Observability and Reconstructibility of Affine Cellular Automata: Example on Random Number Reconstruction

Théo Plénet, Samira El Yacoubi, Clément Raievsky, Laurent Lefevre

Observability and Reconstructibility of Affine Cellular Automata: Example on Random Number Reconstruction.

Théo Plénet[1⋆], Samira El Yacoubi[1], Clément Raïevsky[2], Laurent Lefèvre[2]

[1] IMAGES Espace-Dev, Univ Perpignan Via Domitia, Perpignan, France
ESPACE-DEV, IRD, Univ Montpellier, Montpellier France;
[2] LCIS, Univ. Grenoble Alpes, Grenoble INP, Valence, France

In this paper, the notions of observability and reconstructibility are defined for cellular automata. We extend the Kalman observability criterion to affine cellular automata with a time-varying output operator and apply this characterisation property to the observability and reconstructibility through mobile sensors. Then, a short and simple example is presented in order to detail the method for assessing the observability and reconstructibility of an affine cellular automata. Finally, an example where the random number stream is reconstructed from a cellular automata random number generators is considered in order to illustrate the concept of observability in the context of cybersecurity applications.

Key words: cellular automata, observability, reconstructibility, mobile sensors, Kalman criterion, RNG Attack

1 INTRODUCTION

Observability is a concept studied in systems theory that consists in looking for the extent to which the internal states of a system can be inferred from data and measurements available on the system. However,

⋆ email: theo.plenet@univ-perp.fr

when dealing with complex systems, our limited ability to estimate the internal state from experimentally accessible outputs severely limits their complete description. The problem lies in the ability to build sensors capable of providing measurements allowing to reconstruct the internal state of the system and thus to make it observable. For Distributed Parameter Systems (DPS) analysis and control, the sensors structures play an important role regarding the observability issue. Observability as well as controllability which are important concepts in control theory were introduced by Kalman [15] for finite dimensional linear systems and well developed in the last fifty years for more general systems [19, 24, 20, 1, 12]. Their study through the concepts of sensors and actuators has also been of great interest in the automatic control community [10, 11]. While controllability focuses on the steering capabilities of the controlled evolution processes, observability is dealing with the ability to reconstruct the initial system state, given sufficient knowledge of the system dynamics through some output measurements.

This paper focuses on the observability problem of a distributed parameter system that is assumed to be autonomous. Motivated by some real distributed environmental phenomena (e.g. wildfires, weather, atmosphere or river pollution) we use a group of mobile robots equipped with different sensors [6]. Robots share information with each other and we simply call this group a network of mobile sensors. This network constitute a natural extension of sensors and offers more flexibility in collecting distributed information within its environment. A model-based approach through trajectory optimisation (for the mobile sensors) with partial differential equation constraints (PDE, for the environment dynamical model) would lead to very complicated [2] - sometimes intractable - mathematical issues, particularly in the case of complex geometries and/or non linear dynamics.

Among other modelling approaches that have been developed to describe life phenomena which exhibit complex behaviours, cellular automata (CA) provide powerful models usually viewed as a counterpart of PDEs for modelling spatio-temporal systems. CA are mathematical model which is perfectly suited to complex systems containing a large number of discrete elements with local interactions, for example Ising model, fluid dynamics, traffic flow, growth of crystal [28, 5, 3]. They were first introduced by [32], as a modelling tool to investigate self-organisation and self-reproduction phenomena and become increasingly attractive thanks to their ability to exhibit a wide variety of amazingly

complex behaviours while offering an easiness of implementation.

The research activity regarding cellular automata was recently oriented towards systems theory when CA were presented as distributed parameter system and allowed the study of several concepts of control theory [13]. New tools have been investigated in this direction in order to obtain characterisation results that can extend or substitute the most commonly used Kalman criterion. An interesting study on controllability of CA has been carried out in [9] that highlighted new ways to prove the controllability of complex systems. It mainly focused on regional controllability of Boolean CA that has been proved using Markov chains or graph theory tools [7, 8]. The boundary regional controllability has also been investigated for linear (additive) Boolean CA for which some characterisation results using the Kalman condition were given.

Our interest in this paper is focused on observability as a dual notion of controllability. The purpose is to apply the above mentioned tools in order to prove the observability according to the choice of sensor structures, locations and types (mobile or fixed). We show for the 1D case, that observability of linear (affine) CA can be characterised using the observability matrix.

Although we were initially motivated by the observation of physical systems by a mobile sensor network, observability and reconstructibility can be used in other fields. In this paper, we present a rather interesting example where the observability of affine CA allow the recovery of the random number sequence generated by a random number generating cellular automaton [29]. Past and future random numbers can be deduced from some information about certain random numbers. The attacks by which the random number information is recovered are not described in this paper because the reconstruction method is independent of those. Furthermore, the choice of attack often depends on the physical or digital medium used by the random number generator.

The article is organised as follows: In section 2, the concepts of observability and reconstructibility for cellular automata are defined. Section 3 gives the observability criterion for affine CA as an extension of the rank condition established by Kalman. A complete study of affine CA by means of mobile sensors is carried out in the following section and the last section is dedicated to an important application of the concept in cybersecurity.

2 OBSERVABILITY AND RECONSTRUCTIBILITY FOR CELLULAR AUTOMATA

2.1 Cellular Automata Model

Definitions for control and observation of cellular automata has already been given in [13]. Throughout this article we will reuse these definitions but for the consistency of this article we will redefine some of these.

First, a cellular automaton (CA) is formulated as the quadruple $\mathcal{A} = \{\mathcal{L}, \mathcal{S}, \mathcal{N}, f\}$ where $\mathcal{L}$ is a d-dimensional finite lattice of cells c; $\mathcal{S}$ denotes a discrete set of states $\mathcal{S} = \{0, 1, \ldots, k-1\}$; $\mathcal{N}$ is the mapping which defines the cell's neighbourhood; and f is the transition function. In this paper, the set of states $\mathcal{S}$ must be a field, i.e. that $\mathcal{S}$ is a finite commutative ring with a prime number of states. This set may also be called $\mathbb{Z}/k\mathbb{Z}$, with k a prime number of state.

Throughout this article, we will forego the local properties of CA to focus on their global properties. Therefore, we define the state s_t of the whole CA at time t and the global transition function F.

$$\begin{aligned} s_t \colon \mathcal{L} &\to \mathcal{S} \\ c &\mapsto s_t(c) \end{aligned} \tag{1}$$

$$\begin{aligned} F \colon \mathcal{S}^{\mathcal{L}} &\to \mathcal{S}^{\mathcal{L}} \\ s_t &\mapsto F(s_t) = s_{t+1} \end{aligned} \tag{2}$$

The evolution of the CA can now be written in a form similar to the study of linear systems:

$$\begin{cases} s_{t+1} & = F(s_t) \\ s_0 & \in \mathcal{S}^{\mathcal{L}} \end{cases} \iff s_t = F^t(s_0),\, t \in I \tag{3}$$

With $I = \{0, 1, \ldots, T\}$ a discrete time horizon.

2.2 Sensor Model and Output Operator

To represent the measurements of a physical system modelled by a CA, we extend the previous global CA dynamical models with sensors and and output operator. Their measurements will allow us to reconstruct the initial state of the physical system using the criteria of observability and reconstructibility.

We denote q_i, $i \in [\![1; Q]\!]$, the sensor measuring the state of several cells (we note $\mathcal{L}_{q_i} \subset \mathcal{L}$ the set of these cells). The set of all cells measured by the sensors is denoted $\mathcal{L}_q$ defined by:

$$\mathcal{L}_q = \bigcup_{i=1}^{Q} \mathcal{L}_{q_i} \tag{4}$$

Among all the sensors some can be considered as mobile sensors, i.e. the set of cells they measure changes as a function of time. We will then note $\mathcal{L}_{q_{i,t}}$ the set of cells measured by the sensor q_i at time t and $\mathcal{L}_{q_t}$ the set of cells measured by all the sensors.

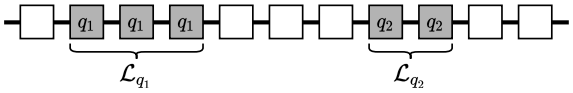

FIGURE 1
Two sensors measuring a one-dimensional CA. Grey cells are measured by a sensor, either q_1 or q_2.

Given this formalisation of sensors' position and motion, we are able to build an operator H_t which maps, at time t, the configuration s_t of the CA with the measurements θ_t obtained by whole set of sensors.

$$\begin{aligned} H_t \colon \mathcal{S}^{\mathcal{L}} &\to \mathcal{O} \\ s_t &\mapsto \theta_t := s_t|_{\mathcal{L}_{q_t}} \end{aligned} \tag{5}$$

, where $s_t|_{\mathcal{L}_{q_t}}$ denotes the restriction of the state s_t to the set $\mathcal{L}_{q_t}$ of cells effectively measured at time t.

By augmenting the state representation (3) with the output θ_t, the system turns into :

$$\begin{cases} s_{t+1} & = F(s_t) \\ \theta_t & = H_t(s_t) \\ s_0 & \in \mathcal{S}^{\mathcal{L}} \end{cases} \tag{6}$$

2.3 Observability and Reconstructibility

Observability, as defined by Kalman [16], determines if it is possible to reconstruct the state of a system based on the measurements obtained

from one or more sensors. Observability focuses on reconstructing the initial state of the system whereas reconstructibility focuses on reconstructing the current state of the system. In the case of discrete time systems, both of these are not equivalent. With a deterministic system, observability is a more general concept as knowing the initial state implies knowing all the evolution of the system. Reconstructibility, on the other hand, is less general but can be easier to assess [23].

To reconstruct the state of the system, observability and reconstructibility uses a sequence of several measurements. This vector composed of the successive output vectors (measurements) generated by the output operator H_t is called an output sequence. The sequence of measurements spanning from t_0 to t_T is noted $\Theta_{0,T} = (\theta_0, \theta_1, ..., \theta_{T-1})$.

An output sequence can be computed from the initial state s_0 using the operator:

$$\Theta_T \colon s_0 \mapsto \Theta_{0,T} = (H_0(s_0), H_1 \circ F(s_0), \ldots, H_{T-1} \circ F^{T-1}(s_0)) \quad (7)$$

Definition 1 (State Observability). A configuration $s_0 \in \mathcal{S}^{\mathcal{L}}$ of a cellular automaton $\mathcal{A}$ is observable by an output operator H at time T if and only if it is possible to reconstruct this initial state s_0 from the corresponding output sequence $\Theta_{0,T}$.

Definition 2 (Global Observability). A cellular automaton $\mathcal{A}$ is observable by an output operator H at time T if and only if all states $s \in \mathcal{S}^{\mathcal{L}}$ are observable by this output operator.

The definition 2 of the global observability is equivalent to the following proposition:

$$\forall s'_0, s''_0 \in \mathcal{S}^{\mathcal{L}}, \Theta_T(s'_0) = \Theta_T(s''_0) \implies s'_0 = s''_0 \quad (8)$$

Definition 3 (State Reconstructiblity). A state $s_T \in \mathcal{S}^{\mathcal{L}}$ of a cellular automaton $\mathcal{A}$ is reconstructible by an output operator H at time T if and only if it is possible to reconstruct the current state s_T from the corresponding output sequence $\Theta_{0,T}$.

Definition 4 (Global Reconstructiblity). A cellular automaton $\mathcal{A}$ is reconstructible by an output operator H at time T if and only if all states $s \in \mathcal{S}^{\mathcal{L}}$ are reconstructible by this output operator.

The definition 4 of the global reconstructibility is the equivalent to the following proposition:

$$\forall s'_0, s''_0 \in \mathcal{S}^{\mathcal{L}}, \Theta_T(s'_0) = \Theta_T(s''_0) \implies F^T(s'_0) = F^T(s''_0) \quad (9)$$

3 OBSERVABILITY CRITERION FOR AFFINE CELLULAR AUTOMATA

This section presents the extension of the Kalman criterion, usually used to determine the observability of continuous time or discrete time linear systems, to linear cellular automata and more generally to affine CA.

3.1 Affine and Linear Cellular Automata

Before presenting the extension of the Kalman criterion to CA, we need first to express the state of a CA in the form of a state vector and then to define the properties of a CA that make it linear or affine.

To express a CA state as a state vector, the CA must have a finite lattice and its cells must be arranged in an arbitrary order. Under this assumption, an isomorphism ξ between the CA state s_t and a state vector representation x_t can be defined.

$$\begin{aligned} \xi &: \mathcal{S}^{\mathcal{L}} \to \mathcal{S}^N \\ s_t \mapsto x_t &= \begin{pmatrix} x_t^1 \\ x_t^2 \\ \dots \\ x_t^N \end{pmatrix} \end{aligned} \tag{10}$$

, where $N = |\mathcal{L}|$ and x_t^i represents the state of the cell c_i at time t.

In the similar way, it is possible to represent the outputs θ_t as a vector denoted y_t thanks to the isomorphism χ defined by :

$$\begin{aligned} \chi &: \mathcal{O} \to \mathcal{S}^Q \\ \theta_t \mapsto y_t &= \begin{pmatrix} y_t^1 \\ y_t^2 \\ \dots \\ y_t^Q \end{pmatrix} \end{aligned} \tag{11}$$

, where $Q = |\mathcal{L}_q|$ and y_t^i represents the ith output at time t.

With this change of basis, the operators F and H_t become respectively $\tilde{F} : \mathcal{S}^N \to \mathcal{S}^N$ and $\tilde{H}_t : \mathcal{S}^N \to \mathcal{S}^Q$ so that :

$$\begin{cases} x_{t+1} & = \tilde{F}(x_t) \\ y_t & = \tilde{H}_t(x_t) \\ x_0 & = \xi(s_0), s_0 \in \mathcal{S}^{\mathcal{L}} \end{cases} \tag{12}$$

Definition 5 (Affine). A cellular automaton (resp. output operator) is affine if and only if $\tilde{F}$ (resp. $\tilde{H}$) is an affine map. Moreover, this affine map can be written in the form of a linear map and a constant, which can be written as a matrix A (resp. C_t) and a constant $\eta = \tilde{F}(0)$ (resp. $\gamma_t = \tilde{H}_t(0)$). The evolution of the cellular automaton can then be written as:

$$\begin{cases} x_{t+1} & = \tilde{F}(x_t) = Ax_t + \eta \\ y_t & = \tilde{H}_t(x_t) = C_t x_t + \gamma_t \\ x_0 & = \xi(s_0), s_0 \in \mathcal{S}^{\mathcal{L}} \end{cases} \tag{13}$$

If an affine CA has a null η constant, this CA is said linear. In the case of elementary CA [33], linear CA are called additive CA. Also, affine CA will be the complement of additive CA. For example, rule 90 and 150 will be considered linear rules, but their complementary rule (165 and 105) will be considered affine rules.

The trajectory of the CA state may be explicitely written in terms of the initial state x_0, as:

$$\begin{cases} x_{t+1} & = A^{t+1}x_0 + J_t\eta \\ x_0 & = \xi\left(s_0\right), s_0 \in \mathcal{S}^{\mathcal{L}} \end{cases} \tag{14}$$

with $J_t = \sum_{k=0}^{t} A^k$

The output sequence Θ_T can also be represented in affine form using the affine forms of the transition function and the output operator. We note Y_T the output sequence for T outputs where O_T is the linear map and Γ_T the constant vector:

$$Y_T = \begin{bmatrix} y_0 \\ y_1 \\ \cdots \\ y_{T-1} \end{bmatrix} = \underbrace{\begin{bmatrix} C_0 \\ C_1 A \\ \cdots \\ C_{T-1}A^{T-1} \end{bmatrix}}_{O_T} x_0 + \underbrace{\begin{bmatrix} \gamma_0 \\ C_1 J_0 \eta + \gamma_1 \\ \cdots \\ C_{T-1}J_{T-2}\eta + \gamma_{T-1} \end{bmatrix}}_{\Gamma_T} \tag{15}$$

with $J_t = \sum_{k=0}^{t} A^k$.

We call O_T the observability matrix as this linear map carries the injectivity property of the output sequence and therefore the observability property.

3.2 Extension of the Kalman Observability Criterion

The Kalman observability criterion [16, 15] is derived from the control of linear dynamical systems and proves the controllability (resp. observability) of a dynamical system when the system is controlled (observed). It has been generalised to discrete-time systems [26] and in this paper we generalise it to cellular automata.

Theorem 1 (Kalman Criterion). Let $\mathcal{A}$ and H_t be an affine CA and affine output operator; A, C_t their matrix form; and η and γ_t their constants.

The pair $(\mathcal{A}, H_t)$ (i.e. the cellular automaton $\mathcal{A}$ with the output operator H_t) is observable if and only if there exists $T \in \mathbb{N}$ such that:

$$rank\ O_T = rank \begin{bmatrix} C_0 \\ C_1 A \\ .. \\ C_{T-1} A^{T-1} \end{bmatrix} = N \tag{16}$$

Proof. Let $\mathcal{A}$ an affine CA and A and η its associated matrix and constant. Let H_t be a time dependant affine output operator associated with the matrix C_t and the constant γ_t. Then, let $x_0 \in \mathcal{S}^N$ the initial state and $Y_T = \begin{bmatrix} y_0 & y_1 & \dots & y_{T-1} \end{bmatrix}$ the output sequence generated by the output operator such that $Y_T = O_T x_0 + \Gamma_T$.

Considering the definition 2 of global observability, then:

$$\begin{aligned}
&(\mathcal{A}, H_t) \text{ is observable} \\
&\iff \forall s'_0, s''_0 \in \mathcal{S}^{\mathcal{L}}, \Theta_T(s'_0) = \Theta_T(s''_0) \implies s'_0 = s''_0 \\
&\iff \forall x'_0, x''_0 \in \mathcal{S}^N, O_T x'_0 + \Gamma_T = O_T x''_0 + \Gamma_T \implies x'_0 = x''_0 \\
&\iff \forall x'_0, x''_0 \in \mathcal{S}^N, O_T(x'_0 - x''_0) = 0 \implies (x'_0 - x''_0) = 0 \\
&\iff ker\ O_T = \{0\} \\
&\iff rank\ O_T = dim\ O_T - dim(ker\ O_T) = N
\end{aligned}$$

□

In linear algebra, the Cayley-Hamilton theorem states that any square matrix over a commutative ring (in our case $\mathcal{S}$) satisfies its characteristic equation. It can be coupled with the Kalman theorem here above to give an upper bound on the time horizon T.

Proposition 1. Suppose a CA observed by a time invariant output operator C (i.e. by a static sensor), the observability matrix O_T is of

size $N \times Q.T$. For the matrix O_T to be of full column rank, the time horizon T has to be bounded by:

$$\frac{N}{Q} \leq T \leq N \tag{17}$$

Proof. The two inequalities are proven by the following:

- $T \leq N$: The Cayley-Hamilton theorem guarantees that A^N is a linear combination of lower powers, the rank of O_T will not increase beyond T = N.
- $T \geq N/Q$: For O_T to have a rank of N, it needs at least N rows and columns, thus $Q.T \geq N$.

□

In the case of a mobile sensor (i.e. a time variant output operator C_t), only the lower bound of the inequation (17) stands true. The Cayley-Hamilton theorem does not apply because $C_T A^T$ is a linear combination of $C_T + C_T A + \cdots + C_T A^{T-1}$ and not of $C_0 + C_1 A + \cdots + C_{T-1} A^{T-1}$

Corollary 1. If the Kalman criterion is verified, then it is possible to reconstruct the initial state by inverting the observability matrix. Indeed, based on the formulation (15) we obtain:

$$x_0 = O_T^{\dagger}(Y_T - \Gamma_T) \tag{18}$$

Proof. Consider an affine CA $\mathcal{A}$ observable by an affine output operator H_t such that $\forall x_0 \in \mathcal{S}^N, Y_T = O_T x_0 + \Gamma_T$ and $rank\ O_T = N$. To simplify the notations, we shall simply note O and Γ to respectively represent O_T and Γ_T.

As $rank\ O = N$, it means that it exists P such that $PO = I$ (but not necessarily $OP \neq I$ because O is full column rank not full row rank). We can find $P = O^{\dagger}$ by computing the pseudo-inverse of O. Using the equation (15) we find that:

$$Y_T = Ox_0 + \Gamma \iff O^{\dagger}(Y_T - \Gamma) = O^{\dagger}Ox_0 \iff O^{\dagger}(Y_T - \Gamma) = x_0$$

As O is full column rank, $O^{\dagger} = (O^t O)^{-1} O^t$. If O is square then $O^{\dagger} = O^{-1}$. □

In the case of linear systems, observability and reconstructibility are equivalent concepts [31]. The Kalman criterion ensure observability, however there are some systems which are reconstructible but not observable [23], for this reason we propose a new theorem which assesses the reconstructibility of affine CA.

Theorem 2 (Reconstructibility Criterion). Let $\mathcal{A}$ and H be an affine CA and affine output operator; A, C their matrix form; and η and γ their constants.

The pair $(\mathcal{A}, H)$ (i.e. the cellular automaton $\mathcal{A}$ with the output operator H) is reconstructible if and only if there exists $T \in \mathbb{N}$ such that:

$$ker\ O_T \subset ker\ A^T \tag{19}$$

If the CA is reversible [17] then A^T is full rank thus reconstructibility is equivalent to observability. Indeed, $ker\ O_T \subset ker\ A^T = \{0\} \iff rank\ O_T = N$.

Proof. Let $\mathcal{A}$ an affine CA and A and η its associated matrix and constant. Let H_t be a time dependant affine output operator associated to the matrix C_t and the constant γ_t. Then, let $x_0 \in \mathcal{S}^N$ be the initial state and $Y_T = \begin{bmatrix} y_0 & y_1 & \dots & y_{T-1} \end{bmatrix}$ the output sequence generated by the output operator such that $Y_T = O_T x_0 + \Gamma_T$.

Consider the definition 4 of the global observability, then:

$$\begin{aligned}
&(\mathcal{A}, H_t) \text{ is reconstructible} \\
&\iff \forall s_0', s_0'' \in \mathcal{S}^{\mathcal{L}}, \Theta_T(s_0') = \Theta_T(s_0'') \implies F^T(s_0') = F^T(s_0'') \\
&\iff \forall x_0', x_0'' \in \mathcal{S}^N, O_T x_0' + \Gamma_T = O_T x_0'' + \Gamma_T \\
&\qquad \implies A^T x_0' + J_{T-1}\eta = A^T x_0'' + J_{T-1}\eta \\
&\iff \forall x_0', x_0'' \in \mathcal{S}^N, O_T(x_0' - x_0'') = 0 \implies A^T(x_0' - x_0'') = 0 \\
&\iff ker\ O_T \subset ker\ A^T
\end{aligned}$$

□

Corollary 2. If the reconstructibility criterion is verified, then it is possible to find a matrix R such that:

$$x_T = R(Y_T - \Gamma_T) + J_{T-1}\eta \tag{20}$$

Proof. Consider an affine CA $\mathcal{A}$ (with a matrix A and a constant η) reconstructible by an affine output operator H_t such that $Y_T = O_T x_0 + \Gamma_T$ and $ker\ O_T \subset ker\ A^T$.

As $ker\ O_T \subset ker\ A^T$, it means there exists a matrix R such that $A^T = RO_T$. With this property, we can find that:

$$\begin{aligned} Y_T = O_T x_0 + \Gamma_T &\iff R(Y_T - \Gamma_T) = RO_T x_0 \\ &\iff R(Y_T - \Gamma_T) + J_{T-1}\eta = A^T x_0 + J_{T-1}\eta \\ &\iff x_T = R(Y_T - \Gamma_T) + J_{T-1}\eta \end{aligned}$$

□

4 OBSERVATION OF AFFINE CELLULAR AUTOMATA THROUGH MOBILE SENSORS

In this section, a simple and didactic example will be presented, it will allow to detail the operations necessary to assess the observability or the reconstructibility for cellular automata. For this purpose, the CA studied will have only one dimension and few cells in order not to overload the calculations. This CA will not have a physical representation nor a numerical utility but the next section will present another example with a numerical utility but without the detail of the calculations.

Let us consider the following one-dimensional cellular automaton defined by:

- $\mathcal{L} = \{0, 1, 2, 3, 4\}$
- $\mathcal{S} = \{0, 1, 2\}$
- $\mathcal{N} \colon c_i \mapsto \{c_{i-1}, c_i, c_{i+1}\}$ with periodic boundaries so $c_{-1} = c_4$ and $c_5 = c_0$.
- $f \colon s_t(\mathcal{N}(c_i)) \mapsto s_t(c_{i-1}) + 2s_t(c_i) + s_t(c_{i+1}) + 1$

Then let us consider two output operators H and H'. Both of these will observe one cell at a time, but H represents a mobile sensor (i.e. $\mathcal{L}_q$ varying over time) while H' represents a stationary sensor. The mobile sensor measure one cell and moves to the right by one cell at each time step: at $t = 0$ it measures cell c_0, at $t = 3$ cell c_3 and at $t = 5$ cell c_0 (because of the periodic boundary conditions).

- Mobile Sensor: $\mathcal{L}_{q_t} = \{c_{t\ mod\ 5}\}$ and $H \colon s_t \mapsto s_t(c_{t\ mod\ 5}) + 2$

0	1	2	2	0
2	2	2	1	0
1	0	2	2	1
1	1	1	2	0
1	2	0	0	1
0	0	0	2	1
2	1	0	0	2
2	2	2	0	1

FIGURE 2
Evolution of the cellular automaton over 8 time steps from the initial configuration $01220|_3$.

- Stationary Sensor: $\mathcal{L}'_q = \{c_0\}$ and $H' \colon s_t \mapsto s_t(c_0) + 2$

From the equations (10) and (11) and the usual order of the cells (i.e. $x_t^i = s_t(c_i)$), the state system (12) can be written with :

$$\tilde{F}(x_t) = \begin{bmatrix} 2x_t^0 + x_t^1 + x_t^4 + 1 \\ x_t^0 + 2x_t^1 + x_t^2 + 1 \\ x_t^1 + 2x_t^2 + x_t^3 + 1 \\ x_t^2 + 2x_t^3 + x_t^4 + 1 \\ x_t^0 + x_t^3 + 2x_t^4 + 1 \end{bmatrix}$$

$$\tilde{H}_t(x_t) = x_t^t + 2 \text{ and } \tilde{H}'(x_t) = x_t^0 + 2$$

The transition function $\tilde{F}$ is an affine map, so it can be written in an affine form with a square matrix A and a constant vector η, which leads to:

$$A = \begin{bmatrix} 2 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 0 & 0 & 1 & 2 \end{bmatrix} \text{ and } \eta = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

The two output operators $\tilde{H}$ and $\tilde{H}'$ being affine, thus their matrix form are:

- Stationary Sensor: $C' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}$ and $\gamma' = 2$
- Mobile Sensor:

$$\begin{aligned} C_0 &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \gamma_0 = 2 \\ C_1 &= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix} \text{ and } \gamma_1 = 2 \\ &\dots \\ C_4 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \gamma_4 = 2 \\ C_5 &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \gamma_5 = 2 \end{aligned}$$

From the equation (17) which uses the Cailey-Hamilton theorem, we are able to compute that the observation horizon $T = 5$ because $Q = 1$ and $N = 5$. We can therefore calculate from (15) the observability matrix O_T and the constant vector Γ_T.

- Stationary: $O'_T = \begin{bmatrix} C' \\ C'A \\ C'A^2 \\ C'A^3 \\ C'A^4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \Gamma_T = \begin{bmatrix} 2 \\ 0 \\ 1 \\ 2 \\ 0 \end{bmatrix}$
- Mobile: $O_T = \begin{bmatrix} C_0 \\ C_1A \\ C_2A^2 \\ C_3A^3 \\ C_4A^4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \Gamma_T = \begin{bmatrix} 2 \\ 0 \\ 1 \\ 2 \\ 0 \end{bmatrix}$

The mobile sensor ensures the observability in a time T because the matrix O_T is full rank. On the contrary, the stationary sensor does not because the rank of the matrix O'_T is not 5. Since observability is not verified at time T, the time horizon T should be increased as long as it respects the inequality (17). In our case, there is only one possibility for T, the next operation would be to assess the reconstructibility using (19). However, this would be pointless in this case because the CA is reversible (rank $A = 5$) and observability and reconstructibility are equivalent in this case.

	c_0	c_1	c_2	c_3	c_4
$t=0$	0	1	0	2	0
$t=1$	2	0	1	2	0
$t=2$	2	1	2	0	2
$t=3$	2	1	0	2	1
$t=4$	1	2	1	0	1
$t=5$	0	1	2	0	1

FIGURE 3
Example of CA evolution for $x_0 = \begin{bmatrix}0 & 1 & 0 & 2 & 0\end{bmatrix}^t$. The time is along the vertical axis. Cells are numbered from left to right with c_0 on the left and c_4 on the right. Grey cells are those observed by the mobile sensor.

As the mobile sensor ensures observability, the initial state can be reconstructed using the corollary (18) from the measurements made by the sensor. As an example, we will reconstruct the initial state $01020|_3$ as presented in figure 3 whose output sequence is $Y_T = \begin{bmatrix}2 & 2 & 1 & 1 & 0\end{bmatrix}^t$.

We start by finding $O_T^\dagger$ and then calculate x_0. We should find $x_0 = \begin{bmatrix}0 & 1 & 0 & 2 & 0\end{bmatrix}^t$.

As O_T is a square matrix we can compute the inverse instead of the pseudo-inverse. To calculate O_T^{-1}, we will use the inverse of the determinant of O_T, $det(O_T)$ and its adjugate matrix $adj(O_T)$.

$$O_T^{-1} = det(O_T)^{-1} adj(O_T) = 2^{-1} \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 \\ 2 & 2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

In modular arithmetic base k, the inverse is obtained by finding b so that $ab \equiv 1 (\text{mod } k)$, yet in the field $\mathcal{S}$ that we have, $2^{-1} = 2$ because $2 \times 2 \equiv 1 (\text{mod } 3)$.

We can now find x_0 using Y_T, Γ_T and O_T^{-1}. We get:

$$x_0 = O_T^{-1}(Y_T - \Gamma_T) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 2 \\ 2 \\ 1 \\ 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 2 \\ 0 \\ 1 \\ 2 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 0 \end{bmatrix}$$

With this example, we have shown the use of observability and reconstructibility through the Kalman criterion for a very simple example. The objective was to describe the computations in order to detail the method to assess the observability and reconstructibility of the system. In the next section, we will make an application on a real system, larger and more complex but we will not detail the calculations. For this example, we will focus on random number generators (RNG) and especially how it is possible to reconstruct the random number sequence using the observability of affine CAs. This example is particularly interesting because RNGs are increasingly used with the increase in cyber security in recent years.

5 APPLICATION OF OBSERVABILITY TO CYBERSECURITY

In cybersecurity, random number generator (RNG) are a crucial element in many applications [22]. They are used to secure https connections with SSL, to secure connections to wifi networks with WPA2 and many others. The robustness of RNGs depends on both the probability distribution and the predictability of the generator. It is also a source of several vulnerabilities that are grouped under the term "Random Number Generator Attack" [18] where the objective is to obtain information about the next generations of random numbers.

Cellular automata random number generators (CA RNG) have been widely studied for more than three decades [4]. CA have local, simple and regular interactions, so they can be easily integrated at large scales. Initially, cellular automata random number generators are one-dimensional [4, 14, 30] but CA with two or more dimensions turn out to generate random numbers of better quality [4, 29] but are more complex to set up. For that, different algorithms have been developed to build "automatically" these CA RNG [29].

In this section, we will use the observability of affine cellular automata to reconstruct past and future random numbers using information

obtained by a random number generator attack. The nature of the attack, as well as the method used, does not matter in the context of applying the Kalman criterion, only the information obtained from the attack is important. The attack will be seen as a sensor that observes the state of the random number generator and therefore represented by the output operator H which will depend solely on the information obtained by the attack. Of these three examples, the first will use knowledge of a random number to deduce past and future numbers, the second will use information about a single bit of the random number and the last will be based on the binary parity of the generated random number. But we will start by presenting the CA RNG of Tomassini et al which will be the subject of our study.

5.1 Tomassini's et al Cellular Automata Random Number Generator

For this example, we will study a cellular automaton generating high quality random numbers proposed by Tomassini et al [29]. The quality of the random numbers generated by this CA RNG was evaluated according to the Diehard tests defined by Marsaglia in [21] which were all passed successfully. This CA RNG is a two dimensional Boolean CA that generates a number consisting of 64 hexadecimal random digits. The CA generates a random number every 4 iterations but for the simplicity of the example, we will consider that it generates a 64 bit random number every iteration rather than a 64 hexadecimal digits random number every 4 iterations.

The CA RNG of Tomassini et al is defined as follows:

- $\mathcal{L} = \{0, 1, \ldots, 7\} \times \{0, 1, \ldots, 7\}$
- $\mathcal{S} = \{0, 1\}$
- $\mathcal{N}$: $c_i, j \mapsto \{c_{i-1,j}, c_{i,j-1}, c_{i,j}, c_{i+1,j}, c_{i,j+1}\}$ with null boundaries so $s(c_{-1}) = 0$ and $s(c_8) = 0$.

In their paper, Tomassini et al describe three limits: cyclic, fixed (full) and fixed (reduce). We can easily model fixed (full) and cyclic boundary conditions but the reduced version requires to model an CA of 10×10 but only the 8×8 cells of the center represents the random number. In our example, we will use the fixed (full) version with a zero value at the boundaries.

As opposed to the definition made at the beginning of the paper, the CA RNG of Tomassini et al is not uniform, i.e. the local transition

function f depends on the cell position. Figure 4 describes the transition function that applies to each cell as a rule whose value is defined by the 6-bit string XCNWSE which corresponds to the following transition function:

$$\begin{aligned} s_{t+1}(c_{i,j}) =& X + C.s_t(c_{i,j}) + N.s_t(c_{i-1,j}) + W.s_t(c_{i,j-1}) \\ &+ S.s_t(c_{i+1,j}) + E.s_t(c_{i,j+1}) \end{aligned} \tag{21}$$

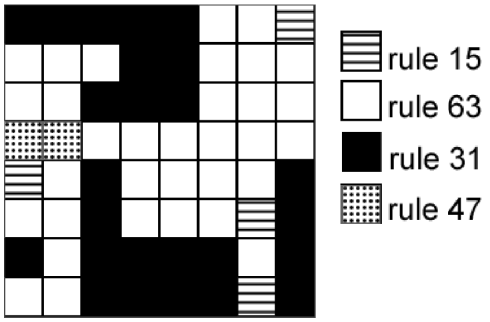

FIGURE 4
A 8×8 non-uniform cellular automaton random number generator proposed by Tomassini et al [29]. The color of the cells represents the transition function associated to this cell according to (21).

Therefore, according to the previous generic transition function, the rules 15, 31, 47 and 63 correspond respectively to the transition functions :

- $s_{t+1}(c_{i,j}) = s_t(c_{i-1,j}) + s_t(c_{i,j-1}) + s_t(c_{i+1,j}) + s_t(c_{i,j+1})$
- $s_{t+1}(c_{i,j}) = s_t(c_{i,j}) + s_t(c_{i-1,j}) + s_t(c_{i,j-1}) + s_t(c_{i+1,j}) + s_t(c_{i,j+1})$
- $s_{t+1}(c_{i,j}) = 1 + s_t(c_{i-1,j}) + s_t(c_{i,j-1}) + s_t(c_{i+1,j}) + s_t(c_{i,j+1})$
- $s_{t+1}(c_{i,j}) = 1 + s_t(c_{i,j}) + s_t(c_{i-1,j}) + s_t(c_{i,j-1}) + s_t(c_{i+1,j}) + s_t(c_{i,j+1})$

Although the system is not uniform, it can be represented with the state representation (13). Therefore, the cells will be sorted by columns, such that $s_t(c_{i,j}) = x_t^{i+j\times 8}$. Moreover, regardless of the rules used, the

cellular automaton will be affine so all other CA that respect Tomassini's definition can be studied in the same way.

In the following sections, we will present three purely theoretical attacks which aim to show a use of Kalman criterion. In each of the examples, we will present the attack and the associated output operator that allows to reconstruct the state of the system.

5.2 Single Measurement Attack

The principle of this attack is to use one of the generated random numbers to deduce the sequence of other random numbers. For that we will not use directly the Kalman criterion because the random number represents directly the state of the system and thus there is no reconstruction. However, we will use the reversibility of the cellular automaton to find random numbers generated previously.

As we consider that the attack provides us with a random number generated by the cellular automaton, we assume that this number corresponds to the measure y_0 with an identity output operator $C = Id_N$. The attack by which this random number is obtained is not specified here (and is not essential for the explanation), but several methods exist in the literature such as intrusive hardware attack [25] or side-channel attack [27]. As the measurement of the state is made with the full state, the initial state is completely reconstructed from the first measurement. Therefore the state representation of the system is the following:

$$\begin{cases} x_{t+1} & = Ax_t + \eta \\ y_t & = x_t \\ x_0 & = \xi(s_0), s_0 \in \mathcal{S}^{\mathcal{L}} \end{cases}$$

In an evident way the observability is assured at time 1 because rank $O_1 = \text{rank } C = \text{rank } Id_N = N$. Therefore, it is possible to deduce the next generations of random numbers using (14) $x_t = A^t y_0 + J_{t-1}\eta$. But also, because of the reversibility of the CA RNG, it is possible to invert the matrix A and deduce the previous generations of random numbers:

$$x_0 = A^t x_{-t} + J_{t-1}\eta \iff x_{-t} = A^{-t}(x_0 - J_{t-1}\eta)$$

In this example, we were able, from a single random number generation, to deduce future but also past random numbers. This "vulnerability" can allow an intrusive (even destructive) hardware attack

to retrieve a single random number in order to deduce the previous random numbers that have been used in critical operations.

5.3 Regular Measurement Attack

To reconstruct the random number stream, we will use partial information about the random numbers. In this example, we use only one of the 64 bits, but more bits could have been used (which could have reduce on the T measurement horizon, see proposition 1). In the same way as before, we will not specify how the bit of the random number is retrieved, only that we have a measurement at each time step.

To reconstruct the state of the system, we need only one bit of the random number at each time step. The measurement can be done on a single digit or change with time, the only information needed is the position of the measured digit at each time step. In this way, it is possible to create the operator C_t which corresponds to the bit of the random number (or the cell associated with this bit) measured at time t. The operator C_t is of the form :

$$C_t = \begin{bmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{bmatrix}$$

, where the 1 corresponds to the measured bit.

Then, we need to know the operators C_t associated with the measurements y_t and from there construct the observability matrix O_T over a time horizon 64. The system is observable (i.e. rank $O_T = 64$) regardless of the bit measured in the static case as well as for the different trajectories we have tried. However, it is not reasonable to test all the possible trajectories (there are 64^{64} trajectories) so we will still have to verify if the system is observable with the given trajectory. Afterwards, it is possible to find the random number (i.e. the state x_0) and to deduce the random number stream as in the previous subsection.

5.4 Parity Attack

The objective of this attack is to reconstruct the random number sequence using only the binary parity of the random numbers. With this method, it is possible to reconstruct the initial state even if the random number information is not directly accessible. One method that seems to be feasible is to correlate the energy consumption of the system with the memory consumption [27].

Regardless of the method used, we assume to have access to the binary parity of the random number generated at each iteration. Therefore,

the equations of state are the following:

$$\begin{cases} x_{t+1} & = Ax_t + \eta \\ y_t & = \sum_{i=0}^{64} x_t^i \\ x_0 & = \xi(s_0), s_0 \in \mathcal{S}^{\mathcal{L}} \end{cases}$$

The sum uses binary modular arithmetic.

The output operator C_t associated with parity is a row vector composed of N 1 which does not depend on time. From there, the observability matrix can be computed with $T = 64$ and it is full rank matrix. The system is observable with the parity measurement, which allows to reconstruct the initial state as well as the past and future states due to the reversibility of the CA RNG.

In this section, we have been able to reconstruct the random number stream from the information, total or partial, about the random numbers. The information obtained by making attacks on the random number generators is not described because the reconstruction of the state is independent of these methods. These attacks vary according to the hardware or digital support used by the CA RNG. The use of the Kalman criterion is therefore added after the recovery of the information by the attacks as a reconstruction of the random number stream. The purpose of the reconstruction was to show the usefulness of observability (and alternatively reconstructibility) for the reconstruction of a random number stream in a random number generator attack context. Although very efficient to reconstruct the random number stream, this method still have shortcoming: the CA RNG must be perfectly known; the random number seed (i.e. the state of the CA) must not be modified by the user during the measurement; and the CA RNG must not have non-linearity (which is not the case with the CA RNG presented by Tomassini).

6 CONCLUSION & PERSPECTIVES

Observability plays a fundamental role in complex systems that may describe the dynamics of a wide range of natural, technological and socioeconomic phenomena. The systems variables are completely dependent of each other due to the strong interaction between the system's

components. Cellular Automata constitute one of the major computational techniques engaged for complex systems modelling. They consist of a large number of interconnected and mutually interacting components according to simple rules that give rise to complex emergent behaviours.

In this paper, we presented a method to prove the observability of affine cellular automata with linear output operators, either time-varying or not. We started by presenting a formulation of cellular automata observed by a mobile sensors network. Then we extended the Kalman criterion from discrete-time linear systems to affine cellular automata and we studied the observability of one-dimensional cellular automata with this method.

A very important application in cybersecurity where random number generator constitute a crucial element was considered in relation with observability of CA. Three theoretical attacks that show the usefulness of observability for the reconstruction of a CA random number were presented. Although the results obtained are still partial and deserve further investigations, they have shown a good efficiency to reconstruct the random number stream.

In a future work, we will generalise our observability analysis to nonlinear cellular automata and construct an associated state estimator. This estimator will make it possible to have an estimate of the state of cellular automata without having to wait for the time necessary for the inversion of the observability matrix. Such an observer would allow the use of cellular automata for control, diagnosis or general supervision purposes, with many potential applications, for instance in wildfire, pollution, or traffic monitoring or tracking problems.

REFERENCES

[1] M Amouroux, A El Jai, and E Zerrik. (1994). Regional observability of distributed systems. International Journal of Systems Science, 25(2):301–313.

[2] Antonios Armaou and Michael A Demetriou. (2006). Optimal actuator/sensor placement for linear parabolic pdes using spatial h2 norm. Chemical Engineering Science, 61(22):7351–7367.

[3] Franco Bagnoli, Nino Boccara, and Raúl Rechtman. (2001). Nature of phase transitions in a probabilistic cellular automaton with two absorbing states. Physical Review E, 63(4):046116.

[4] Parimal Pal Chaudhuri, Dipanwita Roy Chowdhury, Sukumar Nandi, and Santanu Chattopadhyay. (1997). Additive cellular automata: theory and applications, volume 43. John Wiley & Sons.

[5] Bastien Chopard and Michel Droz. (1998). Cellular automata modeling of physical systems. Cambridge UP, pages 122–137.

[6] Michael A Demetriou. (2010). Guidance of mobile actuator-plus-sensor networks for improved control and estimation of distributed parameter systems. IEEE Transactions on Automatic Control, 55(7):1570–1584.

[7] S. Dridi, F. Bagnoli, and S. El Yacoubi. (2019). Markov chains approach for regional controllability of deterministic cellular automata, via boundary actions. Journal of Cellular Automata, 14(5/6):479–498.

[8] S. Dridi, S. El Yacoubi, F. Bagnoli, and A. Fontaine. (2019). A graph theory approach for regional controllability of boolean cellular automata. International Journal of Parallel, Emergent and Distributed Systems, pages 1–15.

[9] Sara Dridi. (November 2019). Recent advances in regional controllability of cellular automata. Theses, Université de Perpignan ; Università degli studi (Florence, Italie).

[10] A El Jai. (1991). Distributed systems analysis via sensors and actuators. Sensors and Actuators A: Physical, 29(1):1–11.

[11] A El Jai and S El Yacoubi. (1992). On the relations between actuator structures and final-constraint minimum-energy problem. Sensors and Actuators A: Physical, 33(3):175–182.

[12] A El Jai, MC Simon, and E Zerrik. (1993). Regional observability and sensor structures. Sensors and Actuators A: Physical, 39(2):95–102.

[13] S El Yacoubi. (2008). A mathematical method for control problems on cellular automata models. International Journal of Systems Science, 39(5):529–538.

[14] Peter D Hortensius, Robert D Mcleod, Werner Pries, D Michael Miller, and Howard C Card. (1989). Cellular automata-based pseudorandom number generators for built-in self-test. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 8(8):842–859.

[15] Rudolf E Kalman. (1960). On the general theory of control systems. In Proceedings First International Conference on Automatic Control, Moscow, USSR.

[16] Rudolf Emil Kalman. (1963). Mathematical description of linear dynamical systems. Journal of the Society for Industrial and Applied Mathematics, Series A: Control, 1(2):152–192.

[17] Jarkko Kari. (2005). Reversible cellular automata. In International Conference on Developments in Language Theory, pages 57–68. Springer.

[18] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. (1998). Cryptanalytic attacks on pseudorandom number generators. In International workshop on fast software encryption, pages 168–188. Springer.

[19] Jacques-Louis Lions. (1986). Controlabilité exacte des systèmes distribués: remarques sur la théorie générale et les applications. In Analysis and optimization of systems, pages 3–14. Springer.

[20] Yang-Yu Liu, Jean-Jacques Slotine, and Albert-László Barabási. (2013). Observability of complex systems. Proceedings of the National Academy of Sciences, 110(7):2460–2465.

[21] George Marsaglia. (1996). Diehard: a battery of tests of randomness. http://stat. fsu. edu/geo.

[22] Kinga Marton, Alin Suciu, and Iosif Ignat. (2010). Randomness in digital cryptography: A survey. Romanian journal of information science and technology, 13(3):219–240.

[23] Théo Plénet, Samira El Yacoubi, Clément Raievsky, and Laurent Lefèvre. (2021). Observability and reconstructibility of cellular automaton. Int. Journal of Systems Science. submitted.

[24] David L Russell. (1978). Controllability and stabilizability theory for linear partial differential equations: recent progress and open questions. Siam Review, 20(4):639–739.

[25] David Samyde, Sergei Skorobogatov, Ross Anderson, and J-J Quisquater. (2002). On a new way to read data from memory. In First International IEEE Security in Storage Workshop, 2002. Proceedings., pages 65–69. IEEE.

[26] PE Sarachik and E Kreindler. (1965). Controllability and observability of linear discrete-time systems. International Journal of Control, 1(5):419–432.

[27] François-Xavier Standaert. (2010). Introduction to side-channel attacks. In Secure integrated circuits and systems, pages 27–42. Springer.

[28] T Toffoli and N Margolus. (1990). A high-performance cellular-automation machine. Physica D, 10.

[29] Marco Tomassini, Moshe Sipper, and Mathieu Perrenoud. (2000). On the generation of high-quality random numbers by two-dimensional cellular automata. IEEE Transactions on computers, 49(10):1146–1151.

[30] Ph Tsalides, TA York, and A Thanailakis. (1991). Pseudorandom number generators for vlsi systems based on linear cellular automata. IEE Proceedings E (Computers and Digital Techniques), 138(4):241–249.

[31] LG Van Willigenburg and Willem L De Koning. (2008). Linear systems theory revisited. Automatica, 44(7):1686–1696.

[32] John Von Neumann, Arthur W Burks, et al. (1966). Theory of self-reproducing automata. IEEE Transactions on Neural Networks, 5(1):3–14.

[33] Stephen Wolfram. (1983). Statistical mechanics of cellular automata. Reviews of modern physics, 55(3):601.