Journal of Statistical Physics, Vol. 90, Nos. 1/2, 1998

On Cesàro Limit Distribution of a Class of Permutative Cellular Automata

Alejandro Maass[1] and Servet Martínez[1]

Received January 14, 1997; final July 8, 1997

We study Cesàro means (time averages) of the evolution measures of the class of permutative cellular automata over $\{0,1\}^{\mathbb{N}}$ defined by $(\varphi_B x)_n = x_{n+R} + \prod_{j=0}^{R-1} (1+b_j+x_{n+j})$, where $B=b_0 \cdots b_{R-1}$ is an aperiodic block in $\{0,1\}^R$ and operations are taken mod 2. If the initial measure is Bernoulli, we prove that the limit of the Cesàro mean of the first column distribution exists. When $R=1$ and $B=1$, φ_B is the mod 2 sum automaton. For this automaton we show that the limit is the (1/2, 1/2)-Bernoulli measure, and if the initial measure is Markov, we show that the limit of Cesàro mean of the one-site distribution is equidistributed.

KEY WORDS: Permutative cellular automata; mod 2 automaton; Cesàro means, Bernoulli measures.

1. INTRODUCTION AND MAIN RESULTS

Let A be a finite alphabet, denote by $X_A = A^{\mathbb{N}}$ the compact product space. For $x \in X_A$ and integers $0 \leqslant n \leqslant m \leqslant \infty$ we denote by $x(n,m)$ the block of x between coordinates n and m; if $n=m$ we also use x_n or $x(n)$. A cellular automaton $\varphi: X_A \to X_A$ is defined by a local rule $\tilde{\varphi}: A^{R+1} \to A$ by means of $(\varphi x)_n = \tilde{\varphi}(x_n, \ldots, x_{n+R})$, and R is called the radius of the automaton. In the sequel we identify $\tilde{\varphi}$ with φ. By $\sigma: X_A \to X_A$ we mean the shift transformation, $(\sigma x)_n = x_{n+1}$. We remind that a transformation $\varphi: X_A \to X_A$ is a cellular automaton if it is continuous and shift-commuting, $\varphi \circ \sigma = \sigma \circ \varphi$.

Let $\mathbb{P}$ be a σ-invariant probability measure on X_A and $\varphi: X_A \to X_A$ a cellular automaton. We denote by $\mathbb{P} \circ \varphi^{-n}$ the induced measure by φ^n on X_A, i.e., $\mathbb{P} \circ \varphi^{-n}(C) = \mathbb{P}(\varphi^{-n} C)$ for $C \subseteq X_A$ a measurable set. The limit

[1] Departamento de Ingeniería Matemática, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Santiago, Chile; e-mail: amaass@dim.uchile.cl, smartine@dim.uchile.cl.

0022-4715/98/0100-0435$15.00/0

of the Cesàro mean law, when it exists, is given by $\mathbb{Q}_\varphi = \lim_{N\to\infty}(1/N+1)\sum_{n\leqslant N}\mathbb{P}\circ\varphi^{-n}$. The limit Cesàro mean of the one-site distribution is $\mathbb{Q}_\varphi[i]_k$ for $i\in A$, where $[i]_k=\{x\in A^{\mathbb{N}}: x_k=i\}$ (since $\mathbb{P}$ is σ-invariant $\mathbb{Q}_\varphi[i]_k$ does not depend on k).

Here we shall study a subclass of right permutative cellular automata. This family of automata has been widely studied in different contexts since the work of Hedlund (1969), and it is a natural class of positively expansive cellular automata. They are defined in the following way. Fix $R\in\mathbb{N}\backslash\{0\}$ to be the radius of the automaton, and for each $w\in A^R$ choose a permutation $\mathcal{G}_w: A\to A$. The permutative cellular automaton $\varphi_{\mathcal{G}}: X_A\to X_A$ associated to $\mathcal{G}=(\mathcal{G}_w: w\in A^R)$ is given by $(\varphi_{\mathcal{G}}x)_n=\mathcal{G}_{x_n\cdots x_{n+R-1}}(x_{n+R})$. Permutative cellular automata are onto and the uniform Bernoulli measure on X_A is $\varphi_{\mathcal{G}}$ invariant. Furthermore, this last property characterize onto cellular automata (see ref. [H]).

To introduce the objects of this work let us fix some notation. The alphabet of our automata is $\mathbb{Z}_2=\{0,1\}$ and we put $X_2=X_{\mathbb{Z}_2}$. By $[i]$ we mean the mod 2 class of $i\in\mathbb{Z}_2$, so $[a+b]$ is the mod 2 sum in $\mathbb{Z}$. We extend the mod 2 sum to X_2, the configuration $[x+y]$ is given by $[x+y]_k=[x_k+y_k]$. In the sequel and if it is clear from the context we will write $a+b$ instead of $[a+b]$ for $a,b\in\mathbb{Z}_2$. For $a\in\mathbb{Z}_2$ we also put $\bar{a}=a+1\in\mathbb{Z}_2$.

Let $R\in\mathbb{N}\backslash\{0\}$ and $B=b_0\cdots b_{R-1}\in\mathbb{Z}_2^R$ be an aperiodic block, that is, $\forall i\in\{0,\dots,R-1\}$, $b_i\cdots b_{R-1}\neq b_0\cdots b_{R-1-i}$. We define the cellular automaton φ_B by

$$(\varphi_B x)_n = x_{n+R} + \prod_{j=0}^{R-1}(x_{n+j}+b_j+1)$$

where operations are taken mod 2. This rule shifts the value of x_{n+R} to position n if $x(n, n+R-1)\neq B$ and shifts $\bar{x}_{n+R}=1+x_{n+R}$ otherwise. This automaton is clearly a permutative one. If $R=1$ and $B=1$, $(\varphi_B x)_n = x_n+x_{n+1}$ and it is called the mod 2 sum automaton. We denote it by φ_2. We can also write $\varphi_2 = id+\sigma$, where *id* is the identity transformation on X_2.

Permutative cellular automata are positively expansive. That is, a point $x\in X_A$ is uniquely determined from $x_\varphi=(\varphi^n x(0,R-1))_{n\in\mathbb{N}}$ (see ref. [BM]). Therefore, the study of the limit Cesàro mean law $\mathbb{Q}_\varphi$ is equivalent to the study of the limit of Cesàro means of type

$$\frac{1}{N+1}\sum_{n\leqslant N}\mathbb{P}\{x\in X_A: (\varphi^{n+j}x)(0,s)=a_j, 0\leqslant j\leqslant \ell-1\}$$

for $\ell\in\mathbb{N}\backslash\{0\}$, $s\in\{0,\dots,R-1\}$ and $a_0,\dots,a_{\ell-1}\in\{0,1\}^{s+1}$.

In this work we shall only deal with Markov invariant measures and with Bernoulli measures on X_2. The notation will be the following one. By $\pi=(\pi_0, \pi_1)$ we mean a non trivial probability vector i.e., $\pi_1 = 1-\pi_0$, $0<\pi_0<1$. The Bernoulli measure on X_2 is denoted by $\mathbb{P}_\pi = \pi^{\mathbb{N}}$. By $P=(p_{ij}: i, j \in \mathbb{Z}_2)$ we denote a transition matrix. The invariant probability vector of P is $\pi^P = (\pi_0^P, \pi_1^P)$ with $\pi_i^P = (p_{1-i,i}/p_{01}+p_{10})$. On X_2 we denote by $\mathbb{P}_P$ the Markov shift invariant measure given by

$$\mathbb{P}_P\{x_0 = i_0,..., x_n = i_n\} = \pi_{i_0}^P p_{i_0 i_1} \cdots p_{i_{n-1} i_n} \qquad \text{for} \quad n \geqslant 0, i_0,..., i_n \in \{0, 1\}$$

A Bernoulli measure is a Markov one by taking $p_{ij} = \pi_j$ for $j \in \mathbb{Z}_2$ and reciprocally a Markov measure $\mathbb{P}_P$ such that $p_{01}+p_{10}=1$, is the Bernoulli measure $\mathbb{P}_{\pi^P}$.

Our main results are the following.

Theorem 1. Let B be an aperiodic block in $\mathbb{Z}_2^R$. For $\mathbb{P}_\pi$ a Bernoulli measure on X_2 we have that the following limit exists

$$\lim_{N\to\infty} \frac{1}{N+1} \sum_{n \leqslant N} \mathbb{P}_\pi\{x \in X_2: (\varphi_B^{n+j} x)(0) = a_j, 0 \leqslant j \leqslant \ell - 1\}$$

for any $\ell \in \mathbb{N}\backslash\{0\}$ and $a_0,..., a_{\ell-1} \in \mathbb{Z}_2$. ∎

In the case that B is a single letter the limit in Theorem 1 can be computed explicitly.

Theorem 2. Let $B=0$ or $B=1$.

(i) For $\mathbb{P}_\pi$ a Bernoulli measure on X_2 the limit of the Cesàro mean law, $\mathbb{Q}_{\varphi B}$, exists and it is the equidistributed Bernoulli measure: $\mathbb{Q}_{\varphi B} = (\frac{1}{2}, \frac{1}{2})^{\mathbb{N}}$.

(ii) For $\mathbb{P}_P$ a Markov invariant measure on X_2 the Cesàro mean of the one-site distribution exists and it is $\mathbb{Q}_{\varphi B}[i]_k = \frac{1}{2}$ for $i \in \mathbb{Z}_2$. ∎

The mod 2 sum automaton has been already studied in different contexts oftenly with respect to the uniform Bernoulli measure $\mathbb{P}_\pi = (\frac{1}{2}, \frac{1}{2})^{\mathbb{N}}$ in which case the statement of the theorem is trivial. In this uniform case, all its ergodic properties are known, for instance see Shereshevsky (1992). Also Wolfram (1986) studied this automaton as a random sequence generator. Lind (1984) studied the automaton $(\varphi x)_k = x_{k-1} + x_{k+1}$ defined in $\mathbb{Z}_2^{\mathbb{Z}}$. He states the analogous of Theorem 2 (i) by considering the automaton as an endomorphism of a compact group. In this context see also Courbage (1989). Our proof is based upon the combinatorial properties of the rule which gives insight on the computations for proving Theorem 1.

Let us remark that Theorem 2 is a tool for improving random generators. In fact, if the generator is biased because the sequence is Bernoulli, but not uniform, part (i) of the Theorem provides a way to suppress the bias because the mod 2 Cesàro evolution approaches uniform random sequences. If the bias is Markovian part (ii) of the Theorem asserts that the Cesàro mean evolution randomized the one-site distribution.

We notice that general permutative cellular automata appears in several ways in the literature. In dynamics they are basic examples of positively expansive cellular automata. Their high degree of sensitivity motivated their use as one-dimensional models for turbulence and non dissipative hydrodynamics. In particular, they present periodic traveling patterns, see Urías *et al.* (1996).

We point out that in general $\mathbb{P} \circ \varphi_B^{-n}$ does not converge. For instance, if $R=1$ and $B=1$ the equalities $(\varphi_2^{2n} x)_0 = x_0 + x_{2^n}$ and $(\varphi_2^{2^n-1} x)_0 = \sum_{i=0}^{2^n-1} x_i$ (see (1) below imply that, if the initial measure is Bernoulli but not equidistributed, then $\lim_{n \to \infty} \mathbb{P} \circ \varphi_B^{-n}$ cannot exist.

2. PROOF OF THEOREM 2

In the sequel we shall need an explicit formula for the iterates of φ_2. It can be directly shown by induction that $\varphi_2^n = \sum_{p \leq n} [\binom{n}{p}]\, \sigma^p$. The binomial coefficient mod 2 can be completely determined. To describe it denote by $\mathscr{P}_f(\mathbb{N}) = \{I \subseteq \mathbb{N} : |I| < \infty\}$ the class of finite subsets of $\mathbb{N}$ and by $\mathscr{N}: \mathscr{P}_f(\mathbb{N}) \to \mathbb{N}, I \to \mathscr{N}(I)$, the function given by $\mathscr{N}(I) = \sum_{p \in I} 2^p$. This mapping is onto and one-to-one and its inverse is denoted by $\mathscr{I}: \mathbb{N} \to \mathscr{P}_f(\mathbb{N}), n \to \mathscr{I}(n)$, so $n = \sum_{p \in \mathscr{I}(n)} 2^p$. Observe that $\mathscr{N}(\phi) = 0$, $\mathscr{I}(0) = \phi$. Disjoint unions of sets in $\mathscr{P}_f(\mathbb{N})$ are transformed by $\mathscr{N}$ into sums in $\mathbb{N}$. An old result of Lucas (1877) states that $[\binom{n}{p}] = 1$ if and only if $\mathscr{I}(p) \subseteq \mathscr{I}(n)$ (see ref. [K]), hence

$$\varphi_2^n = \sum_{I \subseteq \mathscr{I}(n)} \sigma^{\mathscr{N}(I)}, \qquad \text{for} \quad n \in \mathbb{N} \tag{1}$$

Remark. Observe that φ_2^n is 2^n-to-1, $|\varphi_2^{-n}\{x\}| = 2^n\ \forall x \in X_2$. Even so, if $\mathbb{P}_P$ is a Markov measure with $\pi^P \neq (\frac{1}{2}, \frac{1}{2})$ (i.e., $p_{01} \neq p_{10}$) then $\varphi_2^n: X_2 \to X_2$ is $\mathbb{P}_P$ a.e. 1-to-1 for every $n \in \mathbb{N}$. Let us show it.

From (1) we have $(\varphi_2^{2^n} x)_k = x_k + x_{k+2^n}$. Fix $y \in X_2$. For every $z \in \{0,1\}^{2^n}$ the equalities $\varphi_2^{2^n} x = y$ and $x_k = z_k$ for $k < 2^n$ determines a unique $x = x(z)$ because the recurrence relation $x_{k+(\ell+1)2^n} = y_{k+(\ell+1)2^n} + x_{k+\ell 2^n}$. Denote $x^{(k)}(z) = ((x^{(k)}(z))_\ell = x_{k+\ell 2^n} : \ell \in \mathbb{N})$. Let z, z' be such that

$z'_k = 1 - z_k$ then it follows by recurrence that $x_{k+\ell 2^n}(z) = 1 - x_{k+\ell 2^n}(z')$ $\forall \ell \in \mathbb{N}$. Now define

$$\tilde{X}_2 = \left\{ x \in X_2 : \forall n \geqslant 1, \forall k < n, \lim_{L \to \infty} \frac{1}{L+1} |\{\ell \leqslant L : x_{k+\ell 2^n} = 1\}| = \pi_1^P \right\}$$

The ergodic theorem applied to the Markov measure $\mathbb{P}_{P^{2^n}}$ (whose invariant vector is also π^P) implies $\mathbb{P}(\tilde{X}_2) = 1$. Since $\pi^P \neq (\frac{1}{2}, \frac{1}{2})$ at most one of the two points $x^{(k)}(z)$, $x^{(k)}(z')$ verifies the relation defined in $\tilde{X}_2$. This can be made $\forall k < n$ then there is at most one point $x \in \tilde{X}_2$ such that $\varphi_2^{2^n} x = y$, for every $y \in X_2$. Hence $\varphi_2^{2^n}$ is 1-to-1 $\mathbb{P}_P$-a.e. $\forall n$. If $m < 2^n$, the equality $\varphi_2^{2^n} = \varphi_2^{2^n - m} \circ \varphi_2^m$ implies φ_2^m is 1-to-1 on $\tilde{X}_2$. So $\varphi_2^n : \tilde{X}_2 \to X_2$ is 1-to-1 $\forall n \in \mathbb{N}$. ∎

For proving Theorem 2 (ii) it will be useful the following result.

Lemma 3. Let $(x_n : n \in \mathbb{N})$ be distributed according to the Markov invariant measure $\mathbb{P}_P$ with $P \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then there exist $c < \infty$, $\Gamma \in [0, 1)$ such that for any increasing sequence $(r_k : k \in \mathbb{N})$ the sequence of random variables $S_{(n)} = \sum_{k \leqslant n} x_{r_k}$ verifies

$$|\mathbb{P}\{S_{(n)} = i\} - \tfrac{1}{2}| \leqslant c\Gamma^n \qquad \text{for} \quad n \in \mathbb{N}, i \in \mathbb{Z}_2$$

Proof. Define $\gamma_P = 1 - (p_{10} + p_{01}) \in (-1, 1)$. The matrix $P^n = (p_{ij}^{(n)} : i, j \in \mathbb{Z}_2)$ verifies $p_{ij}^{(n)} = \pi_j^P + (-1)^{i+j}(1 - \pi_i^P)\gamma_P^n$ for $n \geqslant 0$. In the sequel we denote $\pi_i = \pi_i^P$, $\gamma = \gamma_P$ and $\mathbb{P} = \mathbb{P}_P$. Define $A_n = \mathbb{P}\{S_{(n)} = 0\} - \frac{1}{2}$. First let us show the following recurrence relation

$$A_n = (\pi_0 - \pi_1)(1 - \gamma^{r_n - r_{n-1}}) A_{n-1} + \gamma^{r_n - r_{n-1}} A_{n-2}, \forall n \geqslant 2 \tag{2}$$

Put $C_n = \mathbb{P}\{S_{(n)} = 0\}$ and $B_n = \mathbb{P}\{S_{(n)} = 0, x_{r_n} = 0\}$. For $n \geqslant 1$, $B_n = \mathbb{P}\{S_{(n-1)} = 0, x_{r_n} = 0\}$. For $n \geqslant 2$ it is satisfied

$$\begin{aligned} C_n &= \mathbb{P}\{S_{(n)} = 0, x_{r_n} = 0\} + \mathbb{P}\{S_{(n)} = 0, x_{r_n} = 1\} \\ &= B_n + \pi_1 - (\mathbb{P}\{S_{(n-1)} = 0\} - \mathbb{P}\{S_{(n-1)} = 0, x_{r_n} = 0\}), \qquad \text{so} \\ C_n &= 2B_n + \pi_1 - C_{n-1} \end{aligned} \tag{3}$$

On the other hand,

$$\begin{aligned} B_n &= \mathbb{P}\{S_{(n-1)} = 0, x_{r_{n-1}} = 0, x_{r_n} = 0\} + \mathbb{P}\{S_{(n-1)} = 0, x_{r_{n-1}} = 1, x_{r_n} = 0\} \\ &= p_{00}^{(r_n - r_{n-1})} B_{n-1} + p_{10}^{(r_n - r_{n-1})} \mathbb{P}\{S_{(n-2)} = 1, x_{r_{n-1}} = 1\} \end{aligned}$$

Since

$$\mathbb{P}\{S_{(n-2)}=1, x_{r_{n-1}}=1\} = \pi_1 - \mathbb{P}\{S_{(n-2)}=0, x_{r_{n-1}}=1\}$$
$$= \pi_1 - C_{n-2} + B_{n-1}, \quad \text{we obtain}$$
$$B_n = (p_{00}^{(r_n - r_{n-1})} + p_{10}^{(r_n - r_{n-1})})\, B_{n-1} + p_{10}^{(r_n - r_{n-1})}\pi_1 - p_{10}^{(r_n - r_{n-1})} C_{n-2} \tag{4}$$

From (3) and (4) we get

$$C_n + (1 - (p_{00}^{(r_n - r_{n-1})} + p_{10}^{(r_n - r_{n-1})}))\, C_{n-1} + (p_{10}^{(r_n - r_{n-1})} - p_{00}^{(r_n - r_{n-1})})\, C_{n-2} - (1 + p_{10}^{(r_n - r_{n-1})} - p_{00}^{(r_n - r_{n-1})})\, \pi_1 = 0$$

Since $C_n = A_n + \frac{1}{2}$ we find that A_n verifies the equation with the same coefficients in A_n, A_{n-1}, A_{n-2} as those of C_n, C_{n-1}, C_{n-2} and with constant term:

$$1 - \tfrac{1}{2}(p_{00}^{(r_n - r_{n-1})} + p_{10}^{(r_n - r_{n-1})}) + \tfrac{1}{2}(p_{10}^{(r_n - r_{n-1})} - p_{00}^{(r_n - r_{n-1})}) - (1 + p_{10}^{(r_n - r_{n-1})} - p_{00}^{(r_n - r_{n-1})})\, \pi_1 = \pi_0 - \pi_0 p_{00}^{(r_n - r_{n-1})} - \pi_1 p_{10}^{(r_n - r_{n-1})} = 0$$

this last equality because $\mathbb{P} = \mathbb{P}_P$ is an invariant Markov measure.

Now $p_{00}^{(r_n - r_{n-1})} = \pi_0 + \pi_1 \gamma^{r_n - r_{n-1}}$, $p_{10}^{(r_n - r_{n-1})} = \pi_0 - \pi_0 \gamma^{r_n - r_{n-1}}$, so $1 - (p_{00}^{(r_n - r_{n-1})} + p_{10}^{(r_n - r_{n-1})}) = (\pi_1 - \pi_0)(1 - \gamma^{r_n - r_{n-1}})$, and $p_{10}^{(r_n - r_{n-1})} - p_{00}^{(r_n - r_{n-1})} = -\gamma^{r_n - r_{n-1}}$. Then the relation (2) is verified.

Assume $\gamma \in [0, 1)$. Observe that

$$|\pi_0 - \pi_1|\,(1 - \gamma^{r_n - r_{n-1}}) + \gamma^{r_n - r_{n-1}} = |\pi_0 - \pi_1| + \gamma^{r_n - r_{n-1}}(1 - |\pi_0 - \pi_1|) \leqslant \Gamma'$$

with $\Gamma' = |\pi_0 - \pi_1| + \gamma(1 - |\pi_0 - \pi_1|)$, which belongs to $(0, 1)$. Hence

$$|A_n| \leqslant \Gamma' \max(|A_{n-1}|, |A_{n-2}|)$$

Analogously we can show $|A_{n+1}| \leqslant \Gamma' \max(|A_{n-1}|, |A_{n-2}|)$. Then, we conclude $\max(|A_{2n+1}|, |A_{2n}|) \leqslant \frac{1}{2}\Gamma'^n$ which implies the result.

Let $\gamma \in (-1, 0)$. We have $|\pi_0 - \pi_1|\, |1 - \gamma^{r_n - r_{n-1}}| + |\gamma^{r_n - r_{n-1}}| \leqslant \Gamma''$ with $\Gamma'' = |\pi_0 - \pi_1|\,(1 + |\gamma|) + |\gamma|$. Let us prove $\Gamma'' < 1$. We have

$$\begin{aligned}\Gamma'' &= |\pi_0 - \pi_1| + |\gamma|\,(1 + |\pi_0 - \pi_1|)\\ &= |\pi_0 - \pi_1| + (p_{10} + p_{01} - 1)(1 + |\pi_0 - \pi_1|)\\ &= (p_{10} + p_{01}) + (p_{10} + p_{01})\frac{|p_{10} - p_{01}|}{p_{10} + p_{01}} - 1 = 2\max(p_{10}, p_{01}) - 1 < 1\end{aligned}$$

By the same arguments as above we can show $|A_n| \leqslant \Gamma'' \max(|A_{n-1}|, |A_{n-2}|)$ and $\max(|A_{2n+1}|, |A_{2n}|) \leqslant \frac{1}{2}\Gamma''^n$. Then the result follows. ∎

Remark. For the particular sequence $(r_k = k, k \in \mathbb{N})$ the proof of last lemma can be made shortly by simply observing that the sequence of random vectors $((S_{(n+1)}, S_{(n)}), n \in \mathbb{N})$ is Markov and by computing its stationary probability vector. ∎

Proof of Theorem 2. It is enough to consider the case $B=1$, then $\varphi_B = \varphi_2$. Fix $\alpha \in (0, \frac{1}{2})$. We remind the following equality, which is shown by using elementary large deviations techniques

$$\sum_{j \leqslant \alpha n} \binom{n}{j} \leqslant 2^n e^{-2(\alpha - 1/2)^2 n} \tag{5}$$

From (1) $(\varphi_2^n x)(0) = \sum_{k \in \mathscr{I}(n)} x_k$. Since $|\{I \subseteq \mathscr{I}(n)\}| = 2^{|\mathscr{I}(n)|}$, Lemma 3 implies

$$\mathbb{P}\{(\varphi_2^n x)(0) = 0\} = \tfrac{1}{2} + h_n \qquad \text{with} \quad |h_n| \leqslant c\Gamma^{|\mathscr{I}(n)|}$$

Then

$$\left| \frac{1}{N+1} \sum_{n \leqslant N} \mathbb{P}\{(\varphi_2^n x)(0) = 0\} - \frac{1}{2} \right| \leqslant \frac{c}{(N+1)} \sum_{n \leqslant N} \Gamma^{|\mathscr{I}(n)|}$$

Consider the family of sets

$$\mathscr{R}_N = \{n \leqslant N : |\mathscr{I}(n)| \geqslant \alpha \log\log N\}, \qquad N \in \mathbb{N} \tag{6}$$

In order to prove Theorem 2 (ii), it suffices to show that the sequence of sets $(\mathscr{R}_N : N \in \mathbb{N})$ has density 1, i.e., it verifies $\lim_{N \to \infty}(|\mathscr{R}_N|/N+1) = 1$. Indeed, from this fact we deduce

$$\frac{c}{|\mathscr{R}_N|} \sum_{n \in \mathscr{R}_N} \Gamma^{|\mathscr{I}(n)|} \leqslant \Gamma^{\alpha \log\log N} \xrightarrow[N \to \infty]{} 0$$

Denote $\mathscr{I}(n) = \{\delta_{1,n} > \delta_{2,n} > \cdots > \delta_{|\mathscr{I}(n)|, n}\}$ and $\delta_{k,n} = -1$ for $k > |\mathscr{I}(n)|$. We set $A_{1,N} = \{n \leqslant N : \delta_{1,n} < \delta_{1,N}\}$ and in general

$$A_{s,N} = \{n \leqslant N : \delta_{r,n} = \delta_{r,N} \text{ for } r < s, \delta_{s,n} < \delta_{s,N}\}, \qquad \text{for} \quad 1 \leqslant s \leqslant |\mathscr{I}(N)|$$

For $s = |\mathscr{I}(N)| + 1$ we put $A_{|\mathscr{I}(N)|+1, N} = \{n \leqslant N : \delta_{r,n} = \delta_{r,N} \forall r\} = \{N\}$.

We have $\{n \leqslant N\} = \bigcup_{1 \leqslant s \leqslant |\mathscr{I}(N)|+1} A_{s,N}$ and $|A_{s,N}| = 2^{\delta_{s,N}}$ for $1 \leqslant s \leqslant |\mathscr{I}(N)|$. Take $s_N = \sup\{s: \delta_{s,N} \geqslant \log\log N\}$. Observe that $s_N \geqslant 1$ because $\delta_{1,N} =$ integer part of $\log N$. From (5) we obtain for $1 \leqslant s \leqslant |\mathscr{I}(N)|$

$$|\{n \in A_{s,N}: |\mathscr{I}(n)| \leqslant \alpha\, \delta_{s,N}\}| \leqslant \sum_{p \leqslant \alpha\delta_{s,N}} \binom{\delta_{s,N}}{p} \leqslant 2^{\delta_{s,N}} e^{-2(\alpha - 1/2)^2 \delta_{s,N}}$$

Now, from the definition of s_N we get $|A_{s,N}| \leqslant 2^{\log\log N}$ for $s_N < s \leqslant |\mathscr{I}(N)|$. Since

$$\{n \leqslant N\} \backslash \mathscr{R}_N \subseteq \bigcup_{1 \leqslant s \leqslant s_N} \{n \in A_{s,N}: |\mathscr{I}(n)| < \alpha\, \delta_{s,N}\} \cup \bigcup_{s_N < s \leqslant |\mathscr{I}(N)|+1} A_{s,N}$$

by using previous inequalities we get

$$\begin{aligned} |\{n \leqslant N\} \backslash \mathscr{R}_N| &\leqslant \sum_{1 \leqslant s \leqslant s_N} 2^{\delta_{s,N}} e^{-2(\alpha - 1/2)^2 \delta_{s,N}} + \sum_{s_N < s \leqslant \mathscr{I}(N)} 2^{\log\log N} + 1 \\ &\leqslant N e^{-2(\alpha - 1/2)^2 \log\log N} + \log N 2^{\log\log N} + 1 \end{aligned}$$

Hence $\lim_{N \to \infty} (1/N+1)\, |\{n \leqslant N\} \backslash \mathscr{R}_N| = 0$, i.e., $(\mathscr{R}_N: N \in \mathbb{N})$ is of density 1.

Let us show Theorem 2 part (i). The sequence $(x_n: n \in \mathbb{N})$ is distributed according to the Bernoulli measure $\mathbb{P}_\pi$. In this case the following equality holds

$$\mathbb{P}\left\{\sum_{k \in J} x_k = i\right\} = \frac{1}{2}(1 + (-1)^i \rho^{|J|}) \qquad \text{with} \quad \rho = \pi_0 - \pi_1,$$
$$\text{for all} \quad J \in \mathscr{P}_f(\mathbb{N}), \qquad i \in \mathbb{Z}_2 \tag{7}$$

Indeed, the sequence of random variables $S_n = \sum_{p \leqslant n} x_p$ is a Markov chain with transition probabilities verifying $\tilde{p}_{ij}^{(n)} = \frac{1}{2}(1 + (-1)^{i+j} \rho^n)$.

The following notation will be helpful. For a fixed $J \in \mathscr{P}_f(\mathbb{N})$ and $(\mathscr{S}_N)$ a sequence of sets such that $\mathscr{S}_N \subseteq \{n \leqslant N\}$, we put $\mathscr{S}_{N,J} = \{n \leqslant N: n + r \in \mathscr{R}_N \text{ for } r \in J\}$. If $(\mathscr{S}_N)$ is of density one then $(\mathscr{S}_{N,J})$ is also of density 1. It is also useful to introduce two sequences of sets of density 1. Denote $G_n = \max(\mathbb{N} \backslash \mathscr{I}(n)) \cap \{p \leqslant \delta_{1,n}\}$ and $(\mathbb{N} \backslash \mathscr{I}(n)) \cap \{p \leqslant \delta_{1,n}\} = \{\beta_{1,n} < \beta_{2,n} < \cdots < \beta_{G_n,n}\}$. Now, fix $\alpha \in (0, \frac{1}{2})$, take $\varepsilon \in (0, \alpha)$ and $\varepsilon' \in (0, \frac{1}{2}(\alpha - \varepsilon))$. For $\ell = \max J$ we define

$$\mathscr{R}'_N = \{n \leqslant N: \log_2(2(\ell+1)) \leqslant G_n \text{ and } \beta_{\lfloor \log_2(2(\ell+1)) \rfloor, n} \leqslant \varepsilon \log\log N\}$$

$$\begin{aligned} \mathscr{R}''_N = \{n \leqslant N: \delta_{1,n} > \varepsilon \log\log N \text{ and } |\mathscr{I}(n) \\ \cap \{\varepsilon \log\log N \leqslant p \leqslant \delta_{1,n}\}| \geqslant \varepsilon' \log\log N\} \end{aligned}$$

It can be easily shown that the sequences of sets $(\mathscr{R}'_N: N \in \mathbb{N})$ and $(\mathscr{R}''_N: N \in \mathbb{N})$ are of density 1.

Now we are ready to prove the result. Notice that for every $(i_k: k < s) \in \mathbb{Z}_2^s$ there exists a $(j_k: k < s) \in \mathbb{Z}_2^s$ such that

$$\{x \in X_2: (\varphi_2^n x)(k) = i_k \text{ for } k < s\} = \{x \in X_2: (\varphi_2^{n+k} x)(0) = j_k \text{ for } k < s\}$$

Then it suffices to show that for any $J \in \mathscr{P}_f(\mathbb{N})$ with $0 \in J$ and $(i_r: r \in J) \in \mathbb{Z}_2^{|J|}$, it is verified

$$\lim_{N \to \infty} \frac{1}{N+1} \sum_{n \leqslant N} \mathbb{P}\{(\varphi_2^{n+r} x)(0) = i_r, r \in J\} = \left(\frac{1}{2}\right)^{|J|}$$

Observe that we only need to prove these set of equalities for $i_r = 0, r \in J$. For the other cylinders the equality follows from well known algebraic relations.

We denote $E_J(n) = \mathbb{P}\{(\varphi_2^{n+r} x)(0) = 0, r \in J\}$, then we must prove that

$$\lim_{N \to \infty} \frac{1}{N+1} \sum_{n \leqslant N} E_J(n) = \left(\frac{1}{2}\right)^{|J|}$$

We have

$$\begin{aligned} E_J(n) &= \mathbb{P}\left\{\sum_{I \subseteq \mathscr{I}(n+r)} x_{\mathscr{N}(I)} = 0, r \in J\right\} \\ &= \mathbb{P}\left\{x_{n+r} = \sum_{\substack{I \subseteq \mathscr{I}(n+r) \\ I \neq \mathscr{I}(n+r)}} x_{\mathscr{N}(I)}, r \in J\right\} \end{aligned}$$

Put $\mathscr{L} = \mathscr{L}_J(n) = \bigcup_{r \in J} \{I \subseteq \mathscr{I}(n+r)\} \setminus \bigcup_{r \in J} \{\mathscr{I}(n+r)\}$. We have

$$E_J(n) = \sum_{(i_I: I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} \mathbb{P}\{x_{\mathscr{N}(I)} = i_I \text{ for } I \in \mathscr{L}, \text{ and } x_{n+r} = j_r \text{ for } r \in J\}$$

where j_r verifies

$$\begin{aligned} j_r &= \sum_{I \in \mathscr{L}} i_I 1_{\{I \subseteq \mathscr{I}(n+r) \wedge (I \subseteq \mathscr{I}(n+r'), I \neq \mathscr{I}(n+r') \quad \text{for} \quad r' < r)\}} \\ &= \sum_{\substack{I \in \mathscr{L} \\ I \subseteq \mathscr{I}(n+r)}} i_I \sum_{r' \in H(r, I)} 1_{I \subseteq \mathscr{I}(n+r')} \qquad \text{for} \quad r \in J \end{aligned}$$

being $H(r, I) = \{r' \in J: \mathscr{I}(n+r') \subseteq \mathscr{I}(n+r)\}$.

We have

$$E_J(n) = \sum_{(i_l:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} \left(\prod_{I \in \mathscr{L}} \frac{1}{2}(1 + (-1)^{i_l} \rho) \right) \left(\prod_{r \in J} \frac{1}{2}(1 + (-1)^{j_r} \rho) \right)$$

$$= \left(\frac{1}{2}\right)^{|\mathscr{L}| + |J|} \sum_{(i_l:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} \prod_{I \in \mathscr{L}} (1 + (-1)^{i_l} \rho) \prod_{r \in J} (1 + (-1)^{j_r} \rho)$$

Now

$$\prod_{k \in K} (1 + a_k) = \sum_{\Lambda \subseteq K} \prod_{j \in \Lambda} a_j = 1 + \sum_{\substack{\Lambda \subseteq K \\ \Lambda \neq \phi}} \prod_{j \in \Lambda} a_j.$$

Then

$$E_J(n) = \left(\frac{1}{2}\right)^{|\mathscr{L}| + |J|} \sum_{(i_l:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} \left(1 + \sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} (-1)^{\Sigma_{I \in \mathscr{L}'} i_l} \rho^{|\mathscr{L}'|} \right)$$

$$\times \left(1 + \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} (-1)^{\Sigma_{r \in J'} j_r} \rho^{|J'|} \right)$$

$$= \left(\frac{1}{2}\right)^{|J|} + \left(\frac{1}{2}\right)^{|\mathscr{L}| + |J|} \sum_{(i_l:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} \left(\sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} (-1)^{\Sigma_{I \in \mathscr{L}'} i_l} \rho^{|\mathscr{L}'|} \right.$$

$$\left. + \sum_{\substack{J' \subseteq J \\ J \neq \phi}} (-1)^{\Sigma_{r \in J'} j_r} \rho^{|J'|} + \sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} \sum_{\substack{J' \subseteq J \\ J \neq \phi}} (-1)^{\Sigma_{J \in \mathscr{L}'} i_l + \Sigma_{r \in J'} j_r} \rho^{|\mathscr{L}'| + |J'|} \right) \tag{8}$$

We shall analyze the three sums appearing (at the right hand side (RHS) in expression (8).

By using the relation

$$\sum_{(i_k:\, k \in K) \in \mathbb{Z}_2^{|K|}} (-1)^{\Sigma_{k \in K'} i_k} = 0 \qquad \text{for all} \quad K' \subseteq K, \quad K' \neq \phi \tag{9}$$

we get

$$\sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} \sum_{(i_l:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\Sigma_{i \in \mathscr{L}'} i_l} \rho^{|\mathscr{L}'|} = 0,$$

then the first sum at the RHS in (8) vanishes.

Let us analyze the second term appearing at the RHS in (8).

$$V_J(n) = \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \sum_{(i_I : I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{r \in J'} j_r} \rho^{|J'|}$$

$$= \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \rho^{|J'|} \sum_{(i_I : I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{r \in J'} \sum_{I \in \mathscr{L},\, I \subseteq \mathscr{I}(n+r)} i_I [\sum_{r' \in H(r, I)} 1_{I \subseteq \mathscr{I}(n+r')}]}$$

$$= \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \rho^{|J'|} \sum_{(i_I : I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{I \in \mathscr{L}} i_I a_{J'}(I)}$$

where $a_{J'}(I) = \sum_{r \in J'} 1_{I \subseteq \mathscr{I}(n+r)} \sum_{r' \in H(r, I)} 1_{I \subseteq \mathscr{I}(n+r')}$.

We shall prove that for $n \in \mathscr{R}'_N \cap \mathscr{R}''_N$ it is satisfied the following property: for every $J' \subseteq J$, $J' \neq \phi$, there exists $I \in \mathscr{L}$ such that $a_{J'}(I) = 1$.

Consider $n \in \mathscr{R}'_N \cap \mathscr{R}''_N$. We denote $\mathscr{I}_+(n+r) = \mathscr{I}(n+r) \cap \{p > \varepsilon \log\log N\}$ and $\mathscr{I}_-(n+r) = \mathscr{I}(n+r) \cap \{p \leqslant \varepsilon \log\log N\}$. From the definition of $\mathscr{R}'_N$ we have that $\mathscr{I}_+(n+r) = \mathscr{I}_+(n)$ for $r \in J$, and since $\mathscr{I}(n+r) \neq \mathscr{I}(n+r')$ for $r \neq r'$ in J we deduce $\mathscr{I}_-(n+r) \neq \mathscr{I}_-(n+r')$ for $r \neq r'$ in J.

For $r \in J$ pick $I'_r \subseteq \mathscr{I}_+(n+r)$, $I'_r \neq \mathscr{I}_+(n+r)$. Notice that $\mathscr{I}_+(n+r)$ is not empty whenever $n \in \mathscr{R}''_N$. Then $\mathscr{I}_-(n+r) \cup I'_r \subseteq \mathscr{I}(n+r)$, $\mathscr{I}_-(n+r) \cup I'_r \neq \mathscr{I}(n+r)$ and $\mathscr{I}_-(n+r) \cup I'_r$ is different to $\mathscr{I}(n+r')$ for all $r' \neq r$ in J. In particular, $\mathscr{I}_-(n+r) \cup I'_r \in \mathscr{L}_J(n)$. Let us prove that $a_{J'}(\mathscr{I}_-(n+r) \cup I'_r) = 1$ for all J' such that $r = \max J'$. If $\mathscr{I}_-(n+r) \cup I'_r \subseteq \mathscr{I}(n+\tilde{r})$ for some $\tilde{r} \in J'$, then $\mathscr{I}_-(n+r) \subseteq \mathscr{I}_-(n+\tilde{r})$ and consequently $r \leqslant \tilde{r} \leqslant \max J = r$. On the other hand, if for some $r' \in J$, $\mathscr{I}_-(n+r) \cup I'_r \subseteq \mathscr{I}(n+r') \subseteq \mathscr{I}(n+r)$, then $r' = r$, proving the assertion.

We deduce that for all $J' \neq \phi$ there exists $I \in \mathscr{L}$ such that $a_{J'}(I) = 1$. From (9) we conclude that $V_J(n) = 0$ for all $n \in \mathscr{R}'_N \cap \mathscr{R}''_N$.

Let us analyze the last term at the RHS in (8).

$$W_J(n) = \sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \left(\sum_{(i_I : I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{I \in \mathscr{L}'} i_I + \sum_{I \in \mathscr{L}} i_I a_{J'}(I)} \rho^{|\mathscr{L}'| + |J'|} \right)$$

$$= \sum_{\substack{\mathscr{L}' \subseteq \mathscr{L} \\ \mathscr{L}' \neq \phi}} \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \left(\sum_{(i_I : I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{I \in \mathscr{L}} i_I [a_{J'}(I) + 1_{\mathscr{L}'}(I)]} \right) \rho^{|\mathscr{L}'| + |J'|}$$

If for a fixed couple $\mathscr{L}', J'$, there exists some term $I \in \mathscr{L}$ such that $[a_{J'}(I) + 1_{\mathscr{L}'}(I)] = 1$, from (9) we deduce that $\sum_{(i_I:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} (-1)^{\sum_{I \in \mathscr{L}} i_I [a_{J'}(I) + 1_{\mathscr{L}'}(I)]} = 0$. Hence we can restrict ourselves to those couples $\mathscr{L}', J'$ such that

$$[a_{J'}(I) + 1_{\mathscr{L}'}(I)] = 0 \qquad \text{for all} \quad I \in \mathscr{L} \tag{10}$$

Fix $J' \subseteq J, J' \neq \phi$. There is only one $\mathscr{L}' \subseteq \mathscr{L}$ such that relation (10) is verified, and it is given by

$$I \in \mathscr{L}' \qquad \text{if and only if} \quad a_{J'}(I) = 1 \tag{11}$$

We denote $\mathscr{L}'(J')$ the set $\mathscr{L}'$ defined by relation (11). If $\mathscr{L}'(J') \neq \phi$ we get

$$W_J(n) = \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \left(\sum_{(i_I:\, I \in \mathscr{L}) \in \mathbb{Z}_2^{|\mathscr{L}|}} 1 \right) \rho^{|\mathscr{L}'(J')| + |J'|} = 2^{|\mathscr{L}|} \sum_{\substack{J' \subseteq J \\ J' \neq \phi}} \rho^{|\mathscr{L}'(J')| + |J'|}$$

Now, we have that $|\mathscr{L}'(J')| = |\{I \in \mathscr{L}\colon a_{J'}(I) = 1\}|$ and from above discussion we get

$$|\mathscr{L}'(J')| \geqslant |\{\mathscr{I}_-(n+r) \cup I'_r\colon I'_r \subseteq \mathscr{I}_+(n+r),\, I'_r \neq \mathscr{I}_+(n+r),\, r = \max J'\}|$$

If $n \in \mathscr{R}''_{N,J}$ we have $\mathscr{I}_+(n+r) \geqslant \varepsilon' \log \log N$, which implies

$$|\mathscr{L}'(J')| \geqslant 2^{\varepsilon' \log \log N - 1} = \tfrac{1}{2} (\log N)^{\varepsilon' \log 2}$$

Hence, $W_J(n) \leqslant 2^{|\mathscr{L}| + |J|} |\rho|^{1/2 (\log N)^{\varepsilon' \log 2} + 1}$ for $n \in \mathscr{R}''_{N,J}$, and we conclude

$$|E_J(n) - (\tfrac{1}{2})^{|J|}| \leqslant |\rho|^{1/2 (\log N)^{\varepsilon' \log 2} + 1} 2^{|J|} \qquad \text{for} \quad n \in \mathscr{R}'_{N,J} \cap \mathscr{R}''_{N,J}$$

Therefore, by taking into account that $(\mathscr{R}_{N,J} \cap \mathscr{R}'_{N,J} \cap \mathscr{R}''_{N,J}, N \in \mathbb{N})$ is of density 1, we get

$$\lim_{N \to \infty} \frac{1}{N+1} \sum_{n \leqslant N} E_J(n) = \lim_{N \to \infty} \frac{1}{|\mathscr{R}_{N,J} \cap \mathscr{R}'_{N,J} \cap \mathscr{R}''_{N,J}|} \times \sum_{n \in \mathscr{R}_{N,J} \cap \mathscr{R}'_{N,J} \cap \mathscr{R}''_{N,J}} E_J(n) = \left(\frac{1}{2}\right)^{|J|}$$

Then the theorem is shown. ∎

3. PROOF OF THEOREM 1

Before proving Theorem 1 we state some basic facts about the automaton φ_B. If $B = b_0 \cdots b_{R-1}$ is the aperiodic block defining φ_B, we denote by $\bar{B}=(b_0+1)\,b_1\cdots b_{R-1}$. In what follows we will extend the action of φ_B to the words of length larger than $R+1$ in the obvious way.

Lemma 4. Let $w_0\cdots w_{R-1}, \bar{w}_0\cdots \bar{w}_{R-1} \in \mathbb{Z}_2^R\backslash\{B\}$, then $\varphi_B(w_0\cdots w_{R-1}\bar{w}_0\cdots \bar{w}_{R-1}) \neq B$.

Proof. Suppose $\varphi_B(w_0\cdots w_{R-1}\bar{w}_0\cdots \bar{w}_{R-1}) = B$. Since each b_i must be equal to $\bar{w}_i$ or $\bar{w}_i+1$, $w_0\cdots w_{R-1}\neq B$ and $\bar{w}_0\cdots\bar{w}_{R-1}\neq B$, there exists $i^*\in\{0,..., R-2\}$ such that $\bar{w}_0\cdots\bar{w}_{i^*}=b_0\cdots b_{i^*}$ and $\bar{w}_{i^*+1}=b_{i^*+1}+1$. Therefore, $w_{i^*+1}\cdots w_{R-1}\bar{w}_0\cdots\bar{w}_{i^*}=B$, which implies that B is not aperiodic. This is a contradiction and the lemma is proved. ∎

Lemma 5. Let $w_0\cdots w_{R-1}\in\mathbb{Z}_2^R$.

(i) $\varphi_B(w_0\cdots w_{R-1}B)\in\{B,\bar{B}\}$. Moreover, $\varphi_B(w_0\cdots w_{R-1}B)=B \Leftrightarrow w_0\cdots w_{R-1}\neq B$ and $\varphi_B(BB)=\bar{B}$.

(ii) $\varphi_B(w_0\cdots w_{R-1}\bar{B})\neq B \Leftrightarrow w_0\cdots w_{R-1}\neq B$, and $\varphi_B(\bar{B}\bar{B})=\bar{B}$, $\varphi_B(B\bar{B})=B$. On the other hand,

(iii) $\varphi_B(Bw_0\cdots w_{R-1})\neq B, \bar{B}$ when $w_0\cdots w_{R-1}\neq B, \bar{B}$, and $\varphi_B(\bar{B}w_0\cdots w_{R-1})\neq B,\bar{B}$ when $w_0\cdots w_{R-1}\neq B,\bar{B}$.

Proof. All the properties follow straightforward from the aperiodicity of B. We only show property (i), the other statements are shown similarly. Since B cannot overlap B in a nontrivial way, only the first coordinate of B can be flipped when we compute $\varphi_B(w_0\cdots w_{R-1}B)$. The result is B when $w_0\cdots w_{R-1}\neq B$ and it is $\bar{B}$ when $w_0\cdots w_{R-1}=B$. ∎

From these lemmas we deduce that the restriction of the map φ_B to $Y_B=\{x\in X_2\colon \forall i\in\mathbb{N}, x(iR, iR+R-1)\in\{B,\bar{B}\}\}$ is topologically conjugate to the mod 2 sum automaton. In fact, the map $\psi\colon Y_B\to X_2$ defined by $(\psi x)_n=1$ if and only if $x(nR, nR+R-1)=B$ is continuous, invertible and $\psi\circ\varphi_B=\varphi_2\circ\psi$. Moreover, since B and $\bar{B}$ are different only in the first letter, if we suppose that $b_0=1$ then the action of φ_B over $x=(x_i)_{i\in\mathbb{N}}\in Y_B$ is determined by the action of φ_2 over the point $y=(y_i)_{i\in\mathbb{N}}=(x_{iR})_{i\in\mathbb{N}}\in X_2$. In the sequel and without loss of generality we shall suppose that $b_0=1$.

It is useful to introduce for each $x\in X_2$ and $n\in\mathbb{N}$, the nth-diagonal produced by the action of φ_B by

$$\begin{aligned} d_n(x) &= x(nR, nR+R-1)\cdots\varphi_B^{n-1}(x)(R, 2R-1)\,\varphi_B^n(x)(0, R-1)\\ &= d_n^{(0)}(x)\,d_n^{(1)}(x)\cdots d_n^{(n-1)}(x)\,d_n^{(n)}(x)\end{aligned}$$

Lemma 6. Let $x\in X_2$ and $n\in\mathbb{N}$. If for some $i\in\{0,..., n\}$, $d_n^{(i)}(x)=B$ then $d_n(x)\in\{B,\bar{B}\}^{n+1}$.

Proof. We show the lemma by induction. It is straightforward for $n=0$. We assume the lemma holds for $n-1$, $n>0$. Let us suppose that $d_n^{(i)}(x)=B$ for some $i\in\{0,..., n\}$. By using Lemma 5, we can distinguish two cases. For all $j\in\{0,..., n\}$ $d_n^{(j)}(x)=B$, in which case the lemma holds, or for some $j\in\{0,..., n\}$ $d_n^{(j)}(x)=\bar{B}$ with $d_n^{(j-1)}(x)=B$ or $d_n^{(j+1)}(x)=B$. In the last case, we deduce from Lemma 5 that $d_{n-1}^{(k)}(x)=B$ for some $k\in\{0,..., n-1\}$. It follows by induction that $d_{n-1}(x)\in\{B, \bar{B}\}^n$.

Since, by Lemma 5, $d_{n-1}(x)$ determines the value of $d_n(x)$ and $d_n^{(i)}(x)=B$, we conclude that $d_n(x)\in\{B, \bar{B}\}^{n+1}$. ∎

Lemma 7. Let $x\in X_2$, $i\in\{0,..., R-1\}$ and $m\in\mathbb{N}$ such that $x(i+mR, i+mR+R-1)\notin\{B, \bar{B}\}$. Then for any $t\geqslant 1$, $(\varphi_B^{m+t}x)(i)=(\varphi_B^{m+t}\tilde{x})(i)$ where $\tilde{x}=x(0, i-1)\,\bar{B}^{m+1}x(i+(m+1)\,R, +\infty)$.

Proof. Since the automaton is one-sided we only have to prove the case $i=0$. We will prove that $d_j^{(k)}(x)\neq B$ if and only if $d_j^{(k)}(\tilde{x})\neq B$ for $k\in\{0,..., j\}$ and $j\geqslant m$, which implies the result. In fact, $(\varphi_B^{m+t}x)(0)$ and $(\varphi_B^{m+t}\tilde{x})(0)$ are determined by the values in $d_{m+t-1}(x)$ and $D_{m+t-1}(\tilde{x})$ respectively. Let us begin by pointing out that $d_m(\tilde{x})=\bar{B}^{m+1}$ and, by Lemma 6, $d_m^{(k)}(x)\neq B$ for all $k\in\{0,..., m\}$. Thus, we have $d_m^{(k)}(x)\neq B$ if and only if $d_m^{(k)}(\tilde{x})\neq B$.

Assume we have already shown that $d_j^{(k)}(x)\neq B$ if and only if $d_j^{(k)}(\tilde{x})\neq B$ for $k\in\{0,..., j\}, j\geqslant m$. We will prove that the same result holds for $j+1$. We have to analyze two cases, when $d_j^{(k)}(x)$ and $d_j^{(k)}(\tilde{x})$ are different from B for all $i\in\{0,..., j\}$ and when $d_j^{(k)}(x)=d_j^{(k)}(\tilde{x})=B$ for some $k\in\{0,..., j\}$. In the first case, if $d_{j+1}^{(0)}(\tilde{x})=B$ then, by Lemma 5, $d_{j+1}(x)=d_{j+1}(\tilde{x})=B^{j+2}$ because $d_{j+1}^{(0)}(\tilde{x})=d_{j+1}^{(0)}(x)$, and the statement for $j+1$ holds. If $d_{j+1}^{(0)}(x)=d_{j+1}^{(0)}(\tilde{x})\neq B$, by Lemma 5, we have that $d_{j+1}^{(k)}(x)$ and $d_{j+1}^{(k)}(\tilde{x})$ are different from B for all $k\in\{0,..., j\}$. In the second case, Lemma 6 and the induction hypothesis implies that $d_j(x)=d_j(\tilde{x})$. Therefore, since $d_{j+1}^{(0)}(x)=d_{j+1}^{(0)}(\tilde{x})$, we conclude that $d_{j+1}(x)=d_{j+1}(\tilde{x})$, proving the lemma. ∎

For $x\in X_2$ define $D(x)=\{m\in\mathbb{N}: x(mR, mR+R-1)\notin\{B, \bar{B}\}\}\cup\{-1\}$. According to the last lemma if we want to compute $(\varphi_B^n x)(0)$ we only need the information of x in the block $x((\bar{m}+1)\,R, nR)$, where $\bar{m}\in D(x)$, $\bar{m}<n$ and $\{\bar{m},..., n-1\}\cap D(x)=\{\bar{m}\}$. Let us define for $x\in X_2$ and $n\in\mathbb{N}$ the interval $I(x, n)=\{\bar{m}+1,..., n\}$.

Following this property we will decompose the set $C_n=\{x\in X_2: (\varphi_B^{n+j}x)(0)=a_j, 0\leqslant j\leqslant \ell-1\}$, where $n\in\mathbb{N}$, $\ell\geqslant 1$ and $a_0,..., a_{\ell-1}\in\{0, 1\}$. Fix $u\in\{0, 1\}^\ell$ and $m\in\{-1, 0,..., n-1\}$. We define

$$C_{n,m,u}=\{x\in C_n: N(x, n)=m\wedge \forall j\in\{0,..., \ell-1\}(n+j)\in D(x)\Leftrightarrow u_j=0\}$$

where $N(x, n) = \inf I(x, n) - 1$. Therefore, $C_n = \bigcup_{u \in \{0,1\}^\ell} \bigcup_{m=-1}^{n-1} C_{n,m,u}$ is a disjoint union. It follows,

$$E_n = \mathbb{P}\{x \in X_2 : (\varphi_B^{n+j} x)(0) = a_j, 0 \leqslant j \leqslant \ell - 1\} = \sum_{u \in \{0,1\}^\ell} \sum_{m=-1}^{n-1} \mathbb{P}(C_{n,m,u})$$

Then

$$\begin{aligned}
L_N &= \frac{1}{N} \sum_{n=0}^{N-1} E_n \\
&= \sum_{u \in \{0,1\}^\ell} \frac{1}{N} \sum_{n=0}^{N-1} \sum_{m=-1}^{n-1} \mathbb{P}(C_{n,m,u}) \\
&= \sum_{u \in \{0,1\}^\ell} \left\{ \frac{1}{N} \sum_{n=0}^{N-1} \{\mathbb{P}\}(C_{n,-1,u}) + \frac{1}{N} \sum_{n=1}^{N-1} \mathbb{P}(C_{n,n-1,u}) \right. \\
&\quad \left. + \frac{1}{N} \sum_{n=2}^{N-1} \sum_{m=0}^{n-2} \mathbb{P}(C_{n,m,u}) \right\}
\end{aligned}$$

By taking k terms from the third sum, we obtain for N enough large

$$\begin{aligned}
L_N = \sum_{u \in \{0,1\}^\ell} &\left\{ \frac{1}{N} \sum_{n=0}^{N-1} \mathbb{P}(C_{n,-1,u}) + \sum_{s=1}^{k} \frac{1}{N} \sum_{n=s}^{N-1} \mathbb{P}(C_{n,n-s,u}) \right. \\
&\left. + \frac{1}{N} \sum_{n=k+1}^{N-1} \sum_{m=0}^{n-k-1} \mathbb{P}(C_{n,m,u}) \right\}.
\end{aligned}$$

We will prove that for each $s \in \{1, \ldots, k\}$ and $u \in \{0,1\}^\ell$ the following limits exist

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mathbb{P}(C_{n,-1,u}) \qquad \text{and} \qquad \lim_{N \to \infty} \frac{1}{N} \sum_{n=s}^{N-1} \mathbb{P}(C_{n,n-s,u})$$

Let us fix $n \in \mathbb{N}$, $m \in \{-1, 0, \ldots, n-1\}$, $u \in \{0,1\}^\ell$ and $j \in \{0, \ldots, \ell - 1\}$. For $x \in C_{n,m,u}$ we have that $(\varphi_B^{n+j} x)(0)$ only depends on the interval of coordinates determined by $I(x, n+j)$. A simple computation yields to $I(x, n+j) = \{M+1, \ldots, n+j\}$, where $M = \max(\{m\} \cup \{n+k : k \in \{0, \ldots, j-1\} \wedge u_k = 0\})$. This fact implies that $I(x, n+j) = I(x', n+j)$ whenever $x, x' \in C_{n,m,u}$. Moreover, if $x \in C_{n,m,u}$ and $x' \in C_{n',m',u}$ with $n - m = n' - m'$ then $I(x, n+j) - m - 1 = I(x', n'+j) - m' - 1$. For $s \in \mathbb{N} \backslash \{0\}$, $u \in \{0,1\}^\ell$ and $j \in \{0, \ldots, \ell - 1\}$ define $J(j, u, s) \subseteq \{0, \ldots, s + \ell - 2\}$ such that $I(x, n+j) = J(j, u, s) + m + 1$ for every $x \in C_{n,m,u}$ and $n - m = s$.

Hence, by using the fact that φ_B is conjugate with the mod 2 sum automaton on Y_B and by using Lemma 7, we obtain

$$\begin{aligned}\mathbb{P}(C_{n,m,u}) &= \mathbb{P}\left\{x \in C_{n,m,u}\colon \sum_{i \in I(x,n+j)} x_{iR} 1_{\mathscr{I}(i) \subseteq \mathscr{I}(n+j)} = a_j,\ 0 \leqslant j \leqslant \ell - 1\right\} \\ &= \lambda(u) \cdot \lambda^{n-1-m} \cdot (1_{\{m=-1\}} + (1-\lambda)\, 1_{\{m \neq -1\}}) \\ &\quad \times \mathbb{P}\left\{y \in \{0,1\}^{n-m+\ell-1}\colon \sum_{i \in J(j,u,n-m)} y_i 1_{\mathscr{I}(i+m+1) \subseteq \mathscr{I}(n+j)} = a_j,\right. \\ &\qquad \left. 0 \leqslant j \leqslant \ell - 1\right\}\end{aligned}$$

where $\lambda = \pi_{b_0} \pi_{b_1} \cdots \pi_{b_{R-1}} + \pi_{\overline{b_0}} \pi_{b_1} \cdots \pi_{b_{R-1}} = \pi_{b_1} \cdots \pi_{b_{r-1}}$, $\lambda(u) = \lambda^{\sum_{i=0}^{\ell-1} u_i} (1-\lambda)^{l - \sum_{i=0}^{\ell-1} u_i}$. If $\lambda = 1$, that is $R = 1$, we have $\lambda(u) = 0$ for $u \in \{0,1\}^{\ell} \setminus \{(1,\ldots,1)\}$ and $\lambda((1,\ldots,1)) = 1$. Also $D(x) = \{-1\}$ for all $x \in X_2$, then $\mathbb{P}(C_n) = \mathbb{P}(C_{n,-1,(1,\ldots,1)})$.

Put

$$g_{n,m,u} = \mathbb{P}\left\{y \in \{0,1\}^{n-m+\ell-1}\colon \sum_{i \in J(j,u,n-m)} y_i 1_{\mathscr{I}(i+m+1) \subseteq \mathscr{I}(n+j)} = a_j,\right. \\ \left. 0 \leqslant j \leqslant \ell - 1\right\}$$

Therefore, by using the equivalence $\mathscr{I}(n-k) \subseteq \mathscr{I}(n) \Leftrightarrow \mathscr{I}(k) \subseteq \mathscr{I}(n)$, we get for $s \geqslant 1$ and $m = n - s$,

$$\begin{aligned} g_{n,n-s,u} &= \mathbb{P}\left\{y \in \{0,1\}^{s+\ell-1}\colon \sum_{i \in J(j,u,s)} y_i 1_{\mathscr{I}(i+n-s+1) \subseteq \mathscr{I}(n+j)} = a_j,\right. \\ &\qquad \left. 0 \leqslant j \leqslant \ell - 1\right\} \\ &= \mathbb{P}\left\{y \in \{0,1\}^{s+\ell-1}\colon \sum_{i \in J(j,u,s)} y_i 1_{\mathscr{I}(s-1+j-i) \subseteq \mathscr{I}(n+j)} = a_j,\right. \\ &\qquad \left. 0 \leqslant j \leqslant \ell - 1\right\}\end{aligned}$$

Let $n, n' \in \mathbb{N}$ be such that $n = \sum_{i \geqslant 0} \beta_i 2^i$, $n' = \sum_{i \geqslant 0} \beta'_i 2^i$ with $\beta_i, \beta'_i \in \{0,1\}$ and $\beta_i = \beta'_i$ for $i \in \{0,\ldots, M(\ell,s) - 1\}$, where $M(\ell,s) = \lfloor \log_2(\ell + s) \rfloor + 1$. The integers verifying the last condition are said to be $M(\ell,s)$-compatible.

Let $n, n' \geqslant s \geqslant 1$ be a couple of $M(\ell, s)$-compatible integers. Then $g_{n, n-s, u} = g_{n', n'-s, u}$ for any $u \in \{0, 1\}^{\ell}$. In fact, if n and n' are $M(\ell, s)$-compatible then

$$\mathscr{I}(s-1+j-i) \subseteq \mathscr{I}(n+j) \Leftrightarrow \mathscr{I}(s-1+j-i) \subseteq \mathscr{I}(n'+j)$$

Therefore we obtain for $s \geqslant 1$

$$\frac{1}{N} \sum_{n=s}^{N-1} \mathbb{P}(C_{n, n-s, u}) = \lambda(u) \cdot \lambda^{s-1} \cdot (1-\lambda) \cdot \sum_{n=0}^{2^{M(\ell, s)}-1} \bar{g}_{n, s, u} \cdot \frac{\#\{s \leqslant n' \leqslant N-1 : n \text{ and } n' \text{ are } M(\ell, s)-\text{compatible}\}}{N}$$

where $\bar{g}_{n, s, u} = g_{n', n'-s, u}$ for any $n' \in \{s, ..., N-1\}$ that is $M(\ell, s)$-compatible with n. We take the limit to get

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=s}^{N-1} \mathbb{P}(C_{n, n-s, u}) = \lambda^{s-1} \cdot (1-\lambda) \cdot \lambda(u) \cdot \frac{1}{2^{M(\ell, s)}} \cdot \sum_{n=0}^{2^{M(\ell, s)}-1} \bar{g}_{n, s-u}, \qquad \text{for} \qquad s \geqslant 1$$

Observe that this limit is 0 when $R = 1$.

On the other hand, for $R > 1$

$$\frac{1}{N} \sum_{n=0}^{N-1} \mathbb{P}(C_{n, -1, u}) = \frac{1}{N} \sum_{n=0}^{N-1} \lambda^n \cdot \lambda(u) \cdot g_{n, -1, u} \leqslant \frac{1}{N} \sum_{n=0}^{N-1} \lambda^n$$

therefore its limit is 0. If $R = 1$ the limit is 0 for $u \in \{0, 1\}^{\ell} \setminus \{(1, ..., 1)\}$ and it coincides with the limit in Theorem 2 when $u = (1, ..., 1)$. This fact proves the theorem in the case $B = 0$ or $B = 1$.

Let us conclude the result of the theorem. Notice that when $\lambda \neq 1$ the series

$$\sum_{s=1}^{\infty} \lambda^{s-1} \cdot \frac{1}{2^{M(\ell, s)}} \sum_{n=0}^{2^{M(\ell, s)-1}} \bar{g}_{n, s, u}$$

exists. Furthermore, for any $N \in \mathbb{N}$ and $k \in \mathbb{N}$ we have

$$\left| \frac{1}{N} \sum_{n=k+1}^{N-1} \sum_{m=0}^{n-k-1} \mathbb{P}(C_{n, m, u}) \right| \leqslant \left| \frac{1}{N} \sum_{n=k+1}^{N-1} \sum_{m=0}^{n-k-1} \lambda^{n-1-m} \right| \leqslant \frac{1}{N} \frac{\lambda^k - \lambda^{N-1}}{(1-\lambda)(\lambda^{-1}-1)} + \frac{\lambda^{k-1}(N-1-k)}{N(\lambda^{-1}-1)}$$

Therefore,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N-1} E_n = \sum_{u \in \{0,1\}^{\ell}} (1-\lambda) \cdot \lambda(u) \cdot \sum_{s \geq 1} \lambda^{s-1} \cdot \frac{1}{2^{M(\ell,s)}} \sum_{n=0}^{2^{M(\ell,s)}-1} \bar{g}_{n,s,u}$$

which proves the theorem. ∎

ACKNOWLEDGMENTS

The authors acknowledge financial support from FONDECYT and ECOS-CONICYT. They also thank the hospitality of the Institut de Mathématiques de Luminy at February 1996 where this work began. We also thank the valuable comments of anonymous referees which allow to improve this work.

REFERENCES

[BM] F. Blanchard, A. Maass, Dynamical Properties of Expansive One-Sided Cellular Automata, *Israel Journal of Mathematics* **99**:149–174 (1997).

[C] M. Courbage, On the approach to statistical equilibrium in an infinite-particle lattice dynamic model, *J. Math. Phys.* **30(8)**:1840–1850 (1989).

[H] G. Hedlund, Endomorphisms and automorphisms of the shift dynamical systems, *Mathematical System Theory* **3**:320–375 (1969).

[K] D. E. Knuth, *The art of computer programming*, second edition, (Addison-Wesley Pub. Company, 1973).

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

[S] M. A. Shereshevsky, Ergodic Properties of Certain Surjective Cellular Automata, *Monatshefte für Mathematik* **114**:305–316 (1992).

[U-E] J. Urías, G. Salazar-Anaya, E. Ugalde, A. Enciso, Traveling Patterns in Cellular Automata, *Chaos* **6(3)**:493–503 (1996).

[W] S. Wolfram, Random Sequence Generation by Cellular Automata, *Advances in Applied Mathematics* **7**:123–169 (1986).