# On the average-case complexity of the reversibilty problem for finite cellular automata

A. Clementi
Dept. of Comp. Science
University of Rome
"La Sapienza"
00198 - Rome, Italy

P. Pierini
Dept. of Mathematics
University of Rome
"La Sapienza"
00185 - Rome, Italy

R. Impagliazzo
Dept. of Comp. Science & Eng.
University of California,
San Diego
92093 - La Jolla, CA

**Abstract**

Of particular relevance in the theory and applications of cellular automata is the concept of invertibility. We study the computational complexity of deciding whether or not a given finite cellular automata is invertible. This problem is known to be CoNP-complete, we prove that the expected-time complexity of its randomized version is "hard": the problem is CoRNP-complete. Finally, we discuss some consequences of this result in the theory and applications of cellular automata.

## 1 Introduction

There is a renewal of interest in studying the fundamental connections between physics and computation [1, 2, 11] and, in particular, in modelling computing systems which explicitly consider the fundamental physical limitations such as finiteness of the speed of light and layout in ordinary space. Cellular automata represent one of the best mathematical model under this point of view [2, 17]. Cellular automata are networks of numerable, identical and uniformly interconnected machines (*cells*) evolving in a parallel, synchronous way. Hence, the local interactions among the cells determine a *global function* acting on the space of all possible configurations. A cellular automaton is *invertible* if its global function is bijective. The invertibility of a cellular automaton is an important issue in modelling reversible physical phenomena.

Kari [12] has recently proved that the problem which consists of deciding whether or not a given cellular automaton is invertible (in short REV) is undecidable. Most of cellular automaton applications in computer science requires to consider a finite number of machines rather than an infinite one. In [5], the complement problem of REV, for finite cellular automata, has been proved to be $NP$-complete. The proof given in [5] holds also under very strong restrictions on the topology (*neighborhood*) of the connections among cells; more recently, a different proof of this result has appeared in [6]. The consequences of these results for computer science and physics are also analysed in [3, 4].

In this paper, we investigate the average-case complexity (see [15, 10]) of a natural generalization of REV. In this new version, the instance specifies also the particular *closed* subset of global configurations on which the invertibility property is required. When an $NP$-completeness result arises, the attention naturally focuses on less ambitious goals than to decide *any* instance of the problem in polynomial time. Several $NP$-complete decision problems have algorithms working in polynomial average-time according to a fixed probability function given on the input space [7, 14] (that is they belong to the complexity class $AP$ - see section 2). However, we show that polynomial average-time algorithms for our problem are unlikely to exist. Indeed, we prove that the generalized version of REV cannot belong to $AP$ unless $RNP$, the randomized version of the class $NP$, is contained in $AP$ (i.e. all $NP$-complete problems would have an algorithm working efficiently in average). To do this, we show that our problem is *complete* for the complement class of $RNP$ (i.e. Co$RNP$). Very few examples of interesting complete problems have been found until now for this class. The average-case complexity of any computational problem depends not only on the problem but on the probability function as well. In particular, the probability function yielding the uniform distribution on the inputs of a fixed size, is often uninteresting from the point of view of practical applications: in most cases, we could prefer to give more "importance" to a fixed subset of inputs rather than to another. Following this line of reasoning, it is interesting to underline that our hardness result holds for *every* choice of the positive probability function given on the space of all finite cellular automata.

Finally, we shall discuss some consequences of this result in the theory and applications of cellular automata.

## 2 Preliminaries

**Finite cellular automata.** A finite two-dimensional cellular automata (in short *ca*) can be formally defined as a fourtuple
$A = (n, Q, N, f)$ where:

- $n$ is the size of the support array; hence, there are $n^2$ finite-state automata (called *cells*) located on



0-8186-6715-X/94 $4.00 © 1994 IEEE

the two-dimensional lattice having periodic structure (i.e. $\mathcal{Z}_n^2$);

- $Q$ is the finite set of cell states;
- $N$ is the set of $\mathcal{Z}_n^2$-vectors determining the *neighborhood*; for any $j \in N$, the cell at position $i+j$ is a *neighbor* of cell at position $i$ (in which follows we shall identify the cell with its position); The set of neighbors of $i$ is denoted as $N(i)$. The *Moore* neighborhood, consisting of the center cell and the eight surrounding cells, is called $N^m$.
- $f : Q^{|N|} \to Q$ is the local function; the state of each cell $i$ is updated according to $f$ which has the state of the neighbors of $i$ as input.

A configuration of $A$ is a function $X : \mathcal{Z}_n^2 \to Q$ (i.e. an element of the set $\Sigma = Q^{\mathcal{Z}_n^2}$) and since the evolution of the system is synchronous (i.e. there is a global, discrete clock which is unique for all the cells) the *local map* consisting of the pair $(N, f)$ uniquely determines a global function $F : \Sigma \to \Sigma$.

**Average-case complexity.** Let us now revise the basic definitions of Levin's theory of the average-case complexity [15]. All definitions and results given below can be found, in a more detailed form, in [10]. A *randomized* decision problem is a pair $(L, Pr)$ where $L$ is a decision problem on the instance set $S^*$ (i.e. a subset of $S^*$) and $Pr$ is a probability function on $S^*$. We call $(L/X, Pr_{/X})$ the restriction of $(L, Pr)$ to a subset $X$ of $S^*$ with $Pr(X) > 0$ ($Pr_{/X}$ is the probability function proportional to $Pr$ in $X$ and zero outside). Given a function $f : S^* \to R^+$, then $f$ is polynomial on $Pr$-average if there exists an $\epsilon > 0$ such that:

$$\Sigma_{\{x:|x|>0\}}(f(x))^{\epsilon} \cdot |x|^{-1} \cdot Pr(x) < \infty.$$

Now, we can introduce the following definitions:

- A randomized decision problem $(L, Pr)$ is in $AP$ if there is a Turing machine deciding $L$ within time polynomial on $Pr$-average. Similarly, a function $f : S^* \to S'^*$ is computable in $AP - time$ with respect to the probability function $Pr$ on $S^*$ if there is a Turing machine which computes $f$ within time polynomial on $Pr$-average.
- Let $Pr_1$ and $Pr_2$ be two probability functions on $S^*$; $Pr_2$ *dominates* $Pr_1$ if there exists a polynomially bounded function $f : S^* \to R^+$ such that, for any $x \in S^*$, we have: $Pr_1(x) \leq f(x)Pr_2(x)$. Then, a randomized decision problem $(L, Pr)$ is in $RNP$ if $L$ is in $NP$ and $Pr$ is dominated by a probability function $Pr_2$ whose distribution $Pr_2^*(y) = \Sigma_{x<y} Pr(x)$ is polynomial-time computable.

A function f *reduces* a decision problem $L_1$ to another $L_2$ if, for any instance $x$ of $L_1$, we have $x \in L_1$ iff $f(x) \in L_2$. Moreover, a function $f : S_1^* \to S_2^*$ *transforms* $Pr_1$ into $Pr_2$ if, for any $y \in S_2^*$, $Pr_2(y) = \Sigma_{\{x:f(x)=y\}} Pr_1(x)$. Thus, we say that $Pr_1$ is dominated by $Pr_2$ with respect to a function $f$ (in symbols $Pr_1 \leq^f Pr_2$) iff there exists a probability function $Pr$ such that $Pr$ dominates $Pr_1$ and $f$ transforms $Pr$ into a restriction of $Pr_2$. For any pair of randomized problem $(L_1, Pr_1)$, $(L_2, Pr_2)$ we say that a polynomial-time function $f$ *Av-reduces* $(L_1, Pr_1)$ into $(L_2, Pr_2)$ iff it reduces $L_1/\{x : Pr_1(x) > 0\}$ to $L_2$ and $Pr_1 \leq^f Pr_2$. This definition extends the concept of reduction among decision problems from $NP$ to $RNP$; indeed, it is possible to prove that the Av-reducibility is a transitive relation in $RNP$. Moreover, if $(L_1, Pr_1)$ Av-reduces to $(L_2, Pr_2)$ and $(L_2, Pr_2)$ is in $AP$ then $(L_1, Pr_1)$ is in $AP$; in particular any restriction of an $AP$ problem is in $AP$. Finally, we say that a randomized decision problem $(L, Pr)$ is $RNP - complete$ if it is in $RNP$ and for any $(L_1, Pr_1) \in RNP$, $(L_1, Pr_1)$ Av-reduces to $(L, Pr)$. In which follows we present a randomized problem that Levin [15] and, more recently, Gurevich [10] proved to be complete for $RNP$.

Given a finite set of *colors* $C$ we call *set of tiles* any subset $\tau \subseteq C^4$ where each $t \in \tau$ represents a $1 \times 1$ square with colored edges. The four edge colors of a fixed tile $t$ will be denoted as: $top(t)$, $right(t)$, $bottom(t)$ and $left(t)$. Moreover, given a finite set of tiles $\tau$, a function

$$r : [0, \ldots, j-1] \to \tau$$

is a $\tau - row$ of length $j$ if $left(r(i+1)) = right(r(i))$ for any $i < j$.

*Randomized bounded Tiling Problem*
**(RTP$(\tau, n, r)$)**[1] Instance: A finite set of tiles $\tau$, the unary notation for an integer $n > 1$, an integer $j$ such that $0 < j < n$ and a $\tau$-row $r$ of length $k$. $r$ is such that either $k = j$ or $k < j$ and $\tau$ has no tiles $t$ having $left(t) = right(r(k))$. Question: Does a correct $\tau$-tiling of the square $T = [0, \ldots, n-1] \times [0, \ldots, n-1]$ exist? (for a correct $\tau$-tiling we intend a function $g : T \to \tau$ such that the common edge of every pair of adjacent tiles has the same color and with $g(0, i) = r(i)$ for any $i < k$; the tiles cannot be rotated). Probability: Choose $\tau$ with any fixed positive probability function; choose $n$ with the "standard" probability[2] proportional to $1/n^2$; choose uniformly $j < n$ (i.e. with probability $1/n$); choose uniformly $r(o)$; choose $r(i+1)$ uniformly in the set $\tau_i = \{t \in \tau : left(t) = right(r(i))\}$, $i = 1, \ldots, k-2$. All these choices are mutually independent, thus the resulting probability of an $RTP$-instance is the product of the probabilities of the single events described above.

**Theorem 2.1** [15, 10] *$RTP(\tau, n, r)$ is $RNP$-complete.*

[1] Observe the "generalization" represented by string $r$ with respect to the classical definition of the Tiling Problem in which no strings are determined (see [8]).

[2] See section 2 of [10], for more discussions on appropriate probability functions on the set of positive integers;

In the following corollary, we summarize a property which is a direct consequence of the proof of theorem 2.1 (see theorem B1 and lemma B6 of appendix B in [10]); such a property will be used for proving our result.

**Corollary 2.1** *RTP remains RNP-complete even when, for $i = 1, \ldots, k-1$, $top(r(i)) \in \{0,1\}$ and the size of $\tau_i$, $i = 0, \ldots, k-2$, is exactly two, that is, when the probability of any possible $\tau$-row $r$ of length $k$ is proportional to $(1/2)^k$.*

**The problem.** A *ca* is *invertible* if its global function is bijective. Thus, the invertibility problem (REV) consists of deciding whether or not a given *ca* is invertible. We define now the generalization of REV's complement problem, since, for proving our result, we will always refer to this problem. However, since the class $AP$ is equal to its complement, it should be clear that any hardness result (like an $RNP$-completeness one) for one of the two problems (i.e. REV and its complement) implies an equivalent hardness result (i.e. Co$RNP$-completeness) for the other as well. Since the set $\Sigma$ is finite, the invertibility property is equivalent to the injectivity one, hence REV's complement (in short NIP) consist of deciding the existence of a pair of different configurations having the same image according to the *ca* global function. Let us consider the concept of *legal* configurations which has been first introduced for other decision problems dealing with *ca* (see for example [9, 16]). Consider a subset[3] $P = (P_1 = \{0, \ldots, k_1\} \times P_2 = \{0, \ldots, k_2\}) \subset \mathcal{Z}_n^2$, the restriction of any configuration $X \in \Sigma$, on the domain $P$, will be denoted as $X_{/P}$. Now, given any *pattern* $x$ for $P$ (i.e. $x : P \to Q$), we can introduce the following *legal configuration set*:

$$\Sigma(P, x) = \{X \in \Sigma \ : \ X_{/P} = x\}.$$

When $P$ is equal to the empty set, we adopt the convention: $\Sigma(\emptyset, *) = \Sigma$. Moreover we say that $\Sigma(P, x)$ is *closed* with respect to the *ca* global function $F$ if, given any $X \in \Sigma$, $X \in \Sigma(P, x)$ iff $F(X) \in \Sigma(P, x)$. Finally, when the state set $Q$ consists of more than one component, we can easily adapt the above definitions: without loss of generality, suppose $Q = Q_a \times Q_b$, then by using the previous notations, given any $P \subset \mathcal{Z}_n^2$ and any $Q_a$-pattern $x$ for $P$, that is any $x : P \to Q_a$, we have the following legal configuration set:

$\Sigma(P, Q_a, x) = \{X \in \Sigma \ : \ X_{/P} = x$
with respect to the component $Q_a\}$.

We are now ready to introduce the formal definition of our problem:

*Randomized Non Invertibility Problem*
**(RNIP**$(A, P, Q_a, x)$**)** Instance: A *ca* $A = (n, Q, N, f)$ with global function $F$, a support subset $P = P_1 \times P_2 \subset \mathcal{Z}_n^2$ and a $Q_a$-pattern[4] $x : P \to Q_a$. Question: Does two different configurations $X$ and $Y$ belonging to the legal set $\Sigma(P, Q_a, x)$, such that $F(X) = F(Y)$, exist? Probability: choose the *ca*-size $n$ with the standard probability $Pr(n)$ proportional to $1/n^2$; choose $(Q, N, f)$ and $Q_a$ with your *favorite* positive probability function; choose the size of $P_1$ and $P_2$, independently, with uniform distribution in the set $\{0, \ldots, n-1\}$; choose a $Q_a$-pattern $x : P \to Q_a$ with uniform probability in the set $Q_a^P$ of all possible $Q_a$-pattern of $P$ (i.e. every possible pattern has probability $1/|Q_a^P|$). All these choices are mutually independent, thus the resulting probability of an $RNIP$-instance is the product of the probabilities of the single events described above.

Let us observe that the above definition contains the classical definiton of NIP as the particular case in which $P = \emptyset$.

## 3 The result

Let us now give the result of this paper:

**Theorem 3.1** *$RNIP$ is $RNP$-complete for any positive probability function given on the space of finite ca. Hence, the generalized version of REV on finite ca, cannot be solved in polynomial time in the average-case, unless $RNP = AP$.*

*Proof.* (Overall Scheme). In order to prove the theorem, we show that RTP Av-reduces to RNIP. Let $z = \langle \tau, n, r \rangle$ (where the $\tau$-row $r$ has length $k$) be a given instance of RTP and let $TOP(r) \subseteq C^4$ be the subset of colors appearing in the Top-component of the tiles in $r$. Basically, the reduction consists of the following three steps (see also [3]).

i) We first transform $z = \langle \tau, n, r \rangle$ to a new instance $z^t = \langle \tau^t, n+1, r^t \rangle$, where $|\tau_i^t| = |\tau_i|$ for any $i = 1, \ldots, k-1$ (see definition of RTP), such that $\tau$ admits a correct tiling for the lattice $\{0, \ldots, n-1\}^2$ iff $\tau^t$ admits a correct tiling for the torus $\mathcal{Z}_{n+1}^2$. Furthermore, we prove that this transformation is an Av-reduction[5] and thus, we can apply the following step.

ii) We transform the instance $z^t$ to a particular *ca* $A = (n+1, \tau^t \times Q^A, N^m, f^A)$ having the following properties:

1. The size of set $\tau^t \times Q^A$ does not depend on $n$;

[3] We remark that it is not a restriction to consider subsets, like $P$, having always $(0,0)$ as the first element since the toroidal structure of the support.

[4] In order to keep this definition as general as possible, the set $Q_a$ can be either a subset of Q or a subset of a component of $Q$. In other words, the particular choice of $Q_a$, among these possibilities, has no relevance for our next result.

[5] This first step shows also an independent result: RTP is RNP-complete also when the lattice has periodic structure.

2. $f^A$ is the identity with respect to the component $\tau^t$, that is, it does not change the tile component;
3. A is not injective in $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t) = \langle top(r^t(0)), top(r^t(1)),\ldots, top(r^t(k-1))\rangle$;
4. In each pair of different configurations $X$ and $Y$ belonging to $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$ such that $F^A(X) = F^A(Y)$, there is no cell having the same value in both $X$ and $Y$.

**iii)** Finally, we transform the *ca* $A$ defined in the previous step to a new *ca* $B = (n+1, \tau^t \times Q^A, N^m, f^B)$ where, for every cell $i \in \mathcal{Z}^2_{n+1}$, we have:

$$f^B = \begin{cases} f^A & \text{if there are no tiling err. in N(i)} \\ \textit{Identity function} & \text{otherwise} \end{cases}$$

Let us now give the proof scheme of the correctness of the above global reduction that will be called $\pi$. In particular, $\pi$ maps each instance $z^t = \langle \tau^t, n+1, r^t\rangle$ to the RNIP-instance $\langle B, P = (\{0,\ldots,k-1\}\times\{0\}, Q_a = TOP(r^t), x(r^t))\rangle$. If the torus $\mathcal{Z}^2_{n+1}$ can be correctly tiled with tiles in $\tau^t$ then $B$ is not injective in $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$; indeed, if we choose the $\tau^t$-component of two different configuration $X$ and $Y$ in order to have the same correct tiling of the torus, then $f^B$ operate like $f^A$ for all the support cells. Since $A$ is not injective in $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$ (see property 3. of $A$), the $Q^A$-component of $X$ and $Y$ can be chosen[6] to form two different configurations of $B$ having the same image with respect to the global function of $B$ (in short $F^B$). Conversely, if $B$ is not injective in $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$ then we have $F^B(X) = F^B(Y)$, for some $X \neq Y$ belonging to this set and, moreover, the tile components of $X$ and $Y$ must be the same (because of property 2. of $A$); therefore, with regard to the state component $Q^A$, we still have two different configurations $X$ and $Y$, belonging to $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$, having the same image also according to $F^A$. From property 4. of $A$, the local function $f^A$ must change the state of every cell in $X$ or in $Y$; same claim must hold for $f^B$, thus, according with the definition of $f^B$, there must be no tiling errors in the neighborhood of each cell and the torus can be correctly tiled.

From step ii) of the above proof, it should be clear that in order to prove our result we have to define the *ca* $A$ having the properties 1.,..,4. This *ca* is crucial since represents the bridge from the definition of a particular local map to the expected macroscopic behaviour. Let us now give an informal description of $A$. The set $Q^A$ has two components: a *tile* component (again!) and a finite set of boolean variables (i.e. an array of bits). The tile component determines one or more *passages* between adjacent cells (see also [4, 12]). When a global configuration defines a correct tiling (with respect to the tile component), we have the following *covering property*: the passages yield a *path* covering all cells of the toroidal support. A boolean variable (i.e. a bit) is defined on each passage. In case of correct tiling of the neighborhood (with respect to the tile component), the local function $f^A$ operates the $XOR$ function between the bits of consecutive passages in the path. A similar construction has been first introduced by Kari in [12], however his method (and, in particular, the set of tiles adopted by him) works on non periodic configurations of the infinite lattice. Under this point of view, our main technical result consists in making the path able to recognize the finite structure of the toroidal support of arbitrary size by using only "local" informations. To do this, we introduce a new set of tiles having the *covering property*; moreover, the cardinality of this tile set doesn't depend on the size of the toroidal support.

Finally, we observe that the set $\Sigma(\{0,\ldots,k-1\}\times\{0\}, TOP(r^t), x(r^t))$ is a closed set with respect to both *ca* global functions $F^A$ and $F^B$ since they keep unchanged the component $\tau^t$; this proves that RNIP is $RNP$-complete even when we consider only closed subsets of $\Sigma$.

**Probability function property**. Let us now prove that $\pi$ is an Av-reduction. From corollary 2.1 and step i) of the reduction $\pi$, we can consider only RTP instances in which the set of the top colors of all possible $\tau^t$-rows is: $TOP(r^t) = \{0,1\}$ and the corresponding probability of a given $\tau^t$-row $r^t$ of length $k$ $(0 \leq k < n)$ is proportional to $(1/2)^k$. Thus, the probability of the RTP instance $z^t$ is $Pr_1(z^t) = c(1/n^3)(1/2)^k$ for some positive constant $c$ depending only on $\tau$. Since the subset $TOP(r^t)$ has always cardinality two, the probability of the RNIP instance $w = \pi(z^t)$, is $Pr_2(w) = \beta(1/n^3)(1/2^k)$ where $\beta$ is a positive constant not depending on $n$ (remark also property 1. of the *ca* $A$). For these reasons, it is easy to verify that $Pr_2$ *dominates* $Pr_1$ with respect to $\pi$.

## 4 Conclusions and future applications

In this paper, we have presented the first example of decision problem, dealing with cellular automata, which can be considered "hard" also in the average-case complexity. In ([18]) a number of open problems concerning cellular automata were posed. One of them is the question of how common "hardness" results are in problems dealing with cellular automata. The answer may have a significant bearing on the practical ability to predict the outcome of various chaotic phenomena based on computation. In addition, some of the practical difficulties of efficiently programming parallel computers might be revealed [19]. In particular, our "hardness" result for REV implies that, in order to obtain a general-purpose computing model based on invertible finite cellular automata, we should

[6] We observe that any configuration for $A$ can be also seen as a configuration of $B$ and viceversa

define a local map together with a closed subset of legal configurations which *a priori* yield a global invertible process, since this property cannot be, in general, efficiently tested (i.e. in polynomial average-time).

On the other hand, the $NP$-completeness result proved in [5] implies the existence of a family of invertible finite ca having local and simple interactions whose inverse maps have, on the contrary, large and complex interactions. This theoretical result, concerning the worst-case complexity, gives no informations about the relative size of this family with respect to the size of the class of all invertible finite *ca*; In other words, it was possible that such a particular behaviour was very "unlikely" and thus difficult to generate. On the contrary, the discrete-probabilistic nature of our result shows that, when the closed set of legal configurations (on which the ca will run on) is also specified, then this family of invertible *ca* has an "important" relative size and its effective contruction[7] could define an interesting class of *one-way functions* having the well-known practical applications in pseudo-random generators and in cryptology.

**Acknowledgments** We would like to thank Patrizia Mentrasti and Tommaso Toffoli for helpful and very crucial comments and advices during this work.

## References

[1] C. H. Bennett, P. Gacs, M. Li, P. Vitanyi, W. Zurek, "Thermodynamics of Computation and Information Distance", *Proc. of the* $25^{th}$ *ACM-STOC*, 21–30, 1993.

[2] C. Bilardi,F. Preparata, "Horizons of Parallel Computation", *Proc. of Symp. of* $25^{th}$ *Anniversary of INRIA, Springer-Verlag LNCS*, 653, 155-174, 1992.

[3] A. Clementi, "On the complexity of Cellular Automata", PhD thesis, University of Rome "La Sapienza", 1994.

[4] A. Clementi, P. Mentrasti, P. Pierini, "Some results on invertible cellular automata", *Proc. of IEEE PhysComp '94*, 1994.

[5] A. Clementi, P. Pierini, "Computational complexity of the finite cellular automata reversibility problem", *Proceedings of the* $4^{th}$ *Italian Conference on Theoretical Computer Science*, L'Aquila, Italy, 165–178, 1992.

[6] B. Durand, "Global invertibility on finite cellular automata", to appear in *Theoretical Computer Science*.

[7] M. Dyer, A. Frieze, "The solution of some random $NP$-complete problems in polynomial expected time", *J. of Algorithms*, 10, 451–462, 1993.

[8] M.R. Garey, D. S. Johnson, *Computers and intractability. A guide to the theory of NP-completeness* Freeman and Company, 1979.

[9] F. Green, "NP-complete problems in cellular automata", *Complex Systems*, 1, 453–474, 1987.

[10] Y. Gurevich, "Average-Case Completeness", *J. of Computer and System Sciences*, 42, 346–360, 1991.

[11] G. Jacopini, G. Sontacchi, "Reversible Parallel Computation: an evolving space model", *Theoret. Comput. Sci.*, 73,1–46, 1990.

[12] J. Kari, "Reversibility of 2D cellular automata is undecidable", *Physica D 45*, 379–385, 1990.

[13] J. Kari, "Reversibility and surjectivity problems of cellular automata", *J. Comp. Syst. Sci.*, 48, 149–182, 1994.

[14] L. Kucera, "Expected behaviour of graph coloring algorithms", *Foundations of Computation Theory '77*, Springer-Verlag LNCS, 56, 447–453, 1977.

[15] L. Levin, "Average-Case Complete Problems", *SIAM J. of Computing*, 15, 285–286, 1986.

[16] K. Sutner, "Computational complexity of finite cellular automata", Tech. Rep., Stevens Institute of Technology, Hoboken, NJ 07030 USA., 1989.

[17] T. Toffoli, N. Margolus, "Invertible cellular automata: a review", *Physica D*, 45, 229–253,1990.

[18] S. Wolfram, "Twenty problems in the theory of cellular automata", *Physica Scrypta*, T9, 170–183 , 1985.

[19] S. Wolfram, "Approaches to complexity engineering", *Physica D*, 22, 246–253, 1986.

[7] From a practical point of view, the formal difference between the definition of REV and the generalization, considered in this paper, has no consequences: indeed, the considered closed subset of legal configurations (i.e. $\Sigma(P, Q_a, x)$) is polynomial-time decidable, hence we can "efficiently" force the *ca* to "run" only on legal starting configurations.