Traced communication complexity of cellular automata[⋆]

Eric Goles[a] Pierre Guillon[b,*] Ivan Rapaport[b]

[a]*Facultad de Ingeniería y Ciencias Universidad Adolfo Ibañez, Santiago, Chile*

[b]*DIM - CMM, UMI CNRS 2807, Universidad de Chile, Santiago, Chile*

Abstract

We study cellular automata with respect to a new communication complexity problem: each of two players know half of some finite word, and must be able to tell whether the state of the central cell will follow a given evolution, by communicating as little as possible between each other. We present some links with classical dynamical concepts, especially equicontinuity, expansivity, entropy and give the asymptotic communication complexity of most elementary cellular automata.

Key words: cellular automata, communication complexity

Introduction

Cellular automata (CA) were introduced in the fifties in order to represent natural complex systems. They were soon studied as a computational model, especially for parallelism. Indeed, they can be seen as wide networks of small machines communicating locally.

Introduced in [11], the communication complexity of a function f measures how much data must be exchanged between two machines which have part of the input of f in order for one to be able to compute f. This approach, representing the degree of parallelism needed, was adapted to the context of CA in

[⋆] This work has been supported by the ECOS-Sud Project (P. G.), Fondecyt 1070022, 1090156, BASAL-CMM (I. R.), Fondecyt 1100003, BASAL-CMM, Anillo Act88, SFI-Santa Fe (E. G.).

[*] Corresponding author.

Email addresses: eric.chacc@uai.cl (Eric Goles), pguillon@dim.uchile.cl (Pierre Guillon), rapaport@dim.uchile.cl (Ivan Rapaport).

[4] and gave interesting results in [5,6,7] that help understand the computation represented by some CA. The complexity notion that these references use is somehow orthogonal to classical ones. For instance, bipermutive CA, which show strongly chaotic behaviors for many reasonable definitions, appear to be simple with respect to this complexity measure.

In this article, we study a new variant of communication complexity problem, which involves more links with dynamical chaos. In the first section, we give the definition of cellular automata and communication complexity. Then we address some properties of cellular automata which allow some simple protocols. The third and forth section are devoted to the links with trace, entropy and expansivity. We finally discuss links with simulations.

1 Definitions

1.1 Cellular automata

A CA consists in a sequence of cells with states in some alphabet A, evolving according to their neighbors. We restrict our study to one-dimensional CA with nearest neighbors. This choice will be crucial for our definitions, but they still somehow apply to all one-dimensional CA since it is known that they can be simulated in a direct way by CA with nearest neighbors. In this context, a *cellular automaton* (CA) is a map $f : A^3 \to A$. In particular, if $A = \{0, 1\}$, there are exactly 256 so-called *elementary* CA, which can be referred to by the following canonical number: $\sum_{a,b,c\in\{0,1\}} f(abc)2^{4a+2b+c}$.

We denote $[i, j]$ the integer interval $\{k \in \mathbb{Z}|\, i \leq k \leq j\,\}$. In order to simplify notation, a *configuration* w is a finite word of odd length $2n+1$ whose indexes are centered around the origin, *i.e.* $w = w_{-n}w_{-n+1} \dots w_n \in A^{[-n,n]}$. Moreover, if $[i, j]$ is a subinterval of an interval I and $w \in A^I$ then $w_{[i,j]}$ represents the pattern $w_i \dots w_j$. If $u \in A^{[i,j]}$ and $v \in A^{]j,k]}$ for some intervals $[i, j]\,,]j, k] \subset \mathbb{Z}$, then we will note $uv \in A^{[i,k]}$ the corresponding obvious juxtaposition of the two words.

The local rule of a CA can be applied in a parallel and synchronous way: $f : A^3 \to A$ is extended to all $w \in A^{[i,j]}$ with $j-i \geq 2$ by defining $\tilde{f}(w) \in A^{[i+1,j-1]}$ as $\tilde{f}(w)_k = f(w_{k-1}, w_k, w_{k+1})$ for all $k \in [i+1, j-1]$; for convenience $\tilde{f}$ is again written as f. We can therefore consider the iteration f^t over any word $w \in A^{[i,j]}$ with $j - i \geq 2t$.

Given an initial configuration $w \in A^{[-n,n]}$, its trace over a non-empty interval $[i, j] \subset [-n, n]$ of cells is the sequence of words $f^t(w)_{[i,j]} \in A^{[i,j]}$ that one observes in the space-time diagram for input w. One has to restrict this to time steps $0 \leq t \leq n - \max(|i|, |j|)$ for which the states of all cells in $[i, j]$ are defined. With the exception of Section 4, in the paper only the special case $i = j$ is considered. One then gets:

$$\begin{aligned} T_f^{\{i\}} : A^{[-n,n]} &\to A^{[0,n-|i|]} \\ w &\mapsto (t \mapsto f^t(w)_i) \ . \end{aligned}$$

We will write $T_f = T_f^{\{0\}}$, corresponding to the central column of the computation triangle. It is a characteristic symbolic system linked to the CA dynamics, which was for instance proved very complex in [1].

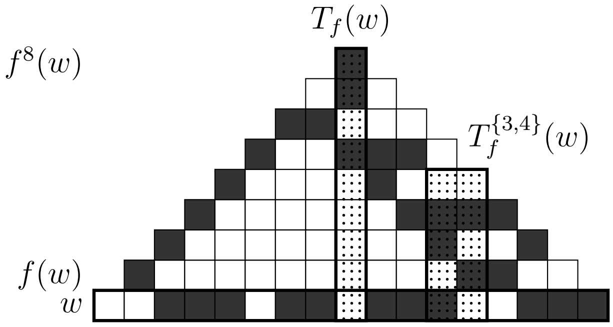

Figure 1. Some traces of the configuration $w = 00101100000101110$ by CA rule 28.

1.2 Communication complexity

Let f be a map defined over some Cartesian product $X \times Y$ into A. If $(x, y) \in X \times Y$, consider that two people, Alice and Bob, are given x and y respectively, and must compute the value $f(x, y)$ by communicating as little as possible between each other. This gives two variants of *communication complexity* (CC). The *multi-round CC* of f is the cost of the best communication protocol between the two players allowing one of them to produce the result $f(x, y)$. In other words, assume Alice and Bob agree on some deterministic protocol depending only on function f (a sequence of data exchange from one to another where each message may depend on the previous ones); we are interested in the maximum for all possible inputs x and y, of the number of bits exchanged between them, eventually allowing one of them to compute the result. The multi-round CC is the minimum of these maxima for all possible protocols they could have agreed on.

The *left* (*one-round*) *CC* is the worst case number of bits that Alice needs to send in order to allow Bob to directly compute the result; it corresponds to a protocol where only Alice sends information. We can similarly define the *right*

CC. Of course, the multi-round CC is at most equal to the minimum between the two one-round CCs.

A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ can be represented by the square matrix M of size 2^n such that $M_{i,j} = f((u_{n-1} \dots u_0), (v_0 \dots v_{n-1}))$ if $i = \sum_{k<n} u_k 2^k$ and $j = \sum_{k<n} v_k 2^k$. Then it is known (see for instance [9]) that the left (resp., right) CC of f can be seen as the logarithm of the number of distinct lines (resp., columns) in the matrix M. Moreover, the multi-round CC is conjectured in [10] to be polylogarithmic in the rank of M. We will see some examples of such matrices, which help to get an intuition of the asymptotic CC: the complexity of the matrix in terms of number of distinct columns or lines is very visual.

A subset $S \subset X \times Y$ is a *fooling set* for f if for every two distinct pairs $(x,y),(x',y') \in S$, we have $f(x,y) = f(x',y')$ and either $f(x',y)$ or $f(x,y')$ is distinct from $f(x,y)$.

Proposition 1 ([9]) *If a function f admits a fooling set S, then its multi-round CC is lower-bounded by* $\log |S|$.

1.3 Traced communication complexity

We can actually view a CA f as computing a function. The sequence of words $f^t(w)$ for $0 \le t < n$ and $w = w_{-n} \dots w_n \in A^{[-n,n]}$ (drawn in Figure 1) is the *computation triangle.* If we consider that Alice initially knows $w_{-n} \dots w_0$ and Bob $w_0 \dots w_n$, it is obvious that the former can compute the word $f^t(w)_{[t-n,-t]}$ and the latter the word $f^t(w)_{[t,n-t]}$, for $0 \le t \le \left\lfloor \frac{n}{2} \right\rfloor$. The other parts of the computation triangle will a priori require information exchange between Alice and Bob.

In [4,5], CC has been applied to CA, basically as that of the computation of the top cell, *i.e.* the CC of the map $(w_{[-n,-1]}, w_{[1,n]}) \mapsto f^n(w)$, for any $n \in \mathbb{N}$, where Alice and Bob share some fixed w_0. We will refer to this notion as *classical CC*. In [6], this notion was generalized to arbitrary cutting position (not always 0) between Alice's word and Bob's. In [7], some new problems, the so-called *invasion* and *cycle length*, were associated to the CA. In each of these, the idea is to consider the CA as complex (resp. simple) if the CC is asymptotically linear (resp. constant) when the size n of the input grows to infinity.

In a binary alphabet, the classical problem is for Alice and Bob to know whether the top cell of the computation triangle is a 1. Instead of this we can require them to determine whether some state 1 appears in the central column, *i.e.* whether $f^t(w)_0 = 1$ for some step $t \in [0,n]$. More generally, having fixed an arbitrary alphabet A, an integer $n \in \mathbb{N}$ and a word $z \in A^{n+1}$, consider the indicator function:

$$\begin{aligned}\hat{f}_z : A^{[-n,1]} \times A^{[1,n]} &\to \{0,1\} \\ (u,v) &\mapsto \begin{cases} 0 & \text{if } T_f(uz_0v) = z \\ 1 & \text{otherwise.} \end{cases}\end{aligned}$$

Its CC will be referred to as the *traced CC.*

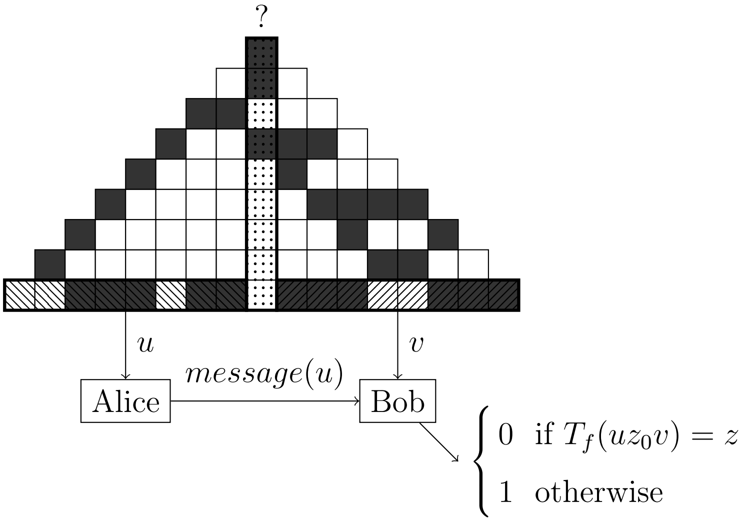
?
u
v
$message(u)$
Alice
Bob
$\begin{cases} 0 & \text{if } T_f(uz_0v) = z \\ 1 & \text{otherwise} \end{cases}$

Figure 2. One-round protocol for the traced CC.

Note that the rule f and the word z are fixed, hence allowing Alice and Bob to agree on a protocol which will depend on them. We will see some examples of simple reasoning on the local rule to bound the CC corresponding to some given word z, often the uniform word $z = 0^{n+1}$. We then study some properties inspired by topological dynamics which imply either low CC for any word z or high CC for some word. The idea is more or less to consider a CA as (extremely) complex if there is a linear map of n which lower-bounds the maximal multi-round CC corresponding to the words of length n. On the contrary, it will be considered as (extremely) simple if any such CC is bounded by a constant. When considering the word 0^{n+1}, note that (each version of) the CC $\hat{f}_{0^{n+1}}$ is nondecreasing on n, since if a 1 appears in the trace within n steps, then in particular it appears within $n+1$ steps. We will abusively say that the CC of $\hat{f}_{0^{n+1}}$ is constant when it is asymptotically, *i.e.* when it is bounded by some constant.

In the next sections, an alphabet A, an integer $n \in \mathbb{N}$ and a word $z \in A^{n+1}$ are fixed, unless explicitly stated otherwise. Each figure presented further will represent, for some elementary CA f, the matrix of the function $\hat{f}_{0^{n+1}}$ (assimilating gray with black), superposed with the corresponding matrix corresponding to the classical CC (assimilating white with gray); in other words, gray cells correspond to the words whose evolution has reached state 1 but eventually came back to state 0.

2 Simple communications

2.1 One-sided rules

Similarly to the classical CC, the traced CC of any one-sided CA, *i.e.* those that depend only on either left cells or right cells, is clearly constant: one of the two parties is completely able to compute the function $\hat{f}_z$ by himself. We can be a little more general in the (nearly) uniform case.

If $B \subset A$, then a CA f is *B-leftsided* if $\forall a, c, d \in A, b \in B, f(abc) = f(abd)$. Similarly, we define *$B$-rightsided* CA. A CA is *B-onesided* if it is either B-leftsided or B-rightsided. If all letters of z are in B, one party can compute the evolution of the central cell if it stays in B; if it does not, then the trace cannot be z. Hence, no communication is needed.

Proposition 2 *For any B-onesided CA f, the one-round CC for $\hat{f}_z$, with $z \in B^{n+1}$, is at most* 1.

Proof. Let us prove the result for left CC; the case of right CC is symmetric.

- If it is B-leftsided, Alice can compute whether some letter which is not in B appears in the central cell and give the answer to Bob.
- If it is B-rightsided, she does not say anything to Bob; he will be able to find the answer by himself. □

For $z = 0^{n+1}$, the previous proposition can be applied to the 64 0-onesided elementary CA (B-onesided for $B = \{0\}$), *i.e.* those whose number can be written as $a_7a_6a_4a_4a_3a_2a_0a_0$ or $a_7a_6a_1a_0a_3a_2a_1a_0$ in base 2.

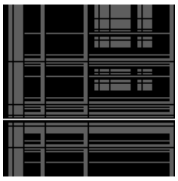

Figure 3. Matrix of the rule 143.

2.2 Spreading states

A state $0 \in A$ is *quiescent* for the CA f if $f(000) = 0$. Consider a subalphabet $B \subset A$. We note $\bar{B}$ the complementary subalphabet $A \setminus B$ (we may also note $\bar{0} = A \setminus \{0\}$). We say that B is *left semi-strongly spreading* (resp., *weakly spreading*) for the CA f if $f(A\bar{B}B) \subset B$ (resp., $f(\bar{B}\bar{B}B) \subset B$). Symmetrically, right spreadingness can be defined.

We can see that any elementary CA for which state 1 is both left and right semi-strongly spreading and state 0 is quiescent has $\hat{f}_{0^{n+1}}(u,v) = 1$ if and only if $u0v$ contains some 1, which will progressively spread towards the center. The following proposition generalizes this observation.

Proposition 3 *If* 0 *is quiescent and* $\bar{0}$ *is left semi-strongly spreading, then the right CC for* $\hat{f}_{0^{n+1}}$ *is at most* 1.

Proof. If Bob has a letter in $\bar{0}$, then he knows that it will spread towards the center, and he can say with one bit to Alice that $\hat{f}$ will give 1. Otherwise Alice knows that he has word $v = 0^n$. □

Symmetrically, if 0 is quiescent and $\bar{0}$ is right semi-strongly spreading, then the left CC for $\hat{f}_{0^{n+1}}$ is constant. On the other hand, if f is an elementary CA such that $\bar{0}$ is semi-strongly spreading but 0 is not quiescent, then a rapid case study shows that we always have $\hat{f}_{0^{n+1}} = 1$ as soon as $n > 1$. We globally obtain, whenever $\bar{0}$ is semi-strongly spreading, a constant CC for $\hat{f}_{0^{n+1}}$. This corresponds to the 96 elementary CA whose number in base 2 can be written either as $a_7a_611a_3a_2a_1a_0$ or as $a_7a_61a_4a_3a_21a_0$.

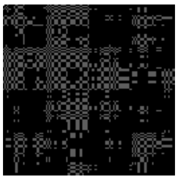

Figure 4. Matrix of the rule 182.

2.3 Stagnating states

A word $u \in A^*$ is *stagnating* for the CA f if $\forall a, b \in A, f(aub) = u$.

In this subsection, we assume $A = \{0,1\}$. Note that if 0 is stagnating, then the rule is both 0-leftsided and 0-rightsided and we have already seen that the one-round CC is constant. We can generalize this to the following case.

Proposition 4 *If* 0 *is quiescent and* 1 *is neither left nor right weakly spreading, then both one-round CCs for* $\hat{f}_{0^{n+1}}$ *are at most* 1.

Proof.

- If $f(101) = 0$, then 0 is stagnating; this is a subcase of Proposition 2.
- If $f(101) = 1$, then 00 is stagnating, but single 0s disappear. Hence $\hat{f}(u, v) = 0$ if and only if $u_{-1} = 0$ or $v_1 = 0$. The result of this test can be transmitted in one bit. □

This proposition applies to the elementary CA who map 0 to any neighborhood containing two consecutive 0s, *i.e.* whose number in base 2 can be written $a_7a_6a_50a_3a_200$.

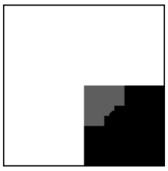

Figure 5. Matrix of the rule 232.

Remark 5 *Any elementary CA* f *with stagnating* 1 *has a CC for* $\hat{f}_{0^{n+1}}$ *equal to its classical CC. Indeed, for any words* $u \in A^{[-n,-1]}$ *and* $v \in A^{[1,n]}$, $\hat{f}_{0^{n+1}}(u, v)$ *is equal to* $f^n(u0v)$. *For instance, from [7], the CA 222 has logarithmic CC for* $\hat{f}_{0^{n+1}}$.

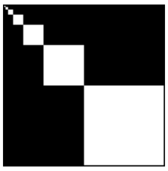

Figure 6. Matrix of the rule 222.

3 Trace protocol

In order to decide whether $T_f(uz_0v) = z$ or not, Alice and Bob need to compute only until the first step $t \in [1, n]$ when the central state does not correspond to z_t. In a first approximation, each of them can compute their side by assuming that the central column corresponds to z – note that this central column and his/her initial word completely determine his/her half-triangle, since the rule has radius 1 – and then check if this assumption could lead to a contradiction.

Formally, for $v \in A^{[1,n]}$ we define $f^0_{\to z}(v) = v$ and for $t < n-1$, $f^{t+1}_{\to z}(v) = f(z_t f^t_{\to z}(v))$, which is still an element of $A^{[1,n]}$. Then $T_{f\to z}(v) = (f^t_{\to z}(v)_1)_{t<n}$ represents the column that should be just right to the column z in a computation triangle where Bob has word v (if ever such a triangle is possible).

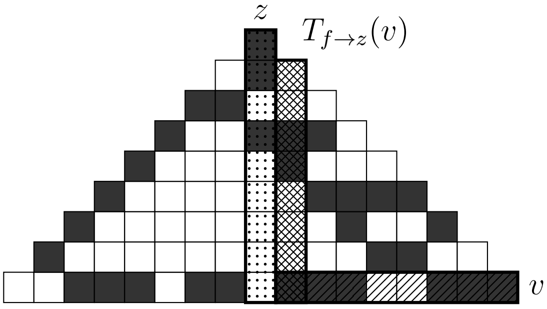

Figure 7. Trace protocol in Bob's side.

The word $T_{f\to z}(v)$ actually represents a valid message from Bob to Alice. In particular, if it has a short algorithmic complexity, then the right CC will be low.

Proposition 6 *The right CC for $\hat{f}_z$ is upper-bounded by $\left\lceil \log \left| T_{f\to z}(A^{[1,n]}) \right| \right\rceil$.*

Proof. If Alice has word u, Bob word v and m is such that for any step $t < m$, the central letter of $f^t(uz_0v)$ is z_t, then by an immediate recurrence, we have $\forall t < m, f^{t+1}(uz_0v)_0 = f(T_{f\leftarrow z}(u)_t z_t T_{f\to z}(v)_t)$. In $\left\lceil \log \left| T_{f\to z}(A^{[1,n]}) \right| \right\rceil$ bits, Bob can encode the data of the word $T_{f\to z}(v)$, and give it to Alice. She can then compute $T_{f\leftarrow z}(v)$; she answers that $\hat{f}_z(u,v) = 0$ if and only if the successive central cells represent a valid application of the local rule when juxtaposing the three columns.

Let us see a little variant of the previous result. Consider the set $\tau_{f\to z} = \left\{ T_f^{\{1\}}(w) \middle| w \in A^{[-n,n]} \text{ and } T_f(w) = z \right\}$ of all possible columns juxtaposed at the right of z in some (full valid) computation triangle. Note that all of its elements can be written as $T_{f\to z}(w_{[1,n]})$, but the converse is false in the sense that the right half-triangle built with some $T_{f\to z}(v)$ could be impossible to extend to the left.

Proposition 7 *The right CC for $\hat{f}_z$ is upper-bounded by $\lceil \log(|\tau_{f\to z}| + 1) \rceil$.*

Proof. Looking back at the previous proof, note that Bob can encode in $\lceil \log(|\tau_{f\to z}| + 1) \rceil$ bits the data of the word $T_{f\to z}(v)$ in the case when it belongs to $\tau_{f\to z}$, and some prespecified extra code otherwise. In the first case, Alice will be able to compute $\hat{f}_z(u,v)$ as before. In the second case, Alice will know that there is no possible initial word of right part v which can give z as a trace, hence $\hat{f}_z(u, v) = 0$. □

Symmetrically, we can define $T_{f\leftarrow z}$ and $\tau_{f\leftarrow z}$ in Alice's side. The left CC for $\hat{f}_z$ is upper-bounded by $\left\lceil \log \left| T_{f\leftarrow z}(A^{[1,n]}) \right| \right\rceil$, and by $\lceil \log \left(|\tau_{f\leftarrow z}| + 1 \right) \rceil$.

3.1 Grouping

Let us see a simple class of CA where Alice and Bob's sides can be seen independently enough, each one with the information of the trace, to get a very low CC: they do not even need to send their $T_{f\rightarrow z}$ or $T_{f\leftarrow z}$ words to one another.

Let $f : A^3 \to A$ be a CA. We define its 2-grouped as the CA $f^{<2>}$ on alphabet A^2 defined by $f^{<2>}((x_{-1}, y_{-1}), (x_0, y_0), (x_1, y_1)) = (f(y_{-1}, x_0, y_0), f(x_0, y_0, x_1))$. It can be seen as the same CA where the cells have been grouped 2 by 2.

Grouping is one of the interesting tools allowing to define cellular simulation and intrinsic universality, which are a way to order the CA in terms of their ability to embed the dynamics of other CA (see for instance [2]). The classical CC of CA has been used to prove the non-ability of a CA to simulate other CA, based on the fact that this CC is nonincreasing with simulation. We will see that it is no more the case for traced CC.

Proposition 8 *For any 2-grouped CA $f = g^{<2>}$ and any word $z \in A^{n+1}$, the one-round CC of $\hat{f}_z$ is at most 1.*

Proof. It can be seen that $T_f(uz_0v) = z$ if and only if both $T_{f\leftarrow z}(u) \in \tau_{f\leftarrow z}$ and $T_{f\rightarrow z}(v) \in \tau_{f\rightarrow z}$: the 2-block construction allows to glue any two valid half-triangles together into a full valid computation triangle. If Alice has word u and Bob v, he can compute $T_{f\rightarrow z}(v)$ and check whether it belongs to $\tau_{f\rightarrow z}$. It only needs to send the result of this test to Alice. □

As a result, even the simplest simulation, *i.e.* the reverse operation of 2-grouping, can increase the traced CC.

3.2 B⋆onesided rules

Let us see a simple case where Proposition 7 can be applied, which corresponds to some other kind of partial onesidedness. If $B \subset A$, then a CA f

is *B⋆leftsided* if $\forall b, c, d \in A, \forall a \in B, f(abc) = f(abd)$. Similarly, we define *B⋆rightsided* CA.

Proposition 9 *If $z \in B^{n+1}$ and f is B⋆leftsided, then the right CC for $\hat{f}_z$ is constant.*

Proof. For any two words $w, w' \in A^{[-n,n]}$, if $T_f(w) = T_f(w') = z$ and $w_1 = w'_1$, then by the $B\star$leftsided property we have $f(w)_1 = f(w')_1$, and by induction, for any $t < n$, $f^t(w)_1 = f^t(w')_1$. It results that the words of $T_{f\to z}(A^{[1,n]})$ are determined by their first letter, which gives $\left|T_{f\to z}(A^{[1,n]})\right| = |A|$. From Proposition 6, the right CC for $\hat{f}_z$ is then bounded by $\lceil \log |A| \rceil$. □

Intuitively, if Bob has the word v, then it is sufficient for him to send to Alice the initial state v_1 of his first cell, since the evolution of this cell will not depend on cells which are on the right if he assumes that the central column is z. Alice can thus compute $T_{f\to z}(v)$ and then know whether the central cell will reach some state which does not correspond to z.

Similarly, if f is $B\star$rightsided, then the left CC for $\hat{f}_z$ is constant. Overall, the proposition applies to the elementary CA whose number in base 2 can be written $a_7a_6a_5a_4a_2a_2a_0a_0$ or $a_7a_2a_5a_0a_3a_2a_1a_0$.

Figure 8. Matrix of the rule 159.

The hypothesis is satisfied in two cases: the cell just on the right of the word z has a state which either loops, or remains always the same. In the latter case and for a binary alphabet, we can be slightly more general if we allow logarithmic communications.

Proposition 10 *If $\exists a \in \{0,1\}, f(0a0) = f(0a1) = a$, then the right CC for $\hat{f}_{0^{n+1}}$ is upper-bounded by $\lceil \log(n+1) \rceil$.*

Proof. Note that $\begin{array}{rcl}\gamma : T_{f\to 0^{n+1}}(A^{[1,n]}) & \to & [0,n[\, \cup \{+\infty\} \\ z' & \mapsto & \min\limits_{z'_t=a} t\end{array}$ is injective, with inverse $\gamma^{-1}(t) = \bar{a}^t a^{n-t}$ if $t < n$, $\bar{a}^n$ if $t = +\infty$. Hence $T_{f\to 0^{n+1}}(A^{[1,n]}) \leq n+1$, and we conclude thanks to Proposition 6. □

Intuitively, if Bob has the word v, then it is sufficient for him to send to Alice the first generation when some a appears in $T_{f\to 0^{n+1}}(v)$ and $+\infty$ if a never appears. Indeed, Alice will then know entirely this word, and be able to compute the result.

Similarly, if $\exists a \in \{0,1\}, f(0a0) = f(1a0) = a$, then the left CC for $\hat{f}_{0^{n+1}}$ is at most logarithmic. Note that the previous case includes that, already seen, of CA having stagnating 0, or stagnating 1, and more generally any elementary CA whose number in base 2 can be written $a_7a_6a_5a_4a_3a_2a_0a_0$ or $a_7a_6a_5a_4a_2a_2a_1a_0$.

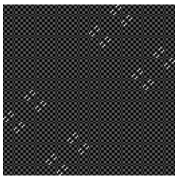

Figure 9. Matrix of the rule 105.

3.3 Entropy

The next notions come from topological dynamics, but we emphasize here the point of view based on the trace of configurations as finite words. Even though it is not crucial, the logarithms will be assumed binary.

The *entropy* of the trace over cells $[i,j[\subset \mathbb{Z}$ is the limit

$$h_{j-i} = \lim_{n\to\infty} \frac{\log \left| T_f^{[i,j[}(A^{[-n,n]}) \right|}{n} \ .$$

Thanks to the parallelism of the rule application, it only depends on the difference $j-i$ (and on the CA). The *entropy* of the CA f is the supremum h of the entropies of the traces over $[i,j[$, when $j-i$ grows. This notion represents somehow the degree of "disorder" in the apparent evolution of the CA.

Proposition 7 gives us the following rough upper bound on the CC of $\hat{f}_z$: $\left\lceil \log \left(\left| T_f^{\{1\}}(A^{[-n,n]}) \right| + 1 \right) \right\rceil$. This allows us to state that null-entropy CA have sublinear one-round CC for $\hat{f}_z$. On the contrary, for CA of entropy $h > 0$, it is known that the entropy h_{j-i} of any nontrivial trace over $[i,j[$ is also strictly positive, and in that case the one-round CC for $\hat{f}_z$ and for a large n is at most $h_1 n + o(1)$ which itself is at most $hn + o(1)$.

The inequality $h_{j-i}n \leq hn$ corresponds to an interesting open problem on the structure of CA computations: whether there exists a computable bound on $[i,j]$ (maybe width 2) such that $h_{j-i} = h$ (see for instance [3]). The inequality

$c \leq h_{j-i}n + o(1)$ is more specific to our problem. It is not tight at all because the entropy gives intuition about the disorder visible in a finite window of the computation, without distinguishing whether the disorder comes from one single side or both, which is our purpose. For instance, onesided CA could give rise to a complex trace – like the shift CA, for which $T_f(A^{[-n,n]})$ is the whole A^{n+1} – but we have already seen that their CC is simple.

3.4 Equicontinuity

A CA f is *equicontinuous* if for any $[i,j] \subset \mathbb{Z}$, the cardinality of $T_f^{[i,j]}(A^{[-n,n]})$, with $n \geq \max(|i|, |j|)$, is bounded by a constant. From [8], this notion corresponds to ultimately periodic CA, or equivalently to those for which the width-1 trace $T_f(A^{[-n,n]})$ has bounded cardinality for $n \in \mathbb{N}$. This notion represents an extreme stability of the system, since distant cells cannot influence each other. Such CA were proved to have simple classical CC in [7]. Here too, thanks to Proposition 7, we can see that equicontinuous CA have a constant one-round CC for $\hat{f}_z$.

4 Expansivity

We now deal with CA presenting some kind of complexity, which will give us high CC. At the extreme opposite of equicontinuity, we say that a CA f is (*positively*) *right-expansive* if there exists some time step $t_f^{\rightarrow} \in \mathbb{N}\backslash\{0\}$ such that any two words $w, w' \in A^{\left[-t_f^{\rightarrow}, t_f^{\rightarrow}\right]}$ with the same trace $T_f^{[-1,0]}(w) = T_f^{[-1,0]}(w')$ have the same letter $w_1 = w'_1$ just on the right. In other words, being given the trace, we can rebuild – in a unique way – the right part of the initial finite word.

The simplest right-expansive CA are the *right-permutive* ones, *i.e.* the rules $f : A^3 \to A$ such that $\forall a, b, c, d \in A, c \neq d \Rightarrow f(abc) \neq f(abd)$. It can be noted that they correspond to $t_f^{\rightarrow} = 1$. In particular, for any $u \in A^{[-n,-1]}$, the restriction of T_f over the set $uA^{[0,n]}$ is a bijection onto A^{n+1}. A well-known example is rule 90, which acts as an exclusive-or gate over the two extreme neighbors.

The notion of expensiveness is rather precise, but we can generalize it to some kind of subsystems of CA, in order for our lower bounds of CC to concern more CA, since it is intuitive that a system is at least as complex as its subsystems. Let us then define, in our setting, what corresponds to the symbolic notion of subshift of finite type. If $\mathcal{F} \subset A^*$ is a finite language of *forbidden patterns* and

$[i,j] \subset \mathbb{Z}$, we note

$$\Sigma_{[i,j]} = \Sigma^{\mathcal{F}}_{[i,j]} = \left\{ w_i \dots w_j \in A^{[i,j]} \middle| \forall\, [i',j'] \subset [i,j]\,, w_{[i',j']} \notin \mathcal{F} \right\} \ .$$

Consider the restriction $f_{|\Sigma}$ of the extended rule of the CA f to $\bigcup_{[i,j] \subset \mathbb{Z}} \Sigma_{[i,j]}$. It is called a *subautomaton* if this set is stable, *i.e.* f does not create forbidden patterns: $\forall\, [i,j] \subset \mathbb{Z}$, $f(\Sigma^{\mathcal{F}}_{[i-1,j+1]}) \subseteq \Sigma^{\mathcal{F}}_{[i,j]}$.

The subautomaton $f_{|\Sigma}$ is *right-expansive* if there exists some time $t_f^{\rightarrow} \in \mathbb{N} \setminus \{0\}$ such that any two words $w, w' \in \Sigma_{[-t_f^{\rightarrow}, t_f^{\rightarrow}]}$ with the same trace $T_f^{[-1,0]}(w) = T_f^{[-1,0]}(w')$ have the same letter $w_1 = w'_1$ just on the right.

If we iterate this with a growing trace size, we can rebuild all letters of the right half of the initial word: for any $n \in \mathbb{N}$ and any $y \in T_f^{[-1,0]}(\Sigma_{[-n,n]})$, there exists a unique $v \in \Sigma_{[1, \lfloor n/t_f^{\rightarrow} \rfloor]}$ such that any $w \in \Sigma_{[-n,n]}$ with $T_f^{[-1,0]}(w) = y$ satisfies $w_{[1, \lfloor n/t_f^{\rightarrow} \rfloor]} = v$. This bijection gives in particular that the entropy of an expansive CA f (with $\Sigma_{[-k,k]} = A^{[-k,k]}$) is at least $\frac{\log|A|}{t_f^{\rightarrow}}$.

Intuitively, if we consider some computation triangle where both the right part $w_{[0,n]}$ of the initial configuration and the trace $T_f(w)$ are fixed, then it is clear that there is always at most one way to complete the right part of the triangle. In the right-expansive case, there is also at most one way to complete a portion $w_{[-\lfloor n/t_f^{\rightarrow} \rfloor, 0]}$ of the left part.

We say that the subautomaton of some CA is *right-permutive* if it is the subautomaton of some (possibly different) right-permutive CA. This implies that it is right-expansive. Symmetrically, we can define *left expansive* CA or subautomata, with some particular time step $t_f^{\leftarrow}$, and *left-permutive* CA or subautomata with $t_f^{\leftarrow} = 1$. A CA or subautomaton is *expansive* if it is both left and right expansive. It is *bipermutive* if it is both left-permutive and right-permutive.

Now the definition of $t_f^{\rightarrow}$ helps us build large fooling sets.

Lemma 11 *Let $f_{|\Sigma}$ be an expansive subautomaton of some CA, $z \in A^{n+1}$, and*

$$W_z = \left\{ w \in \Sigma_{\left[-\left\lfloor \frac{n}{t_f^{\leftarrow}} \right\rfloor, \left\lfloor \frac{n}{t_f^{\rightarrow}} \right\rfloor\right]} \middle| \exists x, y, xwy \in \Sigma_{[-n,n]}, T_f(xwy) = z \right\} \ .$$

Then the multi-round CC of $\hat{f}_z$ is lower-bounded by $\log|W_z|$.

Proof. For any $w \in W_z$, let us define $\gamma(w) = (x_w w_{[-\lfloor n/t_f^{\leftarrow} \rfloor, -1]}, w_{[1, \lfloor n/t_f^{\rightarrow} \rfloor]} y_w)$, where x_w and y_w are fixed words such that $T_f(x_w w y_w) = z$. Note that γ is injective, with $\gamma^{-1}(u,v) = u_{[-\lfloor n/t_f^{\leftarrow}\rfloor,-1]} z_0 v_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]}$. Moreover, let us show that $\gamma(W_z)$ is a fooling set for $\hat{f}_z$. By construction, if $w \in W_z$, then $\hat{f}_z(\gamma(w)) = 1$. Now let $w' \in W_z$ such that $T_f(x_w w_{[-\lfloor n/t_f^{\leftarrow}\rfloor,0]} w'_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]} y_{w'}) = z = T_f(x_w w y_w)$. Right expensiveness will give that the initial configurations $w_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]} y_w$ and $w'_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]} y_{w'}$ of the two triangles begin equally: $w_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]} = w'_{[1,\lfloor n/t_f^{\rightarrow}\rfloor]}$. If besides $T_f(x_{w'} w'_{[-\lfloor n/t_f^{\leftarrow}\rfloor,-1]} w_{[0,\lfloor n/t_f^{\rightarrow}\rfloor]} y_w) = z$, then symmetrically, left expensiveness gives that $w_{[-\lfloor n/t_f^{\leftarrow}\rfloor,-1]} = w'_{[-\lfloor n/t_f^{\leftarrow}\rfloor,-1]}$. We globally obtain that $w = w'$, hence $\gamma(w) = \gamma(w')$, *i.e.* $\gamma(W_z)$ is a fooling set. Thanks to Proposition 1, the CC is at least $\log|\gamma(W_z)| = \log|W_z|$. □

Our interest will be that when W_z is sufficiently large, the CC is linear. If we study combinatorially the set of all possible traces, we will see conditions for it to be large.

Lemma 12 *Let $f_{|\Sigma}$ be an expansive subautomaton of some CA and $k \in \left[1, \left|\Sigma_{[1,n]}\right|\right[$. If p is the number of words $z \in A^{n+1}$ such that the multi-round CC of $\hat{f}_z$ is more than $\log k$, then:*

$$p \geq \frac{\left|\Sigma_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]}\right| - k}{\left|\Sigma_{[1,n]}\right| - k} \ .$$

Proof. For $z \in A^{n+1}$, consider W_z as defined in Lemma 11, and for $w \in W_z$, $\pi(w) = w_{[1,n]}$. Note that if $\pi(w) = \pi(w')$, since $T_f(w) = T_f(w') = z$ and f is left-expansive, then we have $w = w'$. It results that $|W_z| = |\pi(W_z)| \leq \left|\Sigma_{[1,n]}\right|$. Moreover, consider the number q of words $z \in A^{n+1}$ such that W_z admits more than k elements. Then we can distinguish between the sets W_z these q bigger ones (which have cardinality at most $\left|\Sigma_{[1,n]}\right|$ as stated above), with the other, smaller, ones (which have cardinality at most k):

$$\sum_{z\in A^{n+1}} |W_z| = \sum_{|W_z|>k} |W_z| + \sum_{|W_z|\leq k} |W_z| \leq \sum_{|W_z|>k} \left|\Sigma_{[1,n]}\right| + \sum_{|W_z|\leq k} k \ .$$

We obtain:

$$\sum_{z\in A^{n+1}} |W_z| \leq q\left|\Sigma_{[1,n]}\right| + (|A|^{n+1} - q)k \ .$$

On the other hand, we have $\bigcup_{z\in A^{n+1}} W_z = \Sigma_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]}$ (since every word has a trace), hence:

$$\sum_{z\in A^{n+1}} |W_z| \geq \left|\Sigma_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]}\right| \ .$$

Putting the two inequalities together, we get:

$$q\left|\Sigma_{[1,n]}\right| + (|A|^{n+1} - q)k \geq \left|\Sigma_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]}\right| .$$

As a result,

$$q \geq \frac{\left|\Sigma_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]}\right| - |A|^{n+1}k}{\left|\Sigma_{[1,n]}\right| - k} .$$

By Lemma 11, for any of the q words with $|W_z| \geq k$, the multi-round CC of $\hat{f}_z$ is at least $\log k$. □

By symmetry, $\Sigma_{[-n,-1]}$ may replace $\Sigma_{[1,n]}$ in the previous formula.

Let us first see the case of a CA (without forbidden patterns).

Proposition 13 *If f is an expansive CA with $m = 1/t_f^{\rightarrow} + 1/t_f^{\leftarrow} - 1 > 0$ and $n > 0$, then there exists some word $z \in A^{n+1}$ such that the multi-round CC of $\hat{f}_z$ is lower-bounded by $nm\log|A|$.*

Proof. We just use Lemma 12 with $|\Sigma|_{[-\lfloor n/t_f^{\leftarrow}\rfloor,\lfloor n/t_f^{\rightarrow}\rfloor]} = |A|^{nm+n+1}$, $\left|\Sigma_{[1,n]}\right| = \left|A^{[1,n]}\right| = |A|^n$ and $k = 1$. We obtain that the number p of words $z \in A^{n+1}$ such that the multi-round CC of $\hat{f}_z$ is more than $0 = \log 1$ is $p \geq |A|^{n+1}\frac{|A|^{nm}-1}{|A|^n-1} > 0$. □

The previous result cannot hold for all possible words $z \in A^{n+1}$, since there are expansive (not bipermutive) CA for which some of these words do not appear in $T_f(A^{[-n,n]})$, and hence correspond to a trivial CC. In other words, in the case of a large expensiveness speed on both sides, the CC is linear for some words; if we allow an arbitrarily low linearity constant, Lemma 12 can actually give rather large families: if $0 \leq s < m$, then the multi-round CC of $\hat{f}_z$ is more than $ns\log|A|$ for at least $|A|^{n+1}\frac{|A|^{nm}-|A|^{ns}}{|A|^n-|A|^{ns}}$ words. The same inequalities hold when the CA is permutive on one side and expansive on the other one. In the particular case of bipermutivity, we have a linear traced CC associated to any word.

Proposition 14 *For any bipermutive CA and any word $z \in A^{n+1}$, the multi-round CC of $\hat{f}_z$ is equal to $n\log A$.*

Proof. Just apply Lemma 12 with Σ full as in the previous proof, $t_f^{\rightarrow} = t_f^{\leftarrow} = 1$ (*i.e.* $m = 1$), and $k = |A|^n - 1$. We get that the number p of words $z \in A^{n+1}$

such that the multi-round CC of $\hat{f}_z$ is more than $\log k$ is $p \geq |A|^{n+1} \frac{|A|^{nm}-k}{|A|^n-k} = |A|^{n+1}$, *i.e.* all words of A^{n+1} have a CC of at least $n \log |A|$. The converse inequality is obvious. □

The expansive elementary CA are exactly the four bipermutive ones (90, 150, 105, 165) and have thus the maximal possible traced CC for all words.

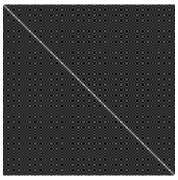

Figure 10. Matrix of the rule 90.

Proposition 13 involves only CA which have an expensiveness speed of more than a half; we will now see that it actually represents the best limit of expensiveness speed we could get for this result.

It is not difficult to observe that the 2-grouped of some expansive CA f is still expansive, with $t^{\leftarrow}_{f^{<2>}} = 2t^{\leftarrow}_f$ and $t^{\rightarrow}_{f^{<2>}} = 2t^{\rightarrow}_f$. Hence we have the following example of expansive CA which is simple with respect to traced CC.

Example 15 *Consider the CA on alphabet* $[0,3]$ *defined by the local rule (where / is the quotient of the Euclidean division):*

$$\begin{aligned} f: \quad & [0,3]^3 \to [0,3] \\ & (a,b,c) \mapsto 2((a+b) \bmod 2) + ((b/2 + c/2) \bmod 2) \ . \end{aligned}$$

If we identify $[0,3]$ *with* $\{0,1\}^2$*, this CA is the* 2*-grouped of the bipermutive CA* 90*. Hence it has* $t^{\leftarrow}_f = t^{\rightarrow}_f = 1/2$*. On the other hand the traced CC of any word is* 1*, by Proposition 8 (the converse inequality is rather obvious).*

4.1 Legal rules

We now see another little application of Lemma 11, in the case of binary alphabet.

For $[i,j] \subset \mathbb{Z}$ and $u \in A^{[i,j]}$, let us denote $\widetilde{u} \in A^{[-j,-i]}$ the *mirror* of u, *i.e.* the word such that $\widetilde{u}_{-k} = u_k$ for any $k \in [i,j]$. If $V \subset A^{[i,j]}$, we note $\widetilde{V} \subset A^{[-j,-i]}$ the set of all mirrors of words of V. The subautomaton $f_{|\Sigma}$ of some CA is 0-*legal*, with $0 \in A$, if for any $u \in \Sigma_{[-1,1]}$, $\widetilde{u} \in \Sigma_{[-1,1]}$ and $f(\widetilde{u}) = \widetilde{f(u)}$, and for any $a \in A$ such that $a0a \in \Sigma_{[-1,1]}$, $f(a0a) = 0$.

Lemma 16 *For any* 0*-legal subautomaton* $f_{|\Sigma}$ *of some CA, any* u *such that* $\widetilde{u}0u \in \Sigma_{[-n,n]}$*, and any* $t \leq n$*,* $f^t(\widetilde{u}0u)_0 = 0$*.*

Proof. This comes from an immediate recurrence: if $n > 0$, then $f(\widetilde{u}0u) = f(\widetilde{u}0)f(u_0 0 u_0)f(0u) = \widetilde{f(0u)}0f(0u)$, which still has the same form. □

The previous lemma allows in this context to establish an equivalence between the problem of the traced CC and the classical equality test of binary words, which is known to have linear CC.

Proposition 17 *Let* $f_{|\Sigma}$ *be a* 0*-legal bipermutive subautomaton of some CA* f *such that* $\Sigma_{[-n,n]}$ *contains some sublanguage of the form* $\widetilde{V}0V$*. Then the multi-round CC of* $\hat{f}_{0^{n+1}}$ *is at least* $\log|V|$*.*

Proof. Just apply Lemma 11, with $W_{0^{n+1}} \supset \widetilde{V}0V$ thanks to Lemma 16. We get a traced CC of at least $\log|W_{0^{n+1}}| = \log\left|\widetilde{V}0V\right| = \log|V|$. □

Corollary 18 *The CA 18, 26, 146, 154, 218 have a multi-round CC in* $\Omega(n)$*.*

Proof. Note that these rules are equal to the bipermutive rule 90 except on neighborhoods $011, 110, 111$. Define Σ as the set of words avoiding the pattern 11 and the patterns $10^{2k}1$, for $k \in \mathbb{N}$. It can be easily seen that Σ is stable by the synchronous application of CA 90, hence by any of these CA.
Let $m \in \mathbb{N}$ and $V = (0100 + 0001)^m$ (standard notation for languages, seen as words indexed in $A^{[1,4m]}$). Note that $\widetilde{V}0V \subset \Sigma_{[-4m,4m]}$. From Proposition 17, the multi-round traced CC corresponding to $f_{|\Sigma}$ and $z = 0^{4m+1}$ is greater than $\log|V| = m$. □

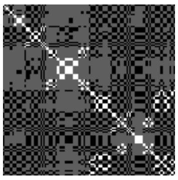

Figure 11. Matrix of the rule 146.

Unfortunately, we do not know similar practical subsystems for the three other bipermutive elementary CA.

Conclusion

In this paper, we have addressed a new problem of communication complexity to get some clues about the information streams present in the evolution of CA. This can help understand their behaviors by exhibiting how much communication is needed to achieve their computation.

We have treated a large number of elementary cellular automata; some of the remaining ones look experimentally simple, other ones rather mysterious, such as 22, which nearly has a bipermutive subautomaton, or as some of the CA for which 1 is weakly but not semi-strongly spreading.

Unlike the classical CC of CA, this notion of complexity does not a priori present links with cellular simulation (see Proposition 8). This could be overpassed by defining a more general problem, where Alice and Bob would need to determine whether the trace belongs to some given subset of A^{n+1} or not. This extends both classical (at least in the binary case) and traced CC, and one should carefully consider what kind of subsets would imply a good notion of complexity for CA.

On the contrary, our approach allows more links with topological dynamics than classical CC. In [8], Petr Kůrka classified the CA into four classes: equicontinuous, almost equicontinuous (and not equicontinuous), sensitive (and not expansive) and expansive. We have proved that the first one implies a trivial CC and a strong version of the last one a very complex one. In the construction of the fooling sets of Section 4, the ability to reconstruct the initial word is crucial; maybe if we ask $\hat{f}_z$ to be complex for any word z, it would imply something close to expensiveness (our condition being then nearly necessary). When fixing the word z, a high complexity for the problem is not possible without a large set of initial words on the right and on the left, independent from each other, and which together can give z in the trace.

Kůrka's intermediary classes do not imply anything on this kind of complexity. Nevertheless, almost equicontinuity may be related to a simple *average CC*, since in that case ergodic theorists know that almost the whole system behaves as an equicontinuous system. Understanding this distinct complexity measure could be a track for future research.

Acknowledgement

Thanks to the referees for their careful reading and precise correction, from a rather rough version of that work.

References

[1] Cervelle, J., E. Formenti and P. Guillon, *Ultimate traces cellular automata*, in: J.-Y. Marion, editor, 27^{th} *International Symposium on Theoretical Aspects of Computer Science (STACS'10)*, Nancy, 2010.

[2] Delorme, M., J. Mazoyer, N. Ollinger and G. Theyssier, *Bulking II: Classifications of cellular automata* (2010), oai:hal.archives-ouvertes.fr:hal-00451729.

[3] di Lena, P. and L. Margara, *Row subshifts and topological entropy of cellular automata*, Journal of Cellular Automata **2** (2007), pp. 131–140.

[4] Dürr, C., I. Rapaport and G. Theyssier, *Cellular automata and communication complexity*, Theoretical Computer Science **322** (2004), pp. 355–368, Discrete Applied Problems - Florilegium for E. Goles.

[5] Goles, E., C. Little and I. Rapaport, *Understanding a non-trivial cellular automaton by finding its simplest underlying communication protocol*, in: *Proceedings of the 19th International Symposium on Algorithms and Computation*, Lecture Notes in Computer Science (2008), pp. 592–604.

[6] Goles, E., P.-E. Meunier, I. Rapaport and G. Theyssier, *Communications in cellular automata*, in: T. Neary, D. Woods, A. K. Seda and N. Murphy, editors, *Complexity of Simple Programs (CSP'08)* (2008), pp. 103–116.

[7] Goles, E., P.-E. Meunier, I. Rapaport and G. Theyssier, *Communication complexity and intrinsic universality in cellular automata* (2010), to appear in Theoretical Computer Science.

[8] Kůrka, P., *Languages, equicontinuity and attractors in cellular automata*, Ergodic Theory & Dynamical Systems **17** (1997), pp. 417–433.

[9] Kushilevitz, E. and N. Nisan, "Communication complexity," Cambridge, 1997.

[10] Nisan, N. and A. Wigderson, *On rank vs. communication complexity*, in: *Electronic Colloquium on Computational Complexity*, number TR94-001 in ECCC Technical Reports, 1994, pp. 831–836.

[11] Yao, A., *Some complexity questions related to distributed computing*, in: *Proceedings of the 11th ACM Symposium on Theory of Computing*, 1979, pp. 209–213.