A SHORT PROOF OF A RIGIDITY RESULT FOR CELLULAR AUTOMATA

ITALO CIPRIANO

Abstract. It is known that for p a prime number, the Haar measure on $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ is the unique ergodic shift invariant measure, which is also invariant and with positive entropy for $F : (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ defined by $F(x)_i = ax_i + bx_{i+1} + c$ for all $i \in \mathbb{N}$, where $a, b \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ and $c \in \mathbb{Z}/p\mathbb{Z}$. We propose a proof using only the decomposition of a measure in its Fourier coefficients and the Birkhoff Ergodic Theorem.

1. Introduction

Let p be a prime number and $\mathbb{Z}/p\mathbb{Z}$ be the set of integers modulo p with the sum and multiplication modulo p.

Denote by $X \doteq (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ the set of all sequences of scalars

$$(x_n)_{n\in\mathbb{N}},\ x_n \in \mathbb{Z}/p\mathbb{Z}.$$

This is a vector space for

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} \stackrel{\text{def}}{=} (x_n + y_n)_{n\in\mathbb{N}}$$

and

$$\alpha(x_n)_{n\in\mathbb{N}} \stackrel{\text{def}}{=} (\alpha x_n)_{n\in\mathbb{N}}.$$

The set X is also metric space with the metric defined by

$$d((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) = 2^{-\inf\{i\in\mathbb{N} | x_i \neq y_i\}}.$$

In dynamical systems, the most studied continuous map from X to itself is the shift, denoted by σ and defined by $\sigma(x)_i = x_{i+1}$ for all $i \in \mathbb{N}$. A cellular automaton is a continuous map from X to itself that commutes with σ. A very special class, in which we know the set of preimages of any element in $x \in X$, corresponds to those maps $F : X \to X$ defined by $F(x)_i = ax_i + bx_{i+1} + c$ for all $i \in \mathbb{N}$, where $a, b \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ and $c \in \mathbb{Z}/p\mathbb{Z}$. They are commonly called linear cellular automata and we will always denote them by F. Clearly any cellular automaton in this family is p-to-1. Notice also that the shift is the cellular automaton corresponding to taking $a = 0, b = 1, c = 0$ in

Date: March 26, 2014.

the definition of F, so it is not in the family of linear cellular automata.

A measure μ on X is uniquely determined by its values on the cylinder sets

$$[x]_k \stackrel{\text{def}}{=} (\mathbb{Z}/p\mathbb{Z})^{k-1} \times \{x_1\} \times \{x_2\} \times \cdots \times \{x_n\} \times X,$$

in which $n, k \in \mathbb{N}$, $x = (x_1, x_2, \ldots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ and $\mathbb{Z}/p\mathbb{Z}$ appears $k-1$ times on the left side of $\{x_1\}$. For example, on X, any vector $(1-q, q)$ such that $0 < q < 1$ defines a measure by setting $\mu_{1-q,q}([x]_k) = \frac{1}{(1-q)^{n_1} q^{n_2}}$, in which n_1 is the number of 0's in x and n_2 the numbers of 1's. This example illustrates the importance of the condition $a \neq 0$ in the definition of F. The Haar measure H on X is defined by

$$H([x]_k) = \frac{1}{p^n},$$

in which $n, k \in \mathbb{N}$ and $x = (x_1, x_2, \ldots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n$.

Given a measure μ on X and a transformation $G : X \to X$, we define the induced measure $G_*\mu(A) = \mu(G^{-1}(A))$. We will say that μ is invariant for G if $G_*\mu = \mu$. For example, $\sigma_*\mu_{1-q,q} = \mu_{1-q,q}$, $\sigma_* H = H$ and $F_* H = H$, where the last identity comes from the fact that F is p-to-1.

In [HMM03], using a "probabilistic approach", it was proved that

Theorem 1.1 ([HMM03], Host, Maass and Martínez)**.** *Let be $F : X \to X$ a linear cellular automata, let be μ a probability measure on X such that $F_*\mu = \mu$ and $\sigma_*\mu = \mu$. Assume that $h_\mu(F) > 0$ and μ is ergodic for σ. Then μ is the Haar measure.*

Let us now change the setup and state an analogous theorem. Define $\mathbb{T}$ to be the set of real numbers modulo 1. For $d \in \{2, 3\}$ define the maps $f_d : \mathbb{T} \to \mathbb{T}$, $x \mapsto dx$ modulo 1 and given a measure μ on $\mathbb{T}$ define the induced measure by f_d by $f_{d*}\mu(A) \doteq \mu(f_d^{-1} A)$.

Theorem 1.2 (Weak version of Rudolph' s theorem)**.** *Let μ be a measure on $\mathbb{T}$ such that $f_{2*}\mu = \mu$ and $f_{3*}\mu = \mu$ Assume that $h_\mu(f_2) > 0$ and μ is ergodic for f_3. Then μ is the Lebesgue measure.*

We will prove Theorem 1.1 by imitating a proof by A. Avila of Theorem 1.2 that appears in Matheus Weblog on the webpage Disquisitiones Mathematicae (see [Mat09]). Our goal is therefore to translate the following procedure. The assumption $h_\mu(f_2) > 0$ implies that there exists a map $T : \mathbb{T} \to \mathbb{T}$ such that $T \neq id$, $T^2 = id$ and $T_*\mu = \mu$. Here it is trivial to see that $T : x \mapsto x + \frac{1}{2}$ modulo 1. This is enough to prove Theorem 1.2, because using the Fourier coefficients $\widehat{\mu}$ of μ, we can prove that for m a strictly positive integer and n, s any pair of non zero integers numbers,

$$T_*\mu = \mu \Rightarrow \widehat{\mu}(2n+1) = \widehat{T_*\mu}(2n+1) = e^{in}\widehat{\mu}(2n+1)$$

and

$$f_{2*}\mu = \mu \Rightarrow \widehat{\mu}(2^m s) = \widehat{\mu}(s).$$

The two conditions together imply that $\widehat{\mu}(k) = 0$ for all $k \in \mathbb{Z} - \{0\}$, and therefore μ is the Lebesgue measure.

Imitating this, to prove the Theorem 1.1, we will use the assumption $h_\mu(F) > 0$ to construct a transformation $T : \mathbb{T} \to \mathbb{T}$ such that $T^k \neq id$ for $k \in \{1, 2, \ldots, p-1\}$, $T^p = id$ and $T_*\mu = \mu$. This is the first time in which we use the fact that our cellular automaton is linear, basically because we need to understand how to permute the p elements in the preimages of each point. After this, using $T_*\mu = \mu$ (for which is important that p is prime), we will prove that $\widehat{\mu}(\xi) = 0$ on some ξ's (analogous to the previous odd number case), again we will require the linearity of the cellular automaton. The remaining part of the proof consists of proving that in fact $\widehat{\mu}(\xi) = 0$ on all $\xi \neq 0$, this problem is reduced to proving that $\widehat{\mu}([x_1]_1) = 0$ for all $x_1 \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, and we will prove it using that $F_*\mu = \mu$ (analogue to the reduction of the even case from the odd when using $f_{2*}\mu = \mu$), in this part is when we will use more strongly the linearity of the cellular automaton.

Up to date, as far as I know, the Theorem 1.1 has been generalised to any cellular automaton $\tilde{F} : \mathcal{A} \to \mathcal{A}$ in which $\mathcal{A}$ is a finite group and $\tilde{F}$ is defined by $\tilde{F}(x)_i = a_1 x_i + a_2 x_{i+1} + \ldots + a_n x_{i+n-1} + c$ for all $i \in \mathbb{N}$, in which $n \in \mathbb{N}$ is fixed and $\{a_i\}_{i=1}^n \subset \mathcal{A}$. By imposing some extra conditions is still being possible to obtain unicity of the invariant measure (see [Sab07]). However, no progress has been done when lacking of linearity (in this more general setting) of the cellular automaton $\tilde{F}$.

2. Main Result

The maps F and σ induce a very "rigid structure" on X, and this is the main reason of measure rigidity.

Lemma 2.1 (Structural Rigidity). *The map F is p-to-1 and there exists a transformation $T : X \to X$ that permutes the p preimages by F of each element $x \in X$. Moreover, T commutes with σ and it has the* *explicit formula $T : x \mapsto x + d$ with $d \in X$, a constant that depend on a and b in the definition of F.*

Proof. To prove the result we are going to find T inductively. First choose any $x \in X$. Find $F^{-1}x = \{x^i\}_{i=0}^{p-1}$ such that $x_i^{i-1} = i$ for any $i \in \{0, 1, \ldots, p-1\}$. By induction on the coordinates number, it is straightforward to prove that for $i \in \{0, 1, \ldots, p-1\}$, $k \in \mathbb{N}$, we have that $x_k^{i+1} = x_k^i + (-b^{-1}a)^k$. By choosing $d \in X$ such that for $k \in \mathbb{N}$, $d_k = (-b^{-1}a)^{k-1}$, it is well defined $T : z \mapsto z + d$ if $z \in F^{-1}x$. We can repeat the same for any $x' \in X$ and define T in the same way in $F^{-1}x'$. It is clear that the transformation T in such a way constructed commutes with the shift and it is defined by $x \in X \mapsto x + d \in X$. $\square$

The next Lemma is true when we are working on $\mathbb{Z}/p\mathbb{Z}$ with p prime. The reason is that we have the following remark.

Remark 2.2. *If we have a permutation π of a set P of cardinality p for p a prime number, then for any $x \neq y \in P$, there exists $n < p$ such that $\tilde{\pi} \doteq \pi^n$ is a permutation of P such that $\tilde{\pi}x = y$.*

Lemma 2.3. *If μ is an ergodic shift invariant measure and $h_\mu(F) > 0$, then $\tilde{T}_*\mu = \mu$, where $\tilde{T} = T^k$ for some $k \in \{1, 2, \ldots, p-1\}$.*

Proof. We have that $h_\mu(F) > 0$ implies that the transformation F is μ-a.s. not 1-to-1. By the pigeonhole principle there must to be at least two disjoint sets A_i, A_j with $i < j < p$ and strictly positive $\mu-$measures such that $T^{j-i} : A_i \to A_j$ is 1-to-1 and onto. Define $\tilde{T} \doteq T^{j-i}$. Remark 2.2 allows to see that $\tilde{T}$ behaves like T, indeed $\tilde{T} : x \mapsto x + (j-i)d$.

The supports of μ and $\tilde{T}_*\mu$ are not disjoint, because if A is a Borelian set such that $\mu(A) = 1$, then $\tilde{T}_*\mu(A) \geq \tilde{T}_*\mu(A_j) = \mu(A_i) > 0$. Also σ is $\tilde{T}_*\mu$-ergodic, because if A is a Borelian set such that $\sigma^{-1}A = A$, then $\tilde{T}^{-1}\sigma^{-1}A = \tilde{T}^{-1}A$ and $\tilde{T}^{-1}\sigma^{-1}A = \sigma^{-1}\tilde{T}^{-1}A$, therefore by μ-ergodicity of σ we have that $\tilde{T}_*\mu(A) = 0$ or 1. By a corollary of Birkhoff ergodic theorem we conclude that $\tilde{T}_*\mu = \mu$. $\square$

Remember that the Fourier coefficients of a measure μ on X are defined for each $s \in \mathbb{N}$ and $\xi \in (\mathbb{Z}/p\mathbb{Z})^n$ with $n \in \mathbb{N}$ as

$$\widehat{\mu}([\xi]_s) \doteq \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^n} \mu([x]_s) w^{\xi^t x}, \text{ where } w \doteq e^{\frac{2\pi i}{p}}.$$

Lemma 2.4. *If μ is an ergodic shift invariant measure, $h_\mu(F) > 0$ and $\xi \in (\mathbb{Z}/p\mathbb{Z})^n - \{0^n\}$ ($n \in \mathbb{N}$) such that $\xi^t d_{[1,n]} \neq 0$ modulo p, then $\widehat{\mu}([\xi]_s) = 0$ for any $s \in \mathbb{N}$.*

Proof. We know that $\widehat{\mu}([\xi]_s) = \widehat{\tilde{T}_*\mu}([\xi]_s)$, but

$$\widehat{\tilde{T}_*\mu}([\xi]_s) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^n} \mu([x]_s) w^{\xi^t \tilde{T} x} = \widehat{\mu}([\xi]_s) w^{k\xi^t d_{[1,n]}},$$

then $\widehat{\mu}([\xi]_s) = 0$. □

Lemma 2.5. *Let μ be an invariant for F and σ. If $\xi \in (\mathbb{Z}/p\mathbb{Z})^n - \{0^n\}$ ($n \in \mathbb{N}$) satisfies $\xi^t d_{[1,n]} = 0$ modulo p, then $\widehat{\mu}([\xi]_s) = 0$ for any $s \in \mathbb{N}$.*

Proof. Notice that if $\xi \in \mathbb{Z}/p\mathbb{Z}$, then $\xi^t d_{[1,1]} = \xi$ so $\xi^t d_{[1,1]} = 0$ if and only if $\xi = 0$. This proves that for any $\xi \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ we are in the case of Lemma 2.4, and therefore $\widehat{\mu}([\xi]_s) = 0$.

There are p non trivial solutions in ξ of $\xi^t d_{[1,n]} = 0$, where by trivial we main any ξ of the form $(0, \ldots, 0, \tilde{\xi}, 0, \ldots, 0), (\tilde{\xi}, 0, \ldots, 0)$ or $(0, \ldots, 0, \tilde{\xi})$ with $\tilde{\xi} \in (\mathbb{Z}/p\mathbb{Z})^m$ for $m < n$. This is enough, because μ-invariance of σ implies that for any ξ of one of these forms $\widehat{\mu}([\xi]_s) = \widehat{\mu}([\tilde{\xi}]_{s'})$ for $s' \in \mathbb{N}$, then recursively we must to arrive to some $\widehat{\mu}([\tilde{\xi}']_{s''})$ in which $\tilde{\xi}'$ is not trivial. We are going to find all non trivial solutions. When $n = 2$, the solution in $\xi \in (\mathbb{Z}/p\mathbb{Z})^2$ of $\xi^t d_{[1,2]} = 0$ is given by $\xi = (a\xi_1, b\xi_1)$ with $\xi_1 \in \mathbb{Z}_p$. Because, $\xi^t d_{[1,2]} = a\xi_1 + b\xi_1(-ab^{-1}) = 0$. Inductively, it is easy to prove that the solution of $\xi^t d_{[1,d]}$ is given by $\xi = (\xi_1 z_1, \xi_1 z_2, \ldots, \xi_1 z_n)$ where $\xi_1 \in \mathbb{Z}/p\mathbb{Z}$ and z_l is the l-th summand in $\sum_{k=1}^n \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} a^{k-1} b^{n-k} = (a+b)^{n-1}$. If we fix an $\xi \in \mathbb{Z}/p\mathbb{Z}$, then

$$\widehat{F_*\mu}([\xi]_s) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \mu(F^{-1}[x]_s) w^{\xi^t x} = \sum_{x \in \mathbb{Z}_p^2} \mu([x]_s) w^{\xi^t F x},$$

where $Fx \doteq F(x_1, x_2) \doteq (ax_1 + bx_2 + c)$, then $\xi^t F x = \tilde{\xi}^t x + \xi^t(c, c)$, where $\tilde{\xi} = (a\xi, b\xi)$. By induction on $n \in \mathbb{N}$, $\xi_1 \in (\mathbb{Z}/p\mathbb{Z})^n$ and $\xi = (\xi_1, \xi_1, \ldots, \xi_1) \in (\mathbb{Z}/p\mathbb{Z})^n$, then $\xi^t F x = \tilde{\xi}^t x + \xi^t(c, c, \ldots, c) = \tilde{\xi}^t x + \xi^t \vec{c}$, where $\tilde{\xi}^t d_{[1,n+1]} = 0$ and $\vec{c} \in (\mathbb{Z}/p\mathbb{Z})^n$. In particular

$$\widehat{F_*\mu}([\xi]_s) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^n} \mu(F^{-1}[x]_s) w^{\xi^t x} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^{n+1}} \mu([x]_s) w^{\tilde{\xi}^t x + \xi^t \vec{c}} = \widehat{\mu}([\tilde{\xi}]_s) w^{\xi^t \vec{c}}.$$

If we assume that F is μ-invariant, then $\widehat{\mu}([\xi]_s) = \widehat{F_*\mu}([\xi]_s)$ for any ξ, but by the previous paragraph if $n \in \mathbb{N}, \tilde{\xi} \in (\mathbb{Z}/p\mathbb{Z})^n$ and $\tilde{\xi}^t d_{[1,n]} = 0$, then $\widehat{\mu}([\tilde{\xi}]_s) = \widehat{\mu}([\xi]_s) w^r$ for some $\xi \in \mathbb{Z}/p\mathbb{Z}, r \in \{0, 1, \ldots, p-1\}$, and therefore $\widehat{\mu}([\tilde{\xi}]_s) = 0$. □

All the Lemmas together prove the Theorem 1.1.

References

[HMM03] Bernard Host, Alejandro Maass, and Servet Martínez. Uniform Bernoulli measures in dynamics of permutative cellular automata with algebraic local rules. *Discrete Contin. Dyn. Syst.*, (9):1423–1446, 2003.

[Mat09] February 2009.

[Sab07] Mathieu Sablik. Measure rigidity for algebraic bipermutative cellular automata. *Ergodic Theory and Dynamical Systems*, 27(6), 2007.

E-mail address: `I.U.Cipriano@warwick.ac.uk`