An update on the topological properties of asynchronous iterations

Christophe Guyeux

February 26, 2019

Abstract

Asynchronous iterations have long been studied from a convergence perspective, and significant results have been obtained over the past fifty years, leading to the successful exploitation of these iterations in the context of asynchronous distributed computing. More recently, many advances in the theoretical study of the randomness of such asynchronous iterations have been achieved, and these results have been successfully applied in various areas of IT security in the past decade. The objective of this article is to review these various advances in the study of the disorder of asynchronous iterations, both theoretically and practically, and to present new avenues of research and the latest results. In detail, we will present the link between asynchronous iterations and a certain category of related graphs, and we will deduce a characterization of the chaos of such iterations, as mathematically defined by Devaney, for Lyapounov's exponent, etc. These results will be put in perspective with those established long ago at the level of the convergence of these asynchronous iterations. New results from measurement theory will then be discussed, and we will then provide an overview of the applications of these results in computer science, focusing in particular on information security and bioinformatics.

Keywords: distributed computing, asynchronous iterations, theoretical modelling, chaos theory.

1 Introduction

Given $f : (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}}$, the asynchronous iterations are defined as follow: $x^0 \in (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}}$, and

$$\forall n \in \mathbb{N}, \forall i \in [\![1, \mathsf{N}]\!], x_i^{n+1} \left\{ \begin{array}{ll} f(x^n)_i & \text{if } i \in s^n \\ x_i^n & \text{else.} \end{array} \right. \tag{1}$$

where $(s^n)_{n\in\mathbb{N}} \in \mathcal{P}\left([\![1, \mathsf{N}]\!]\right)$ is a sequence of subsets of $\{1, 2, ..., \mathsf{N}\}$: $\mathcal{P}(X)$ here refers to all the parts of a set X, when $[\![a, b]\!]$ is the set of integers ranging from a to b; finally, the n-th term of a sequence u is written in exponent notation u^n, as this is a vector with N coordinates: $u_1^n, \dots, u_{\mathsf{N}}^n$. Asynchronous iterations have provided, for decades, a mathematical framework for finding advanced algorithm schemas in distributed computing: roughly speaking, the coordinates of the vector x^n correspond to the calculation units, the function f is the equivalent of the calculation to be distributed, and the sequence s is the way to distribute these calculations: the sequence $\{1, 2, \dots, \mathsf{N}\}, \{1, 2, \dots, \mathsf{N}\}, \{1, 2, \dots, \mathsf{N}\}, \dots$ corresponding to a parallel calculation, when $\{1\}, \{2\}, \dots \{\mathsf{N}\}, \{1\}, \{2\}, \dots$ is a serial calculation, for example.

This mathematical formulation of asynchronous distributed algorithms has made it possible to establish various theoretical frameworks, in which proof of convergence and convergence rate calculations could be established. As an illustrative example, three special cases of the Definition 1 will be recalled in this article, who have a significant theoretical and practical interest. These are Chazan and Miranker's historical approach, asynchronous memory iterations, and Bertsekas' model. Situations for which we can be sure of the convergence of these models will be presented, before discussing the problem of the termination of algorithms. Taking a direction diametrically opposed to these convergence efforts, we will then discuss that the study of chaos of such asynchronous iterations, described as discrete dynamic systems, has been initiated this last decade, and studied in more depth in various publications that followed the founding article of [1].

This topological behaviour, which had never been examined before, has led to interesting applications of such complex dynamics in various domains of computer security like hash functions [2] and digital watermarking [3]. The dynamics studied in this framework can also derive from computers (sensor networks, neural networks, pseudo-random number generators, etc.) or biology (protein folding, genome evolution, etc.). Taking into account these many possibilities, an original approach of asynchronous iterations was to track, model and theoretically study these complex dynamics inherited from computer science or biology. The objective of this article is precisely to take stock of recent advances made in the study of the disorder of asynchronous iterations, and to put them in historical perspective with the results relating to the order and convergence of such iterations.

This article is structured as follows. In the next section, various historical approaches, among the most significant in the theoretical study of the convergence of asynchronous iterations, will be recalled. These theoretical frameworks and convergence results will be put into perspective in Section 3, in which the opposite (disorder and divergence of such iterations) will be followed. This article will conclude with a discussion, in which the applications of such an approach to disorder will be discussed, and avenues for theoretical exploration will be proposed.

2 An historical perspective of the convergence study

2.1 Three historical models

The iterations considered in this manuscript have been studied for more than fifty years, both in terms of their convergence and their applications. In this section, rather than being exhaustive, we have chosen to arbitrarily present three models that have had a significant historical impact.

2.1.1 The Chazan and Miranker model

The first theoretical work on asynchronous algorithms dates back to 1969, it focused on linear system resolutions.

The interest of asynchronism when resolving such systems, using several computers that can communicate with each other, is as follows. In an asynchronous iterative algorithm, the components of the iterated vector are updated in parallel, without any a priori order or synchronization between the machines. The asynchronous implementation allows a better recovery of communications by calculations (no downtime due to synchronizations) and allows failures (temporary or permanent). Asynchronism also has the advantage of better adaptability to changes in the computing infrastructure, such as changes in topology: changes in the number of computers, or in the possible communications between them.

This model, based on the work of Chazan and Miranker [4], Miellou [5], and Baudet [6], has been formalized on the following manner:

Definition 1 (Chazan and Miranker model) Let $\mathcal{X} = \mathbb{R}^{n_1} \times \ldots \times \mathbb{R}^{n_\alpha}$. The *asynchronous iterations* associated to $F : \mathcal{X} \to \mathcal{X}$, with initial condition $x^0 \in \mathcal{X}$, correspond to the sequence $x \in \mathcal{X}^{\mathbb{N}}$ defined by:

$$x_i^t = \begin{cases} F_i\left(x_1^{I_1^t}, \dots, x_\alpha^{I_\alpha^t}\right) & \text{si } i \in S^t \\ x_i^{t-1} & \text{si } i \notin S^t \end{cases}$$

where x_i is the sub-vector of x on $\mathbb{R}^{n_i}$, F_i is the $i-$th block-component of F, and $\forall t \in \mathbb{N}^*, S^t \subset [\![1;\alpha]\!]$ and $I^t \in \mathbb{N}^\alpha$.

In other words, at iteration t, the value of the $i-$th block-component x_i is either the value of x_i at iteration $t-1$, or the mapping $F_i\left(x_1^{I_1^t}, \dots, x_\alpha^{I_\alpha^t}\right)$, in which the current component blocks x_i^t are not taken into account, but one of their previous values $x_i^{I_i^t}$, *i.e.*, the component block that the system had at the time I_i^t. This approach allows for very general transmission delays to be taken into account. Finally, the S^t sequence indicates which cell blocks should be updated at time t. It can be seen that this model of delay iterations is a special case of the Definition 1.

In addition, it is assumed in this model that the S and I sequences test the following assumptions:

H1. The values of the iterated vector used in the calculations at the iteration t come at best from the iteration $t-1$ (notion of delay in transmission): $\forall t \in \mathbb{N}^*, I_i^t \leqslant t-1$,

H2. $I_i^t \to +\infty$, when $t \to +\infty$: the too old values of the components of the iterated vector must be definitively discarded as the calculations progress.

H3. No subvector stops to be updated (so-called pseudo-periodic strategies). In other words, t appears an infinite number of times in S.

This a specific framework of iterations, but the purpose remains relatively general: blocks are considered rather than components; real numbers are manipulated; and delays are taken into account, which depend on the blocks from which the information comes. The only constraints are that no component of the iterated vector should cease to be permanently updated, and that the values of the components associated with too old iterations should cease to be used as the calculations progress. It should be noted, to finish with the introduction of this model, that the above hypotheses H2 and H3 find their natural justification in the fact that the initiators of this theory were exclusively seeking the convergence of asynchronous iterations.

2.1.2 Asynchrones iterations with memory

Asynchronous iterations with memory use at each iteration several values of each component of the iterated vector, which may be related to different iteration numbers. This gives the following definition:

Definition 2 (Asynchrones iterations with memory) Let $n \in \mathbb{N}, \alpha \in [\![0; n]\!]$, and the following decomposition of $\mathbb{R}^n$: $\mathcal{X} = \mathbb{R}^{n_1} \times \ldots \times \mathbb{R}^{n_\alpha}$, where $\sum_{i=1}^{\alpha} n_i = n$. Let $F : \mathcal{X}^m \to \mathcal{X}$, where $m \in \mathbb{N}^*$. One *asynchronous iteration with* $m - 1$ *memories* associated to the application F and to the subset Y of the m first vectors $\{x^0, x^1, \ldots, x^{m-1}\}$, is a sequence $(x^j)_{j\in\mathbb{N}}$ of vectors of $\mathcal{X}$ such that, for $i \in [\![1; \alpha]\!]$ and $j \geqslant m$, we have:

$$\begin{cases} x_i^j &= F_i\left(z^1, \ldots, z^m\right) \quad \text{if } i \in S^j \\ \\ x_i^j &= x_i^{j-1} \quad\quad\quad\quad\quad \text{if } i \notin S^j \end{cases}$$

where $\forall r \in [\![1; m]\!]$, z^r is the vector constituted by the subvectors $z_l^r = x_l^{I_l^r(j)}$, $\left(S^j\right)_{j\geqslant m}$ is a sequence of non-empty subsets of $[\![1; \alpha]\!]$, and $I = \left\{I_1^1(j), \ldots I_\alpha^1(j), I_1^2(j), \ldots I_\alpha^2(j), I_1^m(j), \ldots I_\alpha^m(j) \;/\; j \geqslant m\right\}$ is a sequence of $[\mathbb{N}^\alpha]^m$.

In addition, S and I satisfy the following conditions:

- $\max_{r\in[\![1;m]\!]} \left\{I_i^r(j) \;/\; r \in [\![1; m]\!]\right\} \leqslant j - 1$, for all $j \geqslant m$;
- $\min_{r\in[\![1;m]\!]} \left\{I_i^r(j) \;/\; r \in [\![1; m]\!]\right\}$ tends to infinity when j tends to infinity; and
- i appears an infinite number of times in S.

These iterations, which are also a special case of the Definition 1, have been studied by Miellou [7], El Tarazi [8] and Baudet [6]. Asynchronous iterations with memory have been proposed to deal with the case where an application, whose fixed point is searched by a classical method, is not explicitly defined. They allow to assign some processors to intermediate function calculations, while the others are in charge of updating the components of the iterated vector [9].

2.1.3 Bertsekas model

The Bertsekas model of fully asynchronous iterations differs significantly from the two models presented above. By introducing another formulation of these objects, it makes it possible to better understand their nature, in particular by allowing them to be categorized by classes.

Let:

- $\mathcal{X}_1, \ldots, \mathcal{X}_n$ some sets, and $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$.
- $F_i : \mathcal{X} \to \mathcal{X}_i$ some functions, and $F(x) = (F_1(x), \ldots, F_n(x))$ defined from $\mathcal{X}$ to $\mathcal{X}$.

The Bertsekas model of totally asynchronous algorithms, another special case of the Definition 1, is the following [9].

Definition 3 (Bertsekas model) We assume that there is a sequence of events $T = \{0, 1, 2, \ldots\}$ for which one or more components x_i of the iterative vector x are updated by one of the processors of the parallel or distributed architecture.

Let be T^i the sub-series of events for which x_i is updated. We assume too that the processor updating x_i may not have access to the most recent values of the x components, and for any $t \notin T^i$, x_i remains unchanged.

An *asynchronous iteration of the Bertsekas model* is a x^t sequence of vectors of $\mathbb{R}^n$ such that for any $i \in [\![1;n]\!]$:

$$\begin{cases} x_i^{t+1} = F_i\left(x_1\left(\tau_1^i(t)\right), \ldots, x_n\left(\tau_n^i(t)\right)\right) & \text{if } t \in T^i \\ x_i^{t+1} = x_i^t & \text{if } t \notin T^i \end{cases}$$

where $\tau_l^i(t) \in [\![0;t]\!], \forall l \in [\![1;n]\!], \forall t \in T$.

The T elements are the indices of the sequence of moments at which the updates are delivered. The difference $t - \tau_l^i(t)$, on the other hand, represents the delay in accessing the $i-$th component of the iterated vector, when updating the $i-$th component at the moment t [9].

For the model to be complete, one of the following two assumptions regarding calculations and communications must be added to the above definition:

Hypothesis of total asynchronism. The T^i sets are infinite. Moreover, if t^k is a sub-series of elements of T^i that tends to infinity, then $\lim_{k\to+\infty} \tau_l^i(t_k) = +\infty$, for all $l \in [\![1;n]\!]$.

Partial asynchronism hypothesis. There is a positive integer B, called *asynchronism character*, such as:

1. For any $i \in [\![1;n]\!]$, and for any t, at least one element of the set $[\![t;t+B-1]\!]$ belongs to T^i: each component is refreshed at least once during an interval containing B refreshes.
2. $t - B < \tau_l^i(t) \leqslant t$, $\forall i, l \in [\![1;n]\!]$, and $t \in T^i$: the information used to update a component has a maximum delay of B.
3. $\tau_i^i(t) = t, \forall i \in [\![1;n]\!], \forall t \in T^i$: when updating the component assigned to it, each processor uses the last value of the same component.

Partially asynchronous iterations were introduced by Bertsekas and Tsitsiklis in [10]. They are less general than totally asynchronous iterations: markers are placed on the delays and the duration of the interval between two consecutive updates of the same component. However, they may be of great interest when excessive asynchronism leads to divergence, or does not guarantee convergence.

The use of asynchronous iterative algorithms raises two types of problems: establishing their convergence, and ensuring the termination of algorithms. These problems are reviewed in the next two sections.

2.2 On the usefulness of convergence situations

Convergence in the asynchronous model is more difficult to achieve than in the synchronous model due to the lack of synchronization, and therefore the less regular behaviour of iterative patterns. However, a number of general results could be established. They are for various contexts: (non-linear) systems, fixed point problems, *etc.*

2.2.1 Case of equation systems

The first convergence result, published by Chazan and Miranker in 1969 [4], is a necessary and sufficient condition for the convergence of the asynchronous iterations, as part of the resolution of linear systems. It requires the definition of $H-$matrices:

Definition 4 ($\boldsymbol{H}-$matrices) A matrix N is a $H-$*matrix* if the $\tilde{N}$ matrix consisting of diagonal elements of N minus the absolute value of non-diagonal elements, is a matrix such that its diagonal coefficients are strictly positive, its non-diagonal elements are negative or null, and the opposite of $\tilde{N}$ exists, and has its positive coefficients.

The necessary and sufficient condition for convergence for linear systems can then be stated [4]:

Proposition 1 *Let's say the system of equations $\mathcal{A}x^* = z$, where x^* and z are two vectors of $\mathbb{R}^n$. Then any asynchronous algorithm defined by the Chazan and Miranker model, where F then corresponds to a Jacobi type matrix per point, converges towards the solution of the problem if and only if $\mathcal{A}$ is a $H-$matrix.*

Various sufficient conditions have since been set out in specific frameworks of equation systems, both linear and non-linear [11], for the various asynchronous iteration models mentioned above. Such results can be found in [12], [13], or [9].

2.2.2 Fixed point problems

In the same vein, various convergence results for asynchronous iterations applied to fixed point problem solving have been obtained [14]. One of the most remarkable results is related to the contraction of the function, and is stated as follows [5]:

Proposition 2 *Let be E a reflexive Banach space finished product of a family of Banach spaces $(E_i, ||.||_i)$, $i \in [\![1;\alpha]\!]$. Let us denote by $\varphi(x) = (||x_1||_1, \ldots, ||x_\alpha||_\alpha)$ the canonical vectorial norm of E. Let $F : D(F) \to D(F)$ a function, where $D(F) \subset E$ is non-empty. If*

- *F has a fixed point in $x^* \in D(F)$,*
- *and F is contracting in x^* for the vectorial norm φ,*

then the asynchronous iterative algorithm defined by the Chazan and Miranker model belongs to $D(F)$, and converges to x^*.

This result has been extended to fixed point applications with relaxation parameter [8], [15], asynchronous iterative algorithms with memory in a context of classical contraction [15], and partial order [16]. Other classic results can be found in [7] and [17].

2.2.3 Bertsekas' asynchronous convergence theorem

Bertsekas' theorem provides a set of sufficient conditions for the convergence of asynchronous algorithms for fixed point problems. This result, which is based on Lyapunov's theory of stability, is based on the study of a series of sets to which the elements of the iterated vector suite belong. Its advantage is that it provides a more abstract framework for the analysis of the convergence of asynchronous iterations, which includes in particular the contraction and partial order aspects.

Proposition 3 (Asynchronous convergence of Bertsekas [18]) *Let $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ a cartesian product of sets. Suppose there is a series of non-empty subsets X^j of $\mathcal{X}$, increasing for inclusion, such as $\forall j$, there are sets $X_i^j \subset \mathcal{X}_i$ checking $X^j = X_1^j \times \ldots \times X_n^j$. Let us assume too that:*

- $F(x) \subset X^{j+1}, \forall j, \forall x \in X^j$,
- *if x is a sequence of vectors such as $x^j \in X^j$ for all j, then x tends to a fixed point of F.*

Under these conditions, and if $x^0 \in X^0$, then any fully asynchronous iteration defined according to the Bertsekas model converges to a fixed point of F.

Bertsekas and his team used this theorem to obtain convergence results for various asynchronous algorithms applied to solving a wide variety of problems: dynamic programming, search for minimum paths, optimization problems, network flow, optimal routing... Other convergence results can be found in the literature. Thus, Lubachewski and Mitra have established a sufficient convergence result for asynchronous iterations with bounded delays applied to the resolution of singular Markovian systems [19]. Finally, Frommer and Szyld studied the so-called *multisplitting* and asynchronous decomposition methods [20], [21].

2.3 The problem of algorithm termination

The final termination of the iterative algorithm must occur when the iterated vector is sufficiently close to a solution of the problem, and a special procedure must be designed to detect this termination. Since the number of iterations of the algorithm can be infinite, the calculation processes can never be inactive. There are relatively few effective termination methods for asynchronous algorithms. Indeed, termination presents many difficulties, especially in cases where processors do not share a global clock, or where communication delays can be arbitrarily long.

The most frequently used termination methods are designed empirically. For example, a particular processor can be assigned the task of observing the local termination conditions in each processor: the algorithm terminates when all local conditions are met. This approach is functional in the unique case where the degree of asynchronism is very low. Other empirical methods are possible. For example, Bertsekas and Tsitsiklis proposed in [18] that each processor send termination and restart messages to a central processor in charge of these problems. The Chajakis and Zenios [22] method does not require a central processor: a processor completes its calculations if its local termination condition is satisfied, and if it has received termination messages from other processors, and acknowledgements of all its termination messages. No termination method has been formally validated in the most general case, or almost in the most general case: the Bertsekas and Tsitsiklis solution is one of the few with formal validity. However, this method has a number of disadvantages: complex protocol, many communications, restrictive convergence conditions, *etc.*

As we can see, the problems of convergence of asynchronous iterations and their applications have been widely studied over the past fifty years. The inverse problem of the divergence of these iterations has been studied more recently, over the past decades, and has also proved to be rich in applications. The formal framework and these applications are the subject of the remainder of this article.

3 Theoretical foundations of the divergence

3.1 Asynchronous iterations as a dynamical system

In the absence of ”delay”, asynchronous iterations can be rewritten as a recurring sequence on the product space $\mathcal{X} = (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}} \times \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket)^{\mathbb{N}}$, consisting of the calculated vectors on the one hand, and the series of components to be updated on the other hand. If you enter the functions $i : \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket)^{\mathbb{N}} \to \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket)$, $(s^n)_{n\in\mathbb{N}} \longmapsto s^0$, producing the first subset of the sequence s and $\sigma : \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket)^{\mathbb{N}} \to \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket)^{\mathbb{N}}$, $(s^n)_{n\in\mathbb{N}} \longmapsto (s^{n+1})_{n\in\mathbb{N}}$, performing a shift to head the list, then the asynchronous iterations of the Equation (1) are rewritten as a discrete dynamical system G_f on $\mathcal{X}$: $X^0 \in \mathcal{X}$, et $\forall n \in \mathbb{N}$,

$$\begin{aligned} X^{n+1} &= (F_f(X_1^n, i(X_2^n)); \sigma(X_2^n)) \\ &= G_f(X^n) \end{aligned} \tag{2}$$

where

$$F_f : (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}} \times \mathcal{P}(\llbracket 1, \mathsf{N} \rrbracket) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{\mathsf{N}}, (x, e) \longmapsto (x_i \mathcal{X}_e(i) + f(x)_i \overline{\mathcal{X}_e(i)})_{i\in\llbracket 1, \mathsf{N} \rrbracket},$$

with $\mathcal{X}_X$ as the characteristic function of the set X and $\overline{x} = x + 1\ (mod\, 2)$.

Finally, a relevant distance can be introduced on $\mathcal{X}$, as follows [23]:

$$d((S,E);(\check{S};\check{E})) = d_e(E,\check{E}) + d_s(S,\check{S})$$

where $d_e(E,\check{E}) = \sum_{k=1}^{\mathsf{N}} \delta(E_k,\check{E}_k)$, δ being the Hamming distance, and

$$d_s(S,\check{S}) = \frac{9}{\mathsf{N}} \sum_{k=1}^{\infty} \frac{|S^k - \check{S}^k|}{10^k}.$$

With such a distance, we can state that [1]:

Proposition 4 *$G_f : (\mathcal{X}, d) \to (\mathcal{X}, d)$ is a continuous map.*

Asynchronous iterations had until now been studied with discrete mathematics. Such a rewrite therefore makes it possible to study them with the tools of mathematical analysis. This is all the more relevant since the results of distributed computation algorithms are usually fixed points, and mathematical analysis contains various frameworks for studying fixed points of dynamical systems. Note that we iterate on a topological space composed only of integers, when the associated algorithms manipulate machine numbers: the theoretical framework of study is exactly that of practical applications. We can also, through a topological semi-conjugation, reduce these asynchronous iterations to a simple dynamic system over an interval of $\mathbb{R}$, but the inherited topology is not that of the order [1]. This rewriting of asynchronous iterations in the form of discrete dynamic systems has allowed us to study their dynamics using mathematical analysis tools: mathematical topology, and more recently measurement theory for ergodicity concepts.

In what follows, we will first recall the key concepts of the study of the disorder and randomness of discrete dynamic systems, and then we will see to what extent asynchronous iterations can exhibit such dynamics.

3.2 The mathematical Theory of Chaos

3.2.1 Notations and terminologies

Let's start by introducing the usual notations in discrete mathematics, which may differ from those found in the study of discrete dynamic systems. The $n-$th term of the sequence s is denoted by s^n, the $i-$th component of vector v is v_i, and the $k-$th composition of function f is denoted by f^k. Thus $f^k = f \circ f \circ \ldots \circ f$, k times. The derivative of f is f', while $\mathcal{P}(X)$ is the set of subsets of X. $\mathbb{B}$ stands for the set $\{0;1\}$ with its usual algebraic structure (Boolean addition, multiplication, and negation), while $\mathbb{N}$ and $\mathbb{R}$ are the notations of the natural numbers and real ones. $\mathcal{X}^{\mathcal{Y}}$ is the set of applications from $\mathcal{Y}$ to $\mathcal{X}$, and so $\mathcal{X}^{\mathbb{N}}$ means the set of sequences belonging in $\mathcal{X}$. $\lfloor x \rfloor$ stands for the integral part of a real x (the greatest integer lower than x). Finally, $[\![a;b]\!] = \{a, a+1, \ldots, b\}$ is the set of integers ranging from a to b.

With these notations in place, we are now able to introduce various classical notions of disorder or randomness for discrete dynamic systems.

3.2.2 Devaney-based approaches

In these approaches, three ingredients are necessary for unpredictability [24]. First, the system must be inherently complicated, indecomposable: it cannot be simplified into two systems. Subsystems that do not interact, allowing a divide and conquer strategy to be adopted applied to the system is ineffective. In particular, many orbits must visit the entire space. Second, an element of regularity is added, to offset the effects of inflation. The effects of the first ingredient, leading to the fact that closed points can behave in a completely different way, and this behavior can not be predicted. Finally, system sensitivity is required as a third ingredient, so that close points can eventually become distant during system iterations. This last requirement is often implied by the first two ingredients. Having this understanding of an unpredictable dynamic system, Devaney formalized in the following definition of chaos.

Definition 5 A discrete dynamical system $x^0 \in \mathcal{X}, x^{n+1} = f(x^n)$ on a metric space $(\mathcal{X}, d)$ is chaotic according to Devaney if:

1. *Transitivity:* For each couple of open sets $A, B \subset \mathcal{X}$, $\exists k \in \mathbb{N}$ s.t. $f^k(A) \cap B \neq \varnothing$.
2. *Regularity:* Periodic points are dense in $\mathcal{X}$.
3. *Sensibility to the initial conditions:* $\exists \varepsilon > 0$ s.t.

$$\forall x \in \mathcal{X}, \forall \delta > 0, \exists y \in \mathcal{X}, \exists n \in \mathbb{N}, d(x,y) < \delta \text{ and } d(f^n(x), f^n(y)) \geqslant \varepsilon.$$

With regard to the sensitivity ingredient, it can be reformulated as follows.

- $(\mathcal{X}, f)$ is *unstable* if all its points are unstable: $\forall x \in \mathcal{X}$, $\exists \varepsilon > 0$, $\forall \delta > 0$, $\exists y \in \mathcal{X}$, $\exists n \in \mathbb{N}$, $d(x,y) < \delta$ and $d(f^n(x), f^n(y)) \geqslant \varepsilon$.
- $(\mathcal{X}, f)$ is *expansive* if $\exists \varepsilon > 0$, $\forall x \neq y$, $\exists n \in \mathbb{N}$, $d(f^n(x), f^n(y)) \geqslant \varepsilon$

The system can be intrinsically complicated too for various other understandings of this desire, which are not equivalent to each other, such as:

- *Topological mixing*: for all pairs of open disjointed sets that are not empty U, V, $\exists n_0 \in \mathbb{N}$ s.t. $\forall n \geqslant n_0, f^n(U) \cap V \neq \varnothing$.
- *Strong transitivity*: $\forall x, y \in \mathcal{X}$, $\forall r > 0$, $\exists z \in B(x,r)$, $\exists n \in \mathbb{N}$, $f^n(z) = y$.
- *Total transitivity*: $\forall n \geqslant 1$, the composition f^n is transitive.
- *Undecomposable*: it is not the union of two closed, non-empty subsets that are positively invariant ($f(A) \subset A$).

These various definitions lead to various notions of chaos. For example, a dynamic system is chaotic according to Wiggins if it is transitive and sensitive to initial conditions. It is said to be chaotic according to Knudsen if it has a dense orbit while being sensitive. Finally, we speak of expansive chaos when the properties of transitivity, regularity and expansiveness are satisfied.

3.2.3 Approach from Li and Yorke

The approach to chaos presented in the previous section, considering that a chaotic system is an inherently complicated (non-decomposable) system, with possibly an element of regularity and/or sensitivity, has been supplemented by another understanding of chaos. Indeed, as ”randomness” or ”infiniteness”, it is impossible to find a single universal definition of chaos. The types of behaviours we are trying to describe are too complicated to fit into a single definition. Instead, a wide range of mathematical descriptions have been proposed over the past decades, all of which are theoretically justified. Each of these definitions illustrates specific aspects of chaotic behaviour.

The first of these parallel approaches can be found in the pioneering work of Li and Yorke [25]. In their famous article entitled ”The Third Period Involves Chaos”, they rediscovered a weaker formulation of Sarkovskii's theorem, which means that when a discrete dynamic system $(f, [0.1])$, with continuous f, has a cycle 3, then it also has a cycle n, $\forall n \leqslant 2$. The community has not adopted this definition of chaos, as several degenerate systems satisfy this property. However, on their article [25], Li and Yorke also studied another interesting property, which led to a notion of chaos ”according to Li and Yorke” recalled below.

Definition 6 Let $(\mathcal{X}, d)$ a metric space and $f : \mathcal{X} \longrightarrow \mathcal{X}$ a continuous map on this space. $(x, y) \in \mathcal{X}^2$ is a scrambled couple of points if $\liminf_{n\to\infty} d(f^n(x), f^n(y)) = 0$ and $\limsup_{n\to\infty} d(f^n(x), f^n(y)) > 0$ (in other words, the two orbits oscillate eachother).

A scrambled set is a set in which any couple of points are a scrambled couple, whereas a Li-Yorke chaotic system is a system possessing an uncountable scrambled set.

3.2.4 Lyapunov exponent

The next measure of chaos that will be considered in this document is the Lyapunov exponent. This quantity characterizes the rate of separation of the trajectories infinitely close. Indeed, two trajectories in the phase space with initial separation δ diverge at a rate approximately equal to $\delta e^{\lambda t}$, where λ is the exponent Lyapunov, which is defined by:

Definition 7 Let $x^0 \in \mathbb{R}$ and $f : \mathbb{R} \longrightarrow \mathbb{R}$ be a differentiable function. The Lyapunov exponent is defined by $\lambda(x^0) = \lim\limits_{n\to+\infty} \dfrac{1}{n} \sum\limits_{i=1}^{n} \ln \left| f' \left(x^{i-1}\right) \right|$.

Obviously, this exponent must be positive to have a multiplication of initial errors by an exponentially increasing factor, and therefore be in a situation of chaos according to this formulation.

3.2.5 Topological entropy

Let $(\mathcal{X}, d)$ a compact metric space and $f : \mathcal{X} \longrightarrow \mathcal{X}$ a continuous map for this space. $\forall n \in \mathbb{N}$, a new distance d_n is defined on $\mathcal{X}$ by

$$d_n(x, y) = \max\{d(f^i(x), f^i(y)) : 0 \leq i < n\}.$$

With $\varepsilon > 0$ and $n \geqslant 1$, two points of $\mathcal{X}$ are ε closed compared to this measure if their first n iterates are ε closed. This measurement makes it possible to distinguish in the vicinity of an orbit the points that move away from each other during the iteration of the points that travel together. A subset E of $\mathcal{X}$ is said to be (n, ε)-separated if each pair of distinct points of E is at least ε separated in the metric d_n. Indicates by $N(n, \varepsilon)$ the maximum cardinality of a separate set (n, ε). $N(n, \varepsilon)$ represents the number of distinct orbit segments of length n, assuming that we cannot distinguish the points in ε from each other.

Definition 8 The topological entropy of the map f is equal to

$$h(f) = \lim_{\epsilon \to 0} \left(\limsup_{n \to \infty} \frac{1}{n} \log N(n, \epsilon) \right).$$

The limit defining $h(f)$ can be interpreted as a measure of the average exponential growth of the number of distinct orbit segments. In this sense, it measures the complexity of the dynamical system $(\mathcal{X}, f)$.

3.3 The disorder of asynchronous iterations

The topological space over which asynchronous iterations are defined was first studied, leading to the following result [23]:

Proposition 5 *$\mathcal{X}$ is an infinitely countable metric space, being both compact, complete, and perfect (each point is an accumulation point).*

These properties are required in a specific topological formalisation of a chaotic dynamic system, justifying their proof. Concerning G_{f_0}, it was stated that [23].

Proposition 6 *G_{f_0} is surjective, but not injective, and so the dynamical system $(\mathcal{X}, G_{f_0})$ is not reversible.*

It is now possible to recall the topological behaviour of asynchronous iterations.

We have firstly stated that [23]:

Theorem 1 *G_{f_0} is regular and transitive on $(\mathcal{X}, d)$, so it is chaotic as defined by Devaney. In addition, its sensitivity constant is greater than $\mathsf{N} - 1$.*

Thus the set $\mathcal{C}$ of functions $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ making asynchronous iterations of Definition 2 a case of chaos according to Devaney, is a not empty set. To characterize the functions of $\mathcal{C}$, we first stated that transitivity implies regularity for these particular iterated systems [26].

To achieve characterization, the function F_f allows to define a graph Γ_f, where the vertices are the vectors of $\mathbb{Z}/2\mathbb{Z}$, and there is a ridge labeled $s \in \mathcal{P}\left(\llbracket 1, \mathsf{N} \rrbracket\right)$ from i to j if, and only if $F_f(i, s) = j$. We have shown that the properties of the dynamic system G_f are strongly related to those of the graph $\mathcal{G}_f$. Thus, for example, if the latter is strongly related, then the asynchronous iterations are highly transitive and regular, and therefore chaos in Devaney's mathematical sense. Other properties, such as topological entropy, expansiveness, or sensitivity to initial conditions, defined in topological terms, could also be studied. On the other hand, the subsets of $\llbracket 1, \mathsf{N} \rrbracket$ can be drawn according to a certain probability distribution, which allows to study the associated Markov chain (ergodicity, mixing time, etc.) These various disorder results are presented below [26].

Theorem 2 *G_f is transitive, and thus chaotic according to Devaney, if and only if $\Gamma(f)$ is strongly connected.*

This characterization allows to quantify the number of functions in $\mathcal{C}$: it is equal to $\left(2^{\mathsf{N}}\right)^{2^{\mathsf{N}}}$. Then, the study of the topological properties of the disorder of these iterative systems was the subject of a more detailed study which led to the following results.

Theorem 3 *$\forall f \in \mathcal{C}$, $Per\left(G_f\right)$ is infinitely countable, G_f is strongly transitive and is chaotic according to Knudsen. It is thus undecomposable, unstable, and chaotic as defined by Wiggins.*

Theorem 4 *$(\mathcal{X}, G_{f_0})$ is topologically mixing, expansive (with a constant equal to 1), chaotic as defined by Li and Yorke, and has a topological entropy and an exponent of Lyapunov both equal to $ln(\mathsf{N})$.*

At this stage, a new type of iterative systems that only handle integers has been discovered, leading to the questioning of their computing for security applications. The applications of these chaotic machines and avenues for theoretical exploration will be proposed in the discussion section.

4 Discussion

The theoretical developments around the disorder of asynchronous iterations, presented above, have led to interesting and original advances in applications. In [1], for instance, it is explained how to design finite state machines with truly chaotic behaviour. The idea is to decompartmentalize the machine, and to use at each iteration the values provided to it at the input to calculate the value to be produced at the output. By this process, even if the machine is finite state, it does not always enter a loop, since the input is not necessarily periodic. Since then, we have continued to study these chaotic machines, proposing in particular applications concerning steganography [27,28] and digital watermarking [3,29,30], hash functions [2,31], and the generation of pseudo-random numbers [32,33].

A second field of investigation seemed very interesting based on the modeling, study and simulation of complex systems from disciplines other than computing, that is, processes whose complex dynamics can take the following form: an operation taken from a possible set of functions, and applied only to a variable subset of system coordinates. Such complex dynamics occur naturally in molecular biology, and more particularly in the spatial folding of proteins. This is why the model commonly used in protein conformation prediction tools, known as the 2D/3D HP square lattice model, has been rewritten using a discrete dynamic system in asynchronous iterations, and we proved that this system had several chaos properties [34].

Until now, the rewriting of asynchronous iterations as discrete dynamical systems has only been used to study the disorder, the maximum divergence that can be obtained by such iterations, the application framework targeted being computer security: the generation of pseudo-random numbers, hash functions, and symmetric encryption operation modes. With these elements in mind, we plan to pursue this research in various directions, building on the work carried out over many years on the convergence criteria for asynchronous iterative methods. This will make it possible to deepen the knowledge of cases of divergence (and convergence, studied in particular with tools of measurement theory) of such iterations, taking into account the delay.

Indeed, if the asynchronous iterations were initially studied for their convergence, in particular within the framework of distributed digital algorithmics, their reformulation in the form of a dynamic system, then a graph, was only studied for divergence purposes. We would therefore like to study what these reforms can bring to the study of the convergence of such asynchronous iterations. We also intend to bring convergence results from the world of dynamic systems to that of discrete mathematics. Finally, until now, the delay has not been taken into consideration: we consider that the vector at time t is deduced from the vector at time $t-1$, and depends on a continuous function and a sequence of coordinates to be updated. In other words, we assume that the stochastic process associated with asynchronous iterations satisfies Markov's property, and we wish in further work to consider the case where this is no longer true. This applies to both convergence and divergence. These results will be applied to a better understanding of the spatial and temporal evolution dynamics of biological sequences (genomes and proteins), and in particular will make it possible to increase knowledge about the generation of pseudo-random numbers.

This study was financed in part by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Interreg RESponSE project.

References

[1] C. Guyeux, *Le désordre des itérations chaotiques - Applications aux réseaux de capteurs, à la dissimulation d'information, et aux fonctions de hachage*, Éditions Universitaires Européennes, 2012, ISBN 978-3-8417-9417-8, ISBN 978-3-8417-9417-8. 362 pages. Publication de la thèse de doctorat.

[2] J. Bahi, J.F. Couchot, C. Guyeux, "Quality analysis of a chaotic proven keyed hash function", *International Journal On Advances in Internet Technology*, 5(1): 26–33, 2012.

[3] C. Guyeux, J.M. Bahi, "A new chaos-based watermarking algorithm", in *2010 International Conference on Security and Cryptography (SECRYPT)*, pages 1–4. IEEE, 2010.

[4] D. Chazan, W. Miranker, "Chaotic relaxation", *Linear algebra and its applications*, pages 199–222, 1969.

[5] J.C. Miellou, "Algorithmes de relaxation chaotique à retards", *Rairo*, R1: 148–162, 1975.

[6] G.M. Baudet, "Asynchronous Iterative Methods for Multiprocessors", *J. ACM*, 25(2): 226–244, 1978, ISSN 0004-5411.

[7] J.C. Miellou, "Itérations chaotiques à retards, étude de la convergence dans le cas d'espaces partiellement ordonnés", *C.R.A.S. Paris*, 280: 233–236, 1975.

[8] M.N.E. Tarazi, *Contraction et ordre partiel pour l'étude d'algorithmes synchrones et asynchrones en analyse numérique*, PhD thesis, Faculté des Sciences et Techniques de l'Université de Franche-Comté, Besançon, 1981.

[9] D.E. Baz, *Contribution à l'algorithmique parallèle. Le concept d'asynchronisme : étude théorique, mise en œuvre, et application*, Habilitation à diriger des recherches, Institut national polytechnique de Toulouse, 1998.

[10] D.P. Bertsekas, J.N. Tsitsiklis, "Parallel and distributed iterative algorithms: a selective survey", 1988.

[11] P. Spitéri, *Contribution à l'étude de la stabilite au sens de liapounov de certains systemes differentiels non lineaires*, PhD thesis, Université de Franche-Comté, 1974.

[12] J.M. Bahi, *Algorithmes asynchrones pour des systèmes différentiels-algébriques. Simulation numérique sur des exemples de circuits électriques*, PhD thesis, Université de Franche-Comté, 1991.

[13] J.M. Bahi, *Méthodes itératives dans des espaces produits. Application au calcul parallèle*, Habilitation à diriger des recherches, Université de Franche-Comté, 1998.

[14] J.C. Miellou, P. Spitéri, "Un critère de convergence pour des méthodes générales de point fixe", *Rairo – Modélisation mathématique et analyse numérique*, 19(4): 645–669, 1985.

[15] M.N. El Tarazi, "Some convergence results for asynchronous algorithms", *Numerische Mathematik*, 39: 325–340, 1982, ISSN 0029-599X, URL `http://dx.doi.org/10.1007/BF01407866`, 10.1007/BF01407866.

[16] M.N. El Tarazi, "Algorithmes mixtes asynchrones. Etude de convergence monotone", *Numerische Mathematik*, 44: 363–369, 1984, ISSN 0029-599X, URL `http://dx.doi.org/10.1007/BF01405568`, 10.1007/BF01405568.

[17] C. Jacquemard, *Contribution à l'étude d'algorithmes à convergence monotone*, PhD thesis, Université de Franche-Comté, 1977.

[18] D.P. Bertsekas, J.N. Tsitsiklis, *Parallel and distributed computation: numerical methods*, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989, ISBN 0-13-648700-9.

[19] B. Lubachevsky, D. Mitra, "A chaotic asynchronous algorithm for computing the fixed point of a nonnegative matrix of unit spectral radius", *J. ACM*, 33(1): 130–150, 1986, ISSN 0004-5411.

[20] A. Frommer, D.B. Szyld, "Asynchronous Two-Stage Iterative Methods", 1994.

[21] A. Frommer, H. Schwandt, Daniel, D.B. Szyld, "Asynchronous Weighted Additive Schwarz Methods", *Electronic Transactions on Numerical Analysis*, 5: 48–61, 1997.

[22] E.D. Chajakis, S.A. Zenios, "Synchronous and asynchronous implementations of relaxation algorithms for nonlinear network optimization", *Parallel Comput.*, 17(8): 873–894, 1991, ISSN 0167-8191.

[23] C. Guyeux, J. Bahi, "A Topological Study of Chaotic Iterations. Application to Hash Functions", in *CIPS, Computational Intelligence for Privacy and Security*, Volume 394 of *Studies in Computational Intelligence*, pages 51–73. Springer, 2012, URL `http://dx.doi.org/10.1007/978-3-642-25237-2_5`, Revised and extended journal version of an IJCNN best paper.

[24] E. Formenti, *Automates cellulaires et chaos : de la vision topologique à la vision algorithmique*, PhD thesis, École Normale Supérieure de Lyon, 1998.

[25] T.Y. Li, J.A. Yorke, "Period three implies chaos", *Amer. Math. Monthly*, 82(10): 985–992, 1975.

[26] J. Bahi, J.F. Couchot, C. Guyeux, A. Richard, "On the Link Between Strongly Connected Iteration Graphs and Chaotic Boolean Discrete-Time Dynamical Systems", in *FCT'11, 18th Int. Symp. on Fundamentals of Computation Theory*,

Volume 6914 of *LNCS*, pages 126–137. Oslo, Norway, Aug. 2011, URL `http://dx.doi.org/10.1007/978-3-642-22953-4_11`.

[27] J.F. Couchot, R. Couturier, C. Guyeux, "STABYLO: steganography with adaptive, bbs, and binary embedding at low cost", *annals of telecommunications-annales des télécommunications*, 70(9-10): 441–449, 2015.

[28] J.M. Bahi, J.F. Couchot, C. Guyeux, "Steganography: a class of algorithms having secure properties", in *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 209–212. IEEE, 2011.

[29] C. Guyeux, J.M. Bahi, "An improved watermarking scheme for Internet applications", in *2010 2nd International Conference on Evolving Internet*, pages 119–124. IEEE, 2010.

[30] J.M. Bahi, N. Friot, C. Guyeux, "Lyapunov exponent evaluation of a digital watermarking scheme proven to be secure", in *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 359–362. IEEE, 2012.

[31] Z. Lin, C. Guyeux, S. Yu, Q. Wang, S. Cai, "On the use of chaotic iterations to design keyed hash function", *Cluster Computing*, pages 1–15.

[32] J.F. Couchot, P.C. Heam, C. Guyeux, Q. Wang, J.M. Bahi, "Pseudorandom number generators with balanced gray codes", in *2014 11th International Conference on Security and Cryptography (SECRYPT)*, pages 1–7. IEEE, 2014.

[33] S. Contassot-Vivier, J.F. Couchot, C. Guyeux, P.C. Heam, "Random walk in a n-cube without hamiltonian cycle to chaotic pseudorandom number generation: Theoretical and practical considerations", *International Journal of Bifurcation and Chaos*, 27(01): 1750014, 2017.

[34] J.M. Bahi, N. Côté, C. Guyeux, "Chaos of protein folding", in *The 2011 International Joint Conference on Neural Networks*, pages 1948–1954. IEEE, 2011.