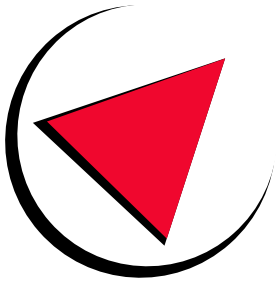

L I F C

LABORATOIRE D'INFORMATIQUE DE L'UNIVERSITE DE FRANCHE-COMTE

EA 4269

Discrete Dynamical Systems: Necessary Divergence Conditions for Synchronous Iterations

Jacques M. Bahi — Jean-François Couchot — Olivier Grasset — Christophe Guyeux

---

Rapport de Recherche no RR 2010–4

THÈME 3 – 1 september 2010

Discrete Dynamical Systems: Necessary Divergence Conditions for Synchronous Iterations

Jacques M. Bahi , Jean-François Couchot , Olivier Grasset , Christophe Guyeux

Thème 3
AND

1 september 2010

Abstract: In the domain of discrete dynamical systems, many works are focused on sufficient conditions for stability. On the contrary, this work takes place into situations where instability is awaited. These situations occur when discrete dynamical systems are used in the computer science security field. A first formalization of instability is introduced, which is called "divergence". Then, some necessary conditions for divergence are established and illustrated through a running example.

Key-words: Discrete dynamical systems, Chaotic iterations, Connection graph, Divergence proof, Stability proof.

Laboratoire d'Informatique de l'Université de Franche-Comté,
Antenne de Belfort — IUT Belfort-Montbéliard,
rue Engel Gros, BP 527, 90016 Belfort Cedex (France)
Téléphone : +33 (0)3 84 58 77 86 — Télécopie : +33 (0)3 84 58 77 32

Conditions nécessaires de divergence d'itérations synchrones de systèmes dynamiques discrets

Résumé : La plupart des travaux traitant des systèmes dynamiques discrets se focalisent sur l'expression de conditions suffisantes de convergence. Cet article se place a contrario dans un contexte où le désordre est recherché. Ce contexte se produit notamment lorsque les systèmes dynamiques discrets sont utilisés dans le domaine de la sécurité informatique. En premier lieu, une formalisation du désordre est exprimée à l'aide de notion de divergence. Ensuite des conditions nécessaires de divergence sont établies et illustrées notamment à l'aide d'un exemple fil-rouge.

Mots-clés : systèmes dynamiques discrets, iterations chaotiques, preuves de convergence et de divergence, graphe de connexion.

Laboratoire d'Informatique de l'Université de Franche-Comté,
Antenne de Belfort — IUT Belfort-Montbéliard,
rue Engel Gros, BP 527, 90016 Belfort Cedex (France)
Téléphone : +33 (0)3 84 58 77 86 — Télécopie : +33 (0)3 84 58 77 32

Discrete Dynamical Systems: Necessary Divergence Conditions for Synchronous Iterations

Jacques M. Bahi, Jean-François Couchot, Olivier Grasset, Christophe Guyeux
{jacques.bahi, jean-francois.couchot, christophe.guyeux}@univ-fcomte.fr,
olivier.grasset@edu.univ-fcomte.fr

LIFC, EA 4269, University of Franche-Comté
IUT Belfort-Montbéliard, France

Abstract. In the domain of discrete dynamical systems, many works are focused on sufficient conditions for stability. On the contrary, this work takes place into situations where instability is awaited. These situations occur when discrete dynamical systems are used in the computer science security field. A first formalization of instability is introduced, which is called "divergence". Then, some necessary conditions for divergence are established and illustrated through a running example.

1 Introduction

Chaotic iterations have been introduced on the one hand by Chazan, Miranker [5] and Miellou [7] in a numerical analysis context and on the other hand by Robert [11] and Pellegrin [8] in the discrete dynamical systems framework. In both cases, the objective was to derive conditions of convergence of such iterations to a fixed state.

Contrary to previous studies on chaotic iterations (CIs), the goal in [2] was to derive conditions under which chaotic iterations admit a chaotic behavior in a rigorous mathematical sense: convergence or stability is avoided. More precisely, we have established in [2] a link between the concept of chaotic iterations on a finite set and the notion of topological chaos, as it is defined by Devaney [6]. This formal definition of chaos allows us to apply the approach to the critical domains of security, particularly in cryptographically, secure pseudo-random number generators [4], steganography and digital watermarking [3], *etc.*

In this paper, this new approach is deepened by studying the divergence of CIs under the numerical analysis point of view. More precisely, two new convergence results are given, the second shows the first one in a different light. Two corollaries rewrite these theorems in terms of divergence. These properties are the main contributions of this paper. As a conclusion, a better understanding of the manner to use CIs in an unpredictable way is given, reinforcing by doing so the topological study formerly proposed in [2].

The rest of this paper is organized as follows. The Section 2 formalizes synchronous discrete dynamical systems. A running example is proposed for easy

understanding. Additionally, new definitions concerning convergence and divergence in parallel and chaotic modes are proposed. In Sect. 3 some necessary conditions for divergence are given and proven. Particularly, two new theorems of convergence are proven and their contrapositions lead to necessary setups for divergence. The paper ends with a conclusion section where the contribution is summed up and the planned future work is discussed.

2 Formalization

This section formalizes synchronous iterations of discrete dynamical systems (DDS) as sketched in introduction. It is a particularization of [1] to iterations without delay transmission. It furthermore introduces the running example and formalizes the convergence and divergence in the context of DDS allowing the document to be self-contained.

2.1 Algebraic View of Discrete Dynamical Systems

First of all, formalisation developed along the following lines needs often quantifiers. For conciseness reasons, quantifications are postfixed with their universe of interpretation: $\forall_{\mathcal{U}}$ (resp. $\exists_{\mathcal{U}}$) denotes the universal (resp. existential) quantification over elements taking values into the universe $\mathcal{U}$. Next, let us recall that $\mathbb{N}_k$ denotes the set $\{0, 1, \ldots, k\}$, for $k \in \mathbb{N}$.

A DDS is a collection of n components. Each component i, $1 \leqslant i \leqslant n$, takes its value X_i among a finite domain E_i. Let E be the space product $E = \Pi_{i=1}^{n} E_i$. A configuration of the system at discrete time t (also called at iteration t) is the vector

$$X^{(t)} = (X_1^{(t)}, \ldots, X_n^{(t)}) \in E.$$

The dynamic of the system is described according to a function $F : E \to E$ such that:

$$F(X) = (F_1(X), \ldots, F_n(X)).$$

In the sequel, the *strategy* $(J^{(t)})^{t \in \mathbb{N}}$ is the sequence of characteristic functions of components that may be updated at time t. Practically, each $J^{(t)}$ is represented as a $n \times n$ diagonal matrix such that $J_{ii}^{(t)} = 1$ if and only if it is allowed to modify $X_i \in E_i$ at time t. Moreover, the strategy $(J^{(t)})^{t \in \mathbb{N}}$ is *pseudo-periodic* if for each component i, the set $\{t \in \mathbb{N} \mid J_{ii}^{(t)} = 1\}$ is infinite. With these notations, the finite sequence $J^{(1)}; \ \ldots; \ J^{(t')}$ is called the *first pseudo-period*, if t' is the smallest integer of the set

$$\{t \in \mathbb{N} \mid \forall_{\mathbb{N}_n^*} \, i \, . \, \exists_{\mathbb{N}^*} \, k \, . \, k \leqslant t \wedge J_{ii}^{(k-1)} = 1\}.$$

Let I be the identity matrix of size n, and $X^0 = (X_1^0, \ldots, X_n^0)$ an initial configuration. The synchronous iterations modes (including pure parallel mode, sequential mode, and chaotic modes) are defined for times $t = 0, 1, 2, ...$, by:

$$X^{(t+1)} = (I - J^{(t)})X^{(t)} + J^{(t)}F(X^{(t)}) \tag{1}$$

Indeed:

- pure parallel iterations constrain $J^{(t)}$ to be equal to the identity matrix for any t: all the elements are updated at each iteration;
- sequential iterations constrain $J_{ii}^{(t)}$ to be null, except for i equal to $1 + (t \bmod n)$, where it is 1;
- chaotic iterations do not constrain $(J^{(t)})^{t\in\mathbb{N}}$.

Let d denotes the vectorial distance defined for any $(X, Y) \in E^2$ by [12]:

$$d(X, Y) = \begin{pmatrix} \delta_1(X_1, Y_1) \\ \vdots \\ \delta_n(X_n, Y_n) \end{pmatrix},$$

where $\delta_i, 1 \leqslant i \leqslant n$, is the discrete distance on E_i. This vectorial distance satisfies the axioms below, $\forall (X, Y, Z) \in E^3$:

$$\begin{cases} d(X, Y) = 0 \Leftrightarrow X = Y, \\ d(X, Y) = d(Y, X), \\ d(X, Z) \leqslant d(X, Y) + d(Y, Z). \end{cases}$$

Let us now recall the definition of a contracting map in this context.

Definition 1 *F is a contracting map if there exists a matrix M whose spectral radius is zero and where*

$$\forall_{E^2}(X, Y)\,.\, d(F(X), F(Y)) \leqslant Md(X, Y)$$

is established.

2.2 Running Example

We consider five elements taking their value in the set $\{0, 1\}$. Thus, a configuration is an element of $\{0, 1\}^5$, *i.e.*, a binary number between 0 and 31 (for example $(1, 0, 0, 1, 1) = 19$). Let $X \in \{0, 1\}^5$ and consider the map:

$$F(X) = \begin{cases} f_1(X_1, X_2, X_3, X_4, X_5) = X_1\overline{X_2} + \overline{X_1}X_2 \\ f_2(X_1, X_2, X_3, X_4, X_5) = \overline{X_1 + X_2} \\ f_3(X_1, X_2, X_3, X_4, X_5) = X_3\overline{X_1} \\ f_4(X_1, X_2, X_3, X_4, X_5) = X_5 \\ f_5(X_1, X_2, X_3, X_4, X_5) = \overline{X_3} + X_4 \end{cases}$$

where $\overline{a}$, sum, and product are the classical Boolean operators. It associated connection matrix is

$$B = \begin{pmatrix} 1\,1\,0\,0\,0 \\ 1\,1\,0\,0\,0 \\ 1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1 \\ 0\,0\,1\,1\,0 \end{pmatrix}$$

The connection graph is given in Figure 1. It contains five cycles.

2.3 Convergence or Divergence of a Discrete Dynamical System

Definition 2 (Convergence, Divergence) *Let be given a strategy* $(J^{(t)})^{t\in\mathbb{N}}$. *If any sequence* $(X^{(t)})^{t\in\mathbb{N}}$ *such that*

$$\begin{cases} X^{(0)} \in E \\ X^{(t+1)} = (I - J^{(t)})X^{(t)} + J^{(t)}F(X^{(t)}) \end{cases}$$

satisfies the following property:

$$(\exists_{\mathbb{N}}\, n\,.\,(\forall_{\mathbb{N}}\, t\,.\, t \geq n \Rightarrow X^{(t)} = X^{(n)})),$$

then iterations of F *are* convergent *w.r.t. the strategy* $(J^{(t)})^{t\in\mathbb{N}}$. *Otherwise iterations of* F *are* divergent.

This definition has the advantage to group both definitions of parallel mode convergence and chaotic mode convergence.

Running example. In the running example, if we take $n = 5$ and if we consider a strategy corresponding to pure parallel iterations, we have for $t \geqslant 5$ and $X^{(0)} \in E$, $X^{(t)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$. So F is convergent in pure parallel mode.

In what follows and for brevity reasons, configurations are represented as decimal numbers instead of binary numbers. The graph of parallel iterations is given in Figure 2. Starting from any configuration, the network converges to the fixed point corresponding to the decimal number 19.

An extract of the graph of chaotic iterations is given in Figure 3. Arc label is the characteristic function of activated elements (*i.e.*, the matrix $J^{(t)}$) expressed as a decimal number. It allows us to shortly represent the strategy. For instance, in this graph we only consider the pseudo-periodic strategy that alternately activates both the first two elements and the last four elements. This is formalized as $J^{2p} = \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 \end{pmatrix}$ and $J^{2p+1} = \begin{pmatrix} 0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix}$, $p = 0, 1, 2, \ldots$. The former matrix is represented as 24 and the later as 15.

Iterations do not converge for this strategy: for instance, starting from the configuration 3 (resp. configuration 7), the network goes to the configuration 11 (resp. configuration 15) and goes back to the configuration 3 (resp. configuration 7) by applying the strategy depicted above.

3 Necessary Divergence Conditions

In this section, we present necessary conditions for divergence, by making the contraposition of new theorems of convergence.

3.1 Convergence under the Contracting Condition

What follows is the first convergence scenario of this paper.

Theorem 1 (Contraction) *If F is a contracting map, then for each pseudo-periodic strategy, each chaotic iteration converges at most in n pseudo-periods.*

Proof. Since F is a contracting map, we have the following inequality due to [12, Proposition 3.1]:

$$\forall_{E^2}(X, Y)\,.\, d(F(X), F(Y)) \leqslant B(F)d(X, Y),$$

where $B(F)$ is the connection matrix associated to F. This matrix is strictly lower triangular since F is a contracting map (by swapping the variable, if necessary). Hence, there exists $p \in \mathbb{N}$ such that $B(F)^p = (0)$. Due to [12, Proposition 3.4], we have $B(F^p) \leqslant B(F)^p \leqslant (0)$, *i.e.*, F^p is a constant map. Thus, there exists $X^* \in E$ such that for all $X \in E$, $F^p(X) = X^*$. Moreover we have

$$\begin{aligned} F^{p+1}(X^*) &= F^p(F(X^*)) = X^* \\ &= F(F^p(X^*)) = F(X^*). \end{aligned}$$

So X^* is a fixed point of F. Additionally, $d(F(X), X^*) \leqslant B(F)d(X, X^*)$. The strict triangular form of $B(F)$ leads to:

1. $\delta_1(F(X), X^*) = 0$,
2. $\forall_{\mathbb{N}_n^*}\, i\,.\, i \geqslant 2 \Rightarrow \delta_i(F(X), X^*) \leqslant \sum_{j=1}^{i-1} \delta_j(X, X^*)$.

So, if the length of the first pseudo-period is t, then $X_1^{(t)} = X_1^*$. After n pseudo-periods, all of the components will be activated in the right order, to set the sum $\sum_{j=1}^{i-1} \delta_j(X, X^*)$ to 0. If $X^{(t')}$ denotes the vector after n pseudo-periods, then $d(X^{(t')}, X^*) = 0$, and thus $X^{(t')} = X^*$. Lastly, $X^{(t'+1)} = (I - J^{(t')})X^{(t')} + J^{(t')}F(X^{(t')}) = (I - J^{(t')})X^{(t')} + J^{(t')}X^{(t')} = X^{(t')} = X^*$. An immediate induction concludes the proof of this theorem.

It can be noticed that this theorem is an extension of a well-known result (see [12, Proposition 13.5]): Indeed, Robert setup to one the number of elements allowed to be modified at each iteration whereas we accept any subset of $\{1, \ldots, n\}$.

3.2 Local Convergence Result under Weaken Contracting Condition

We can weaken the contracting condition to give a local version of the previous theorem.

Theorem 2 (Local Condition) *Let $V \subseteq E$ and $X^* \in E$. If*

1. *X^* is a fixed point of F,*
2. *V is stable for any chaotic iteration of F, and*
3. *by eventually swapping variables, there exists a strictly lower triangular matrix K in $\mathbb{B}(n,n)$ such that for each $X \in V$:*

$$d(F(X), X^*) \leqslant Kd(X, X^*), \tag{2}$$

then for each pseudo-periodic strategy, each chaotic iteration which starts in V converges to X^* at most in n pseudo-periods.

Proof. Let X be a configuration in V. As K is a strictly lower triangular matrix:

1. $\delta_1(F(X), X^*) = 0$,
2. $\forall_{\mathbb{N}^*_n}\, i \,.\, i \geqslant 2 \Rightarrow \delta_i(F(X), X^*) \leqslant \sum_{j=1}^{i-1} \delta_j(X, X^*)$.

For p, $1 \leqslant p \leqslant n$, let k_p be the smallest number of iterations leading to p pseudo periods and k'_p be the smallest number s.t. $(J^{(k'_p-1)})_{pp} = 1$ and $k_{p-1} < k'_p \leqslant k_p$. In other words, k'_p is the smallest date where the element p is activated inside the p^{th} pseudo period. To achieve the proof, let us consider the following lemma.

Lemma 1 *Under the hypotheses of the previous theorem, for p, $1 \leqslant p \leqslant n$, and for any $X \in V$, we have*

$$\forall_{\mathbb{N}^*}\, t \,.\, t \geqslant k_p \Rightarrow \delta_p(X^{(t)}, X^*) = 0 \tag{3}$$

Proof of Lemma. For the first step (i.e., $p = 1$), since V is stable for any chaotic iteration of F, starting with $X \in V$ leads to $X^{(t)} \in V$ for any t, $t \in \mathbb{N}^*$. Since $\delta_1(F(X), X^*)$ is null, X^* is a fixed point, and due to the equation (1), the result is established.

For the induction step, let us suppose the result to be established until some $p-1$, $1 \leqslant p-1 < n$. Let t be k'_p, then $\delta_p(X^{(k'_p)}, X^*)$ is equal to $\delta_p(F(X^{(k'_p-1)}), X^*)$, which is lesser than or equal to $\sum_{j=1}^{p-1} \delta_j(X^{(k'_p-1)}, X^*)$. Due to the induction hypothesis, this sum is null. To conclude the proof of lemma, one notice that for a t that is greater than k'_p, $X_p^{(t)}$ is either equal to $X_p^{(t-1)}$ or equal to $F_p(X^{(t-1)})$, i.e., X_p^* for similar reasons.

Finally, the theorem is a direct consequence of this lemma.

3.3 Necessary conditions for divergence

The following corollaries give the counterpart results in terms of divergence.

Corollary 1 *Let $F : E \to E$ be an iterated function, $X^{(0)}$ be a configuration in E and σ be a strategy. If chaotic iterations following the equation (1) do not converge, then either F is not a contracting map, or σ is not pseudo-periodic.*

Now we take benefit of Theorem 2 to make the divergence possible, when a pseudo-periodic strategy is given.

Corollary 2 *Let $V \subseteq E$ and $X^* \in E$. If there is a pseudo-periodic strategy σ such that chaotic iterations starting in V do not converge to X^*, then at least one of the following condition is true:*

1. *X^* is not a fixed point of F,*
2. *V is not stable with respect to σ,*
3. *for all strictly lower triangular matrix $K \in \mathbb{B}(n,n)$, there exists $X \in V$ such that $d(F(X), X^*) > Kd(X, X^*)$.*

We can remark that if $V = E$, then the three conditions can be replaced by "F is not a contracting map", thus obtaining the Corollary 1. Indeed, conditions 1 and 3 imply that F is not a contracting map.

Running example. In the running example, F is not a contracting map, so convergence is not necessarily the sole behavior of the system. However, this lack of contraction is not sufficient to ensure divergence and the study must be deepened. Considering the same strategy (an alternating of integers {24,15}), at least three cases of divergence can be stated as early depicted in Fig. 3.

In this scenario, divergence is related to 2-cycles: the set V of Corollary 2 is equal to this 2-cycle and is stable for the strategy. However, in this situation, $\forall\, X, X^* \in V, d(F(X), X^*) = (0)$, and a matrix satisfying the third item cannot be found. So, only the first item of this corollary is satisfied.

In our understanding, a 2-cycle is a kind of weak divergence. A stronger divergence is obtained when cycles are as long as possible (cycles containing all of the nodes of the graph are desired). To achieve a kind of unpredictability when iterating, an idea is to increase the number of these edges among the graph, hoping by doing so the emergence of new paths. In our previous example, we have considered a strategy where the length of the pseudo-period is equal to 2, and we have obtained a 2-cycle. To increase the number of edges into the graph, we now consider a strategy where the length of the pseudo-period is 3: $\{24, 15, 20, 24, 15, 20, ...\}$, where the number 20 is associated to the matrix $J_{20} = \begin{pmatrix} 1&0&0&0&0\\ 0&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{pmatrix}$. We thus obtain the following 3-cycle: $7, 15, 31$. We can obtain a 6-cycle with the following strategy : $\{24, 3, 15, 3, 20, 24, 3, 15, 3, 20, 3, ...\}$. It can be noticed that to obtain a 6-cycle, a strategy where the length of the pseudo-period is 6 has been used. After having studied various examples, it appears that the lengths of cycles and pseudo-periods are strongly linked. This point will be deepen in a future work.

If we focus on the set V of the corollary, we can remark a structural change in the graph. The nodes which compose V are not the same depending on the length of the pseudo-period. Indeed if the length is equal to 2 or 3, the set of

nodes $\{3, 11, 4, 12, 7, 15\}$ is found in the different cycles. But if the length is equal to 4, 5, or 6, this set becomes to $\{5, 6, 13, 14, 29, 30\}$. This modification will be studied in a future work.

4 Conclusion and Future Work

In this paper is explained how to obtain instability in discrete dynamical systems (DDS) with synchronous iterations. This instability, denoted by "divergence" in this paper, is required when DDS are used to produce algorithms in the computer science security field, such as pseudo-random generator [4], hash functions [2], or information hiding [3]. This work enlarges the topological approach presented in [2] with a numerical analysis point of view.

Convergence under the hypotheses of contracting maps acting with pseudo-periodic strategies has been recalled in a more general framework. Additionally, a new theorem of convergence under some local hypotheses has been proved. These two theorems have led to two necessary conditions of divergence, namely the Corollaries 1 and 2.

Pseudo-periodic strategies play an important role in these corollaries: without this hypothesis, new local fixed points can appear. The consequences of this fact in terms of divergence will be studied in a future work. Additionally, trap domains and attractors introduced in [10,9] will be used to obtain a better understanding of the conditions under which a given DDS becomes unpredictable. We plan to express new links between divergence and graphs of chaotic iterations, of connection in terms of graph theory. Lastly, we will deepen the study of the necessary conditions under which divergence is obtained, and discuss about the consequences concerning potential applications in the computer science security field recalled above.

References

1. J. M. Bahi, S. Contassot-Vivier, and J.-F. Couchot. Convergence results of combining synchronism and asynchronism for discrete-state discrete-time dynamic network. Research Report RR2010-02, LIFC - Laboratoire d'Informatique de l'Université de Franche Comté, May 2010.
2. J. M. Bahi and C. Guyeux. Hash functions using chaotic iterations. *Journal of Algorithms & Computational Technology*, 4(2):167–181, 2010. Accepted manuscript. To appear.
3. J. M. Bahi and C. Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT 2010, International conference on security and cryptography*, pages ***–***, Athens, Greece, 2010. To appear.
4. J. M. Bahi, C. Guyeux, and Q. Wang. A novel pseudo-random generator based on discrete chaotic iterations. In *Internet 2009*, pages 71–76, Cannes, France, 2009.
5. D. Chazan and W. Miranker. Chaotic relaxation. *Linear algebra and its applications*, pages 199–222, 1969.
6. R. L. Devaney. *An Introduction to Chaotic Dynamical Systems, 2nd Edition*. Westview Pr., 2003.

7. J.-C. Miellou. Algorithmes de relaxation chaotique à retards. *Rairo*, R1:148–162, 1975.
8. D. Pellegrin. *Algorithmique discrète et réseaux d'automates*. PhD thesis, Grenoble, 1986.
9. A. Richard. Positive circuits and maximal number of fixed points in discrete dynamical systems. *Discrete Applied Mathematics*, 157(15):3281–3288, 2009.
10. A. Richard. Negative circuits and sustained oscillations in asynchronous automata networks. *Advances in Applied Mathematics*, 44(4):378–392, 2010.
11. F. Robert. *Discrete Iterations: A Metric Study*, volume 6 of *Springer Series in Computational Mathematics*. Springer, 1986.
12. F. Robert. *Les systèmes dynamiques discrets*, volume 19 of *Mathématiques et Applications*. Springer, 1995.

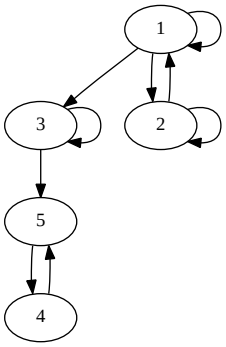

Fig. 1. Connection graph of running example

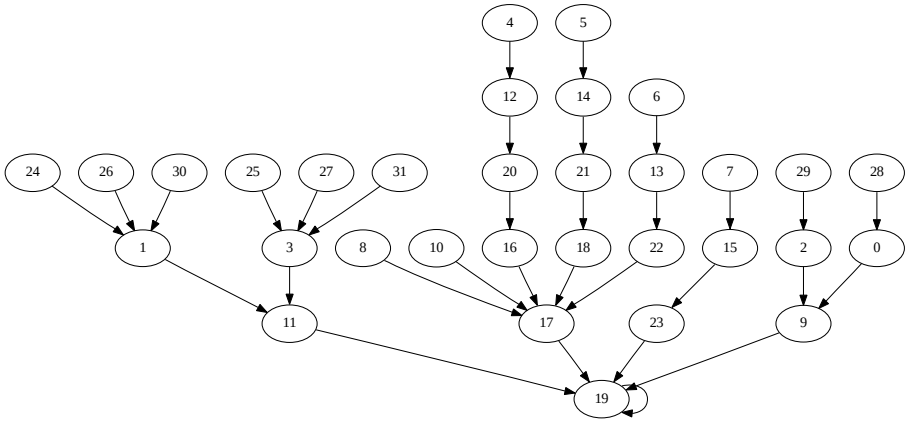

Fig. 2. Parallel iterations of running example

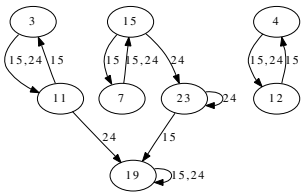

Fig. 3. Excerpt of chaotic iterations of running example

Laboratoire d'Informatique de l'université de Franche-Comté
UFR Sciences et Techniques, 16, route de Gray - 25030 Besançon Cedex (France)

LIFC - Antenne de Belfort : IUT Belfort-Montbéliard, rue Engel Gros, BP 527 - 90016 Belfort Cedex (France)
LIFC - Antenne de Montbéliard : UFR STGI, Pôle universitaire du Pays de Montbéliard - 25200 Montbéliard Cedex (France)

http://lifc.univ-fcomte.fr