How Common Can Be Universality for Cellular Automata?

Guillaume Theyssier*

LIP (UMR CNRS, ENS Lyon, INRIA, Univ. Claude Bernard Lyon 1),
École Normale Supérieure de Lyon,
46 allée d'Italie 69364 LYON cedex 07 FRANCE

Abstract. We address the problem of the density of intrinsically universal cellular automata among cellular automata or a subclass of cellular automata. We show that captive cellular automata are almost all intrinsically universal. We show however that intrinsic universality is undecidable for captive cellular automata. Finally, we show that almost all cellular automata have no non-trivial sub-automaton.
Keywords: cellular automata, universality, zero-one law.

Cellular automata are simple discrete dynamical systems involving full uniformity and perfect synchronism. They are capable of producing very complex behaviours despite their apparent simplicity and therefore constitute an idealistic model to study the paradigm of complex systems. Besides its ability to capture any sequential computations, the model of cellular automata possesses a natural notion of intrinsic universality. A cellular automaton is intrinsically universal if it is able to directly simulate any other cellular automaton. There is no general definition of what is an acceptable simulation but in [1] a natural and rather minimal class of acceptable simulation is introduced and give rise to the formal notion of intrinsic universality adopted in this paper.

Since the very beginning of cellular automata theory great efforts have been devoted to the design of particular cellular automata having some desired property. The property of being intrinsically universal was of course especially studied and the quest for the smallest intrinsically universal cellular automaton has now almost reached the limits (closed in dimension 2 and higher by [2] and reduced to a 4 states gap in dimension 1 by [3]). However, these tricky constructions only give results concerning *sufficient* conditions and do not respond to the problem of how strong is the intrinsic universality requirement for a cellular automaton in general, or, said differently, how many different ways there are to achieve intrinsic universality. Unfortunately, this converse problem reveals to be difficult since the set of non intrinsically universal cellular automata is not recursively enumerable (see [1]) whereas the set of intrinsically universal one is.

In the present paper we tackle this problem using a different point of view: we study *density* of intrinsically universal cellular automata. Our main result is that a simple hypothesis on the local transition map gives rise to a class of

* `Guillaume.Theyssier@ens-lyon.fr`

cellular automata (namely *captive* cellular automata) for which density follows a zero-one law over an interesting class of properties. We then show that intrinsic universality belongs to that class and, using the zero-one law, that almost all captive cellular automata are intrinsically universal. We show however that the set of non intrinsically universal captive cellular automata is not recursively enumerable. Back to the general case, we show that almost all cellular automata lack of any non-trivial local structure making a strong difference with the captive case.

1 Formal framework

Although many results extend to higher dimensions, we will only consider one-dimensional CA. Besides, this paper is not concerned with comparisons between different shapes of neighbourhood and we consider only VON NEUMANN-like neighbourhood (connected and centred). Formally a CA is triple $\mathcal{A} = (A, r, f_{\mathcal{A}})$ where A is a finite set of *states*, r is a positive integer (the *radius* of the neighbourhood) and $\mathcal{A}$ is a map from A^{2r+1} to A. Configurations are maps from $\mathbb{Z}$ to A giving each cell a particular state. The local transition function $f_{\mathcal{A}}$ induces a global evolution rule on configurations denoted $\mathcal{A}$ and defined as follows: $\forall c \in A^{\mathbb{Z}}$, $\mathcal{A}(c)$ is such that $\forall i \in \mathbb{Z}$, $\big(\mathcal{A}(c)\big)(i) = f_{\mathcal{A}}\big(c(i-r), c(i-r+1), \ldots, c(i+r)\big)$. In the sequel, when considering a CA $\mathcal{A}$ (resp. $\mathcal{B}$), we implicitly refer to the triple $(A, r_{\mathcal{A}}, \mathcal{A})$ (resp. $(B, r_{\mathcal{B}}, \mathcal{B})$) where the same symbol $\mathcal{A}$ (resp. $\mathcal{B}$) denotes both the local and the global map.

Local maps in CA are arbitrary, but in this paper we pay a special attention to a particular regularity they may possess which is captured by the notion of *sub-automaton*. Up to renaming, a *sub-automaton* of a CA $\mathcal{A}$ is a subset of the states set which is stable under iterations of $\mathcal{A}$. Formally the sub-automaton relation, denoted by $\sqsubseteq$, is defined as follows.

Definition 1. *$\mathcal{A} \sqsubseteq \mathcal{B}$ if there is an injective map i from A to B such that $\bar{i} \circ \mathcal{A} = \mathcal{B} \circ \bar{i}$, where $\bar{i} : A^{\mathbb{Z}} \to B^{\mathbb{Z}}$ denotes the uniform extension of i.*

When $X \subseteq A$ is stable for $\mathcal{A}$ ($\mathcal{A}(X^{\mathbb{Z}}) \subseteq X^{\mathbb{Z}}$), we denote by $\mathcal{A}_X$ the restriction of $\mathcal{A}$ to X (then $\mathcal{A}_X \sqsubseteq \mathcal{A}$). Besides, when $|A| = |B|$, $\mathcal{A} \sqsubseteq \mathcal{B}$ implies $\mathcal{B} \sqsubseteq \mathcal{A}$ and $\mathcal{A}$ is isomorphic to $\mathcal{B}$ what is denoted by $\mathcal{A} \sim \mathcal{B}$.

Intrinsic universality we now define relies on a formal notion of direct simulation between CA. A restricted version of this notion was first introduced by J. MAZOYER and I. RAPAPORT in [4] and N. OLLINGER extended it in [5]. $\mathcal{A}$ can simulate $\mathcal{B}$ (denoted by $\mathcal{A} \preceq \mathcal{B}$) if, up to some regular spatio-temporal transformations, $\mathcal{A}$ is a sub-automaton of $\mathcal{B}$. Transformations considered here are very simple: they allow grouping several cells in one block and running several steps of a CA in one. Formally, for any finite set A and any $m \in \mathbb{N}$ ($m \neq 0$), let $o^m : A^{\mathbb{Z}} \to (A^m)^{\mathbb{Z}}$ be the map such that

$$\forall c \in A^{\mathbb{Z}}, \forall z \in \mathbb{Z} : \big(o^m(c)\big)(z) = \big(c(mz), c(mz+1), \ldots, c(m(z+1)-1)\big).$$

Then, denoting the CA $o^m \circ \mathcal{A}^n \circ (o^m)^{-1}$ (with states set A^m) by $\mathcal{A}^{<m,n>}$, the relation $\preceq$ is defined as follows:

$$\mathcal{A} \preceq \mathcal{B} \Leftrightarrow \exists m_a, m_b, n_a, n_b : \mathcal{A}^{<m_a,n_a>} \sqsubseteq \mathcal{B}^{<m_b,n_b>}.$$

$\preceq$ defines a quasi-order on the set of CA (see [5]) and naturally induces an equivalence relation denoted by $\simeq$ and an order on equivalence classes of $\simeq$. In addition to being natural for the model of CA, this simulation relation nicely captures the examples of intrinsically universal CA already present in the literature (see [2, 6]).

Definition 2. *$\mathcal{A}$ is intrinsically universal if* $\forall \mathcal{B}, \exists m, n : \mathcal{B} \sqsubseteq \mathcal{A}^{<m,n>}$.

An important fact is that the set of intrinsically universal CA is exactly the maximal class of $\simeq$ (see [5] for a detailed proof) and we will use alternatively this characterisation and the definition above.

A *property* $\mathcal{P}$ is a set of CA. $\mathcal{A}$ has the property $\mathcal{P}$ if $\mathcal{A} \in \mathcal{P}$. A property $\mathcal{P}$ is said to be *increasing* if: $\forall \mathcal{A}, \forall \mathcal{B}$, $\mathcal{A} \sqsubseteq \mathcal{B}$ implies $\mathcal{A} \in \mathcal{P} \Rightarrow \mathcal{B} \in \mathcal{P}$. Similarly, $\mathcal{P}$ is said to be decreasing if: $\forall \mathcal{A}, \forall \mathcal{B}$, $\mathcal{A} \sqsubseteq \mathcal{B}$ implies $\mathcal{B} \in \mathcal{P} \Rightarrow \mathcal{A} \in \mathcal{P}$. Notice that since the $\sim$ relation is included in $\sqsubseteq$, increasing (or decreasing) properties are closed under renaming of states—a natural requirement when studying CA. We will specifically concentrate on monotonic properties in section 2. For now, just notice that intrinsic universality is an increasing property.

To measure how common a property is among CA, we consider its density using the following canonical enumeration of CA: a radius r is fixed and we let the number of states grow. To avoid irrelevant consideration of states renaming we consider only CA whose states are integers. Precisely, A_n denotes the set of CA of radius r with states set $\{1, \ldots, n\}$ and the density of properties is defined as follows.

Definition 3. *The* density *of property $\mathcal{P}$ is* $\mu(\mathcal{P}) = \lim_{n\to\infty} \frac{|A_n \cap \mathcal{P}|}{|A_n|}$ *when the limit exists.*

To end this section, we give some useful notations. If $a \in A$ then $\overline{a}$ denotes the configuration of $A^{\mathbb{Z}}$ made solely of a. Similarly, if $f : A \to A$, $\overline{f}$ denotes its uniform extension to configurations of $A^{\mathbb{Z}}$, and f^k its extension to A^k ($f^k(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$). If c is a configuration, $L(c)$ denotes the set of words appearing in c. Finally, if w is a word, $\Sigma(w)$ denotes the set of letters appearing in w.

2 A class of cellular automata inducing a zero-one law for monotonic properties

In this section we consider a sub-class of CA (namely *captive* cellular automata) which was first introduced in [7]. Captive cellular automata are CA such that any subset of the states set is stable (*i.e.* induces a sub-automaton). We insist that this class does not rely on any structural assumption on the states set and that it is characterised a property of the local transition map.

Definition 4. *$\mathcal{A}$ of radius r is a* captive *cellular automaton (*CCA *for short) if $\forall u \in A^{2r+1}$ we have $\mathcal{A}(u) \in \Sigma(u)$.*

We address the problem of the density of universality among CA from that class. Formally, if C_n denotes the set of CCA on states set $\{1, \ldots, n\}$, the density of a property $\mathcal{P}$ among CCA is $\mu_C(\mathcal{P}) = \lim_{n\to\infty} \frac{|C_n \cap \mathcal{P}|}{|C_n|}$ when the limit exists.

Quite surprisingly, the structure of CCA allows to globally solve the problem of density for any monotonic property.

Lemma 1. *For any $\mathcal{B} \in C_n$ $(n \geq 2)$, there exists a rational $\lambda_{\mathcal{B}} \in]0, 1[$ such that for all $m \geq n$ and $X = \{a_1, \ldots, a_n\} \subseteq \{1, \ldots, m\}$, we have :*

$$\frac{\left|\left\{\mathcal{A} \in C_m : \mathcal{A}_X \sim \mathcal{B}\right\}\right|}{|C_m|} = \lambda_{\mathcal{B}}.$$

Proof. Let $m \geq n$ be fixed and consider X a subset of $\{1, \ldots, m\}$ of size n. The equivalence relation $\equiv_X$ such that $\mathcal{A} \equiv_X \mathcal{B} \Leftrightarrow \mathcal{A}_X = \mathcal{B}_X$ is well-defined on C_m since the set X always induces a sub-automaton for any CCA. It is clear that $\equiv_X$ has exactly $|C_n|$ equivalence classes (independently of X), each of the same size $\frac{|C_m|}{|C_n|}$. Besides, $\{\mathcal{A} : \mathcal{A}_X \sim \mathcal{B}\}$ is the union of a number b of classes of $\equiv_X$ depending only on $\mathcal{B}$. Therefore,

$$\frac{\left|\left\{\mathcal{A} \in C_m : \mathcal{A}_X \sim \mathcal{B}\right\}\right|}{|C_m|} = \frac{b}{|C_n|}$$

and the lemma follows. □

Theorem 1. *For any monotonic property $\mathcal{P}$ which is non-trivial in C, we have:*

- *if $\mathcal{P}$ is decreasing in C then $\mu_C(\mathcal{P}) = 0$;*
- *if $\mathcal{P}$ is increasing in C then $\mu_C(\mathcal{P}) = 1$.*

Proof. First suppose $\mathcal{P}$ is non-trivial and decreasing. There must therefore be some $\mathcal{B} \in C_n \setminus \mathcal{P}$ for some $n \in \mathbb{N}$. Now for $m \in \mathbb{N}$ let $m = kn + r$ be the Euclidean division of m by n and for $1 \leq i \leq k$ let $X_i = \{(i-1)n + 1, \ldots, in\}$. Then we have:

$$\mathcal{P} \cap C_m \subseteq \bigcap_{1\leq i\leq k} \{\mathcal{A} \in C_m : \mathcal{A}_{X_i} \not\sim \mathcal{B}\}$$

because $\mathcal{A} \in \mathcal{P}$ implies $\forall i, 1 \leq i \leq k : \mathcal{A}_{X_i} \in \mathcal{P}$. Now since the sets X_i are pairwise disjoint, the events "$\mathcal{A}_{X_i} \not\sim \mathcal{B}$" are pairwise independent. Hence, expressing the set inclusion above in terms of probabilities we get:

$$\frac{\left|\mathcal{P} \cap C_m\right|}{|C_m|} \leq \prod_{1\leq i\leq k} \frac{\left|\{\mathcal{A} \in C_m : \mathcal{A}_{X_i} \not\sim \mathcal{B}\}\right|}{|C_m|} = (1 - \lambda_{\mathcal{B}})^k,$$

the right-hand equality being derived from lemma 1. Finally, taking the limit when $m \to \infty$ for both sides, we conclude: $\mu_C(\mathcal{P}) \leq \lim_{k\to\infty}(1-\lambda_{\mathcal{B}})^k = 0$.

Now suppose $\mathcal{P}$ is a non-trivial increasing property. Then $\neg\mathcal{P}$ is a non-trivial decreasing property. From what we have shown before $\mu_C(\neg\mathcal{P}) = 0$. Thus $\mu_C(\mathcal{P}) = 1$. □

The first immediate implication of theorem 1 is of dynamical nature (see [8] for a definition of expansivity).

Corollary 1. *For any fixed radius, almost no* CCA *is injective, or expansive, or surjective.*

Proof. Since the surjectivity property is obviously non-trivial for CCA, it is sufficient to show that it is decreasing and applying theorem 1 we get that almost no CCA is surjective. The fact that surjectivity is decreasing comes directly from theorem 5.9 of [9] which states that $\mathcal{A}$ is surjective if and only if the number of preimages of any word under $\mathcal{A}$ is uniformly bounded (independently of the word).

The facts that both injectivity and expansivity implies surjectivity are classical results (see [9]), but we insist that injectivity and expansivity are also decreasing non-trivial properties. □

In the case of CCA, the answer to the central question addressed in this paper is now obtained as a direct corollary of theorem 1.

Corollary 2. *There exists an integer r_0 such that for any fixed radius $r \geq r_0$, almost all* CCA *are intrinsically universal:* $\mu_C\big(\{\mathcal{A} : \forall\mathcal{B}, \mathcal{B} \preceq \mathcal{A}\}\big) = 1$.

Proof. The property of being intrinsically universal is obviously increasing so it is sufficient to show that it is non-trivial and the result follows from theorem 1. The existence of intrinsically universal CCA was first pointed out in [7]. Definition 5 and lemma 2 show that there is an intrinsically universal CCA of radius 7 and it is not difficult to tune the construction to lower its radius down to 5. □

Although almost all CCA are intrinsically universal as shown above, we are going to show that the problem of whether a given CCA is intrinsically universal or not is undecidable. This fact may seem scheming compared with the ubiquity of universality in CCA. But, overall, it has a noticeable structural consequence on the class CCA concerning the limit between universality and non-universality as pointed out by corollary 3.

The proof is a reduction from the same decision problem with any CA as input. It essentially relies on the transformation τ (given hereafter). We insist that algorithmic constructions on captive cellular automata are non-classical and involve new construction techniques because no Cartesian product can generally be used and every state which eventually appears at a position must already be present locally—thus a fixed radius implies a limited number of states being potentially used at each time whatever the states set is.

We now give the construction τ. It transforms a CA $\mathcal{A}$ into a CCA $\tau(\mathcal{A})$ simulating it. As usual, the simulation occurs on a particular set of "legal" configurations. On such configurations each cell of $\mathcal{A}$ is directly simulated by some *data cell* of $\tau(\mathcal{A})$ surrounded by several *control cells*. The main idea is as follows. For a *data cell* to change its state we must guarantee that its future state already appears in its neighbourhood. For that purpose, *signal cells* placed regularly along the line take periodically each state of A (thanks to a shift behaviour) and thus eventually allow the transition of their neighbouring *data cell*. The construction uses 3 other types of *control cells*: 2 are used to ensure the global synchronism of the simulation—which is the difficult part—and 1 is used to propagate encoding errors—a feature essential for the correctness of the reduction. The synchronism is controlled by *offset cells* and *memory cells*. The configuration formed by successive *signal cells* is spatially periodic and consist in an alternation of letters of A and offset indicators. Offset indicators are placed in such a way that all *offset cell* are "aligned" with their corresponding offset indicator at the same time. Finally, the *memory cells* are used to keep the result of transitions—which occur asynchronously—until *offsets cells* are "aligned" with their indicators. Each time this "alignment" occurs *data cells* are updated with saved transition results and *memory cells* are cleaned up. For sake of simplicity we only give the explicit construction of τ on CA with radius 1 but it is straightforward to extend it to any radius.

Definition 5. *Let $\mathcal{A}$ be a* CA *(supposed of radius 1 in the present definition). Let $O = \{o_0, \dots, o_{n-1}\}$ (with $n = |A|$) and $\{\kappa\}$ be sets of states disjoint with A. Denote by $W_{\mathcal{A}}$ the set of words of the form $O \cdot (A \cup O) \cdot \{\kappa\} \cdot (A \cup O) \cdot (A \cup O) \cdot A$. Let $C_{\mathcal{A}}$ be the set of configurations which are a bi-infinite concatenation of words of $W_{\mathcal{A}}$. Finally let $K_S = \{a_j o_{j+1 \bmod n}, 0 \le j \le n-1\} \cup \{o_j a_j, 0 \le j \le n-1\}$ and $K_O = \{o_j o_{j+1 \bmod n}, 0 \le j \le n-1\}$. $\tau(\mathcal{A})$ is the* CCA *of radius 7 and state set $A_\tau = A \cup \{\kappa\} \cup O$ defined as follows:*

1. *for any* offset *states $o, o', o'' \in O$,* signal *states $s_1, s'_1, s''_1, s_2, s'_2, s''_2 \in A \cup O$,* memory *states $m, m', m'' \in A \cup O$ and* data *states $d, d', d'' \in A$,*

u	$\tau(\mathcal{A})(u)$
$d''\, o\, s_1\, \kappa\, s_2\, m\, d\, \boxed{o'}\, s'_1\, \kappa\, s'_2\, m'\, d'\, o''\, s''_1$	$\begin{cases} o' & \text{if } oo' \in K_O \\ \kappa & \text{otherwise,} \end{cases}$
$o\, s_1\, \kappa\, s_2\, m\, d\, o'\, \boxed{s'_1}\, \kappa\, s'_2\, m'\, d'\, o''\, s''_1\, \kappa$	$\begin{cases} s'_2 & \text{if } s'_1 s'_2 \in K_S \\ \kappa & \text{otherwise,} \end{cases}$
$s_1\, \kappa\, s_2\, m\, d\, o'\, s'_1\, \boxed{\kappa}\, s'_2\, m'\, d'\, o''\, s''_1\, \kappa\, s''_2$	κ
$\kappa\, s_2\, m\, d\, o'\, s'_1\, \kappa\, \boxed{s'_2}\, m'\, d'\, o''\, s''_1\, \kappa\, s''_2\, m''$	$\begin{cases} s''_1 & \text{if } s'_2 s''_1 \in K_S \\ \kappa & \text{otherwise,} \end{cases}$
$s_2\, m\, d\, o'\, s'_1\, \kappa\, s'_2\, \boxed{m'}\, d'\, o''\, s''_1\, \kappa\, s''_2\, m''\, d''$	$\begin{cases} s'_1 & \text{if } s'_1 \in \{\mathcal{A}(dd'd''), o'\}, \\ m' & \text{otherwise,} \end{cases}$
$m\, d\, o'\, s'_1\, \kappa\, s'_2\, m'\, \boxed{d'}\, o''\, s''_1\, \kappa\, s''_2\, m''\, d''\, o$	$\begin{cases} m' & \text{if } s'_1 = o' \\ d' & \text{otherwise,} \end{cases}$

2. for any $u \in A_\tau^{15} \setminus L(C_\mathcal{A})$, $\tau(\mathcal{A})(u) = \begin{cases} u_8 & \text{if } \kappa \notin \Sigma(u), \\ \kappa & \text{if } \kappa \in \Sigma(u) \end{cases}$

The 6 cases in the first part of the definition above are mutually exclusive because of a different position of state κ in u. Actually, in a configuration of $C_\mathcal{A}$, the type of a cell and the way it behaves is determined by its distance to the closest κ on its left, precisely: 3 for data cells, 2 for memory cells, 1 and 5 for signal cells and 4 for offset cells. Besides notice that for any configuration $c \in C_\mathcal{A}$, $\tau(\mathcal{A})$ checks whether

- the configuration formed by the successive offset cells in c, the *offset configuration* of c, is periodic of period $o_0 \dots o_{n-1}$;
- the configuration formed by the successive signal cells in c, the *signal configuration* of c, is periodic of period $o_0 a_0 o_1 a_1 \dots o_{n-1} a_{n-1}$.

Such configurations are characterised by the set of words of length 2 they contain (K_O and K_S respectively) and thus the checks can be done locally (line 1, 2 and 4 of the first point of definition 5). In the following, we will denote by $\Gamma_\mathcal{A}$ the set of configurations from $C_\mathcal{A}$ whose offset configuration and signal configuration are periodic with the respective periods given above. Informally, $\Gamma_\mathcal{A}$ is the set of "legal" configurations and it is straightforward to verify that $\Gamma_\mathcal{A}$ is stable under $\tau(\mathcal{A})$. The following lemma shows that $\tau(\mathcal{A})$ can simulate $\mathcal{A}$ on such configurations.

Lemma 2. *For any* CA $\mathcal{A}$, $\mathcal{A} \preceq \tau(\mathcal{A})$.

Proof. We show that $\mathcal{A}^{<n,1>} \sqsubseteq \tau(\mathcal{A})^{<6n,2n>}$ where $n = |A|$. Adopting the notations of definition 5, denote by ψ the following map from $A \times \{0, \dots, n-1\}$ to A_τ^6:

$$(\alpha, j) \mapsto o_j a_j \kappa o_{j+1 \bmod n} o_j a.$$

Then we define an injection Υ from A^n to A_τ^{6n} as follows:

$$\Upsilon(\alpha_0, \dots, \alpha_{n-1}) = \psi(\alpha_0, 0) \dots \psi(\alpha_j, j) \dots \psi(\alpha_{n-1}, n-1).$$

Now consider the set E of configurations of the form $\Upsilon(A^n)^\mathbb{Z}$. E is precisely the set of "legal" configurations ($E \subseteq \Gamma_\mathcal{A}$) which have just been "synchronised" (copy of memory cells to data cells and cleaning of memory cells). It is easy to verify that for $c \in E$ we have $\tau(\mathcal{A})^{<6n,2n>}(c) \in E$ (the spatial period of the signal configuration of c has length $2n$). Finally, $\tau(\mathcal{A})$ simulate 1 iteration of $\mathcal{A}$ every $2n$ iterations through the encoding Υ, precisely:

$$\begin{array}{ccc} (A^n)^\mathbb{Z} & \xrightarrow{\overline{\Upsilon}} & E \\ \big\downarrow \mathcal{A}^{<n,1>} & & \big\downarrow \tau(\mathcal{A})^{<6n,2n>} \\ (A^n)^\mathbb{Z} & \xrightarrow{\overline{\Upsilon}} & E \end{array}$$

To see this, first notice that starting from $c \in E$ data cells remain in the same state during $2n - 1$ steps until they take the state of their neighbouring memory cell at step $2n$. Second, memory cells are initially in a state from O and they wait for a particular state of A to be displayed by their corresponding signal cell. It is precisely the state obtained when applying a transition of $\mathcal{A}$ to the 3 local data cells. This state must eventually appear within $2n-1$ steps in each signal cell (thanks to the particular form of the signal configuration) so that after $2n-1$ steps, each memory cell contains the result of the transition of $\mathcal{A}$. After $2n$ steps the configuration is finally synchronised by the copy of memory cells to data cells and the cleaning of memory cells. □

Lemma 3. *For any* CA $\mathcal{A}$ *and any surjective* CA $\mathcal{B}$*, if* $\mathcal{B} \sqsubseteq \tau(\mathcal{A})^{<m,m'>}$ *for some* $m, m' \in \mathbb{N}$ *then either* $\mathcal{B}$ *is the identity map, or* $\mathcal{B} \preceq \mathcal{A}$*.*

Proof. Let $\phi : B \to A_\tau^m$ be the injection involved in the relation $\mathcal{B} \sqsubseteq \tau(\mathcal{A})^{<m,m'>}$ and let L_ϕ be the semi-group generated by the set of words $\{\phi(b), b \in B\}$. Comparing L_ϕ to the language $L(\Gamma_\mathcal{A})$, two cases are to be considered:

- if $L_\phi \nsubseteq L(\Gamma_\mathcal{A})$ then either κ does not appear in L_ϕ and then $\mathcal{B} = id$ (since $\tau(\mathcal{A})$ does nothing on configuration without κ), or there is some $b_0 \in B$ such that κ appears in $\phi(b_0)$. In the latter case let $w \in L_\phi \setminus L(\Gamma_\mathcal{A})$ be a concatenations of words from $\phi(B)$ and consider the periodic configuration c_0 of period $\phi(b_0)w$. c_0 can be chosen different from $\overline{\kappa}$ (otherwise it implies that $\phi(b) = \kappa^m \;\; \forall b \in B$, hence $\mathcal{B}$ has only 1 state and then clearly $\mathcal{B} \preceq \mathcal{A}$). Let $p = |\phi(b_0)w|$. Then $\kappa^p \notin L(c_0)$. Besides, since $\mathcal{B}$ is surjective and $c_0 \in (\phi(B))^\mathbb{Z}$, the simulation of $\mathcal{B}$ by $\tau(\mathcal{A})$ implies that there exists some $c_{-1} \in \phi(B)^\mathbb{Z}$ such that $\tau(\mathcal{A})^{m'}(c_{-1}) = c_0$. Then, if $p-1 \geq 2$, $\kappa^{p-1} \notin L(c_{-1})$ (otherwise $\kappa^p \in L(c_0)$) and we can continue the same reasoning so that there must be some $c \in \phi(B)^\mathbb{Z}$ such that $\kappa^2 \notin L(c)$ and $\tau(\mathcal{A})^t(c) = c_0$ for some t. Clearly $\kappa \in L(c)$ since $\kappa \in L(c_0)$ and $\tau(\mathcal{A})$ is a CCA. Finally, by surjectivity of $\mathcal{B}$, there is c' such that $\tau(\mathcal{A})(c') = c$. Again we have $\kappa \in L(c')$ and thus $c' \in \Gamma_\mathcal{A}$ because a configurations not in $\Gamma_\mathcal{A}$ containing a κ necessarily leads to a configuration containing κ^2. Since $\Gamma_\mathcal{A}$ is stable under $\tau(\mathcal{A})$, we must have $c_0 \in \Gamma_\mathcal{A}$: contradiction with the initial choice of c_0.
- now suppose $L_\phi \subseteq L(\Gamma_\mathcal{A})$. If $c \in \Gamma_\mathcal{A}$ and c' are such that $\tau(\mathcal{A})^t(c') = c$ for some t then $c' \in \Gamma_\mathcal{A}$ because any $d \in \tau(\mathcal{A})\big(A_\tau^\mathbb{Z} \setminus \Gamma_\mathcal{A}\big)$ is such that $\kappa^2 \in L(d)$. Moreover the orbit of c' enters E (defined in proof of lemma 2) every $2n$ steps, so when $t \geq 2n$ we can consider

  $$\chi(c) = \max_{t' \leq t} \{\tau(\mathcal{A})^{t'}(c') : \tau(\mathcal{A})^{t'}(c') \in E\}.$$

  Notice that the definition is independent of t and c' (because from $\chi(c)$ to c, $\tau(\mathcal{A})$ does not alter the state of data cells and since $\chi(c) \in E$ it is entirely determined by its data cells). Since $\mathcal{B}$ is surjective, any configuration of $\phi(B)^\mathbb{Z}$ can be reached in arbitrarily many steps so χ is well-defined on $\phi(B)^\mathbb{Z}$. Notice also that χ is a local mapping (each bloc of 6 states of c is mapped to a single bloc of 6 states in $\chi(c)$) and that it is injective (by determinism of $\tau(\mathcal{A})$). Moreover, on $\phi(B)^\mathbb{Z}$, χ commutes with $\tau(\mathcal{A})^{2n}$. Finally, notice that the mapping $\overline{\Upsilon}$ is one-to-one from $(A^n)^{\mathbb{Z}}$ to E. Then, from lemma 2 and properties of χ, we have the following commutative diagram :

$$\begin{array}{ccccccc}
(B^{6n})^{\mathbb{Z}} & \xrightarrow{\overline{\phi^{6n}}} & (A_\tau^{6mn})^{\mathbb{Z}} & \xrightarrow{\overline{\chi^{mn}}} & (\Upsilon(A^n)^m)^{\mathbb{Z}} & \xrightarrow{\overline{(\Upsilon^m)^{-1}}} & (A^{mn})^{\mathbb{Z}} \\
\big\downarrow \mathcal{B}^{<6n,2n>} & & \big\downarrow \tau(\mathcal{A})^{<6nm,2nm'>} & & \big\downarrow \tau(\mathcal{A})^{<6nm,2nm'>} & & \big\downarrow \mathcal{A}^{<nm,m'>} \\
(B^{6n})^{\mathbb{Z}} & \xrightarrow{\overline{\phi^{6n}}} & (A_\tau^{6mn})^{\mathbb{Z}} & \xrightarrow{\overline{\chi^{mn}}} & (\Upsilon(A^n)^m)^{\mathbb{Z}} & \xrightarrow{\overline{(\Upsilon^m)^{-1}}} & (A^{mn})^{\mathbb{Z}}
\end{array}$$

(here χ denotes the local map from A_τ^6 to A_τ^6 mentioned above). This shows $\mathcal{B}^{<6n,2n>} \sqsubseteq \mathcal{A}^{<nm,m'>}$ by the injection $(\Upsilon^m)^{-1} \circ \chi^{mn} \circ \phi^{6n}$. Hence $\mathcal{B} \preceq \mathcal{A}$ by definition. □

Theorem 2. *There exists r_0 such that for any fixed radius $r \geq r_0$, it is undecidable to know whether a* CCA *of radius r is intrinsically universal or not.*

Proof. Let $\mathcal{X}$ be the following CA over $\{0,1\}$: $\mathcal{X}(a,b,c) = b + c \bmod 2$. $\forall m, n$, $\mathcal{X}^{<m,n>}$ is always surjective but neither the identity map so we deduce from lemma 2 and lemma 3 that $\forall \mathcal{A}$: $\mathcal{X} \preceq \mathcal{A} \Leftrightarrow \mathcal{X} \preceq \tau(\mathcal{A})$.

N. Ollinger established in [1] the undecidability of intrinsic universality[1] by giving a recursive construction U_q such that for any CA $\mathcal{A}$ of radius 1:

- $U_q(\mathcal{A})$ has radius r_U (where r_U only depends on U_q, not on $\mathcal{A}$),
- if $\mathcal{A}$ is q-nilpotent over periodic configurations then $\mathcal{X} \not\preceq U_q(\mathcal{A})$,
- and if $\mathcal{A}$ is not q-nilpotent over periodic configurations then $U_q(\mathcal{A})$ is intrinsically universal.

A CA is q-nilpotent over periodic configurations if every periodic configuration leads to the same configuration $\overline{q}$ in finite time. The problem of nilpotency over periodic configurations for CA of radius 1 was proven undecidable in [10]. From the previous observation, the recursive construction $\tau \circ U_q$ has the same properties as U_q and maps to CCA of fixed radius $r_0 = 7r_U$. □

The following corollary shows that, as in the general case, there is no limit on how complex a CCA of fixed radius can be without being intrinsically universal. Hence non-universal CCA cannot be reduced to a negligible set of simple exceptions among an overwhelming majority of universal objects.

Corollary 3. *There exits r_0 such that for any $r \geq r_0$ and for any non-universal* CCA *$\mathcal{A}$ of radius r, there is a non-universal* CCA *$\mathcal{B}$ of radius r such that $\mathcal{A} \preceq \mathcal{B}$ but $\mathcal{B} \not\preceq \mathcal{A}$.*

Proof. Let $r \geq r_0$ be a fixed radius for all following CA, where r_0 is the constant of theorem 2. First we show that there is no CCA $\mathcal{A}$ which is non-universal and such that for all non-universal CCA $\mathcal{B}$, $\mathcal{B} \preceq \mathcal{A}$. As already pointed out in

[1] In [1], the undecidability result is not formulated for a fixed radius, but it is easy to check that the result remains true.

the general case by N. Ollinger in [5], this follows from the semi-decidability of intrinsic universality: with a maximal CCA for non-universal CCA we could semi-decide non-universality and combining the two semi-decision procedures we could finally decide intrinsic universality which contradicts theorem 2.

Now let us show that for any pair $\mathcal{A}$, $\mathcal{B}$ of non-universal CCA, there is a non-universal CCA $\mathcal{C}$ such that $\mathcal{A} \preceq \mathcal{C}$ and $\mathcal{B} \preceq \mathcal{C}$. This fact complete the proof since it implies that there cannot be more than one non-universal CCA which is maximal for non-universal CCA. $\mathcal{C}$ can be chosen as follows. Let $\ll$ be a total ordering on $A \cup B$ such that $\forall a \in A$ and $\forall b \in B$: $b \ll a$ (up to renaming of states, we can suppose $A \cap B = \emptyset$). Then for any $u \in (A \cup B)^{2r+1}$, $\mathcal{C}$ is defined by:

$$\mathcal{C}(u) = \begin{cases} \mathcal{A}(u) & \text{if } u \in A^{2r+1}, \\ \mathcal{B}(u) & \text{if } u \in B^{2r+1}, \\ \max \Sigma(u) & \text{otherwise,} \end{cases}$$

where max is relative to the order $\ll$. Clearly $\mathcal{C}$ is a CCA and $\mathcal{A} \preceq \mathcal{C}$ and $\mathcal{B} \preceq \mathcal{C}$. Moreover if $\mathcal{C}$ is universal, then $\mathcal{A}$ or $\mathcal{B}$ must also be universal. To see this consider a universal CA $\mathcal{U}$ such that for any pair a, b of states the periodic configuration of period ab is a fixed point (to be convinced of the existence of $\mathcal{U}$ notice that any behaviour can be specified on "non-coding" configurations in the construction of a universal CA). Hence, if $\mathcal{C}$ is universal then $\mathcal{U} \sqsubseteq \mathcal{C}^{<m,n>}$ for some $m, n \in \mathbb{N}$. And, denoting by ϕ the injection involved in this relation, we must have $\phi(U) \subseteq A^m$ or $\phi(U) \subseteq B^m$ because, otherwise, there would exists u_1 and u_2 in U such that the word $\phi(u_1)\phi(u_2)$ contains both a state from A and a state from B. From the definition of $\mathcal{C}$, the periodic configuration of period $\phi(u_1)\phi(u_2)$ cannot be a fixed point (because any state of B ultimately disappears) which contradicts the property of $\mathcal{U}$. Therefore we must have either $\mathcal{U} \sqsubseteq \mathcal{A}^{<m,n>}$ or $\mathcal{U} \sqsubseteq \mathcal{B}^{<m,n>}$. □

3 What about the general case?

There is no zero-one law for monotonic properties on CA in general. Indeed, let $\mathcal{P}$ be the property of possessing at least one quiescent state ($q \in A$ is quiescent for $\mathcal{A}$ if $\mathcal{A}(\overline{q}) = \overline{q}$). Then $\mathcal{P}$ is an increasing property but $0 < \mu(\mathcal{P}) < 1$. To be precise, it is not difficult to show that

$$\mu(\neg\mathcal{P}) = \lim_{n\to\infty} \left(1 - \frac{1}{n}\right)^n = \frac{1}{e}.$$

Actually, there are also increasing properties with density 0. This is what we are going to show with the property $\mathcal{P}_{\sqsubseteq}$ of possessing a non trivial sub-automaton: $\mathcal{P}_{\sqsubseteq} = \{\mathcal{A} : \exists \mathcal{B}, 1 < |B| < |A| \text{ and} \mathcal{B} \sqsubseteq \mathcal{A}\}$.

Before giving the proof, notice that this shows at least that arguments similar to those of theorem 1 cannot be used in the general case. The following lemma establish a useful upper bound.

Lemma 4. $\exists n_0 \forall n \geq n_0 \forall k, 2 \leq k \leq n-1 : \left(\frac{k}{n}\right)^{k^{2r+1}} \leq n^{-2k}$.

Proof. Taking the log of the expression, it is sufficient to show that the following relation eventually holds uniformly for k: $\frac{k^{2r}}{2} \log \frac{n}{k} \geq \log n$. This majoration is obtained by a standard analysis of the real function

$$f(k,n) : k, n \mapsto \frac{k^{2r}}{2} \log \frac{n}{k}$$

as follows. First, $f(2,n) \geq \log n$ and $f(n-1,n) \geq \log n$ are eventually true. Then $\frac{\partial f}{\partial k}(k,n) = rk^{2r-1} \log \frac{n}{k} - \frac{k^{2r-1}}{2}$ so it equals zero for $k = e^{-\frac{1}{2r}} n$. Finally, for any $0 < \alpha < 1$, $f(\alpha n, n)$ is eventually greater than $\log n$ since it is a monomial in n with a positive coefficient. ☐

Proposition 1. *For any fixed radius, almost no* CA *possesses a non-trivial sub-automaton:* $\mu(\mathcal{P}_{\sqsubseteq}) = 0$.

Proof. For $2 \leq k \leq n-1$, the probability that $\mathcal{A} \in A_n$ has a sub-automaton with k states is bounded by $C_n^k \left(\frac{k}{n}\right)^{k^{2r+1}}$: for a fixed choice of k states, each transition involving only these k states must lead to one of them. Hence we have:

$$\mu(\mathcal{P}_{\sqsubseteq}) \leq \lim_{n\to\infty} \sum_{k=2}^{n-1} C_n^k \left(\frac{k}{n}\right)^{k^{2r+1}}. \tag{1}$$

Using majoration of lemma 4 in the inequality, we obtain:

$$\begin{aligned}
\mu(\mathcal{P}_{\sqsubseteq}) &\leq \lim_{n\to\infty} \sum_{k=2}^{n-1} C_n^k \left(\frac{1}{n^2}\right)^k \\
&\leq \lim_{n\to\infty} \left(\sum_{k=0}^{n} C_n^k \left(\frac{1}{n^2}\right)^k - \sum_{k\in\{0,1,n\}} C_n^k \left(\frac{1}{n^2}\right)^k \right) \\
&\leq \lim_{n\to\infty} \left(\left(1 + \frac{1}{n^2}\right)^n - 1 - \frac{1}{n} - \frac{1}{n^{2n}} \right).
\end{aligned}$$

Thus $\mu(\mathcal{P}_{\sqsubseteq}) = 0$. ☐

4 Perspectives and open problems

We have shown that intrinsic universality is ubiquitous in CCA. Actually, the result extends to any reasonable notion of universality including Turing universality. We insist however that the set of intrinsically universal CCA is rich because non recursive. Moreover, lemma 3 shows that it is possible given any CA to construct a CCA that is somehow similar with respect to $\preceq$. Can this lemma be extended and more precisely can we characterise $\simeq$-classes containing a CCA? Or at least give a large collection of $\simeq$-classes containing a CCA?

Besides, although the density result for CCA gives a lower bound on the growing rate of intrinsically universal CA, the density problem for CA remains open since CCA constitute a negligible subset of cellular automata (see proposition 1). However, if this density turned out to be non-zero, it would mean that a significant part of CA acquire any sub-structure by simple spatio-temporal transformation while they are locally totally unstructured (proposition 1). To that extent, a study of the way a CA can or cannot acquire structure by spatio-temporal transformations reveals to be essential to decide the density problem. In [11] it is shown that some CA avoid some sub-automaton size even up to spatio-temporal transformations. Can we extend this kind of result and show that there exists some CA which has no non-trivial sub-automaton at any scale? Or conversely is there for any CA some unavoidable transformation giving him some non-trivial structure even if it is totally unstructured locally?

5 Acknowledgement

We thank E. Jeandel for helpful discussions regarding proposition 1.

References

1. Ollinger, N.: The intrinsic universality problem of one-dimensional cellular automata. In: Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science (2003) 632–641
2. Banks, E.R.: Universality in cellular automata. In: Eleventh Annual Symposium on Switching and Automata Theory, Santa Monica, California, IEEE (1970)
3. Ollinger, N.: The quest for small universal cellular automata. In: International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science (2002) 318–330
4. Mazoyer, J., Rapaport, I.: Inducing an Order on Cellular Automata by a Grouping Operation. In: Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science (1998)
5. Ollinger, N.: Automates Cellulaires : structures. PhD thesis, École Normale Supérieure de Lyon (2002)
6. Albert, J., Čulik, II, K.: A simple universal cellular automaton and its one-way and totalistic version. Complex Systems **1** (1987) 1–16
7. Theyssier, G.: Captive cellular automata. In: Mathematical Foundations of Computer Science, Lecture Notes in Computer Science (2004) 427–438
8. Kůrka, P.: Languages, equicontinuity and attractors in cellular automata. Ergodic Theory and Dynamical Systems **17** (1997) 417–433
9. Hedlund, G.A.: Endomorphisms and Automorphisms of the Shift Dynamical Systems. Mathematical Systems Theory **3** (1969) 320–375
10. Mazoyer, J., Rapaport, I.: Global fixed point attractors of circular cellular automata and periodic tilings of the plane: undecidability results. Discrete Mathematics **199** (1999) 103–122
11. Mazoyer, J., Rapaport, I.: Additive cellular automata over Z_p and the bottom of $(CA, \leq)$. In: Mathematical Foundations of Computer Science, Lecture Notes in Computer Science (1998) 834–843