Commun. Math. Phys. 136, 599–605 (1991)

Communications in Mathematical Physics

On Ergodic One-Dimensional Cellular Automata*

M. Shirvani and T. D. Rogers

Department of Mathematics, University of Alberta, Edmonton, Alberta, Canada

Received May 10, 1989

Abstract. We show that all onto cellular automata defined on the binary sequence space are invariant with respect to the Haar measure, and that an extensive class of such maps (including many nonlinear ones) are strongly mixing with respect to the Haar measure.

I. Introduction

Let X denote the space of bi-infinite sequences $a=(a_i)_{i\in\mathbb{Z}}$, where each $a_i=0$ or 1, regarded as a compact abelian group under component-wise addition. Denote the normalized Haar measure on X by μ. Let σ be the shift map defined by $\sigma(a)_i=a_{i+1}$ for all $i\in\mathbb{Z}$ and all $a\in X$. If $f\colon\{0,1\}^n\to\{0,1\}$ is a Boolean function of n variables and $r\leqq s$ are fixed integers with $s-r=n+1$, then we write f_∞ for the corresponding cellular automaton: $f_\infty(a)_i=f(a_{i+r},\ldots,a_{i+s})$ for all $i\in\mathbb{Z}$. Surjective such maps have been analyzed in great detail from both the combinatorial and the topological points of view [1, 3, 8]. We characterize those f_∞ which preserve the Haar measure [i.e. $\mu(f_\infty^{-1}(A))=\mu(A)$ for all measurable subsets A of X] in Theorem 2.4, in particular showing that f_∞ is onto if and only if it preserves the Haar measure. (The latter result was announced by J. Milnor in [2].) We show further that certain of the f_∞ are actually ergodic with respect to μ (Theorems 3.2 and 3.4), although our results here are not complete since we suspect that all onto one-dimensional cellular automata (with the exception of the identity and the inversion map) are ergodic with respect to μ. Nonetheless, 3.4 shows that certain nonlinear automata considered by Wolfram in [7, Chap. 2.3], are in fact strongly mixing. To our knowledge these are the first examples of nonlinear ergodic automata in the literature.

* This work was supported in part by grants from NSERC of Canada

II. Measure-Preserving Maps

We begin by defining a class of open sets which will be extensively used in what follows. Let $k=\{0,1\}$ be the field of two elements, and let $R=k[x_i : i\in\mathbb{Z}]$ denote the free k-algebra in the commuting variables x_i subject to the relations $x_i^2=x_i$ for all i. (In other words R is the quotient of the polynomial algebra $k[X_i : i\in\mathbb{Z}]$ by the ideal generated by all the polynomials $X_i^2-X_i$.) It is well-known (and trivial to prove) that every Boolean function in a finite number of variables can be regarded as an element of R. (To be more precise, disjunction, conjunction and negation are defined as follows: $p\cup q=p+q+pq$, $p\cap q=pq$, and $p'=1+p$, where the operations on the right-hand side are the ring operations.)

If $p=p(x_i,\ldots,x_j)\in R$ (it is understood that $i\leqq j$) and $a\in X$ define $p(a)$ to be $p(a_i,\ldots,a_j)$, and let

$$V(p)=\{a\in X : p(a)=0\}.$$

Clearly every $V(p)$ is a finite disjoint union of cylinder sets, and conversely every cylinder set is of the form $V(p)$ for some $p\in R$ [e.g. the cylinder set $\{a\in X : a_0=1$ and $a_1=0\}$ is $V(1+x_0+x_0x_1)$]. The following properties of $V(p)$ are easy to verify.

2.1. Lemma. *Let $p, q\in R$. Then*

(i) $X-V(p)=V(1+p)$.
(ii) $V(pq)=V(p)\cup V(q)$.
(iii) $V(p\cup q)=V(p)\cap V(q)$.
(iv) $V(p)=V(q)$ *if and only if* $p=q$.
(v) $V(p)\subseteqq V(q)$ *if and only if* $q(a)\leqq p(a)$ *for all* $a\in X$. □

Given $p\in R$, where $p=p(x_i,\ldots,x_j)$, write $\operatorname{supp}(p)=\{x_m : i\leqq m\leqq j\}$, $|p|=j-i+1=$ the number of variables in $\operatorname{supp}(p)$, and $r(p)=$ the number of roots of p, i.e. the number of vectors $(b_1,\ldots,b_r)$ (where $r=j-i+1$) such that $p(b_1,\ldots,b_r)=0$. [There is some ambiguity about the number of variables involved in a polynomial p, and so in the above definitions. For example $p=x_1x_2$ can also be written $p=x_0+x_1x_2+x_0$, thereby changing $\operatorname{supp}(p)$, $|p|$, and $r(p)$. In what follows, however, no contradiction will arise if it is borne in mind that the determination of the above quantities refers to a *fixed* representation of a Boolean function as a polynomial in R.] For example if $p=x_0+x_2$ then $|p|=3$ (regarding p as a function of x_0, x_1, and x_2) and $r(p)=4$ [since there are four vectors (b_1,b_2,b_3) with $b_1+b_3=0$].

We can now determine the measure of the sets $V(p)$.

2.2. Lemma. *Let $p, q\in R$. Then:*

(i) $\mu(V(p))=r(p)2^{-|p|}$.
(ii) *If* $\operatorname{supp}(p)\cap\operatorname{supp}(q)=\phi$ *then* $\mu(V(p)\cap V(q))=\mu(V(p))\mu(V(q))$.
In particular $\mu(V(x_{i_1}\cup\ldots\cup x_{i_r}))=2^{-r}$.

Proof. (i) If $p=p(x_i,\ldots,x_j)$ then clearly $V(p)$ is the union of $r(p)$ disjoint cylinder sets [each being the set of all $a\in X$ such that $(a_i,\ldots,a_j)$ is equal to one of the $r(p)$ roots of p]. Since each such cylinder set has measure $2^{-|p|}$ we have the result.
(ii) The condition $\operatorname{supp}(p)\cap\operatorname{supp}(q)=\phi$ means that p and q have no variable in common, so the number of roots of $p\cup q$ is $r(p)r(q)$, and $|p\cup q|=|p|+|q|$. Thus by 2.1 and part (i),

$$\mu(V(p)\cap V(q))=\mu(V(p\cup q))=r(p\cup q)2^{-|p\cup q|}=\mu(V(p))\mu(V(q)).$$ □

The shift automorphism σ acts on R in the obvious way: if $p=p(x_i,\ldots,x_j)$ then $p\sigma=p(x_{i+1},\ldots,x_{j+1})$, and clearly $(p\sigma)(a)=p(\sigma(a))$ for all $a\in X$ (the use of the same letter to denote the shifts on X and R should cause no confusion). It is also obvious that

$$V(p\sigma)=\sigma^{-1}(V(p)) \quad \text{for all } p\in R.$$

Given an element $f\in R$ define an algebra homomorphism $\theta_f: R\to R$ as follows: $\theta_f(x_i)=f\sigma^i$ for all $i\in\mathbb{Z}$ and θ_f is extended multiplicatively and linearly to all of R. In other words if $p=p(x_i,\ldots,x_j)$ then $\theta_f(p)=p(f\sigma^i,\ldots,f\sigma^j)$. In particular $f=\theta_f(x_0)$.

Given $f\in R$ define $f_\infty: X\to X$ by $f_\infty(a)_i=f(\sigma^i(a))$ for all $i\in\mathbb{Z}$ and all $a\in X$ [so if $f=f(x_r,\ldots,x_s)$ then $f_\infty(a)_i=f(a_{i+r},\ldots,a_{i+s})$]. It is well-known that f_∞ is continuous and commutes with σ (cf. Hedlund [3]). If $f, g\in R$ [say $f=f(x_r,\ldots,x_s)$] then

$$\begin{aligned} f_\infty(g_\infty(a))_i &= f(\sigma^i(g_\infty(a))) = f(g_\infty(\sigma^i a)) \\ &= f(g_\infty(\sigma^i a)_r,\ldots,g_\infty(\sigma^i a)_s) = f(g(\sigma^{i+r}a),\ldots,g(\sigma^{i+s}a)). \end{aligned}$$

Put $h=\theta_g(f)=f(g\sigma^r,\ldots,g\sigma^s)$. Then

$$h_\infty(a)_i=h(\sigma^i a)=f(g\sigma^r(\sigma^i a),\ldots,g\sigma^s(\sigma^i a))=f_\infty(g_\infty(a))_i.$$

We have shown that

$$f_\infty g_\infty=(\theta_g(f))_\infty \quad \text{for all } f, g\in R,$$

and in particular

$$f_\infty^n=(\theta_f^n(x_0))_\infty.$$

We also have the following result:

2.3. Lemma. *For all $p\in R$,*

$$f_\infty^{-1}(V(p))=V(\theta_f(p)).$$

Proof. Suppose $p=p(x_i,\ldots,x_j)$. Then

$$\begin{aligned} a\in f_\infty^{-1}(V(p)) &\Leftrightarrow f_\infty(a)\in V(p)\Leftrightarrow p(f_\infty(a))=0 \\ &\Leftrightarrow p(f_\infty(a)_i,\ldots,f_\infty(a)_j)=0\Leftrightarrow p(f\sigma^i(a),\ldots,f\sigma^j(a))=0 \\ &\Leftrightarrow \theta_f(p)(a)=0\Leftrightarrow a\in V(\theta_f(p)). \quad \square \end{aligned}$$

We can now prove the equivalence of onto-ness and measure-preservation, and at the same time provide an algorithm for determining whether a map is measure-preserving:

2.4. Theorem. *For $f\in R$ the following are equivalent:*

(i) *f_∞ is measure-preserving.*

(ii) *f_∞ is onto.*

(iii) *For all integers $i_1, i_2,\ldots$ with $i_1<i_2<\ldots<i_r$ we have*

$$\mu(V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_r}))=2^{-r}.$$

(iv) *For all non-negative integers $i_1, i_2,\ldots$ with $0=i_1<i_2<\ldots<i_r$ we have*

$$\mu(V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_r}))=2^{-r}.$$

Proof. (i)$\Rightarrow$(ii): In general $f_\infty(X)$ is a closed subset of X since f_∞ is continuous and X is compact. Further, since f_∞ is measure-preserving we have $\mu(f_\infty(X))=\mu(f_\infty^{-1}(f_\infty(X)))=\mu(X)=1$, so $f_\infty(X)$ is dense in X. Therefore $f_\infty(X)=X$.

(ii)⇒(iii): Since σ is a measure-preserving homeomorphism of X and $f_\infty\sigma^k=(f\sigma^k)_\infty$, by applying a suitable power of σ to f we may assume that $f=f(x_1,\ldots,x_m)$ for some $m\geqq 1$. Also since

$$\mu(V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_r}))=\mu(V(f)\sigma^{-i_1}\cap\ldots\cap V(f\sigma^{i_r-i_1})\sigma^{-i_1})$$
$$=\mu(V(f)\cap\ldots\cap V(f\sigma^{i_r-i_1}))$$

we may assume that $i_1=0$. Put $p=f\sigma^{i_1}\cup\ldots\cup f\sigma^{i_r}$ and $i=i_r$, so we need to show that $\mu(V(p))=2^r$. Consider the set T of all $(i+1)$-dimensional vectors $b=b_0\ldots b_i$, where $b_j=0$ if $j\in\{i_1,\ldots,i_r\}$, and $b_j\in\{0,1\}$ is arbitrary otherwise. Clearly the cardinality of T is $|T|=2^{i+1-r}$. As in [3] define the map $f_i:\{0,1\}^{i+m}\to\{0,1\}^{i+1}$ as follows: given $a=(a_1,\ldots,a_{i+m})$ let $f_i(a)=(f(a_1,\ldots,a_m),\ f(a_2,\ldots,a_{m+1}),\ldots,$ $f(a_{i+1},\ldots,a_{i+m}))$. Observe that $f_i(a)\in T$ if and only if $f(a_{1+i_k},\ldots,a_{m+i_k})=0$ for $k=1,\ldots,r$. On the other hand, for $u\in X$ we have $u\in V(p)$ if and only if $f\sigma^{i_k}(u)=0$ for $1\leqq k\leqq r$, which happens if and only if $f(u_{1+i_k},\ldots,u_{m+i_k})=0$ for $1\leqq k\leqq r$. In other words, $u\in V(p)$ if and only if $u_1\ldots u_{i+m}\in\bigcup_{b\in T} f_i^{-1}(b)=f_i^{-1}(T)$. By Theorem 5.4 of [3], the onto-ness of f_∞ implies that each $f_i^{-1}(b)$ has cardinality 2^{m-1}, and so $|f_i^{-1}(T)|=2^{m-1}\times 2^{i+1-r}=2^{m+i-r}$. It is now clear that $\mu(V(p))=2^{i+m-r}/2^{i+m}=2^{-r}$, as required.

(iii)⇒(iv) is trivial.

(iv)⇒(iii): This is proved by induction on r, the case $r=1$ being equivalent to $\mu(V(f))=1/2$. In general since

$$V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_r})=[V(f)\cap\ldots\cap V(f\sigma^{i_r-i_1})]\sigma^{-i_1},$$

we may assume that $i_1=0$. If $i_r\geqq|f|$ then $\operatorname{supp}(f)\cap\operatorname{supp}(f\sigma^{i_r})=\phi$, so by 2.2 (ii) we have

$$\mu(V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_r}))=\mu(V(f\sigma^{i_1})\cap\ldots\cap V(f\sigma^{i_{r-1}}))\mu(V(f\sigma^{i_r}))$$
$$=2^{-(r-1)}\times 2^{-1}=2^{-r},$$

by the inductive hypothesis. If $i_r<|f|$ then the inductive step is given directly by (iv).

(iii)⇒(i): Take any $u\in\{0,1\}$, and consider the function $p_u=(x_{i_1}+u_1)\cup\ldots$ $\cup(x_{i_r}+u_r)$, where $i_1<\ldots<i_r$ are arbitrary integers. Then $p_u(u)=0$ and $p_u(v)=1$ if $v\neq u$. We claim that $\mu(f_\infty^{-1}(V(p_u)))=\mu(V(p_u))=2^{-r}$ if (iii) holds. If every $u_i=0$ then this is simply (iii). As an example of what happens when some of the u_i are nonzero, consider the case where only $u_1=1$. If $p=x_{i_1}\cup\ldots\cup x_{i_r}$ and $q=x_{i_2}\cup\ldots\cup x_{i_r}$, then $pp_u=q$, so $V(p)\cup V(p_u)=V(q)$ and hence $f_\infty^{-1}(V(p))\cup f_\infty^{-1}(V(p_u))=f_\infty^{-1}(V(q))$. Since the union is disjoint and $f_\infty^{-1}(V(p))$ and $f_\infty^{-1}(V(q))$ have measure 2^{-r} and $2^{-(r-1)}$ respectively [by (iii)] we obtain $\mu(f_\infty^{-1}(V(p_u)))=2^{-r}$. Similarly reasoning establishes the result for all u. For a general $p\in R$ it is clear that $V(p)$ is the disjoint union of the $V(p_u)$, where u ranges over the $r(p)$ roots of p. Since $\mu(f_\infty^{-1}(V(p_u)))$ $=2^{-|p|}$ for each u we get $\mu(f_\infty^{-1}(V(p)))=r(p)2^{-|p|}=\mu(V(p))$. Finally since the $V(p)$ generate the Borel σ-algebra of X it follows that f_∞ is measure-preserving. □

2.5. Remark. Theorem 2.4 provides an effective algorithm for deciding whether a given f_∞ is onto: let $m=|f|-1$. Then f_∞ is onto if and only if $f_m:\{0,1\}^{2m+1}$ $\to\{0,1\}^{m+1}$ is an exactly 2^m-to-1 map. It is known [8] that the onto-ness of a cellular automaton in dimensions higher than 1 is undecidable.

For example it can be verified that the only measure-preserving cellular automata f_∞ with $f=f(x_1,x_2,x_3)$ are the following ($c=0$ or 1): $c+x_1$, $c+x_2$,

$c+x_3$, $c+x_1+x_2$, $c+x_1+x_3$, $c+x_2+x_3$, $c+x_1+x_2+x_3$, $c+x_1+x_2x_3$, $c+x_1+x_2+x_2x_3$, $c+x_1+x_3+x_2x_3$, $c+x_1+x_2+x_3+x_2x_3$, $c+x_3+x_1x_2$, $c+x_3+x_1+x_1x_2$, $c+x_3+x_2+x_1x_2$, $c+x_3+x_1+x_2+x_1x_2$.

It is perhaps worth mentioning that if f_∞ is not onto, then $f_\infty(X)$ has measure 0. For $f_\infty(X)$ is always a closed subset of X, and clearly $\sigma^{-1}(f_\infty(X))=f_\infty(\sigma^{-1}(X))=f_\infty(X)$. Since σ^{-1} is ergodic it follows that $f_\infty(X)$ has measure 0 or 1, and if f_∞ is not onto then $\mu(f_\infty(X))\neq 1$, as claimed.

III. Ergodicity

Throughout this section $f=f(x_r,\ldots,x_s)$ is a fixed element of R. In contrast to the property of being measure-preserving, ergodicity and the various forms of mixing are shift-dependent, in the sense that f_∞ and $f_\infty\sigma$ may have different properties (think of the identity map). We begin with the following lemma:

3.1. Lemma. *Let $p=p(x_i,\ldots,x_j)\in R$, and let $n\geqq 0$. Then*

$$\operatorname{supp}(\theta_f^n(p))\subseteqq\{x_k: i+nr\leqq k\leqq j+ns\}.$$

Proof. Since $f\sigma^k=f(x_{r+k},\ldots,x_{s+k})$, we have $\theta_f(p)=p(f\sigma^i,\ldots,f\sigma^j)=p(f(x_{i+r},\ldots,x_{j+r}),\ldots,f(x_{i+s},\ldots,x_{j+s}))$, so $\operatorname{supp}(\theta_f(p))\subseteqq\{x_{r+i},\ldots,x_{s+j}\}$. The result follows by induction on n. □

We now come to our first result concerning the ergodicity of the f_∞. It is in fact easier to prove that f_∞ is strongly mixing [i.e. $\mu(A\cap f_\infty^{-n}(B))\to\mu(A)\mu(B)$ as $n\to\infty$ for all measurable subsets A and B of X] and to deduce ergodicity from this ([4], p. 142).

3.2. Theorem. *Let $f=f(x_r,\ldots,x_s)$, where either $0<r\leqq s$ or $r\leqq s<0$, and assume that f_∞ is onto. Then for all $p_0,p_1\in R$ we have $\mu(V(p_0)\cap f_\infty^{-n}(V(p_1)))=\mu(V(p_0))\mu(V(p_1))$ for all sufficiently large n. In particular f_∞ is strongly mixing and hence ergodic.*

Proof. Consider first the case $0<r\leqq s$, and suppose $\operatorname{supp}(p_i)=\{x_k:\alpha_i\leqq k\leqq\beta_i\}$ for $i=0,1$. By 3.1 we have $\operatorname{supp}(\theta^n(p_1))\subseteqq\{x_k:\alpha_1+nr\leqq k\leqq\beta_1+ns\}$. Since $r>0$, for all sufficiently large n we have $\beta_0<\alpha_1+rn$, which implies that p_0 and $\theta^n(p_1)$ have disjoint supports. By 2.2(ii) this implies that

$$\begin{aligned}\mu(V(p_0)\cap f_\infty^{-n}(V(p_1)))&=\mu(V(p_0)\cap V(\theta^n(p_1)))=\mu(V(p_0))\mu(V(\theta^n(p_1)))\\&=\mu(V(p_0))\mu(V(p_1)),\end{aligned}$$

the finally equality following from the fact that f_∞ is measure-preserving, by 2.4.

The case $r\leqq s<0$ can be established analogously, since $\beta_1+ns<\alpha_0$ for all sufficiently large n. □

Question 1. Is f_∞ above m-mixing for all $m\geqq 1$? The method of proof does not allow us to establish this fact. When f_∞ is a linear map then it is known that f_∞ is m-mixing for all $m\geqq 1$, cf. [5].

We can also say something about those maps f for which the conditions on r and s stipulated in 3.2 do not hold. For brevity we introduce the following terminology: let $p=p(x_i,\ldots,x_j)\in R$. Say p *has k roots in* $[i,j]$ if there are exactly k vectors $u=(u_i,u_{i+1},\ldots,u_j)$ for which $p(u)=0$. We need the following.

3.3. Lemma. *Let $r<\alpha<\beta$ and $s>r$ be given integers, and consider the polynomial*

$$h=[x_r+g(x_{r+1},\ldots,x_s)]\cup p(x_\alpha,\ldots,x_\beta),$$

where $p, g\in R$ and p has k roots in $[\alpha,\beta]$. Then h has

$$k2^{\alpha-r-1} \quad \text{roots in } [r,\beta], \quad \text{if} \quad s\leqq\beta,$$

$$k2^{\alpha-r+s-\beta-1} \quad \text{roots in } [r,s], \quad \text{if} \quad \beta<s.$$

Proof. Consider first the case $s\leqq\beta$. If $u=(u_r,\ldots,u_\alpha,\ldots,u_\beta)$ is a root of h then $(u_\alpha,\ldots,u_\beta)$ is a root of p, so there are k possibilities for $(u_\alpha,\ldots,u_\beta)$. Now for every choice of a root $(u_\alpha,\ldots,u_\beta)$ of p and every arbitrary choice of $u_{r+1},\ldots,u_{\alpha-1}$ we get a unique root of h by setting $u_r=g(u_{r+1},\ldots,u_{\alpha-1})$. Thus the number of roots of h is $k2^{(\alpha-1)-(r+1)+1}=k2^{\alpha-r-1}$. Similarly in the case $\beta<s$, if $(u_r,\ldots,u_s)$ is a root of h then $(u_\alpha,\ldots,u_\beta)$ must be a root of p, $u_{r+1},\ldots,u_{\alpha-1}$ and $u_{\beta+1},\ldots,u_s$ (whence the factor of $2^{s-\beta}$) can be chosen arbitrarily, and $u_r=g(u_{r+1},\ldots,u_s)$. This proves the second formula. □

Our next result has some affinity to a result of Willson [6, Theorem A]:

3.4. Theorem. *Let $f=f(x_r,\ldots,x_s)$, and assume that either f is permutive in x_r and $r<0\leqq s$, or f is permutive in x_s and $r\leqq 0<s$. Then for all $p_0,p_1\in R$ we have $\mu(V(p_0)\cap f_\infty^{-n}(V(p_1)))=\mu(V(p_0))\mu(V(p_1))$ for all sufficiently large n. In particular f_∞ is strongly mixing and hence ergodic.*

Proof. Assume, for definiteness sake, that f is permutive in x_r, say $f=x_r+g(x_{r+1},\ldots,x_s)$, where $r<0\leqq s$. Since $f=\theta_f(x_0)$, it is easy to prove by induction on n, that

$$\theta^n(x_m)=x_{nr+m}+g_n(x_{nr+m+1},\ldots,x_{ns+m}),$$

for some $g_n\in R$. We may clearly assume that $V(p_0)$ and $V(p_1)$ are cylinder sets, say $p_0=x_{i_1}\cup\ldots\cup x_{i_l}$ and $p_1=x_{m_1}\cup\ldots\cup x_{m_k}$. Since $r<0$ we may choose n sufficiently large so that $nr+1<i_1<\ldots<i_l\leqq ns+m_k$. [In the case $s=0$ we may clearly assume that $i_l\leqq m_k$, since those x_{i_t} with $i_t>m_k$ can be disposed of by means of 2.2 (ii) as they do not appear in any of the $\theta^n(x_{m_i})$.] We have to find the number of roots of

$$h_1=[x_{rn+m_1}+g_n(x_{rm+m_1+1},\ldots,x_{sn+m_1})]\cup\ldots$$
$$\cup[x_{rn+m_k}+g_n(x_{rn+m_k+1},\ldots,x_{sn+m_k})]\cup p_0.$$

Consider

$$h_k=[x_{rn+m_k}+g_n(x_{rn+m_k+1},\ldots,x_{sn+m_k})]\cup p_0.$$

The number of roots of $p_0=x_{i_1}\cup\ldots\cup x_{i_l}$ in $[i_1,i_l]$ is clearly $k=2^{i_l-i_1+1-l}$, and so the second formula of 3.3 gives the number of roots of h_k in $[nr+m_k, ns+m_k]$ as

$$2^{i_l-i_1+1-l}\times 2^{i_1-1-(rn+m_k)+sn+m_k-i_l}=2^{sn-rn-l}.$$

Next consider

$$h_{k-1}=[x_{rn+m_{k-1}}+g_n(x_{rn+m_{k-1}+1},\ldots,x_{sn+m_{k-1}})]\cup h_k.$$

By the first formula of 3.3, the number of roots of h_{k-1} in $[rn+m_{k-1}, sn+m_k]$ is

$$2^{sn-rn-l}\times 2^{rn+m_k-1-(rn+m_{k-1})}=2^{sn-rn-l-1+m_k-m_{k-1}}.$$

Inductively the number of roots of

$$h_{k-t}=[x_{rn+m_{k-t}}+g_n(x_{rn+m_{k-t}+1},\ldots,x_{sn+m_{k-t}})]\cup h_{k-t+1}$$

in $[rn+m_{k-t}, sn+m_k]$ is $2^{sn-rn-l-t+m_k-m_{k-t}}$. In particular for $t=k-1$ we find that the number of roots of h_1 in $[rn+m_1, sn+m_k]$ is $s(h_1)=2^{sn-rn-l-k+1+m_k-m_1}$. Thus

$$\mu(V(h_1))=s(h_1)/2^{sn+m_k-(rn+m_1)+1}=s^{-l-k}=\mu(V(p_0))\mu(V(p_1)),$$

as claimed. The proof of the other case is entirely analogous.

3.5. Corollary. *All one-dimensional affine cellular automata f_∞ (i.e. those with $f=c+x_r+\ldots+x_s$, $c=0$ or 1) except the identity ($f=x_0$) and the inversion ($f=1+x_0$) are strongly mixing and hence ergodic.*

Proof. In all cases other than the ones excluded in the statement, one of 3.2 or 3.4 will apply. □

Question 2. Are all onto one-dimensional cellular automata (other than the identity and the inversion maps), strongly mixing?

It is perhaps worth mentioning that by 3.2, Wolfram's nonlinear rules $30(f=x_{-1}+x_0+x_1+x_0x_1)$ and $45(f=1+x_{-1}+x_0+x_1+x_0x_1)$ are now known to be strongly mixing. In [7, Paper 2.3], he studies the former map, particularly from the point of view of its potential as a random sequence generator.

References

1. Amoroso, S., Patt, Y.N.: Decision procedures for surjectivity and injectivity of parallel maps for tesselation structures. J. Comput. Syst. Sci. **6**, 448–464 (1972)
2. Bienenstock, E., Fogelman Soulié, F., Weisbuch, G. (eds.): Disordered systems and biological organization. Berlin, Heidelberg, New York: Springer 1986
3. Hedlund, G.A.: Endomorphisms and automorphisms of the shift dynamical system. Math. Syst. Theory **3**, 320–375 (1970)
4. Mañé, R.: Ergodic theory and differentiable dynamics. Berlin, Heidelberg, New York: Springer 1987
5. Shirvani, S., Rogers, T.D.: Ergodic endomorphisms of compact abelian groups. Commun. Math. Phys. **118**, 401–410 (1988)
6. Willson, S.J.: On the ergodic theory of cellular automata. Math. Syst. Theory **9**, 132–141 (1975)
7. Wolfram, S. (ed.): Theory and applications of cellular automata. Singapore: World Scientific 1986
8. Yaku, T.: The constructibility of a configuration in a cellular automator. J. Comp. Syst. Sci. **7**, 481–496 (1973)

Communicated by J.-P. Eckmann