5.8:

1) Let $v \in V$. Then there exists $\omega \in \Omega$ such that $v = \omega_V$. Since V is a stopping time, it follows from (8) that, for any $\omega' \in \uparrow v$, one has $\omega' \geq \omega_V$, and thus $\omega'_V = \omega_V$. Hence $\omega' \in V^{-1}\big(\{v\}\big)$. Conversely, if $\omega \in V^{-1}\big(\{v\}\big)$, then by definition of stopping times, one has $v \leq \omega$, that is to say: $\omega \in \uparrow v$.
2) Let $v, v' \in V$ be two trajectories. By the previous point, one has:

$$\uparrow v \cap \uparrow v' = V^{-1}\big(\{v\} \cap \{v'\}\big).$$

Hence, if $v \neq v'$, one has $\uparrow v \cap \uparrow v' = \emptyset$.

□

Proof of Proposition 5.10: It was already observed in the core of the paper that (U, Q) is exhaustive.

We now prove that (U, Q) is invariant (Def. 5.6), with p_i as parameters occurring in (21). Points 1–2 derive from the forms (10)(11) obtained for ω_U , or more generally from the definition (9) of U for point 1. Point 3 amounts to show that, for any $u \in U$, the probability $Q(\omega_U = u)$ is given by the following function:

$$\lambda(u) = p_1^{k_1}\, p_2^{k_2}\, p_3^{k_3}\, p_4^{k_4}\,, \qquad (28)$$

where k_1, k_2, k_3, k_4 are the numbers of occurrences of transitions $\tau_1, \tau_2, \tau_3, \tau_4$ respectively that appear in u (note that k_2, k_3 are arbitrary, while $k_1, k_4 \leq 1$ and $k_1 + k_4 = 1$).

Let $u \in U$, and assume that the first coordinate of u is x_1 . Then, according to (10), u has the following form:

$$u = \tau_3^{j_1}\cdot\tau_2\cdot\ldots\cdot\tau_3^{j_k}\cdot\tau_2\cdot\tau_1\,,$$

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

$$Q(\omega_U = u) = \\ \rho_1 \frac{1 - p_2 - p_3}{1 - p_3} \Big(\frac{p_2}{1 - p_3} \Big)^k (1{-}p_3) p_3^{j_1} \cdots (1{-}p_3) p_3^{j_k} \,. \tag{29}$$

Since $\rho_1 = \frac{p_1(1-p_3)}{1-p_2-p_3}$, (29) yields:

$$Q(\omega_U = u) = p_1 \cdot p_2^k \cdot p_3^{j_1 + \cdots + j_k} \,. \tag{30}$$

Given the values for k_1, k_2, k_3, k_4, this is indeed: $Q(\omega_U = u) = \lambda(u)$.

Assume now that the first coordinate of u is x_4 . Then u has the following form, according to (11):

$$u = \tau_2^{j_1} \cdot \tau_3 \cdot \ldots \cdot \tau_2^{j_k} \cdot \tau_3 \cdot \tau_4 \,, \tag{31}$$

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

$$Q(\omega_U = u) = (1 - \rho_1) \cdot \\ \frac{1 - p_2 - p_3}{1 - p_2} \Big(\frac{p_3}{1 - p_2} \Big)^k (1 - p_2) p_2^{j_1} \cdots (1 - p_2) p_2^{j_k} \,. \tag{32}$$

Based on (15), it is then readily seen that:

$$1 - \rho_1 = \frac{p_4(1 - p_2)}{1 - p_2 - p_3} \,. \tag{33}$$

Using (33), (32) yields:

$$Q(\omega_U = u) = p_4 \cdot p_3^k \cdot p_2^{j_1 + \cdots + j_k} \,. \tag{34}$$

Given the values for k_1, k_2, k_3, k_4, this is indeed: $Q(\omega_U = u) = \lambda(u)$. □

3. Proof of Lemma 5.9

For the proof of Lemma 5.9, we need some auxiliary results, some of which might be found in the literature for related models. For the sake of completeness, we give proofs adapted to the multi-sites model. The key result is Lemma A.4 below.

We recall first a well-known definition that applies to various models.

Definition A.1: Two finite trajectories $s, s' \in \mathcal{S}$ are said to be *compatible* if there exists a finite trajectory u such that $s \leq u$ and $s' \leq u$.

In the following lemma, we extend to $\mathcal{S}$ the independence relation $\parallel$ originally defined on $\mathscr{T}$, by defining $u \parallel u'$ for $u, u' \in \mathcal{S}$ whenever $t \parallel t'$ for any transition t, t' that compose u and u' respectively. This definition is meaningful since only the order of occurrence may change for transitions composing a given finite trajectory. Of course, $u \parallel u' \Rightarrow u \cdot u' = u' \cdot u$.

Lemma A.2: Let $x, y \in \mathcal{S}$ be two finite and compatible trajectories. Then $x \wedge y = \emptyset \Rightarrow x \parallel y$.

Proof: Let $x_1, \ldots, x_k$ and $y_1, \ldots, y_p$ be transitions such that $x = x_1 \cdot \ldots \cdot x_k$ and $y = y_1 \cdot \ldots \cdot y_p$. Assume that x and y are compatible, and that $x \wedge y = \emptyset$.

Let $i \in \{1, \ldots, n\}$ be any site, and consider the homomorphism $\theta^i : \mathcal{S} \to (S^i)^*$ defined earlier. Since θ^i is a lattice homomorphism when restricted to subtrajectories of a given trajectory (by Prop. 2.1), the assumptions imply that the sequences $\theta^i(x)$ and $\theta^i(y)$ are compatible (prefixes of a common sequence), and $\theta^i(x) \wedge \theta^i(y) = \emptyset$. It follows that, for each i, at least one of $\theta^i(x)$ and of $\theta^i(y)$ is empty. Therefore no two transitions x_j and y_q have any resource in common, and thus $x_j \parallel y_q$ for all $j \in \{1, \ldots, k\}$ and for all $q \in \{1, \ldots, p\}$. Hence $x \parallel y$. □

Lemma A.3: Let $a, b, c \in \mathcal{S}$. Assume that a and c are compatible and that $a \wedge c = \emptyset$. Then we have:

$$c \wedge (a \cdot b) = c \wedge b. \tag{35}$$

Proof: Let us first prove the formula:

$$u \wedge (v \cdot w) = u \wedge w \tag{36}$$

if u, v, w are three words on a same alphabet such that u and v are compatible (prefixes of a same word) and such that $u \wedge v = \emptyset$. Indeed, in that case, at least u or v is empty. If $u = \emptyset$ then $u \wedge (v \cdot w) = \emptyset = u \wedge w$. And if v is empty, then $u \wedge (v \cdot w) = u \wedge w$ trivially. This proves (36).

Now, to prove (35), it is enough to show that:

$$\theta^i\big(c \wedge (a \cdot b)\big) = \theta^i(c \wedge b) \tag{37}$$

for all $i \in \{1, \ldots, n\}$. Since θ^i is both a monoid homomorphism and a lattice homomorphism (as in the proof of Lemma A.2), (37) is equivalent to:

$$\theta^i(c) \wedge \big(\theta^i(a) \cdot \theta^i(b)\big) = \theta^i(c) \wedge \theta^i(b).$$

And this follows from (36). □

Lemma A.4: 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: Assume first that $a \wedge c = \emptyset$. Observe that a and c are compatible since they both divide $a \cdot b = c \cdot d$ on the left. Hence, by Lemma A.3, we have that $c \wedge (a \cdot b) = c \wedge b$. But $a \cdot b = c \cdot d$, and we obviously have $c \wedge (c \cdot d) = c$. Hence $c \wedge b = c$, and thus $c \leq b$. Let $b' \in \mathcal{S}$ be such that $b = c \cdot b'$. We put:

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

Then one has by construction: $a = a_1 \cdot a_2$, $b = b_1 \cdot b_2$ and $c = a_1 \cdot b_1$. It remains to show that $d = a_2 \cdot b_2$, that is to say: $d = a \cdot b'$. For this, we write down: $a \cdot b = c \cdot d$, or equivalently:

$$a \cdot c \cdot b' = c \cdot d. \tag{38}$$

But $a \wedge c = \emptyset$ by assumption and a and c are compatible as we already observed. Therefore, by Lemma A.2, one has $a \parallel c$, which implies $a \cdot c = c \cdot a$. Hence, (38) yields $c \cdot (a \cdot b') = c \cdot d$, and thus $a \cdot b' = d$, as expected.

For the general case, let $a', c' \in \mathcal{S}$ such that:

$$a = (a \wedge c) \cdot a'\,, \qquad c = (a \wedge c) \cdot c'\,.$$

Then $a' \wedge c' = \emptyset$, and from $a \cdot b = c \cdot d$ we deduce by left cancellability of $\mathcal{S}$: $a' \cdot b = c' \cdot d$. From the previous case, we pick $a_1', a_2, b_1, b_2 \in \mathcal{S}$ as follows:

$$\begin{aligned} a_1' &= \emptyset\,, & a_2 &= a'\,, \\ b_1 &= c'\,, & b_2 &= b'\,, \end{aligned}$$

where b' is such that $b = c' \cdot b'$. Then we have:

$$b = b_1 \cdot b_2\,, \qquad d = a_2 \cdot b_2\,.$$

Then we put $a_1 = a \wedge c$, and we get:

$$\begin{aligned} a &= (a \wedge c) \cdot a' = a_1 \cdot a_2\,, \\ c &= (a \wedge c) \cdot c' = a_1 \cdot b_1\,. \end{aligned}$$

This completes the proof in the general case. □

Lemma A.5: Let $k \geq 0$ be an integer, and let $u, v_1, \ldots, v_k$ be finite trajectories. Put $v = v_1 \cdot \ldots \cdot v_k$, and assume that $u \leq v$. Then there are finite trajectories $\zeta_1, \ldots, \zeta_k$ such that:

$$\forall i \in \{1, \ldots, k\} \quad \zeta_i \leq v_i\,, \tag{39}$$

$$v - u = (v_1 - \zeta_1) \cdot \ldots \cdot (v_k - \zeta_k)\,. \tag{40}$$

Proof: We prove the result by induction on the integer $k \geq 0$. The result is obvious if $k = 0$ or $k = 1$. Assume it is true until $k \geq 1$, and let $u, v, v_1, \ldots, v_{k+1} \in \mathcal{S}$ with $v = v_1 \cdot \ldots \cdot v_{k+1}$ and $u \leq v$. Let $c = v_1 \cdot \ldots \cdot v_k$ and $d = v_{k+1}$. Then, by assumption, we have $u \leq c \cdot d$, and thus there exists $b \in \mathcal{S}$ such that $u \cdot b = c \cdot d$.

We apply the result of Lemma A.4 to get finite trajectories a_1, a_2, b_1, b_2 such that $u = a_1 \cdot a_2$, $b = b_1 \cdot b_2$, $c = a_1 \cdot b_1$, $d = a_2 \cdot b_2$.

On the one hand, we put $\zeta_{k+1} = a_2$, so that we have:

$$b_2 = d - a_2 = v_{k+1} - \zeta_{k+1}\,. \tag{41}$$

On the other hand, from $c = a_1 \cdot b_1$, we get $a_1 \leq v_1 \cdot \ldots \cdot v_k$. We apply thus the induction hypothesis, and we obtain finite trajectories $\zeta_1, \ldots, \zeta_k$ such that $\zeta_i \leq v_i$ for all $i \in \{1, \ldots, k\}$ and:

$$c - a_1 = (v_1 - \zeta_1) \cdot \ldots \cdot (v_k - \zeta_k)\,. \tag{42}$$

Since $b_1 = c - a_1$, and since $v - u = b = b_1 \cdot b_2$, we get from (41)(42):

$$v - u = (v_1 - \zeta_1) \cdot \ldots \cdot (v_{k+1} - \zeta_{k+1})\,,$$

which completes the induction. □

Proof of Lemma 5.9: Let $u, v_1, \ldots, v_k \in \mathcal{S}$ be such that $u \leq v_1 \cdot \ldots \cdot v_k$, with $v_i \in U$ for all $i \in \{1, \ldots, k\}$. According to Lemma A.5, there are finite trajectories $\zeta_1, \ldots, \zeta_k$ with $\zeta_i \leq v_i$ for all $i \in \{1, \ldots, k\}$, and such that:

$$v - u = (v_1 - \zeta_1) \cdot \ldots \cdot (v_k - \zeta_k)\,. \tag{43}$$

Put $u_i = v_i - \zeta_i$ for $i \in \{1, \ldots, k\}$. By assumption, since U satisfies point 1 of Def. 5.6, and since $v_i \in U$ for all i, each trajectory u_i is either empty or $u_i \in U$. Removing all the empty u_i's in (43) yields indeed $v - u = v_1' \cdot \ldots \cdot v_{k'}'$ with all $v_i' \in U$ for $i \in \{1, \ldots, k'\}$, for some integer $k' \leq k$. □