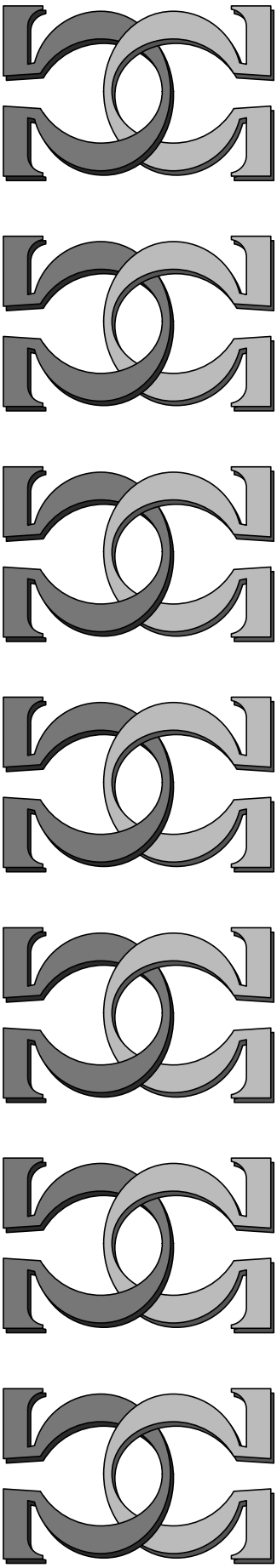

CDMTCS Research Report Series

Randomness on Full Shift Spaces

Cristian S. Calude
Peter P. Hertling
Department of Computer Science
University of Auckland

Helmut Jürgensen
Department of Computer Science
University of Western Ontario, Canada

Klaus Weihrauch
Theoretische Informatik I, Fern-Universität
Hagen, Germany

CDMTCS-100
April 1999

Centre for Discrete Mathematics and
Theoretical Computer Science

Randomness on Full Shift Spaces*

Cristian S. Calude,† Peter P. Hertling,‡ Helmut Jürgensen,§ Klaus Weihrauch¶

Abstract

We give various characterizations for algorithmically random configurations on full shift spaces, based on randomness tests. We show that all nonsurjective cellular automata destroy randomness and surjective cellular automata preserve randomness. Furthermore all one-dimensional cellular automata preserve nonrandomness. The last three assertions are also true if one replaces randomness by richness,—a form of pseudorandomness, which is compatible with computability, the last assertion even for an arbitrary dimension.

1 Introduction

Cellular automata were originally introduced by Ulam and von Neumann [28] as models for natural complex systems, especially self–reproducing biological systems. Since then they have been analyzed in many other contexts, e.g. for the simulation of physical phenomena, for computability questions (cellular automata are capable of universal computation), for random number generation, in the framework of formal language theory, in symbolic dynamics, and many more; compare e.g. Wolfram [30] and other papers in the same volume, Toffoli, Margolus [27], Culik, Hurd, Yu [11], and Lind, Marcus [17].

Cellular automata show a uniform behavior over a certain region of the space. They operate on configurations which consist of a discrete lattice of cells each of which is in one of finitely many states. Time is discrete; at each time step the value of each cell is updated uniformly according to a finite set of rules. The new value of a cell depends only on the current values of finitely many cells in its neighborhood. Although cellular automata can be described easily by a finite set of rules (the local function) they exhibit a rich and complicated global behavior which often seems chaotic or random. In [31] Wolfram discussed some aspects of cellular automata with respect to randomness in the sense of

*Calude was supported in part by AURC Grants, A18/XXXXX/62090/F3414044-50. Hertling was supported by the DFG Research Grant No. HE 2489/2-1. Jürgensen was supported by National Sciences and Engineering Council of Canada Grant OGP0000243.

†Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand, email: cristian@cs.auckland.ac.nz.

‡Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand, email: hertling@cs.auckland.ac.nz.

§Department of Computer Science, The University of Western Ontario, London, Ontario, Canada N6A 5B7, and Institut für Informatik, Universiät Potsdam, Am Neunen Palais 10, D-14469, Potsdam, Germany, email: helmut@uwo.ca.

¶Theoretische Informatik I, Fern-Universität Hagen, D-58084 Hagen, Germany, email: klaus.weihrauch@fernuni-hagen.de.

algorithmic information theory; compare Chaitin [7], Calude [4]. In this paper we give several rigorous mathematical characterizations of random configurations and analyze the behavior of cellular automata on random and nonrandom configurations.

The characterizations of random configurations are based on Martin–Löf's [19] idea to use randomness tests and the generalization of his ideas carried out by Hertling and Weihrauch [13, 14]. We show that a cellular automaton is surjective if and only if it preserves randomness of configurations. This gives a new characterization of the class of surjective cellular automata. Note that the analysis and comparison of the classes of injective (or reversible) cellular automata and surjective cellular automata have received great attention in the past, starting with Moore's *Garden of Eden Theorem* [22]; compare Myhill [23], Richardson [24], Maruoka and Kimura [20, 21], and others. It follows directly from known results that nonsurjective cellular automata destroy randomness. Furthermore, we show that every cellular automaton of dimension 1 preserves nonrandomness, i.e., if started on a nonrandom configuration then the following configuration is nonrandom as well. The same statements are shown to be true also if randomness is replaced by the simpler "richness" property (following Compton's [10] terminology for one way infinite sequences we call a configuration *rich* if it contains every finite pattern). In fact, cellular automata of arbitrary dimension preserve nonrichness. At present it seems to be open whether arbitrary cellular automata of dimension 2 or greater preserve nonrandomness. These definitions and results may serve as a first step towards a better understanding of the "random" behavior of cellular automata. Further possible questions in this context are formulated in the conclusions section.

We give a short overview over the paper. In the next section we introduce and describe full shift spaces and basic notions connected with them. We also introduce the notion of an algorithmically random configuration. In Section 3 more characterizations (based on randomness tests) and properties of random configurations are discussed; the construction of new randomness spaces in terms of products and quotients of randomness spaces is also analyzed. In Section 4, we define cellular automata and analyze their behavior with respect to randomness and nonrandomness of configurations. Finally, in Section 5, we indicate some possible further questions for study.

2 Full Shift Spaces

We introduce full shift spaces and several elementary notions connected with them, especially richness of configurations.

By $\mathbf{N}, \mathbf{Z}$ we denote the sets $\{0, 1, 2, \ldots\}$ (of nonnegative integers) and $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ integers, respectively. Let Σ be a finite set with at least 2 elements, and let $d \geq 1$ be a positive integer. Then $\mathbf{Z}^d$ is the d–dimensional lattice over the integers $\mathbf{Z}$. The space $\Sigma^{\mathbf{Z}^d}$ is called a *full shift space*. We call the elements of Σ the *states*, the number d the *dimension*, and the elements $c \in \Sigma^{\mathbf{Z}^d}$ the *configurations* of the full shift space. On such spaces we use the product topology induced by infinitely many copies of the discrete topology on the finite space Σ. For a configuration $c \in \Sigma^{\mathbf{Z}^d}$ and $a \in \mathbf{Z}^d$ we write c_a instead of $c(a)$; elements of $\mathbf{Z}^d$ will be sometimes called cells and c_a will then be the content s of cell a. For $r \in \mathbf{N}$, let $[-r, r]$ denote the set $\{-r, \ldots, 0, \ldots, r\}$. By Tychonoff's Theorem the space $\Sigma^{\mathbf{Z}^d}$ is compact because it is a countable product of compact spaces.

This space is in fact a metric space. One can, for example, use the metric *dist* defined by $dist(c, c') = 2^{-m(c,c')}$ where

$$m(c, c') = \min\{r \in \mathbf{N} \mid \ \exists a \in [-r, r]^d : \ c_a \neq c'_a\},$$

for $c, c' \in \Sigma^{\mathbf{Z}^d}$; here $\min \emptyset = \infty$. The sets

$$\{c \in \Sigma^{\mathbf{Z}^d} \mid c_z = s\}, \quad s \in \Sigma, \ z \in \mathbf{Z}^d$$

form a subbase of the topology on $\Sigma^{\mathbf{Z}^d}$. Cellular automata operate on full shift spaces. Related questions will be discussed in Section 4.

The name *shift spaces* comes from the fact that the *shift mappings* on the space $\Sigma^{\mathbf{Z}^d}$ play an important role. Each integer vector $a = (\alpha_1, \ldots, \alpha_d) \in \mathbf{Z}^d$ induces a bijection $\sigma_a^{(d)} : \Sigma^{\mathbf{Z}^d} \to \Sigma^{\mathbf{Z}^d}$ defined by $\sigma_a^{(d)}(c)_b = c_{b+a}$, for every $b \in \mathbf{Z}^d$; it is called the *shift map associated with* a. In the sequel the superscript (d) will be omitted when the dimension is clear from the context. The shift map σ_{e_i} associated with the unit vector $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbf{Z}^d$ having a 1 in position i and zeroes on all other positions is also written σ_i. The shift mapping σ_1 is the usual left shift in the one-dimensional case.

We wish to define a random configuration of a full shift space. First let us look at the simplest case, when the dimension d is equal to 1. For one-way infinite sequences[1] in $\Sigma^{\mathbf{N}} = \{p \mid p : \mathbf{N} \to S\}$ one obtains the well–known randomness notion from algorithmic information theory; see Calude [4], Li, Vitányi [16]. Random one-way sequences can be defined via Martin–Löf's [19] randomness tests or Chaitin [6, 7, 9] program–size complexity. This "notion of randomness" will be defined precisely below. The simplest way to define randomness for two-way infinite sequences over Σ, that is, for elements of $\Sigma^{\mathbf{Z}}$, is to use a standard bijection from $\mathbf{Z}$ to $\mathbf{N}$, e.g. the bijection $\langle \cdots \rangle : \mathbf{Z} \to \mathbf{N}$ defined by

$$\langle z \rangle = \begin{cases} 2z, & \text{if } z \geq 0, \\ 2(-z) - 1, & \text{if } z < 0. \end{cases}$$

This bijection induces a bijection from $\Sigma^{\mathbf{N}}$ to $\Sigma^{\mathbf{Z}}$ in the obvious way: one maps an element $p = (p_i)_i \in \Sigma^{\mathbf{Z}}$ to the one-way sequence $q = (q_z)_z \in \Sigma^{\mathbf{N}}$ defined by $q_z = p_{\langle z \rangle}$, for all $z \in \mathbf{Z}$. Now it seems natural to call a two-way infinite sequence $q \in \Sigma^{\mathbf{Z}}$ *random* if and only if the corresponding one-way infinite sequence $p \in \Sigma^{\mathbf{N}}$ is random.

This procedure can also be carried out in the case of a dimension $d \geq 1$. For this aim we use a bijection from $\mathbf{Z}^d$ onto $\mathbf{N}$. The mapping $\pi : \mathbf{N}^2 \to \mathbf{N}$ defined by $\pi(i, j) = (i + j)(i + j + 1) + i$ is a bijection. For $d \geq 2$ we define $\langle \cdots \rangle : \mathbf{Z}^d \to \mathbf{N}$ recursively by

$$\langle z_1, \ldots, z_d \rangle = \pi(\langle z_1 \rangle, \langle z_2, \ldots, z_d \rangle).$$

This is a bijection for each $d \geq 1$.

If L_1 and L_2 are countable sets, then a total mapping $f : L_1 \to L_2$ induces a mapping $\overline{f} : \Sigma^{L_2} \to \Sigma^{L_1}$ via

$$\overline{f}(p)_{l_1} = p_{f(l_1)},$$

for all $p \in \Sigma^{L_2}$ and $l_1 \in L_1$. If f is a bijection, then also $\overline{f}$ is a bijection. Hence, for each $d \geq 1$, the induced mapping $\overline{\langle \cdots \rangle} : \Sigma^{\mathbf{N}} \to \Sigma^{\mathbf{Z}^d}$ is a bijection. It is clear that it is

[1] In formal language theory one writes Σ^ω instead of $\Sigma^{\mathbf{N}}$ and the elements of $\Sigma^{\mathbf{N}}$ are called ω-words.

even a homeomorphism, and induces a bijection of the following subbases of the respective topologies: the pre-image under $\overline{\langle\cdots\rangle}$ of the cylinder $\{c \in \Sigma^{\mathbf{Z}^d} \mid c_z = s\} \subseteq \Sigma^{\mathbf{Z}^d}$ for $s \in \Sigma$ and $z \in \mathbf{Z}^d$ is the cylinder $\{c \in \Sigma^{\mathbf{N}} \mid c_{\langle z \rangle} = s\}$, and these sets form a subbase of the product topology on $\Sigma^{\mathbf{N}}$. Furthermore, if we consider the product measure $\tilde{\mu}$ on $\Sigma^{\mathbf{N}}$ and $\tilde{\mu}$ on $\Sigma^{\mathbf{Z}^d}$ of the uniform measure μ on Σ, given by $\mu(\{s\}) = 1/|\Sigma|$, then $\overline{\langle\cdots\rangle}$ is also measure preserving, i.e., $\tilde{\mu}(\overline{\langle\cdots\rangle}^{-1}(U)) = \tilde{\mu}(U)$ for all open $U \subseteq \Sigma^{\mathbf{Z}^d}$. Thus, the mapping $\overline{\langle\cdots\rangle}$ really shows that the spaces $\Sigma^{\mathbf{N}}$ and $\Sigma^{\mathbf{Z}^d}$ are identical with respect to topology and measure. Using these considerations we shall see later that it makes sense to call a configuration $c \in \Sigma^{\mathbf{Z}^d}$ random if and only if the one-way infinite sequence $\overline{\langle\cdots\rangle}(c) \in \Sigma^{\mathbf{N}}$ is random.

There is just one more point which should be discussed: does the construction above depend upon the bijection $\langle\cdots\rangle : \mathbf{Z}^d \to \mathbf{N}$? Does the choice of the bijection influence the definition? Certainly it does, because the notion of randomness for elements of $\Sigma^{\mathbf{N}}$ is not invariant under an arbitrary permutation of its entries.

Example 2.1 For every sequence $c_0c_1c_2\ldots \in \Sigma^{\mathbf{N}}$, there exists a bijection $\psi : \mathbf{N} \to \mathbf{N}$ such that the sequence $c_{\psi(0)}c_{\psi(1)}c_{\psi(2)}\ldots \in \Sigma^{\mathbf{N}}$ is nonrandom. Such a ψ can be obtained for example as follows. If the $c_0c_1c_2\ldots$ is not random we can take ψ to be the identity. Otherwise we can assume, without loss of generality, that $\Sigma = \{0, 1, \ldots, q-1\}$, for some $q \geq 2$. Some element of Σ appears in the sequence infinitely many times, say $c_i = 0$, for infinitely many i. Let $f : \mathbf{N} \to \mathbf{N}$ be the unique and increasing function such that $c_{f(i)}$ is the $(i+1)$–st zero in $c_0c_1c_2\ldots$ for all i. We define ψ by

$$\psi(i) = \begin{cases} f(2j+1), & \text{if } i = f(2j)+1, \\ f(2j)+1, & \text{if } i = f(2j+1), \\ i, & \text{if } i \notin \bigcup_{j\in\mathbf{N}}\{f(2j)+1, f(2j+1)\}. \end{cases}$$

Then the sequence $c_{\psi(i)}c_{\psi(1)}c_{\psi(2)}\ldots$ does not contain an isolated zero, hence it does not contain the word 101, hence it is nonrandom.[2]

But if $\psi : \mathbf{N} \to \mathbf{N}$ is a computable bijection, then a sequence $c_0c_1c_2\ldots \in \Sigma^{\mathbf{N}}$ is random if and only if the sequence $c_{\psi(0)}c_{\psi(1)}c_{\psi(2)}\ldots \in \Sigma^{\mathbf{N}}$ is random (see Book, Lutz, Martin [2, Lemma 3.4] or Hertling, Weihrauch [14, Corollary 4.9]). Hence, *if a bijection $b : \mathbf{Z}^d \to \mathbf{N}$ is chosen such that $\langle\cdots\rangle \circ b^{-1}$ is computable we obtain via b the same randomness notion on $\Sigma^{\mathbf{Z}^d}$ as via the bijection $\overline{\langle\cdots\rangle}$.*

We would like to consider also a very weak form of randomness for which this is not true: richness. Following Compton [10], we call a one-way infinite sequence $c \in \Sigma^{\mathbf{N}}$ *rich* if and only if every word $w \in \Sigma^*$ occurs in c.[3] This can be transferred to configurations as follows.

Two elements $v \in \Sigma^A$ and $w \in \Sigma^B$ for finite sets $A, B \subseteq \mathbf{Z}^d$ are called *equivalent* if and only if there exists an integer vector $a \in \mathbf{Z}^d$ such that $A = a + B$, and $v_{a+b} = w_b$ for all $b \in B$. The equivalence classes of elements of Σ^A for finite subsets $A \subseteq \mathbf{Z}^d$ are called *patterns (over Σ and of dimension d)*. The equivalence classes of elements of $\Sigma^{\{1,2,\ldots,n\}^d}$ for any positive integer n are called *cube patterns*. The number n is called the *side length* of such a cube pattern. We say that a pattern, given by a representative $w \in \Sigma^A$ for some

[2] A random sequence in $\Sigma^{\mathbf{N}}$ contains every word in Σ^*, see Calude [4].

[3] Richness is called disjunctiveness in formal language theory, cf. Jürgensen and Thierrin [15].

finite set $A \subseteq \mathbf{Z}^d$, *occurs* or *is contained* in a configuration $c \in \Sigma^{\mathbf{Z}^d}$ if there exists an integer vector $b \in \mathbf{Z}^d$ such that $c_{b+a} = w_a$ for all $a \in A$.

Definition 2.2 We call a configuration $c \in \Sigma^{\mathbf{Z}^d}$ *rich* if and only if every pattern over Σ and of dimension d occurs in c.

It is clear that a configuration is rich if and only if every cube pattern (over Σ, of dimension d) occurs in c.

We conclude this section with the observation that in contrast to randomness richness is very fragile even under computable rearrangement of sequences. *If a one-way infinite sequence $c = c_0c_1c_2\ldots \in \Sigma^{\mathbf{N}}$ is rich, then also the two-way infinite sequence $\overline{\langle\cdots\rangle}(c) = \ldots c_3c_1c_0c_2c_4\ldots \in \Sigma^{\mathbf{Z}}$ is rich, but the converse is not true.* Indeed, let c be a one-way rich sequence and define another one-way sequence $\tilde{c}$ by $\tilde{c}_{2i} = c_i$ and $\tilde{c}_{2i+1} = s$ for all i where s is a fixed element of Σ. Then $\tilde{c}$ is not rich, but the corresponding two-way sequence $\overline{\langle\cdots\rangle}(\tilde{c}) = \ldots sssc_0c_1c_2c_3\ldots$ is rich. Yet, by choosing a different bijection from $\mathbf{Z}$ to $\mathbf{N}$ one can achieve equivalence of the richness notions on $\Sigma^{\mathbf{N}}$ and $\Sigma^{\mathbf{Z}}$: it is not difficult to check that a two-way sequence $c = \ldots c_{-2}c_{-1}c_0c_1c_2\ldots$ is rich if and only if the one-way sequence

$$c_0c_{-1}c_{-2}c_{-3}c_1c_2c_3c_{-4}c_{-5}c_{-6}c_{-7}c_{-8}c_4c_5c_6c_7c_8c_{-9}\ldots c_{-15}c_9\ldots c_{15}\ldots$$

is rich. Note also that randomness is base invariant but richness is not base invariant: a real number α has a random binary representation if and only if all representations of α to any base are random; see Calude, Jürgensen [5, 4]; for different proofs see Hertling, Weihrauch [13], and Staiger [26]. But for any two bases $b, c \geq 2$ such that $b^n \neq c^m$ for all $n, m \geq 1$, there are real numbers which have a rich representation to base b, but a nonrich representation to base c; see Schmidt [25], compare also Hertling [12].

3 Full Shift Spaces as Randomness Spaces

In this section we give another characterization of algorithmically random elements of full shift spaces. We further study randomness spaces and the construction of new randomness spaces in terms of products and quotients of randomness spaces.

In the previous section we introduced randomness in $\Sigma^{\mathbf{Z}^d}$ by identifying $\Sigma^{\mathbf{N}}$ and $\Sigma^{\mathbf{Z}^d}$ via a standard bijection between $\mathbf{Z}^d$ and $\mathbf{N}$ and by using the randomness notion on $\Sigma^{\mathbf{N}}$. There is another more direct way to define randomness on full shift spaces, without reference to random one-way infinite sequences: one can formulate Martin–Löf's [19] idea to define randomness for one-way infinite sequences in $\Sigma^{\mathbf{N}}$ via so–called randomness tests in a much more general setting. This has been carried out by Hertling and Weihrauch [13, 14]. One can apply the definition of randomness spaces in [13, 14] especially to full shift spaces. We repeat the definition of randomness spaces, randomness test and random elements from Hertling, Weihrauch [13, 14].

Definition 3.1 (Hertling, Weihrauch [13, 14]) A *randomness space* is a triple (X, B, μ), where X is a topological space, $B : \mathbf{N} \to 2^X$ is a total numbering of a subbase of the topology of X, and μ is a measure defined on the σ-algebra generated by the topology of X (notation: $B_i = B(i)$).

Recall that a subbase of a topology is a set β of open sets such that the sets $\bigcap_{U\in E} U$, for finite, nonempty sets $E \subseteq \beta$ form a basis of the topology. Random points of a randomness space are defined via randomness tests. Before we define them we introduce the numbering B' of a base derived from a numbering B of a subbase, and define computable sequences of open sets. In the following definition we use the bijection $D : \mathbf{N} \to \{E \mid E \subseteq \mathbf{N} \text{ is finite}\}$ defined by $D^{-1}(E) = \sum_{i\in E} 2^i$.

Definition 3.2 (Hertling, Weihrauch [13, 14]) Let X be a topological space and $(U_n)_n$ be a sequence of open subsets of X.

1. A sequence $(V_n)_n$ of open subsets of X is called *U–computable* if there is a c.e. set $A \subseteq \mathbf{N}$ such that
$$V_n = \bigcup_{\substack{i\in\mathbf{N},\\ \pi(n,i)\in A}} U_i,$$
for all $n \in \mathbf{N}$.

2. The sequence $(U'_n)_n$ of open sets defined by
$$U'_i = U'(i) = \bigcap_{j\in D_{1+i}} U_j,$$
for all $i \in \mathbf{N}$, is called the *sequence derived from U*.

Note that if B is a numbering of a subbase of a topology, then $B' = (U'_i)_i$ is a numbering of a base of the same topology. The next definition generalizes Martin–Löf's [19] definition of random sequences to points from arbitrary randomness spaces.

Definition 3.3 (Hertling, Weihrauch [13, 14]) Let (X, B, μ) be a randomness space.

1. A *randomness test on X* is a B'–computable sequence $(U_n)_n$ of open sets with $\mu(U_n) \leq 2^{-n}$ for all $n \in \mathbf{N}$.

2. An element $x \in X$ is called *nonrandom* if $x \in \bigcap_{n\in\mathbf{N}} U_n$ for some randomness test $(U_n)_n$ on X. It is called *random* if it is not nonrandom.

Examples 3.4 *1.* (Hertling, Weihrauch [14]) The simplest examples of randomness spaces are spaces (Σ, B, μ) where $\Sigma = \{s_0, \ldots, s_k\}$ is a finite, nonempty set, the numbering B is given by $B_i = \{s_i\}$ for $i \leq k$ and $B_i = X$ for $i > k$, and the measure μ is given by $\mu(\{s_i\}) = \frac{1}{k+1}$. Notice that μ is a probability measure. Every element of Σ is random because the measure of any nonempty open set is at least $\frac{1}{k+1}$.

2. (Hertling, Weihrauch [13, 14]) The original randomness spaces are the spaces $(\Sigma^{\mathbf{N}}, B, \tilde{\mu})$ of infinite sequences over a finite alphabet Σ with at least two elements (Martin-Löf [19]). The numbering B of a subbase (in fact a base) of the topology is given by $B_i = \nu(i)\Sigma^{\mathbf{N}} = \{p \in \Sigma^{\mathbf{N}} \mid \nu(i) \text{ is a prefix of } p\}$, where $\nu : \mathbf{N} \to \Sigma^*$ is the length–lexicographical bijection between $\mathbf{N}$ and the set Σ^* of finite words over Σ. The measure $\tilde{\mu}$ is the product measure of the measure in the first example, i.e., $\tilde{\mu}(w\Sigma^{\mathbf{N}}) = |\Sigma|^{-|w|}$ for $w \in \Sigma^*$.

3. Let $\Sigma = \{s_0, \ldots, s_k\}$ have $k+1 \geq 2$ elements and $d \geq 1$. In order to view the full shift space $\Sigma^{\mathbf{Z}^d}$ as a randomness space $(\Sigma^{\mathbf{Z}^d}, \tilde{B}, \tilde{\mu})$ we have to describe the measure $\tilde{\mu}$ and the numbering $\tilde{B}$ of a subbase of the topology. The measure $\tilde{\mu}$ is the product measure of the measure in the first example, i.e., given by $\tilde{\mu}(\{c \in \Sigma^{\mathbf{Z}^d} \mid c_z = s\}) = 1/(k+1)$ for $s \in \Sigma$ and $z \in \mathbf{Z}^d$. The numbering $\tilde{B}$ is defined by

$$\tilde{B}_{j+(k+1)\cdot\langle z_1,\ldots,z_d\rangle} = \{c \in \Sigma^{\mathbf{Z}^d} \mid c_{(z_1,\ldots,z_d)} = s_j\}$$

for $0 \leq j \leq k$ and $(z_1, \ldots, z_d) \in \mathbf{Z}^d$. Here $\langle \cdots \rangle$ is the bijection from $\mathbf{Z}^d$ to $\mathbf{N}$ defined above.

Example 3.4.2 gives us the usual randomness notion for one-way infinite sequences over a finite alphabet. The numbering B used in Example 3.4.2 is already a numbering of a base, and it is easy to see that a sequence $(U_i)_i$ of open subsets $U_i \subseteq \Sigma^{\mathbf{N}}$ is B'–computable if and only if it is B–computable. Thus, a sequence $(U_i)_i$ of open sets is a randomness test if and only if it is B–computable and satisfies $\mu(U_i) \leq 2^{-i}$ for all i. Example 3.4.3 gives us a randomness notion for elements of full shift spaces. This is the same randomness notion as the notion which one obtains by identifying the full shift space $\Sigma^{\mathbf{Z}^d}$ with $\Sigma^{\mathbf{N}}$ via the bijection $\overline{\langle \cdots \rangle}$ and the usual randomness notion on $\Sigma^{\mathbf{N}}$.

Proposition 3.5 *Let Σ be a finite set with at least 2 elements and let $d \geq 1$ be a positive integer. For a configuration $c \in \Sigma^{\mathbf{Z}^d}$ the following conditions are equivalent:*

1. *The infinite one-way sequence $\overline{\langle \cdots \rangle}(c) \in \Sigma^{\mathbf{N}}$ is random (or, equivalently, a random element of the randomness space $(\Sigma^{\mathbf{N}}, (\nu(i)\Sigma^{\mathbf{N}})_i, \tilde{\mu})$ of Example 3.4.2.*

2. *The configuration c is a random element of the randomness space $(\Sigma^{\mathbf{Z}^d}, \tilde{B}, \tilde{\mu})$ of Example 3.4.3).*

Before we prove this we give another characterization for computable sequences of open sets in $\Sigma^{\mathbf{Z}^d}$. For an arbitrary finite set $A \subseteq \mathbf{Z}^d$ and $v \in \Sigma^A$ we set

$$[v] = \{c \in \Sigma^{\mathbf{Z}^d} \mid c_z = v_z \text{ for all } z \in A\}.$$

The set

$$\mathrm{Cubes}(\Sigma, d) = \bigcup_{r \geq 0} \Sigma^{[-r,r]^d}$$

is countable and we can fix a bijection $\mathrm{Cube} : \mathbf{N} \to \mathrm{Cubes}(\Sigma, d)$. The sets $[v]$ for elements $v \in \mathrm{Cubes}(\Sigma)$ form a base of the topology on $\Sigma^{\mathbf{Z}^d}$. The following lemma is useful when one considers randomness tests on $\Sigma^{\mathbf{Z}^d}$.

Lemma 3.6 *For a sequence $(U_i)_i$ of open subsets of $\Sigma^{\mathbf{Z}^d}$ the following conditions are equivalent:*

1. *It is $\tilde{B}'$–computable.*

2. *It is* Cube*–computable.*

3. *The sequence* $(\overline{\langle\cdots\rangle}^{-1}(U_i))_i$ *of open subsets of* $\Sigma^{\mathbf{N}}$ *is* $(\nu(j)\Sigma^{\mathbf{N}})_j$*-computable.*

Proof of Proposition 3.5. The assertion follows from Lemma 3.6 and from the fact that the homeomorphism $\overline{\langle\cdots\rangle} : \Sigma^{\mathbf{N}} \to \Sigma^{\mathbf{Z}^d}$ is measure preserving. □

Definition 3.7 Let $d \geq 1$ and Σ be a finite set with at least two elements. If a configuration $c \in \Sigma^{\mathbf{Z}^d}$ satisfies one and then all conditions in Proposition 3.5, then we call it *random.*

First we observe:

Lemma 3.8 *Every random configuration is rich.*

Proof. Fix an arbitrary cube pattern. By a simple counting argument one can easily prove in an effective way that the set of all configuration which do not contain this pattern has measure zero. Therefore all such configurations are nonrandom. Since this is true for all cube patterns, it follows that all random configurations are rich. □

Remark 3.9 In fact, much more is true. One can define in a natural way *normal* configurations, in which all patterns occur with the expected frequency. In the same way as one proves that every random real number has a normal binary expansion, one can also prove that every random configuration is normal. It is clear that every normal configuration is rich.

It is well–known that on $\Sigma^{\mathbf{N}}$ there exists a *universal* randomness test, i.e., a randomness test $(U_i)_i$ such that for every other randomness test $(V_i)_i$ on $\Sigma^{\mathbf{N}}$ there exists a nonnegative integer c such that $V_{n+c} \subseteq U_n$ for all n. From the fact that $\Sigma^{\mathbf{N}}$ and $\Sigma^{\mathbf{Z}^d}$ are essentially the same randomness spaces (as expressed by Lemma 3.6 and Proposition 3.5) we conclude that also on $\Sigma^{\mathbf{Z}^d}$ there exists a universal randomness test. In fact, if $(U_i)_i$ is a universal randomness test on $\Sigma^{\mathbf{N}}$, then $(\overline{\langle\cdots\rangle}(U_i))_i$ is a universal randomness test on $\Sigma^{\mathbf{Z}^d}$.

In the case of dimension $d = 1$ the first of the conditions in Proposition 3.5 says that a two-way infinite sequence $c = \ldots c_{-3}c_{-2}c_{-1}c_0c_1c_2c_3 \ldots \in \Sigma^{\mathbf{Z}}$ is random if and only if the one-way infinite sequence $c_0c_{-1}c_1c_{-2}c_2c_{-3}c_3 \ldots \in \Sigma^{\mathbf{N}}$ is random. It is instructive to notice that this is also equivalent to the following condition:

3. *the pair* $((c_0, c_1, c_2, \ldots), (c_{-1}, c_{-2}, c_{-3}, \ldots))$ *of infinite one-way sequences is random, i.e., it is a random element of the product randomness space* $((\Sigma^{\mathbf{N}})^2, B^2, \mu^2)$

(compare Hertling, Weihrauch [13, 14]). This last condition is often expressed by saying that the two sequences $(c_0, c_1, c_2, \ldots)$ and $(c_{-1}, c_{-2}, c_{-3}, \ldots)$ are "independently random".

We would like to add one "caveat" with respect to randomness tests and two-way infinite sequences: one must distinguish between randomness tests for two-way infinite sequences and for one-way infinite sequences. Let $(U_i)_i$ be a universal randomness test on the space $(\Sigma^{\mathbf{N}}, B, \tilde{\mu})$ of one-way infinite sequences, and let $A \subseteq \mathbf{N}$ be a computably enumerable set such that $U_n = \bigcup_{\pi(n,i)\in A} \nu(i)\Sigma^{\mathbf{N}}$ for all n (where $\nu : \mathbf{N} \to \Sigma^*$ is the standard bijection between natural numbers and finite words over Σ used in Example 3.4.2). Let $A_n = \{\nu(i) \mid$

$\pi(n,i) \in A\}$, for all n. We assume without loss of generality that all sets A_n are suffix–closed, i.e., if a prefix of a word w is contained in A_n then also w itself is in A_n. Then a two-way infinite sequence $c = \ldots c_{-3}c_{-2}c_{-1}c_0c_1c_2c_3 \ldots \in \Sigma^{\mathbf{Z}}$ is nonrandom if and only if for each $n \in \mathbf{N}$ there is an $m \in \mathbf{N}$ with $c_0c_{-1}c_1c_{-2}c_2 \ldots c_{-m}c_m \in A_n$. But notice that we cannot replace $c_0c_{-1}c_1c_{-2}c_2 \ldots c_{-m}c_m$ by $c_{-m} \ldots c_{-1}c_0c_1 \ldots c_m$ in this condition:

Proposition 3.10 *Every random two-way infinite sequence $c = \ldots c_{-2}c_{-1}c_0c_1c_2 \ldots \in \Sigma^{\mathbf{Z}}$ has the property that for every $n \in \mathbf{N}$ there is an $m \in \mathbf{N}$ with $c_{-m} \ldots c_{-1}c_0c_1 \ldots c_m \in A_n$.*

Proof. Let us fix a number n and an arbitrary word $w = w_1 \ldots w_l \in A_n$. For every random sequence $c = \ldots c_{-2}c_{-1}c_0c_1c_2 \ldots \in \Sigma^{\mathbf{Z}}$ there exists an $m > l$ such that $c_{-m} \ldots c_{-m+l-1} = w$, hence such that the word w is a prefix of $c_{-m} \ldots c_{-1}c_0c_1 \ldots c_m$. Because A_n is assumed to be suffix–closed we conclude that $c_{-m} \ldots c_{-1}c_0c_1 \ldots c_m \in A_n$. □

We end this section with a remark on randomness on the space obtained by dividing the full shift space $\Sigma^{\mathbf{Z}^d}$ by the equivalence relation induced by shift mappings. First we observe that the shift mappings preserve randomness.

Proposition 3.11 *Let $d \geq 1$, Σ a finite set with at least two elements, and $a \in \mathbf{Z}^d$ an integer vector. If $c \in \Sigma^{\mathbf{Z}^d}$ is random, then also $\sigma_a(c)$ is random.*

Proof. If $(U_i)_i$ is a randomness test on $\Sigma^{\mathbf{Z}^d}$, then also $((\sigma_a)^{-1}(U_i))_i$ is a randomness test on $\Sigma^{\mathbf{Z}^d}$ for arbitrary $a \in \mathbf{Z}^d$. Since $(\sigma_a)^{-1} = \sigma_{-a}$ this proves the assertion. □

Let us call two configurations $c^{(1)}, c^{(2)} \in \Sigma^{\mathbf{Z}^d}$ *equivalent* (written: $c^{(1)} \equiv_{\text{Shift}} c^{(2)}$) if one of them can be obtained by shifting the other one appropriately, i.e., if there exists an integer vector $a \in \mathbf{Z}^d$ with $c^{(2)} = \sigma_a^{(d)}(c^{(1)})$. This defines an equivalence relation on the space $\Sigma^{\mathbf{Z}^d}$, and often instead of the space $\Sigma^{\mathbf{Z}^d}$ one considers the quotient space $\Sigma^{\mathbf{Z}^d}/\equiv_{\text{Shift}}$ obtained by identifying equivalent configurations. Proposition 3.11 tells us that the randomness notion on $\Sigma^{\mathbf{Z}^d}$ induces a natural randomness notion on this quotient space. Is it also possible to obtain this randomness notion directly by applying the definition of a randomness space to the quotient space? It is interesting that this is **not** the case, at least not by using the quotient topology on the quotient space. We give the reason for the one-dimensional case. A base of the quotient topology on $\Sigma^{\mathbf{Z}}/\equiv_{\text{Shift}}$ is given by the sets

$$\{[c]_{\equiv_{\text{Shift}}} \mid c \in \Sigma^{\mathbf{Z}^d} \text{ and } c \text{ contains the word } w\},$$

for arbitrary $w \in \Sigma^*$. But any of these basic open sets contains the $\equiv_{\text{Shift}}$–equivalence classes of all rich sequences! Hence, any open set in the quotient space contains the $\equiv_{\text{Shift}}$–equivalence classes of all rich sequences. Especially, for any sequence $(U_i)_i$ of open subsets U_i of the quotient space, the $\equiv_{\text{Shift}}$–equivalence classes of all rich sequences lie in the intersection $\bigcap_{i\in\mathbf{N}} U_i$. Therefore, any randomness test on the quotient space would show that these classes are nonrandom. Hence, the direct approach via randomness test cannot give the seemingly most natural randomness notion on the quotient space $\Sigma^{\mathbf{Z}^d}/\equiv_{\text{Shift}}$.

4 Cellular Automata and Random Configurations

In this section we investigate what happens when a cellular automaton is started on a random or on a nonrandom configuration. We observe the following three facts: 1. every nonsurjective cellular automaton destroys randomness, 2. every surjective cellular automaton preserves randomness, 3. every one dimensional cellular automaton preserves nonrandomness. The above statements remain true if we replace randomness by richness, the last assertion even for an arbitrary dimension.

First we give a precise definition of cellular automata. Cellular automata are continuous functions which operate on a full shift space $\Sigma^{\mathbf{Z}^d}$ and commute with the shift mappings σ_a, for $a \in \mathbf{Z}^d$.

Definition 4.1 A *cellular automaton* (short: *CA*) is a triple (Σ, d, F) consisting of a finite set Σ containing at least two elements, called the *set of states*, a positive integer d, called the *dimension*, and a continuous function $F : \Sigma^{\mathbf{Z}^d} \to \Sigma^{\mathbf{Z}^d}$ which commutes with the shift mappings. The function F is called the *global map* of the CA.

This definition does not reflect the usual characterization via a so-called local function. Since the space $\Sigma^{\mathbf{Z}^d}$ is a compact metric space any continuous function $F : \Sigma^{\mathbf{Z}^d} \to \Sigma^{\mathbf{Z}^d}$ is uniformly continuous. Hence, if F is continuous and commutes with the shift mappings, then there exist a finite set $A \subseteq \mathbf{Z}^d$ and a function $f : \Sigma^A \to \Sigma$ such that $F(c)_b = f(c_{b+A})$, for all $c \in \Sigma^{\mathbf{Z}^d}$ and $b \in \mathbf{Z}^d$, where $c_{b+A} \in \Sigma^A$ is defined in the obvious way: $(c_{b+A})_a = c_{b+a}$ for all $a \in A$. The function f is called a *local* function for F and we say that F *is induced* by f. Obviously, one could choose A to be the d-dimensional cube $[-r, r]^d$ for some sufficiently large r. On the other hand it is clear that any function F induced by a local function f is the global map of a cellular automaton. Whenever we consider a local function for some cellular automaton we will assume that there is a natural number r such that f maps $\Sigma^{[-r,r]^d}$ to Σ. The number r will be called the *radius* of f.

Let $f : \Sigma^{[-r,r]^d} \to \Sigma$ be a local function with radius r. It induces a function f^* mapping any $v \in \Sigma^{[-k,k]^d}$ for arbitrary $k \geq 2r+1$ to an element $f^*(v) \in \Sigma^{[-k+r,k-r]^d}$ in the obvious way. This function induces a mapping f^{pattern} which maps any cube pattern (introduced in Section 2) of side length k for any $k \geq 2r+1$ to a cube pattern of side length $k-2r$ in the obvious way.

Our first observation is that *a cellular automaton preserves randomness if and only if it is surjective.* This is interesting as in the past, starting with Moore's [22] *Garden of Eden Theorem*, the characterization of surjective cellular automata and the distinction between surjective and injective (which are automatically surjective) cellular automata has received great attention, see e.g. Myhill [23], Richardson [24], Maruoka and Kimura [20, 21], and others. Thus, a new characterization of the class of surjective cellular automata is obtained in terms of randomness. Richness can be equally used for this purpose. Thus, surprisingly, in this situation randomness and richness can be used for the same purpose. In the following theorem we summarize a list of characterizations of surjective cellular automata. The equivalence of the first five of them are classical results or straightforward strengthenings of classical results. We shall give the proofs nevertheless for completeness sake.

A cellular automaton (Σ, d, F) is called *finitely injective* if and only if for all configurations $c^{(1)}, c^{(2)} \in \Sigma^{\mathbf{Z}^d}$ with $c^{(1)} \neq c^{(2)}$ and $c^{(1)}_a = c^{(2)}_a$ for almost all $a \in \mathbf{Z}^d$ we have

$F(c^{(1)}) \neq F(c^{(2)})$. We call a function $F : \Sigma^{\mathbf{Z}^d} \to \Sigma^{\mathbf{Z}^d}$ *measure preserving* if and only if $\tilde{\mu}(F^{-1}(U)) = \tilde{\mu}(U)$ for all open $U \subseteq \Sigma^{\mathbf{Z}^d}$.

Theorem 4.2 *Let (Σ, d, F) be a cellular automaton, and $f : \Sigma^{[-r,r]^d} \to \Sigma$ be a local function inducing F. The following conditions are equivalent.*

1. *F is surjective.*
2. *For every finite pattern w there exists a configuration c such that w occurs in $F(c)$.*
3. *F is finitely injective.*
4. *For every $n \geq 2r+1$ and every cube pattern w of side length n we have*
$$|(f^{\text{pattern}})^{-1}\{w\}| = |\Sigma|^{(n+2r)^d - n^d}. \tag{1}$$
5. *F is measure preserving.*
6. *For all configurations c, if c is rich, then also $F(c)$ is a rich configuration.*
7. *For all configurations c, if c is random, then also $F(c)$ is a random configuration.*

Proof. "1. $\Rightarrow$ 2.": trivial.

"2. $\Rightarrow$ 1.": Let $c \in \Sigma^{\mathbf{Z}^d}$ be an arbitrary configuration. By 2., for each n there exists a configuration $c^{(n)}$ such that $F(c^{(n)})|_{[-n,n]^d} = c|_{[-n,n]^d}$. The sequence $(c^{(n)})_n$ has an accumulation point $\bar{c}$ in the compact space $\Sigma^{\mathbf{Z}^d}$. By continuity of F we conclude that $F(\bar{c}) = c$.

"4. $\Rightarrow$ 2.": It is sufficient to deduce from 4. that for every cube pattern w there exists a configuration c such that w occurs in $F(c)$. For a cube pattern w this is the case if and only if $|(f^{\text{pattern}})^{-1}\{w|\}| \geq 1$. Therefore, 2. follows immediately from 4.

"2. $\Rightarrow$ 3.": This implication is a straightforward strengthening of Moore's [22] *Garden of Eden Theorem*. We follow Moore's proof. We assume that 3. is not true and derive that then also 2. is not true. Let $c^{(1)}, c^{(2)} \in \Sigma^{\mathbf{Z}^d}$ be two different configurations with $c^{(1)}_a = c^{(2)}_a$ for almost all $a \in \mathbf{Z}^d$, and with $F(c^{(1)}) = F(c^{(2)})$. Let $l = \max\{|a| \mid a \in \mathbf{Z}^d \ \&\ c^{(1)}_a \neq c^{(2)}_a\}$ and $k = 4r + 2l + 1$, where $|a| = \max\{|a_1, \ldots, |a_d|\}$ for $a = (a_1, \ldots, a_d) \in \mathbf{Z}^d$.

We introduce an equivalence relation between cube patterns of side length k by calling two cube patterns v and w of side length k *interchangeable* if they are equal or if each of them is equal to the pattern represented by $c^{(1)}_{[-2r-l,2r+l]^d}$ or to the pattern represented by $c^{(2)}_{[-2r-l,2r+l]^d}$. Obviously, if v and w are interchangeable, then $f^{\text{pattern}}(v)$ and $f^{\text{pattern}}(w)$ are equivalent. For a moment let us fix a positive integer i. We can extend this relation to cube patterns of side length ik in the following way. Each cube pattern of side length ik can be viewed as consisting out of i^d nonoverlapping cube patterns of side length k. Two cube patterns v and w of side length ik are called *interchangeable* if and only if each of these i^d cube sub–patterns of v of side length k is interchangeable with the cube sub–pattern of w of side length k at the corresponding position. Since the outer $2r$ layers of any two interchangeable cube patterns of side length k are identical (this is especially true for the the two cube patterns represented by $c^{(1)}_{[-2r-l,2r+l]^d}$ and by $c^{(2)}_{[-2r-l,2r+l]^d}$), we conclude that

$f^{\text{pattern}}(v) = f^{\text{pattern}}(w)$ for any two interchangeable cube patterns of side length ik. With respect to the equivalence relation called "interchangeable" the set of all cube patterns of side length ik splits into exactly $(|\Sigma|^{k^d}-1)^{i^d}$ equivalence classes. Hence, the set f^{pattern}(cube patterns of side length ik) contains at most $(|\Sigma|^{k^d}-1)^{i^d}$ cube patterns. They have side length $ik-2r$, of course. But there are altogether $|\Sigma|^{(ik-2r)^d}$ cube patterns of side length $ik-2r$. We claim that for sufficiently large i

$$(|\Sigma|^{k^d}-1)^{i^d} < |\Sigma|^{(ik-2r)^d} \tag{2}$$

Before we prove this claim, we finish the argument. According to the claim, for sufficiently large i there exists a cube pattern of side length $ik-2r$ which is not in the set f^{pattern}(cube patterns of side length ik). This cube pattern cannot occur in $F(c)$, for any configuration c.

In order to prove the claim we choose i so large that

$$k^d - (k-\frac{2r}{i})^d < \log_{|\Sigma|} \frac{|\Sigma|^{k^d}}{(|\Sigma|^{k^d}-1)}.$$

Raising $|\Sigma|$ to these powers and rearranging gives

$$(|\Sigma|^{k^d}-1) < |\Sigma|^{-k^d+(k-\frac{2r}{i})^d} \cdot |\Sigma|^{k^d} = |\Sigma|^{(k-\frac{2r}{i})^d},$$

and raising both sides to the power i^d finally gives (2).

"3. $\Rightarrow$ 4.": This implication is a straightforward strengthening of a result by Maruoka and Kimura [20]. We follow their proof. We assume that 4. is not true and derive that then also 3. is not true. If there exists a cube pattern w of side length n such that equation (1) is not true then there must be a pattern v of side length n such that

$$|(f^{\text{pattern}})^{-1}\{v\}| > |\Sigma|^{(n+2r)^d-n^d}. \tag{3}$$

We set $M = |(f^{\text{pattern}})^{-1}\{v\}|$ and $k = n+2r$. Let us fix a state $s \in \Sigma$ and let $\overline{r} = (r, r, \ldots, r) \in \mathbf{Z}^d$ be the integer vector with constant value r. For a moment we fix a positive integer i. We consider the set $\mathcal{S}$ of all configurations $c \in \Sigma^{\mathbf{Z}^d}$ such that each of the i^d cube patterns represented by $c_{\overline{r}+ka+\{1,\ldots,k\}^d}$ for some $a \in \{0,\ldots,i-1\}^d$ is one of the patterns in $(f^{\text{pattern}})^{-1}\{v\}$, and such that $c_a = s$ for all $a \in \mathbf{Z}^d \setminus \{r+1,\ldots,r+ik\}^d$. There are exactly M^{i^d} such configurations, i.e., $|\mathcal{S}| = M^{i^d}$. The images $F(c^{(1)})$ and $F(c^{(2)})$ of any two configurations $c^{(1)} \in \mathcal{S}$ and $c^{(2)} \in \mathcal{S}$ are identical outside the cube $\{1,\ldots,2r+ik\}^d$, i.e., $F(c^{(1)})_a = F(c^{(2)})_a$ for all $a \in \mathbf{Z}^d \setminus \{1,\ldots,2r+ik\}^d$. Furthermore the i^d cube subpatterns $F(c^{(1)})_{2\overline{r}+ka+\{1,\ldots n\}^d}$ for $a \in \{0,\ldots,i-1\}^d$ are all equal to v. Hence, the set $F(\mathcal{S})$ contains at most $|\Sigma|^{(2r+ik)^d-i^dn^d}$ configurations. We claim that for sufficiently large i

$$M^{i^d} > |\Sigma|^{(2r+ik)^d-i^dn^d}. \tag{4}$$

Before we prove this claim, we finish the argument. According to the claim, for sufficiently large i there exist two different configurations $c^{(1)}$ and $c^{(2)}$ with $c^{(1)}_a = s = c^{(2)}_a$ for all $a \in \mathbf{Z} \setminus \{1,\ldots,2r+ik\}^d$ and with $F(c^{(1)}) = F^(c^{(2)})$. This shows that F is not finitely injective.

In order to prove the claim we choose i so large that

$$(k + \frac{2r}{i})^d - k^d < \log_{|\Sigma|} \frac{M}{|\Sigma|^{k^d - n^d}}$$

(remember $M > |\Sigma|^{k^d - n^d}$). Raising $|\Sigma|$ to these powers and rearranging gives

$$|\Sigma|^{k^d - n^d} \cdot |\Sigma|^{(k+\frac{2r}{i})^d - k^d} = |\Sigma|^{(k+\frac{2r}{i})^d - n^d} < M\,,$$

and raising both sides to the power i^d finally gives (4).

"4. $\iff$ 5.": For a vector $a \in \mathbf{Z}^d$, a positive number n, and a cube pattern w of side length n, the set

$$C_{a,w} = \{c \in \Sigma^{\mathbf{Z}^d} \mid c_{a+\{1,\ldots,n\}^d} \text{ is a representative for } w\}$$

has measure $1/|\Sigma|^{n^d}$, and its pre-image

$$F^{-1}(C_{a,w}) = \{c \in \Sigma^{\mathbf{Z}^d} \mid f^*(c_{-\overline{r}+a+\{1,\ldots,n+r\}^d}) \text{ is a representative for } w\}$$

has measure $|(f^{\text{pattern}})^{-1}(v)|/|\Sigma|^{(n+2r)^d}$. Therefore, if F is measure preserving, also 4. is true. On the other hand, if 4. is true then each set $C_{a,w}$ has the same measure as its pre-image $F^{-1}(C_{a,w})$. Since every open set can be written as the disjoint union of sets $C_{a,w}$ we conclude that 4. implies 5.

"2. $\iff$ 6.": trivial.

"7. $\Rightarrow$ 2.": by Lemma 3.8.

"5. $\Rightarrow$ 7.": Assume that c is a configuration such that $F(c)$ is nonrandom. Then there is a randomness test $(U_i)_i$ such that $F(c) \in \bigcap_{i\in\mathbf{N}} U_i$. The sequence of open sets $(F^{-1}(U_i))_i$ is also a randomness test: we have $\tilde{\mu}(F^{-1}(U_i)) = \tilde{\mu}(U_i) \leq 2^{-i}$ by condition 5.; and the facts that F is induced by a local function f and that the sequence $(U_i)_i$ of open sets is $\tilde{B}'$–computable, imply that also the sequence $(F^{-1}(U_i))_i$ of open sets is $\tilde{B}'$–computable. We have $c \in \bigcap_{i\in\mathbf{N}} F^{-1}(U_i)$. Hence, also c is nonrandom. □

From Condition 2. in Theorem 4.2 we conclude that if F is not surjective, then there does not exist a configuration c such that $F(c)$ is rich or random. Hence, a nonsurjective cellular automaton "destroys" both richness and randomness.

Secondly we ask what happens when one applies a cellular automaton to a nonrandom configuration or to a nonrich configuration. Note that there are very simple effective functions on the space of one-way infinite sequences which transform some nonrandom sequences into random ones.

Example 4.3 The function $F : \Sigma^{\mathbf{Z}} \to \Sigma^{\mathbf{Z}}$ with

$$F(\ldots c_{-4}c_{-3}c_{-2}c_{-1}c_0c_1c_2c_3c_4\ldots) = \ldots c_{-4}c_{-2}c_0c_2c_4\ldots$$

is computable and measure preserving. If all odd entries c_{2i+1} are equal to one fixed element $s \in \Sigma$, then the sequence $\ldots c_{-4}c_{-3}c_{-2}c_{-1}c_0c_1c_2c_3c_4\ldots$ is certainly nonrandom. But its image under F, the sequence $\ldots c_{-4}c_{-2}c_0c_2c_4\ldots$ can still be random.

It is not clear a priori whether the same phenomenon can occur when one considers cellular automata. We could prove that one dimensional cellular preserve nonrandomness, i.e., they transform nonrandom two-way infinite sequences into nonrandom two-way infinite sequences. But at present it is not clear whether the same holds true also for higher dimensional cellular automata. That arbitrary cellular automata preserve nonrichness can be proved by using the idea behind the proof of Moore's [22] *Garden of Eden Theorem*, which we have implicitly formulated in the previous Theorem 4.2.

Theorem 4.4 *Let (Σ, d, F) be a cellular automaton.*

1. *If a configuration $c \in \Sigma^{\mathbf{Z}^d}$ is not rich, then also $F(c)$ is not rich.*

2. *If $d = 1$ and a configuration $c \in \Sigma^{\mathbf{Z}^d}$ is nonrandom, then also $F(c)$ is nonrandom.*

Proof. Let $f : \Sigma^{[-r,r]^d} \to \Sigma$ be a local function inducing F.

1. The first assertion is proved by using the idea behind the proof of Moore's [22] Garden of Eden Theorem. Let us fix a nonrich configuration c and a cube pattern of side length, say, k which does not occur in c. Hence, at most $|\Sigma|^{k^d} - 1$ cube patterns of side length k can occur in c. Let us consider cube patterns of side length ik, for an arbitrary positive integer i. Since cube pattern of side length ik can be viewed as consisting out of i^d nonoverlapping cube patterns of side length k, we conclude that at most $(|\Sigma|^{k^d} - 1)^{i^d}$ different cube patterns of side length ik can occur in c. Let $\mathcal{P}_{ik}$ denote the set of all cube patterns of side length ik which occur in c. We have just proved $|\mathcal{P}_{ik}| \leq (|\Sigma|^{k^d} - 1)^{i^d}$. Hence, also the set $f^{\text{pattern}}(\mathcal{P}_{ik})$ contains at most $(|\Sigma|^{k^d} - 1)^{i^d}$ different cube patterns. These cube patterns have side length $ik - 2r$, of course. But there are altogether $|\Sigma|^{(ik-2r)^d}$ cube patterns of side length $ik - 2r$. By exactly the same counting argument as in the proof of the implication "2. $\Rightarrow$ 3." of Theorem 4.2 we conclude that for sufficiently large i there exists a cube pattern of side length $ik - 2r$ which is not in the set $f^{\text{pattern}}(\mathcal{P}_{ik})$. This cube pattern cannot occur in $F(c)$. Hence, $F(c)$ is not rich.

2. For the second assertion we assume that the dimension d of the cellular automaton is 1. We fix a nonrandom configuration c and a randomness test $(U_i)_i$ on $\Sigma^{\mathbf{Z}^d}$ such that $c \in \bigcap_{i \in \mathbf{N}} U_i$. We show that there is a randomness test $(V_i)_i$ on $\Sigma^{\mathbf{Z}^d}$ such that $F(c) \in \bigcap_{i \in \mathbf{N}} V_i$. By Lemma 3.6 and by a compactness argument one deduces from the fact that the sequence $(U_i)_i$ of open sets is $\tilde{B}'$–computable, that the set

$$\{\pi(i, j) \in \mathbf{N} \mid [\text{Cube}(j)] \subseteq U_i\} \tag{5}$$

is computably enumerable. We set $l = \lceil \log_2(|\Sigma|^{2r}) \rceil$, and define

$$V_i = \bigcup \{[f^*(v)] \mid v \in \text{Cubes}(\Sigma, 1) \ \ \& \ \ \text{side length}(v) \geq 2r + 1 \ \ \& \ \ [v] \subseteq U_{l+i}\}.$$

We claim that the sequence $(V_i)_i$ is a randomness test with $F(c) \in \bigcap_{i \in \mathbf{N}} V_i$. It is clear that it is a sequence of open sets and that it is $\tilde{B}'$–computable (use the fact that the set in equation 5 is computably enumerable and Lemma 3.6). For arbitrary i we have $c \in U_{l+i}$. Hence, there is an element $v \in \text{Cubes}(\Sigma, 1)$ of side length $\geq 2r+1$ with $c \in [v]$ and $[v] \subseteq U_{l+i}$. This shows $F(c) \in V_i$. Finally we have to show that $\tilde{\mu}(V_i) \leq 2^{-i}$, for all i. We fix an i. There exists a set

$$W \subseteq \{v \in \text{Cubes}(\Sigma, d) \mid \ \text{side length}(v) \geq 2r + 1 \ \ \& \ \ [v] \subseteq U_{l+i}\}$$

such that $\bigcup_{v\in W}[v] = U_{l+i}$ and for any two $v, w \in W$, the sets $[v]$ and $[w]$ are disjoint. If $v, w \in \mathrm{Cubes}(\Sigma, d)$ and $[v] \subseteq [w]$, then also $[f^*(v)] \subseteq [f^*(w)]$. Hence, $V_i = \bigcup_{v\in W}[f^*(v)]$. Since for arbitrary $v \in \mathrm{Cubes}(\Sigma, 1)$ with $\mathrm{sidelength}(v) \geq 2r+1$ we have $\tilde{\mu}([f^*(v)]) = |\Sigma|^{2r} \cdot \tilde{\mu}([v])$, we obtain

$$\begin{aligned}
\tilde{\mu}(V_i) &= \tilde{\mu}\left(\bigcup_{v\in W}[f^*(v)]\right) \\
&\leq \sum_{v\in W}\tilde{\mu}([f^*(v)]) \\
&= \sum_{v\in W}|\Sigma|^{2r}\cdot\tilde{\mu}([v]) \\
&= |\Sigma|^{2r}\cdot\tilde{\mu}(U_{l+i}) \\
&\leq |\Sigma|^{2r}\cdot 2^{-l-i} \\
&\leq 2^{-i}\,.
\end{aligned}$$

This ends the proof for the assertion that $(V_i)_i$ is a randomness test with $F(c) \in \bigcap_{i\in\mathbf{N}} V_i$. Hence, $F(c)$ is nonrandom. □

5 Conclusion

We have given various characterizations, based on randomness tests, for algorithmically random configurations in full shift spaces. We have also compared this randomness notion with the richness notion for configurations. Furthermore we have shown that a) surjective cellular automata preserve richness and randomness, b) nonsurjective cellular automata destroy both properties, c) all cellular automata preserve nonrichness, and d) one dimensional cellular automata also preserve nonrandomness. *It is open whether arbitrary cellular automata of higher dimension preserve nonrandomness.*

There are at least two areas of further questions in this context. In this paper we have defined and analyzed only randomness and nonrandomness of configurations as opposing notions, and we have used randomness tests in order to define these notions. They can also be defined via program–size complexity of finite patterns, see Chaitin [8]. It might be interesting to analyze the behavior of cellular automata with respect to complexity of finite patterns in this sense. The other area concerns ergodic theory and algorithmic information theory. The randomness notion of algorithmic information theory depends on the considered measure. In this paper we have considered only the product measure induced by the uniform measure on the finite set of states. We have seen that surjective cellular automata are measure preserving with respect to this measure, hence they are dynamical systems in the sense of ergodic theory and can be analyzed by the means of this theory. For nonsurjective automata one has to consider other measures in order to apply results from ergodic theory. For an application of ergodic theory to cellular automata see Lind [18]. It might be interesting to try to combine algorithmic information theory and ergodic theory in the study of cellular automata and also in the study of other dynamical systems; see, for example, White [29], Batterman and White [1].

References

[1] R. W. Batterman, H. S. White. Chaos and algorithmic complexity. *Found. Phys.* 26:307–336, 1996.

[2] R. Book, J. Lutz, and M. Martin. The global power of additional queries to random oracles. In *Proc. of STACS 94*, pages 403–414, Berlin, 1994. Springer-Verlag.

[3] A. W. Burks. *Essays on Cellular Automata.* University of Illinois Press, Urbana, 1970.

[4] C. S. Calude. *Information and Randomness, an Algorithmic Perspective.* Springer-Verlag, Berlin, 1994.

[5] C. S. Calude and H. Jürgensen. Randomness as an invariant for number representations. In H. Maurer, J. Karhumäki, and G. Rozenberg, editors, *Results and Trends in Theoretical Computer Science*, pages 44–66. Springer-Verlag, Berlin, 1994.

[6] G. J. Chaitin. On the length of programs for computing finite binary sequences. *J. of the ACM*, 13:547–569, 1966.

[7] G. J. Chaitin. A theory of program size formally identical to information theory. *J. of the ACM*, 22:329–340, 1975.

[8] G. J. Chaitin. Towards a mathematical definition of "life". In R. D. Levine and M. Tribus, editors, *The Maximum Entropy Formalism*, pages 477–498. MIT Press, 1979.

[9] G. J. Chaitin. *The Unknowable*, Springer-Verlag, Singapore, 1999.

[10] K. Compton. On rich words. In L. J. Cummings, editor, *Combinatorics on Words*, pages 39–61. Academic Press, Toronto, 1983.

[11] K. Culik II, L. P. Hurd, and S. Yu. Computation theoretic aspects of cellular automata. *Physica D*, 45:357–378, 1990.

[12] P. Hertling. Disjunctive omega-words und real numbers. *Journal of Universal Computer Science*, 2(7):549–568, 1996.

[13] P. Hertling and K. Weihrauch. Randomness spaces. In K. G. Larsen, S. Skyum, and G. Winskel, editors, *Automata, Languages and Programming*, volume 1443 of *LNCS*, pages 796–807, Berlin, 1998. Springer. 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 1998.

[14] P. Hertling and K. Weihrauch. Randomness spaces. Technical Report 079, CDMTCS, Auckland, January 1998.

[15] H. Jürgensen and G. Thierrin. Some structural properties of ω-languages. *13th Nat. School with Internat. Participation "Applications of Mathematics in Technology"*, Sofia, pages 56–63, 1988.

[16] M. Li, P. M. Vitányi. *Kolmogorov Complexity and Its Applications.* Springer-Verlag, Berlin, 1997.

[17] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, Cambridge, 1995.

[18] D. A. Lind. Applications of ergodic theory and sofic systems to cellular automata. *Physica D*, 10:36–44, 1984.

[19] P. Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, 1966.

[20] A. Maruoka and M. Kimura. Conditions for injectivity of global maps for tessellation automata. *Information and Control*, 32:158–162, 1976.

[21] A. Maruoka and M. Kimura. Injectivity and surjectivity of parallel maps for cellular automata. *Journal of Computer and System Sciences*, 18:47–64, 1979.

[22] E. F. Moore. Machine models of self reproduction. *American Mathematical Society, Proceedings of Symposia in Applied Mathematics*, 14:17–33, 1962. Reprinted in [3], 187–203.

[23] J. Myhill. The converse to Moore's Garden-of-Eden theorem. *Proc. of the AMS*, pages 685–686, 1963. Revised version in [3], 204–205.

[24] D. Richardson. Tesselations with local transformations. *Journal of Computer and System Sciences*, 6:373–388, 1972.

[25] W. M. Schmidt. On normal numbers. *Pacific J. Math.*, 10:661–672, 1960.

[26] L. Staiger. The Kolmogorov complexity of Liouville numbers, *CDMTCS Research Report* 096, 1999.

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

[28] J. von Neumann. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, Illinois, 1966. Edited and completed by A. Burks.

[29] H. S. White. Algorithmic complexity of points in dynamical systems. *Ergodic Theory Dynam. Systems*, 13:807–830, 1993.

[30] S. Wolfram. Universality and complexity in cellular automata. *Physica D*, 10:1–35, 1984.

[31] S. Wolfram. Origins of randomness in physical systems. *Physical Review Letters*, 55:298–301, 1985.