Bernoulliness of $[T, \mathrm{Id}]$ when T is an irrational rotation: towards an explicit isomorphism

Christophe Leuridan

Bernoulliness of $[T, \mathrm{Id}]$ when T is an irrational rotation: towards an explicit isomorphism.

Christophe Leuridan

February 6, 2023

Abstract

Let θ be an irrational real number. The map $T_\theta : y \mapsto (y+\theta) \mod 1$ from the unit interval $\mathbf{I} = [0,1[$ (endowed with the Lebesgue measure) to itself is ergodic.

In a short paper [**?**] published in 1996, Parry provided an explicit isomorphism between the measure-preserving map $[T_\theta, \mathrm{Id}]$ and the unilateral dyadic Bernoulli shift when θ is extremely well approached by the rational numbers, namely if

$$\inf_{q\geq 1} q^4 4^{q^2} \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) = 0.$$

A few years later, Rudolph and Hoffman showed in [**?**] that for every irrational number, the measure-preserving map $[T_\theta, \mathrm{Id}]$ is isomorphic to the unilateral dyadic Bernoulli shift. Their proof is not constructive.

In the present paper, we relax notably Parry's condition on θ and show that actually, the explicit map provided by Parry's method is an isomorphism between the map $[T_\theta, \mathrm{Id}]$ and the unilateral dyadic Bernoulli shift whenever

$$\inf_{q\geq 1} q^4 \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) = 0.$$

We also provide a weaker sufficient condition involving the expansion of $||\theta|| := \mathrm{dist}(\theta, \mathbf{Z})$ in continued fraction. Set $||\theta|| = [0; a_1, a_2, \ldots]$ and call $(p_n/q_n)_{n\geq 0}$ the sequence of convergents. Then Parry's map is an isomorphism between the map $[T_\theta, \mathrm{Id}]$ and the unilateral dyadic Bernoulli shift whenever

$$\inf_{n\geq 1} q_n^3 \ (a_1 + \cdots + a_n) \ |q_n\theta - p_n| < +\infty.$$

Whether Parry's map is an isomorphism for every θ or not is still an open question, although we expect a positive answer.

MSC Classification : 37A05,60J05.
Keywords : diophantine approximation, irrational rotations, skew products, Bernoulli shifts, dyadic filtrations, head-and-tail filtrations, constructive Markov chains, coupling from the past.

1 Introduction

Let $X = \{0,1\}^{\mathbf{Z}_+}$, endowed with the product sigma-field $\mathcal{X}$ and the product measure

$$\mu = \bigotimes_{n\in\mathbf{Z}_+} (\delta_0 + \delta_1)/2.$$

The shift operator on X is the map $S : X \to X$ defined by

$$S(x)(n) := x(n+1) \text{ for every } x \in X \text{ and } n \in \mathbf{Z}_+.$$

The map S preserves the measure μ, and the dynamical system $(X, \mathcal{X}, \mu, S)$ is the unilateral dyadic Bernoulli shift.

Given any invertible dynamical system $(Y, \mathcal{Y}, \nu, T)$, one gets a measure-preserving map $[T, \mathrm{Id}]$ on the product space $(X \times Y, \mathcal{X} \otimes \mathcal{Y}, \mu \otimes \nu)$ by setting

$$[T, \mathrm{Id}](x, y) := (S(x), T^{x(0)}y).$$

The map $[T, \mathrm{Id}]$ is not invertible. More precisely, each element $(x', y') \in X \times Y$ have exactly two inverse images namly $(0x', y')$ and $(1x', T^{-1}(y'))$.

Moreover, if (ξ, η) is a random variable with distribution $\mu \otimes \nu$, then the law of (ξ, η) given $[T, \mathrm{Id}](\xi, \eta) = (x', y')$ is the uniform law on the pair $\{(0x', y'), (1x', T^{-1}(y'))\}$. One says that the dynamical system $(X \times Y, \mathcal{X} \otimes \mathcal{Y}, \mu \otimes \nu, [T, \mathrm{Id}])$ is dyadic, like the unilateral Bernoulli shift $(X, \mathcal{X}, \mu, S)$.

By replacing $\mathbf{Z}_+$ with $\mathbf{Z}$ in the definitions above, we transform the non-invertible dynamical systems $(X, \mathcal{X}, \mu, S)$ and $(X \times Y, \mathcal{X} \otimes \mathcal{Y}, \mu \otimes \nu, [T, \mathrm{Id}])$ into two invertible ones, namely the bilateral dyadic Bernoulli shift $(\overline{X}, \overline{\mathcal{X}}, \overline{\mu}, \overline{S})$ and $(\overline{X} \times Y, \overline{\mathcal{X}} \otimes \mathcal{Y}, \overline{\mu} \otimes \nu, \overline{[T, \mathrm{Id}]})$. These latter two systems are the natural extensions of the former two.

Let us come back to $[T, \mathrm{Id}]$. For every $n \geq 0$, set $\mathcal{D}_n := [T, \mathrm{Id}]^{-n}(\mathcal{X} \otimes \mathcal{Y})$. Call $\alpha = \{A_0, A_1\}$ the partition of $X \times Y$ defined by $A_i = \{(x, y) \in X \times Y : x(0) = i\}$. Then under $\mu \otimes \nu$,

- the blocks A_0 and A_1 have probability $1/2$;
- the partition α and the σ-field $\mathcal{D}_1$ are independent;
- the σ-field generated by α and $\mathcal{D}_1$ is $\mathcal{D}_0$.

More generally, since $[T, \mathrm{Id}]$ preserves $\mu \otimes \nu$, each σ-field $\mathcal{D}_n$ is generated by $\mathcal{D}_{n+1}$ and the independent partition $[T, \mathrm{Id}]^{-n}\alpha$ into two blocks of probability $1/2$ each. In particular, the sequence $(\mathcal{D}_n)_{n \geq 0}$ thus defined is decreasing and the partitions $([T, \mathrm{Id}]^{-n}\alpha)_{n \geq 0}$ carry the information lost at each iteration of the map $[T, \mathrm{Id}]$.

For every $n \geq 0$, and $i \in \{0, 1\}$, $[T, \mathrm{Id}]^{-n}(A_i) = \{(x, y) \in X \times Y : x(n) = i\}$, so the partition $[T, \mathrm{Id}]^{-n}\alpha$ is the partition given by the coordinate n on the factor $X = \{0, 1\}^{\mathbf{Z}_+}$. Therefore, the σ-field generated by the partitions $([T, \mathrm{Id}]^{-n}\alpha)_{n \leq 0}$ is $\mathcal{X} \otimes \{\emptyset, Y\}$ and not $\mathcal{X} \otimes \mathcal{Y}$. Hence, natural questions arise.

Exactness

First, consider the asymptotic σ-field

$$\mathcal{D}_\infty := \bigcap_{n \geq 0} \mathcal{D}_n.$$

Is it trivial (i.e. does it contain only set having probability 0 or 1 under $\mu \otimes \nu$)? If yes, one says that the measure-preserving map $[T, \mathrm{Id}]$ on $(X \times Y, \mathcal{X} \otimes \mathcal{Y}, \mu \otimes \nu)$ is *exact*. As recalled in the introduction of [**?**], if $[T, \mathrm{Id}]$ is exact, then $\overline{[T, \mathrm{Id}]}$ is a K-automorphism, which implies that both $[T, \mathrm{Id}]$ and $\overline{[T, \mathrm{Id}]}$ are strongly mixing.

Moreover, the converse (if $\overline{[T,\mathrm{Id}]}$ is a K-automorphism then $[T,\mathrm{Id}]$ is exact) holds provided $[T,\mathrm{Id}]$ has a finite generator, that is a finite measurable partition β of $X\times Y$ such that $\mathcal{D}_0=\sigma(([T,\mathrm{Id}]^{-n}\beta)_{n\geq 0})$ modulo the $\mu\otimes\nu$-null sets.

Melijson's theorem [**?**] shows that $\overline{[T,\mathrm{Id}]}$ is a K-automorphism if T is totally ergodic (i.e. all positive powers of T are ergodic). Actually, assuming that T is ergodic is sufficient. A more precise statement, obtained by a different method, is given in [**?**]: the endomorphism $[T,\mathrm{Id}]$ is exact if and only if T is ergodic. In particular, $[T,\mathrm{Id}]$ is exact when T is an irrational rotation or a Bernoulli shift.

Standardness

We have already noticed that the independent partitions $([T,\mathrm{Id}]^{-n}\alpha)_{n\leq 0}$ do not generate the whole partition $\mathcal{D}_0$. Is it still possible to find a sequence $(\beta_n)_{n\geq 0}$ of independent partitions into two blocks of probability $1/2$ each such that for every $n\geq 0$, $\mathcal{D}_n=\sigma((\beta_k)_{k\geq n})\mod \mu\otimes\nu$? If yes, one says that the decreasing sequence of σ-fields $(\mathcal{D}_n)_{n\geq 0}$, or the measure-preserving map $[T,\mathrm{Id}]$ on $(X\times Y,\mathcal{X}\otimes\mathcal{Y},\mu\otimes\nu)$ is *standard*.

By Kolmogorov zero-one law, exactness of $[T,\mathrm{Id}]$ is a necessary condition of standardness of $[T,\mathrm{Id}]$, but this condition is not sufficient: for example when T is a Bernoulli shift, the map $[T,\mathrm{Id}]$ is not standard. A variant of this non-trivial result has been established by Heicklen and Hoffman in [**?**]. Heicklen and Hoffman consider the map $[T,T^{-1}]$, which can be defined by the same formula as the map $[T,\mathrm{Id}]$, provided $\{0,1\}^{\mathbf{Z}_+}$ is replaced by $\{-1,1\}^{\mathbf{Z}_+}$. Answering to a question raised by Vershik in [**?**], they prove that the map $[T,T^{-1}]$ is not standard when T is a Bernoulli shift. In [**?**], we prove again the non-standardness of $[T,T^{-1}]$ with the help of the *nibbled-word process* introduced by Stephane Laurent in [**?**] and show that this proof still works with $[T,\mathrm{Id}]$.

The main tools to determine whether a dyadic (or poly-adic) measure-preserving map is standard or not, are Vershik standardness criteria [**?**]. As an application, Vershik states (page 744) that when T is an irrational rotation, the measure preserving map $[T,T^{-1}]$ is standard. The same arguments work with $[T,\mathrm{Id}]$.

This result has a striking probabilistic interpretation: consider a (stationnary) irrational simple symmetric random walk $(X_n)_{n\in\mathbf{Z}}$ on the circle $\mathbf{R}/\mathbf{Z}$, indexed by $\mathbf{Z}$. The steps $(X_n-X_{n-1})_{n\in\mathbf{Z}}$ are independent and uniformly distributed random variables on $\{\theta,-\theta\}$ where θ is some fixed irrational number, and they generate a filtration which is smaller than $(\mathcal{F}_n^X)_{n\in\mathbf{Z}}$, the natural filtration of $(X_n)_{n\in\mathbf{Z}}$. Yet, one can generate (up to null sets) $(\mathcal{F}_n^X)_{n\in\mathbf{Z}}$ by some sequence of independent uniform Bernoulli random variables. An explicit construction is given in [**?**] in a slightly more general context.

In [**?**], Feldman and Rudolph prove a general result: the measure-preserving map $[T,\mathrm{Id}]$ is standard when T is rank-1. This condition includes all pure-point spectrum transformations and in particular irrational rotations of the circle.

Bernoulliness

In the same vein, one can also ask two seemingly close questions:

1. Is $\overline{[T,\mathrm{Id}]}$ isomorphic to the bilateral Bernoulli shift $\overline{S}$? Equivalently, is it possible to find a partition $\overline{\beta}$ of $\overline{X}\times Y$ into two blocks of probability $1/2$ each, such that the partitions $(\overline{[T,\mathrm{Id}]}^{-n}\overline{\beta})_{n\in\mathbf{Z}}$ are independent and generate $\overline{\mathcal{X}}\otimes\mathcal{Y}$ modulo $\mu\otimes\nu$?

2. Is $[T,\mathrm{Id}]$ isomorphic to the unilateral Bernoulli shift S? Equivalently, is it possible to find a partition β of $X\times Y$ into two blocks of probability $1/2$ each, such that the partitions $([T,\mathrm{Id}]^{-n}\beta)_{n\geq 0}$ are independent and generate $\mathcal{X}\otimes\mathcal{Y}$ modulo $\mu\otimes\nu$?

Call $F : \overline{X} \times Y \to X \times Y$ the map given by $F((x_n)_{n\in\mathbf{Z}}, y) = ((x_n)_{n\geq 0}, y)$. If a partition β of $X \times Y$ fulfills the latter condition, then $\overline{\beta} := F^{-1}(\beta)$ fulfills the former. Hence the Bernoulliness of $[T, \mathrm{Id}]$ implies the Bernoulliness of its natural extension $\overline{[T, \mathrm{Id}]}$.

The Bernoulliness of the non-invertible map $[T, \mathrm{Id}]$ also implies its standardness. Indeed, since $[T, \mathrm{Id}]$ preserves the law $\mu \otimes \nu$ the equality $\sigma\big(([T, \mathrm{Id}]^{-k}\beta)_{k\geq 0}\big) = \mathcal{X} \otimes \mathcal{Y}$ mod $\mu \otimes \nu$ implies for every $n \geq 0$

$$(\sigma([T, \mathrm{Id}]^{-k}\beta)_{k\geq n}) = [T, \mathrm{Id}]^{-n}(\mathcal{X} \otimes \mathcal{Y}) = \mathcal{D}_n \mod \mu \otimes \nu.$$

Yet, as observed by Hoffman and Rudolph in [**?**], there is no relation between the standardness of $[T, \mathrm{Id}]$ and the Bernoulliness of $\overline{[T, \mathrm{Id}]}$. In the one hand, the standardness of $[T, \mathrm{Id}]$ is the possibility to generate the filtration $(\mathcal{D}_{-n})_{n\leq 0}$ (obtained by time reversal) by some sequence of independent uniform Bernoulli random variables. In the other hand, the Bernoulliness of $\overline{[T, \mathrm{Id}]}$ is the existence of *one* measurable finite partition β of the space $\overline{X} \times Y$ whose images by all the powers (positive, null and negative) of $\overline{[T, \mathrm{Id}]}$ are independent and generate the whole σ-field $\overline{\mathcal{X}} \otimes \mathcal{Y}$ modulo the null sets. The former property requires adaptation to some filtration whereas the latter requires stationarity. Indeed, various examples and counter-examples confirm the absence of implication between these two properties. See also [**?**].

When T is a Bernoulli shift, the endomorphisms $[T, \mathrm{Id}]$ and $[T, T^{-1}]$ are not Bernoulli since they are not standard. Yet, Feldman observes that the automorphism $\overline{[T, \mathrm{Id}]}$ is Bernoulli and has a simple independent generator (Theorem 2 in [**?**]). But later, Kalikow as shown that the automorphism $\overline{[T, T^{-1}]}$ is not Bernoulli (see [**?**]).

In 1972-1974, Adler and Shields proved in [**?**, **?**] the Bernoulliness of many measure preserving maps including $\overline{[T, \mathrm{Id}]}$ when T is an irrational rotation.

In 2002, Rudolph and Hoffman proved in [**?**] the Bernoulliness of $[T, \mathrm{Id}]$ itself when T is an irrational rotation. Their proof is not constructive and relies on the notion of tree very weak Bernoulli endomorphism.

Constructive proof of Bernoulliness in the case of irrational rotations

Actually, a few years before, Parry gave in [**?**] a constructive proof of the Bernoulliness of $[T, \mathrm{Id}]$ in a very particular case. Let us detail Parry's result.

For any real number θ (rational or not), let the map $T_\theta : y \mapsto (y + \theta) \mod 1$ is an automorphism of the unit interval $\mathbf{I} = [0, 1[$ endowed with the Borel σ-field and Lebesgue measure ν. Set $S_\theta = [T_\theta, \mathrm{Id}]$. Since the maps T_θ and S_θ depend only on the fractional part of θ, we may and we will assume from now on that $\theta \in [0, 1[$.

On the set $X \times \mathbf{I}$, the partition α associated to the map $(x, y) \mapsto x(0)$ has two blocks with probability $1/2$, it is independent of $\mathcal{D}_1$ and we have $\mathcal{D}_0 = \sigma(\alpha) \vee \mathcal{D}_1$. Parry defines another partition $\alpha_\theta = \{A_0^\theta, A_1^\theta\}$ by

$$A_0^\theta = \{x \in X : x(0) = 0\} \times [0, \theta[\cup \{x \in X : x(0) = 1\} \times [0, 1 - \theta[,$$

$$A_1^\theta = \{x \in X : x(0) = 0\} \times [\theta, 1[\cup \{x \in X : x(0) = 1\} \times [1 - \theta, 1[.$$

By construction, for every $(x, y) \in X \times \mathbf{I}$,

$$(x, y) \in A_0^\theta \iff x(0) = \mathbf{1}_{[\theta,1[}(T_\theta^{x(0)}(y)).$$

But $x(0)$ is a $\sigma(\alpha)$-measurable function of (x, y), whereas $T_\theta^{x(0)}(y)$ - the second component of $S_\theta(x, y)$ - is a $\mathcal{D}_1$-measurable function of (x, y). Hence, $\mu \otimes \nu[A_0^\theta | \mathcal{D}_1] = 1/2$, so

- the blocks A_0^θ and A_1^θ have probability $1/2$;
- the partition α_θ and the σ-field $\mathcal{D}_1$ are independent;
- the σ-field generated by α_θ and $\mathcal{D}_1$ is $\mathcal{D}_0$.

Therefore, $(S_\theta^{-n}\alpha_\theta)_{n\geq 0}$ are independent and uniform partitions into two blocks.

For every $(x,y) \in X \times \mathbf{I}$, denote by $\alpha_\theta(x,y) = \mathbf{1}_{A_1^\theta}(x,y)$ the index of the only block containing (x,y) in the partition α_θ and set

$$\Phi_\theta(x,y) = \big((\alpha_\theta \circ S_\theta^n)(x,y)\big)_{n\geq 0}.$$

Then the 'α_θ-name' map $\Phi_\theta : X \times \mathbf{I} \to X$ thus defined is a factor map which sends the dynamical system $(X \times \mathbf{I}, \mathcal{X} \otimes \mathcal{B}(\mathbf{I}), \mu \otimes \nu, S_\theta)$ on the Bernoulli shift $(X, \mathcal{X}, \mu, S)$. This factor map is more interesting than the canonical projection from $X \times \mathbf{I}$ to X.

When θ is irrational and under the very strong assumption

$$\liminf_{q\to+\infty} q^4 4^{q^2} \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) = 0,$$

Parry proves that the partitions $(S_\theta^{-n}\alpha_\theta)_{n\geq 0}$ generate the whole σ-field $\mathcal{X}\otimes\mathcal{B}(\mathbf{I})$ modulo the null sets, so the map Φ_θ is an explicit isomorphism between $S_\theta = [T_\theta, \mathrm{Id}]$ and the dyadic unilateral Bernoulli shift S.

In the present paper, we improve on Parry's method and relax Parry's additional assumption into far weaker conditions.

Theorem 1 *Parry's map Φ_θ is an isomorphism between $[T_\theta, \mathrm{Id}]$ and the Bernoulli shift S whenever*

$$\inf_{q\geq 1} q^4 \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) = 0. \tag{1}$$

Theorem 2 *Set $||\theta|| = \mathrm{dist}(\theta, \mathbf{Z}) = [0; a_1, a_2, \ldots]$ and call $(p_n/q_n)_{n\geq 0}$ the sequence of convergents. Then Parry's map is an isomorphism between the map $[T_\theta, \mathrm{Id}]$ and the unilateral dyadic Bernoulli shift whenever*

$$\inf_{n\geq 1} q_n^3 \ (a_1 + \cdots + a_n) \ |q_n\theta - p_n| = 0.$$

Actually, theorem **??** is a generalization of theorem **??**. Indeed, if the condition of theorem **??** holds, then one can find integers q such that $q^4 \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z})$ is as small as one wants and in particular less that $1/2$. These integers q are necessarily denominators of convergents of the expansion of θ and also of $||\theta||$ in continued fractions, since

$$q^2 \ \mathrm{dist}(||\theta||, q^{-1}\mathbf{Z}) = q^2 \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) \leq q^4 \ \mathrm{dist}(\theta, q^{-1}\mathbf{Z}) < 1/2.$$

Moreover, since the partial quotients $a_1, a_2, \ldots$ are greater or equal to 1, a recursion on n shows that for every $n \geq 1$,

$$q_n \geq a_1 + a_1a_2 + \cdots + a_1 \cdots a_n \geq a_1 + a_2 + \cdots + a_n.$$

Hence the condition of theorem **??** implies the condition of theorem **??**. Yet, theorem **??** is much simpler to establish, that is why we will prove it first.

A theorem of Khintchine [**?**] states that of θ is chosen randomly according to the Lebesgue measure on $[0,1[$, then

$$\frac{a_1+\cdots+a_n}{n\ln(n)} \to \ln 2 \text{ in probability.}$$

But q_n is at least equal to ϕ^n, where ϕ is the golden ratio (since $\mathrm{dist}(\theta,\mathbf{Z})<1/2$). Hence the typical size of $a_1+\cdots+a_n$ is $O(\ln q_n \ln(\ln q_n))$.

Unfortunately, the set of all θ satisfying the condition of theorem **??** has a zero Lebesgue measure. Yet, one can construct uncontably many such θ, either as the intersection of nested intervals of the form $[p/q-\varepsilon_q/q^4, p/q-\varepsilon_q/q^4]$ where the ε_q are positive real numbers tending to 0, or by choosing recursively the sequence $(a_n)_{n\geq 1}$ in such a way that

$$\inf_{n\geq 1} q_n\ (a_1+\cdots+a_n)/a_{n+1}=0.$$

This is sufficient since for every $n\geq 0$, $|q_n\theta-p_n|<1/(a_{n+1}q_n)$.

Whether the diophantine condition on θ can be removed or not is still an open question. To indicate the remaining gap, recall that the theory of continued fractions yields

$$\liminf_{q\to+\infty} q^2\ \mathrm{dist}(\theta,q^{-1}\mathbf{Z}) \leq 1/\sqrt{5} \text{ for every } \theta\in\mathbf{R},$$

and Khintchine theorem [**?**] yields that for every non-increasing function $\psi:\mathbf{R}_+^*\to\mathbf{R}_+^*$,

$$\liminf_{q\to+\infty} \frac{q}{\psi(q)}\mathrm{dist}(\theta,q^{-1}\mathbf{Z}) = \left|\begin{array}{ll} 0 & \\ +\infty & \text{for almost every } \theta \text{ if } \displaystyle\sum_{q\geq 1}\psi(q) \end{array}\right| \begin{array}{l} =+\infty \\ <+\infty \end{array}.$$

For example,

$$\liminf_{q\to+\infty} q^2\ln(q)\ln(\ln(q))\ \mathrm{dist}(\theta,q^{-1}\mathbf{Z})=0 \text{ for almost every } \theta\in\mathbf{R}.$$

2 Strategy of the proof

Let us first reformulate the strategy used by Parry. The reader will find at the end of the paper an index recalling the main notations used throughout the paper.

2.1 Parry's method

Recall that we assume that the irrational number θ lies in $]0,1[$.

Each element $(x,y)\in X\times\mathbf{I}$ has exactly two inverse images by S_θ, which are $(0x,y)$ and $(1x,T_\theta^{-1}(y))$. One of them belongs to A_0^θ and the other one to A_1^θ, respectively

$$F_0^\theta(x,y)=\big(\mathbf{1}_{[\theta,1[}(y)x, f_0^\theta(y)\big) \text{ where } f_0^\theta(y)=T_\theta^{-\mathbf{1}_{[\theta,1[}(y)}(y)=y-\theta\mathbf{1}_{[\theta,1[}(y),$$

$$F_1^\theta(x,y)=\big(\mathbf{1}_{[0,\theta[}(y)x, f_1^\theta(y)\big) \text{ where } f_1^\theta(y)=T_\theta^{-\mathbf{1}_{[0,\theta[}(y)}(y)=y+(1-\theta)\mathbf{1}_{[0,\theta[}(y).$$

As a result, for every $(x,y)\in X\times\mathbf{I}$,

$$(x,y)=F^\theta_{\alpha_\theta(x,y)}(S_\theta(x,y)),$$

and of course the same formula hold when we replace (x,y) by $S_\theta^n(x,y)$ for every $n\geq 0$.

We have to prove that outside of null set, (x, y) can be recovered from the knowledge of its α_θ-name $\Phi_\theta(x, y) = \big((\alpha_\theta \circ S_\theta^n)(x, y)\big)_{n\geq 0}$. Checking that y can be recovered is sufficient, since it implies (by translation) that the second component of each $\alpha_\theta(S_\theta^n)(x, y)$, namely $(y + (x(0) + \cdots + x(n-1))\theta) \mod 1$ can be recovered, so the sequence x can also be recovered.

To do this, Parry fixes an extremely good rational approximation $r = p/q$ of the irrational number θ, where $q > p > 0$ are relatively prime integers, and he approaches the map $S_\theta = [T_\theta, \mathrm{Id}]$ by $S_r = [T_r, \mathrm{Id}]$.

Unlike T_θ, the rotation T_r is not ergodic since it preserves the partition of $\mathbf{I}$ into q intervals with lengths $1/q$. One checks that the factor map $\Psi_r : X \times \mathbf{I} \to X \times [\![0, q-1]\!]$ defined by $\Psi_r(x, y) = (x, \lfloor qy \rfloor)$ transforms the measure preserving map $S_r = [T_r, \mathrm{Id}]$ into a discrete analogue, namely $S_{p,q} = [T_{p,q}, \mathrm{Id}]$ where $T_{p,q}$ is the permutation map on $[\![0, q-1]\!]$ defined by $T_{p,q}(z) = (z + p) \mod q$. Since $T_{p,q}$ preserves ν_q, the uniform law on $[\![0, q-1]\!]$, the map $S_{p,q}$ preserves $\mu \otimes \nu_q$.

Moreover, Ψ_r sends the partion α_r on the partition $\alpha_{p,q} = \{A_0^{p,q}, A_1^{p,q}\}$ where

$$A_0^{p,q} = \{x \in X : x(0) = 0\} \times [\![0, p-1]\!] \ \cup \ \{x \in X : x(0) = 1\} \times [\![0, q-1-p]\!],$$
$$A_1^{p,q} = \{x \in X : x(0) = 0\} \times [\![p, q-1]\!] \ \cup \ \{x \in X : x(0) = 1\} \times [\![q-p, q-1]\!].$$

Like before, each element $(x, z) \in X \times [\![0, q-1]\!]$ has exactly two inverse images by $S_{p,q}$, which are $(0x, z)$ and $(1x, (z-p) \mod q)$. One of them belongs to $A_0^{p,q}$, namely

$$F_0^{p,q}(x, z) = \big(\mathbf{1}_{[\![p,q-1]\!]}(z)x, f_0^{p,q}(z)\big) \text{ where } f_0^{p,q}(z) = z - p\mathbf{1}_{[\![p,q-1]\![}(z),$$

and the other one belongs to $A_1^{p,q}$, namely

$$F_1^{p,q}(x, z) = \big(\mathbf{1}_{[\![0,p-1]\!]}(z)x, f_1^{p,q}(z)\big) \text{ where } f_1^{p,q}(z) = z + (q-p)\mathbf{1}_{[\![0,p-1]\!]}(z).$$

As a result, for every $(x, z) \in X \times \mathbf{I}$,

$$(x, z) = F_{\alpha_{p,q}(x,z)}(S_{p,q}(x, z)).$$

For every $n \geq 0$, call z_n the second component of $S_{p,q}^n(x, z)$. Then the equality

$$(x, z) = F^{p,q}_{\alpha_{p,q}(x,z)} \circ F^{p,q}_{\alpha_{p,q}\circ S_{p,q}(x,z)} \circ \cdots \circ F^{p,q}_{\alpha_{p,q}\circ S_{p,q}^{n-1}(x,z)}(S_{p,q}^n(x, z))$$

yields

$$z = f^{p,q}_{\alpha_{p,q}(x,z)} \circ f^{p,q}_{\alpha_{p,q}\circ S_{p,q}(x,z)} \circ \cdots \circ f^{p,q}_{\alpha_{p,q}\circ S_{p,q}^{n-1}(x,z)}(z_n).$$

Then Parry uses a coupling-from-the-past argument: he establishes the existence of some ℓ-uple $(i_1, \ldots, i_\ell) \in \{0, 1\}^\ell$ with length $\ell \leq q^2$ such that the map $f_{i_\ell}^{p,q} \circ \cdots \circ f_{i_1}^{p,q}$ is constant. [1] But when (x, z) is randomly chosen according to the law $\mu \otimes \nu_q$, the indexes $(\alpha_{p,q} \circ S_{p,q}^n(x, z))_{n\geq 0}$ form an i.i.d. uniform Bernoulli sequence. Almost surely, the word $(i_\ell, \ldots, i_1)$ appears infinitely many times in this sequence, so the value z is completely determined by the indexes $(\alpha_{p,q} \circ S_{p,q}^n(x, z))_{n\geq 0}$.

[1] To get such an ℓ-uple, set $i_{n+1} = \mathbf{1}_{[\![0,p-1]\!]}(u_n)$ for every $n \geq 0$, where $u_n = (f_{i_n}^{p,q} \circ \cdots \circ f_{i_1}^{p,q})(0)$. This recursion begins with $u_0 = 0 \in [\![0, p-1]\!]$, so $i_1 = 1$. Then $u_{n+1} = f_{i_{n+1}}(u_n) = (u_n - p) \mod q$ for every $n \geq 0$. Since p and q are relatively prime, the sequence $(u_n)_{n\geq 0}$ visits every element of $[\![0, p-1]\!]$ and is q-periodic. For the same reason, q is the least period of the map $z \mapsto \mathbf{1}_{[\![0,p-1]\!]}(z \mod q)$.

Now, consider the sequence given by $v_n = (f_{i_n}^{p,q} \circ \cdots \circ f_{i_1}^{p,q})(v_0)$ where $v_0 \in [\![1, p-1]\!]$ is any other starting point. For every $n \geq 0$, $v_{n+1} = (v_n - p) \mod q$ or $v_{n+1} = v_n$ according that $\mathbf{1}_{[\![0,p-1]\!]}(v_n) = \mathbf{1}_{[\![0,p-1]\!]}(u_n)$ or not. Thus, if the difference $d_t = (v_t - u_t) \mod q$ is not 0 at a given time t, there exists some $n \in [\![t+1, t+q]\!]$ such that $d_n = (d_t + p) \mod q$: otherwise, the equality $\mathbf{1}_{[\![0,p-1]\!]}(v_n) = \mathbf{1}_{[\![0,p-1]\!]}(u_n)$ would hold during the time interval $[\![t, t+q-1]\!]$, so the map $z \mapsto \mathbf{1}_{[\![0,p-1]\!]}(z \mod q)$ would be d_t-periodic. Hence the sequence $(d_n)_{n\geq 0}$ reaches 0 in at most $q(q-1)$ steps.

Using the factor map Ψ_r, one deduces that for $\mu\otimes\nu$-almost every $(x,y)\in x\times\mathbf{I}$, the integer $\lfloor qy\rfloor$ is completely determined by the indexes $(\alpha_r\circ S_r^n(x,z))_{n\geq 0}$. Furthermore, the probability that the knowledge of the first ℓn indexes is not sufficient is at most $(1-2^{-\ell})^n\leq\exp(-n2^{-\ell})$: to see this, split these indexes into n disjoint intervals with length ℓ each. This upper bound invites us to choose n much larger than 2^ℓ.

Using the extremely good approximation of θ by r, one can check that the integer $\lfloor qy\rfloor$ is determined with probability close to 1 by the indexes $(\alpha_\theta\circ S_\theta^n(x,z))_{n\geq 0}$. The result follows by using better and better approximations.

Actually, given an extremely good rational approximation r of θ, Parry uses the following upper bound of the relative entropy when $n\geq 1$ and $2n|\theta-r|$ is small:

$$H(S_r^{-n}\alpha_r|S_\theta^{-n}\alpha_\theta)\leq -2n|\theta-r|\log_2(2n|\theta-r|).$$

2.2 Our refinements and key tools

Following Parry's method and keeping the notations above, we bring two improvements, which require less precision in the approximation of θ by rational numbers.

First, whereas Parry proved the existence of *one* constant map obtained by coupounding q^2 maps chosen in $\{f_0^{p,q},f_1^{p,q}\}$, our first improvement is to get *many* constant maps by composing $O(q^3)$ such maps.

Theorem 3 *Let $(\eta_t)_{t\geq 1}$ be a sequence of independent uniform Bernoulli random variables. Set*

$$T_c^{p,q}=\inf\{t\geq 0: f_{\eta_t}^{p,q}\circ\cdots\circ f_{\eta_1}^{p,q}\text{ is a constant function}\}.$$

Moreover, let Z_0 be a uniform random variable with values in $[\![0,q-1]\!]$ and independant of $(\eta_t)_{t\geq 1}$. Fix $z_0'\in[\![0,q-1]\!]$ and set

$$T_{f,z_0'}^{p,q}=\inf\{t\geq 0: f_{\eta_t}^{p,q}\circ\cdots\circ f_{\eta_1}^{p,q}(Z_0)=f_{\eta_t}^{p,q}\circ\cdots\circ f_{\eta_1}^{p,q}(z_0')\}.$$

Then

$$\mathbf{E}[T_c^{p,q}]\leq 5q^3/3\text{ and }(q^2-1)/6\leq\mathbf{E}[T_{f,z_0'}^{p,q}]\leq q^3/3.$$

Actually, we will only use the upper bound of $\mathbf{E}[T_{f,z_0'}^{p,q}]$, which is easier to prove.

Next, instead of introducing the partition of $\mathbf{I}$ into q intervals with lengths $1/q$, we will consider only the partition into q intervals provided by the subdividision $(x_k)_{0\leq k\leq q-1}$, where $x_k=k\theta-\lfloor k\theta\rfloor=T_\theta^k(0)$ for every $k\geq 0$.

The well-known three gaps [**?**, **?**, **?**, **?**] theorem states that the lengths of those intervals take at most three distinct value and that when there are exactly three different lengths, the largest is the sum of the other two. Actually, the next proposition shows that when p/q is a reasonably good rational approximation of θ, there are at most two distinct values.

To abbreviate the notations, when there is no ambiguity on the approximation p/q considered, we will sometimes abbreviate $f_0^{p,q}$ and $f_1^{p,q}$ into f_0 and f_1. In the same way, we will not always indicate the dependance with regard to (p,q) of many objects introduced below, namely the partition ι of $\mathbf{I}$, the set L, the maps g_0, g_1 and h below.

Proposition 4 *Fix two relatively prime integers $q > p > 0$. Call h the permutation map on $[\![0, q-1]\!]$ defined by $h(\ell) = (p\ell) \bmod q$. Let $u = h^{-1}(1)$ be the inverse of p modulo q, and $v \in [\![0, p-1]\!]$ the integer such that $pu - qv = 1$. Set*

$$\begin{aligned} I_\ell &= [x_\ell, x_{\ell+u}[\quad \text{if} \quad \ell \in [\![0, q-u-1]\!] \\ I_\ell &= [x_{q-u}, 1[\quad \text{if} \quad \ell = q-u \\ I_\ell &= [x_\ell, x_{\ell+u-q}[\quad \text{if} \quad \ell \in [\![q-u+1, q-1]\!], \end{aligned}$$

and $E = [0, q\theta - p[$ if $\theta > p/q$, $E = [1 + q\theta - p, 1[$ if $\theta < p/q$. Assume that

$$-\frac{1}{u} < q\theta - p < \frac{1}{q-u} \text{ or, equivalently, } \frac{v}{u} < \theta < \frac{p-v}{q-u}.$$

Then

1. *the sequence $(x_{h^{-1}(k)})_{0 \le k \le q-1}$ is increasing.*
2. *the intervals $(I_\ell)_{0 \le \ell \le q-1}$ form a partition ι of $\mathbf{I}$;*
3. *the intervals $(I_\ell)_{0 \le \ell \le q-u-1}$ have the same length $u\theta - v$;*
4. *the intervals $(I_\ell)_{q-u \le \ell \le q-1}$ have the same length $(p-v) - (q-u)\theta$;*
5. *if $|q\theta - p| < \min(1/u, 1/(q-u))$, both lengths are less than $2/q$;*
6. *for every $\ell \in [\![0, q-1]\!] \setminus \{q-u-1, q-1\}$, the rotation T_θ maps I_ℓ onto $I_{\ell+1}$;*
7. *if $\theta > p/q$, then $T_\theta(I_{q-1}) = I_0 \setminus E$ and $T_\theta(I_{q-u-1}) = I_{q-u} \cup E$;*
8. *if $\theta < p/q$, then $T_\theta(I_{q-1}) = I_0 \cup E$ and $T_\theta(I_{q-u-1}) = I_{q-u} \setminus E$.*

Remark 5 *Actually, the inequalities $-1/u < q\theta - p < 1/(q-u)$ hold if and only if p/q is a semi-convergent (or, according to Khintchine's terminology, an intermediate fraction) in the continued fraction expansion of θ. See [**?**] for a proof of this statement. The stronger inequality $|q\theta - p| < 1/q$ holds whenever p/q is a convergent.*

Proposition **??** provides a decomposition of $\mathbf{I}$ into two Rokhlin towers with heights $q-u$ and u (see figures **??** and **??**). If I_ℓ is not a top interval, T_θ maps each point of I_ℓ on the point above in $I_{\ell+1}$. The curved arrows show the image of the top intervals. Note that the difference between the two lengths, $|q\theta - p|$ is also the length of the exceptional interval E.

For every $y \in \mathbf{I}$, denote by $\iota(y)$ the only index $\ell \in [\![0, q-1]\!]$ such $y \in I_\ell$. When $|q\theta - p|$ is small with regard to $1/q$, the lengths of the intervals $(I_\ell)_{0 \le \ell \le q-1}$ are almost $1/q$, so the map $\iota : \mathbf{I} \to [\![0, q-1]\!]$ thus defined is close to be a factor map transforming T_θ into the ν_q-preserving map $T_{1,q} : z \mapsto (z+1) \bmod q$. To use a coupling-from-the-past argument, we will work with inverses of these maps, i.e. with the maps $T_{-\theta}$ and $T_{-1,q} : z \mapsto (z-1) \bmod q$.

Corollary 6 *Under the assumptions of proposition **??**, E is a subinterval of length $|q\theta - p|$ and the equality $\iota(T_{-\theta}(y)) = T_{-1,q}(\iota(y))$ holds everywhere on $\mathbf{I} \setminus E$.*

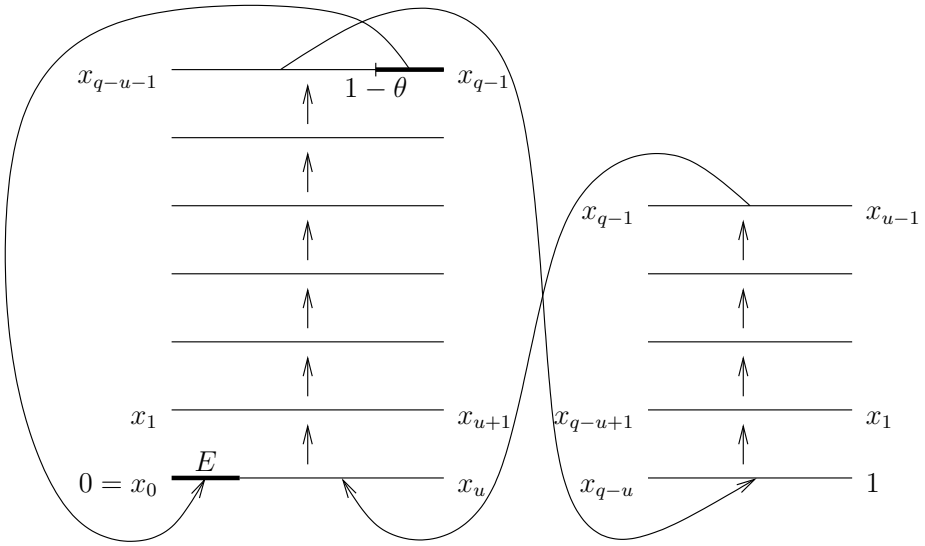

Figure 1: Behaviour of T_θ on the intervals $I_0, \ldots, I_{q-1}$ when $\theta > p/q$.

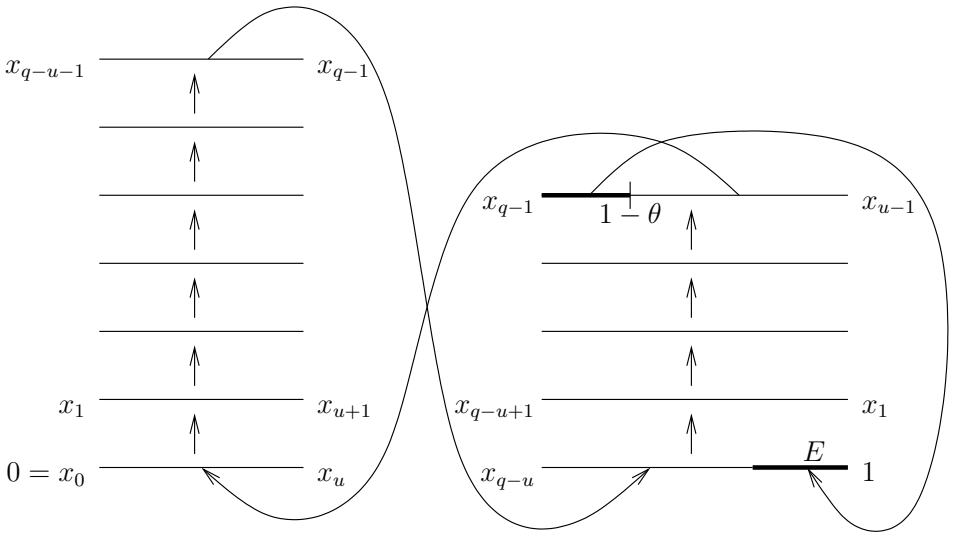

Figure 2: Behaviour of T_θ on the intervals $I_0, \ldots, I_{q-1}$ when $\theta < p/q$.

Consider again the maps f_0^θ and f_1^θ defined by

$$f_0^\theta(y) = y - \theta \mathbf{1}_{[\theta,1[}(y) \text{ and } f_1^\theta(y) = y + (1-\theta)\mathbf{1}_{[0,\theta[}(y)$$

Set $L_{p,q} = h^{-1}([\![0, p-1]\!])$. Then $0 \in L_{p,q}$ whereas $q - u \notin L_{p,q}$, and

$$[0,\theta[= [x_0, x_1[= \bigcup_{\ell \in L_{p,q}} I_\ell.$$

Define two maps $g_0^{p,q}$ and $g_1^{p,q}$ from $[\![0, q-1]\!]$ to itself by

$$g_0^{p,q}(\ell) = \ell - \mathbf{1}_{L_{p,q}^c}(\ell) \mod q \text{ and } g_1^{p,q}(\ell) = \ell - \mathbf{1}_{L_{p,q}}(\ell) \mod q.$$

Indeed, corollary **??** yields the following consequence.

Corollary 7 *Assume that $|q\theta - p| < 1/(q-1)$ and keep the notations of corollary* **??**.

If $\theta > p/q$, then the equality $\iota(f_0^\theta(y)) = g_0^{p,q}(\iota(y))$ holds everywhere on $\mathbf{I}$ and the equality $\iota(f_1^\theta(y)) = g_1^{p,q}(\iota(y))$ holds everywhere on $\mathbf{I} \setminus E$.

If $\theta < p/q$, then the equality $\iota(f_1^\theta(y)) = g_1^{p,q}(\iota(y))$ holds everywhere on $\mathbf{I}$ and the equality $\iota(f_0^\theta(y)) = g_0^{p,q}(\iota(y))$ holds everywhere on $\mathbf{I} \setminus E$.

Actually, the maps $g_0 = g_0^{p,q}$ and $g_1 = g_1^{p,q}$ are conjugated to the maps $f_0 = f_0^{p,q}$ and $f_1 = f_1^{p,q}$ previously introduced (see figure **??** below).

Lemma 8 *One has $h \circ g_0 = f_0 \circ h$ and $h \circ g_1 = f_1 \circ h$.*

Proof. Let $\ell \in [\![0, q-1]\!]$. Then $h(g_0(\ell))$ and $f_0(h(\ell))$ belong to $[\![0, q-1]\!]$ and

$$h(g_0(\ell)) \equiv pg_0((\ell) \equiv p\ell - p\mathbf{1}_{L^c}(\ell) \equiv h(\ell) - p\mathbf{1}_{[\![p,q-1]\!]}(h(\ell)) = f_0(h(\ell)) \quad [q].$$

Hence $h(g_0(\ell)) = f_0(h(\ell))$. A similar proof yields $h(g_1(\ell)) = f_1(h(\ell))$.

Therefore, theorem **??** can be reformulated and precised as follows.

Theorem 9 *Let $(\eta_t)_{t\geq 1}$ be a sequence of independent uniform Bernoulli random variables. Set*

$$T_c^{p,q} = \inf\{t \geq 0 : g_{\eta_t}^{p,q} \circ \cdots \circ g_{\eta_1}^{p,q} \text{ is a constant function}\}.$$

Then the expectation of T_c is at most $5q^3/3$. Moreover, let Z_0 be a uniform random variable with values in $[\![0, q-1]\!]$ and independent of $(\eta_t)_{n\geq 1}$. Fix $z_0' \in [\![0, q-1]\!]$ and set

$$T_{g,z_0'}^{p,q} = \inf\{t \geq 0 : g_{\eta_t}^{p,q} \circ \cdots \circ g_{\eta_1}^{p,q}(Z_0) = g_{\eta_t}^{p,q} \circ \cdots \circ g_{\eta_1}^{p,q}(z_0')\}.$$

Then

$$\mathbf{E}[T_c^{p,q}] \leq 5q^3/3 \quad \text{and} \quad \frac{q^2-1}{6} \leq \mathbf{E}[T_{g,z_0'}^{p,q}] \leq \frac{q^3}{3}.$$

We provide also a sharper upper bound relying on the expansion of $\mathrm{dist}(\theta, \mathbf{Z})$ in continued fraction.

Theorem 10 *Keep the notations of theorem* **??**, *set $\mathrm{dist}(\theta, \mathbf{Z}) = [0; a_1, a_2, \ldots]$ and call $(p_n/q_n)_{n\geq 0}$ the sequence of convergents. Then*

$$\mathbf{E}[T_{g,z_0'}^{p_n,q_n}] \leq q_n^2 \times (a_1 + \ldots + a_n).$$

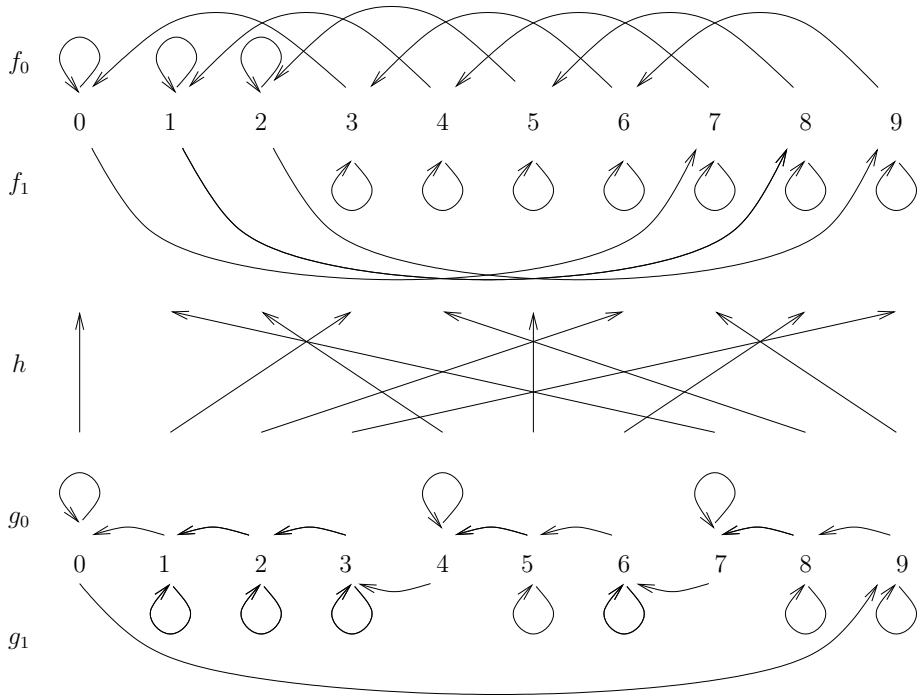

Figure 3: The maps f_0, f_1, h, g_0, g_1 when $p = 3$ and $q = 10$, so $u = 7$, $v = 2$ and $L = \{0, 4, 7\}$.

We will prove theorem **??** in section **??**.

Let us make an observation (not used in the sequel) on the set L. Figure **??** suggests that its points are well spread in the set $[\![0, q-1]\!]$. Indeed, the next statement holds.

Proposition 11 *Assume that $p \geq 2$. Call $0 = z_0 < \ldots < z_{p-1}$ the points of L. Then the differences $z_1 - z_0, \ldots, z_{p-1} - z_{p-2}, q - z_{p-1}$ are equal to $\lfloor q/p \rfloor$ or $\lceil q/p \rceil$.*

Proof. Since $up - vq = 1$, one has

$$\frac{u}{q} - \frac{v}{p} = \frac{1}{pq} < \frac{1}{p(p-1)}.$$

Hence proposition **??** applies, with θ, p and q replaced by u/q, v and p. We get that the points $(ku/q \mod 1)_{0 \leq k \leq p-1}$ split the interval $[0, 1[$ into p intervals having only two different lengths, and the difference between these lengths is $p(u/q) - v = 1/q$. Therefore, the points $(ku \mod q)_{0 \leq k \leq p-1}$ split the interval $[0, q[$ into p intervals having only two different lengths, and the difference between these lengths is 1. Since

$$L = h^{-1}\big([\![0, p-1]\!]\big) = \{ku \mod q : 0 \leq k \leq p-1\},$$

the statement follows.

2.3 End of the proof

Recall that we only have to prove that for $\mu \otimes \nu$-almost every $(x, y) \in X \times \mathbf{I}$, the second component y can be recovered from the knowledge of the sequence $\big((\alpha_\theta \circ S_\theta^n)(x, y)\big)_{n \geq 0}$.

It is now convenient to introduce probabilistic notations. We consider a stationary Markov chain $(\xi_n, Y_n)_{n\in\mathbf{Z}}$ defined on some probability space $(\Omega, \mathcal{A}, \mathbf{P})$, with values in $\{0,1\}\times\mathbf{I}$, such that for every $n\in\mathbf{Z}$,

- the law of (ξ_n, Y_n) is $\mu\otimes\nu$;
- ξ_n is independent of $\mathcal{F}_{n-1}^{\xi,Y} := \sigma((\xi_k, Y_k)_{k\le n-1})$;
- $Y_n = (Y_{n-1} - \theta\xi_n) \mod 1$.

If we identify the unit interval $\mathbf{I}$ with the circle $\mathbf{R}/\mathbf{Z}$, then $(Y_n)_{n\in\mathbf{Z}}$ is just a random walk whose steps $(-\theta\xi_n)_{n\in\mathbf{Z}}$ are uniformly distributed on $\{0,-\theta\}$. The Markov chain $(\xi_n, Y_n)_{n\in\mathbf{Z}}$ is related to the measure preserving map $S_\theta = [T_\theta, \mathrm{Id}]$ by the relations

$$S_\theta((\xi_{n-k})_{k\ge0}, Y_n) = ((\xi_{n-1-k})_{k\ge0}, Y_{n-1}).$$

Note that Y_0 is independent of the sequence $(\xi_n)_{n\le0}$. Indeed, for every $n\le0$, one has $Y_0 = T_{-\theta}^{\xi_{n+1}+\cdots+\xi_0}(Y_n)$. But Y_n is independent of $(\xi_{n+1},\cdots,\xi_0)$ and its law ν is invariant by $T_{-\theta}$. Hence Y_0 is also independent of $(\xi_{n+1},\cdots,\xi_0)$.

We now construct another sequence $(\eta_n)_{n\in\mathbf{Z}}$ of uniform Bernoulli random variables governing the Markov chain $(Y_n)_{n\in\mathbf{Z}}$. For every $n\in\mathbf{Z}$, set

$$\begin{aligned}
\eta_n &= \alpha_\theta((\xi_{n-k})_{k\ge0}, Y_n)\\
&= \mathbf{1}_{[\xi_n=0;Y_n\ge\theta]} + \mathbf{1}_{[\xi_n=1;Y_n\ge1-\theta]}\\
&= \mathbf{1}_{[\xi_n=0;Y_{n-1}\ge\theta]} + \mathbf{1}_{[\xi_n=1;Y_{n-1}<\theta]}\\
&= \big(\xi_n + \mathbf{1}_{[Y_{n-1}\ge\theta]}\big) \mod 2.
\end{aligned}$$

By construction, η_n is a $\mathcal{F}_n^{\xi,Y}$-measurable Bernoulli random variable, and

$$\mathbf{P}\big[\eta_n = 1\big|\mathcal{F}_{n-1}^{\xi,Y}\big] = \mathbf{E}\big[\eta_n\big|\mathcal{F}_{n-1}^{\xi,Y}\big] = \frac{1}{2}\mathbf{1}_{[Y_{n-1}\ge\theta]} + \frac{1}{2}\mathbf{1}_{[Y_{n-1}<\theta]} = \frac{1}{2},$$

so η_n is independent of $\mathcal{F}_{n-1}^{\xi,Y}$ and uniform. Moreover, since $\xi_n = \big(\eta_n + \mathbf{1}_{[Y_{n-1}\ge\theta]}\big) \mod 2$, one has $[\xi_n=1] = [\eta_n=1]\triangle[Y_{n-1}\ge\theta]$, so one checks that

$$Y_n = f_{\eta_n}^\theta(Y_{n-1}).$$

Note that when $n\le0$, $\eta_n = \alpha_\theta\circ S_\theta^{|n|}\big((\xi_{-k})_{k\ge0}, Y_0\big)$. Hence, we get the following probabilistic reformulation of what we have to prove.

Proposition 12 *The following statements are equivalent*

1. *the partition α_θ is a generator of the endomorphism S_θ.*
2. *for $\mu\otimes\nu$-almost every $(x,y)\in X\times\mathbf{I}$, the second component y can be recovered from the knowledge of the sequence $\Phi_\theta(x,y) = \big((\alpha_\theta\circ S_\theta^n)(x,y)\big)_{n\ge0}$.*
3. *the value Y_0 is almost surely determined by the knowledge of the sequence $(\eta_n)_{n\le0}$.*

Proof. The equivalence 1 $\iff$ 2 follows the remarks made at the beginning of subsection **??**.

The equivalence 2 $\iff$ 3 follows from the equality $(\eta_{-n})_{n\geq 0} = \Phi_\theta\big((\xi_{-n})_{n\geq 0}, Y_0\big)$. Indeed, given any measurable function $\psi : \{0,1\}^{\mathbf{Z}_+} \to \mathbf{I}$, we derive

$$\mathbf{P}\big[Y_0 = \psi\big((\eta_{-n})_{n\geq 0}\big)\big] = (\mu\otimes\nu)\{(x,y)\in X\times\mathbf{I} : y = \psi(\Phi_\theta(x,y))\},$$

since $(\eta_{-n})_{n\geq 0}$ and Y_0 are independent with respective laws μ and ν.

The proof is complete.

To approach Y_0 in probability by measurable fonctions of the sequence $(\eta_n)_{n\leq 0}$, we fix two integers $q > p > 0$ such that $|q\theta - p| < 1/(q-1)$, we consider the partition ι provided by proposition **??** and the associated map $\iota : \mathbf{I} \to [\![0, q-1]\!]$. Then, we set $Z_n = \iota(Y_n)$ for every $n \leq \mathbf{Z}$. Corollaries **??** and **??** show that the recursion formula $Z_n = g^{p,q}_{\eta_n}(Z_{n-1})$ holds with probability close to 1.

Lemma 13 *Assume that $|q\theta - p| < 1/(q-1)$ and keep the notations of corollary **??**. Then for every $n \in \mathbf{Z}$,*

1. *If $\theta > p/q$, then $[Z_n \neq g^{p,q}_{\eta_n}(Z_{n-1})] = [\eta_n = 1\ ;\ Y_{n-1} < q\theta - p]$.*
2. *If $\theta < p/q$, then $[Z_n \neq g^{p,q}_{\eta_n}(Z_{n-1})] = [\eta_n = 0\ ;\ Y_{n-1} \geq 1 + q\theta - p]$.*

In both cases,

$$\mathbf{P}\big[Z_n \neq g^{p,q}_{\eta_n}(Z_{n-1})\big] = \frac{1}{2}|q\theta - p|.$$

We have now all the ingredients to deduce theorems **??** and **??** from theorems **??** and **??**. The final argument is given by the next lemma.

Lemma 14 *Assume the existence of a sequence of rational numbers $(p_n/q_n)_{n\geq 1}$ in $]0,1[$, written in irreducible form such that $\lim_{n\to+\infty} q_n = +\infty$ and*

$$\lim_{n\to+\infty} \mathbf{E}[T^{p_n,q_n}_{g,0}] \times |q_n\theta - p_n| = 0.$$

*Then the equivalent statements of proposition **??** are true.*

Proof. Given $\varepsilon \in]0,1[$, one can fix two integers $q \geq 5$ and $p \in [\![1, q-1]\!]$ such that

$$\mathbf{E}[T^{p,q}_{g,0}] \times |q\theta - p| \leq \varepsilon^2.$$

Since

$$(q-1) \leq \frac{q^2-1}{6} \leq \mathbf{E}[T^{p,q}_{g,0}],$$

one has $(q-1)|q\theta - p| \leq \varepsilon^2 < 1$, so the results of the last subsection apply.

We now omit the superscripts p, q. For every $t \geq 1$, set $G_t = g_{\eta_t} \circ \cdots \circ g_{\eta_1}$ and $Z_t = \iota(Y_t)$. Let $t(\varepsilon) = \lfloor \mathbf{E}[T_{g,0}]/\varepsilon \rfloor$. By Markov inequality,

$$\mathbf{P}[G_{t(\varepsilon)}(Z_0) \neq G_{t(\varepsilon)}(0)] = \mathbf{P}[T^{p,q}_{g,0} \geq t(\varepsilon)+1] \leq \frac{\mathbf{E}[T^{p,q}_{g,0}]}{t(\varepsilon)+1} \leq \varepsilon.$$

But

$$[Z_{t(\varepsilon)} \neq G_{t(\varepsilon)}(Z_0)] \subset \bigcup_{t=1}^{t(\varepsilon)} [Z_t \neq g_{\eta_t}(Z_{t-1})],$$

so lemma **??** yields

$$\mathbf{P}[Z_{t(\varepsilon)} \neq G_{t(\varepsilon)}(Z_0)] \leq t(\varepsilon) \times \frac{1}{2}|q\theta - p| \leq \frac{1}{2}\varepsilon^{-1}\mathbf{E}[T_{g,0}^{p,q}]|q\theta - p| \leq \varepsilon/2.$$

Hence,

$$\mathbf{P}[Z_{t(\varepsilon)} \neq G_{t(\varepsilon)}(0)] \leq 3\varepsilon/2.$$

Let $\zeta = g_0 \circ \cdots \circ g_{\eta_{-t(\varepsilon)+1}}(0)$ and call Υ_0 the middle of the interval I_ζ (remind that the length of this interval is at most $2/q$). Then Υ_0 is a measurable function of the sequence $(\eta_t)_{t\leq 0}$ and by stationarity,

$$\mathbf{P}\big[|Y_0 - \Upsilon_0| > 1/q\big] \leq \mathbf{P}[Y_0 \notin I_\zeta] = \mathbf{P}[Z_0 \neq \zeta] \leq 3\varepsilon/2.$$

Since ε can be taken as small as one wants, the conclusion follows.

3 Proof of proposition ??

Let us define real numbers $y_0, \ldots, y_{q-1}$ in the same way as $x_0, \ldots, x_{q-1}$ by replacing θ with p/q: for every $\ell \in [\![0, q-1]\!]$, let

$$y_\ell := \ell \times \frac{p}{q} - \left\lfloor \ell \times \frac{p}{q} \right\rfloor = \frac{(\ell p) \bmod q}{q} = \frac{h(\ell)}{q}.$$

Then for every $k \in [\![0, q-1]\!]$, $y_{h^{-1}(k)} = k/q$, so $0 = y_{h^{-1}(0)} < y_{h^{-1}(1)} < \ldots < y_{h^{-1}(q-1)}$. The idea is to check that inequalities $-1/u < q\theta - p < 1/(q-u)$ imply that the real numbers $x_0, \ldots, x_{q-1}$ are close to real numbers $y_0, \ldots, y_{q-1}$ and are in the same order.

Preliminary. First, let us prove that

$$\forall k \in [\![0, q-1]\!], \quad x_{h^{-1}(k)} = \frac{k}{q} + h^{-1}(k)\Big(\theta - \frac{p}{q}\Big). \tag{2}$$

In equality **??**, equality modulo 1 follows from the definition of $x_{h^{-1}(k)}$ and $y_{h^{-1}(k)}$ and from the equality $y_{h^{-1}(k)} = k/q$. So it remains to check that the right-hand side belongs to $[0, 1[$, like $x_{h^{-1}(k)}$.

If $k > 0$, the inequalities $q\theta - p > -1/u$ and $h^{-1}(k) \leq ku$ (since $ku \geq 0$ and $h^{-1}(k) = (ku) \mod q$) yield

$$\frac{k}{q} + h^{-1}(k)\Big(\theta - \frac{p}{q}\Big) \geq \frac{k}{q} - \frac{h^{-1}(k)}{qu} \geq 0,$$

whereas the inequalities $h^{-1}(k) > 0$, $q\theta - p < 1/(q-u)$ and $h^{-1}(k) \leq (q-k)(q-u)$ (since $h^{-1}(k) = ((q-k)(q-u)) \mod q$ and $(q-k)(q-u) \geq 0$) yield

$$\frac{k}{q} + h^{-1}(k)\Big(\theta - \frac{p}{q}\Big) < \frac{k}{q} + \frac{h^{-1}(k)}{q(q-u)} \leq \frac{k}{q} + \frac{q-k}{q} = 1.$$

Equality **??** follows. If $k = 0$, then $h^{-1}(k) = 0$, so the equality **??** still holds.

Proof of items 1, 2, 3 and 4. For every $k \in [\![0, q-2]\!]$, $h^{-1}(k+1) \equiv h^{-1}(k)+u \quad [q]$.

If $h^{-1}(k) \leq q-u-1$, then $h^{-1}(k+1) = h^{-1}(k)+u$, so equality **??**, inequality $q\theta - p > -1/u$ and equality $up - vq = 1$ yield

$$x_{h^{-1}(k+1)} - x_{h^{-1}(k)} = \frac{1}{q} + u\Big(\theta - \frac{p}{q}\Big) = u\theta - v > 0.$$

If $q-u \leq h^{-1}(k) \leq q-2$, then $h^{-1}(k+1) = h^{-1}(k)-(q-u)$, so equality **??**, inequality $q\theta - p < 1/(q-u)$ and equality $up - vq = 1$ yield

$$x_{h^{-1}(k+1)} - x_{h^{-1}(k)} = \frac{1}{q} - (q-u)\Big(\theta - \frac{p}{q}\Big) = (p-v) - (q-u)\theta > 0.$$

By the same arguments, we have also

$$1 - x_{h^{-1}(q-1)} = \frac{1}{q} - (q-u)\Big(\theta - \frac{p}{q}\Big) = (p-v) - (q-u)\theta > 0.$$

As a result, we get $0 = x_{h^{-1}(0)} < x_{h^{-1}(1)} < \ldots < x_{h^{-1}(q-1)} < 1$, so the intervals $J_k = [x_{h^{-1}(k)}, x_{h^{-1}(k+1)}[$ for $k \in [\![0, q-2]\!]$ and $J_{q-1} = [x_{h^{-1}(q-1)}, 1[$ form a partition of $\mathbf{I}$. But $J_k = I_{h^{-1}(k)}$ for every $k \in [\![0, q-1]\!]$. Items 1, 2, 3 and 4 follow.

Proof of item 5. Under the assumption of item 5 that $|q\theta - p| < \min(1/u, 1/(q-u))$, we have

$$u\theta - v = u\Big(\theta - \frac{p}{q}\Big) + u\frac{p}{q} - v < \frac{u}{qu} + \frac{1}{q} = \frac{2}{q}$$

and

$$(p-v) - (q-u)\theta = (p-v) - (q-u)\frac{p}{q} - (q-u)\Big(\theta - \frac{p}{q}\Big) \leq \frac{1}{q} + \frac{q-u}{q(q-u)} = \frac{2}{q}.$$

Items 5 follows.

Proof of items 6, 7 and 8. By definition, the map T_θ coincides with a translation on each interval $[0, 1-\theta[$ and $[1-\theta, 1[$, sends $1-\theta$ on 0 and sends each x_ℓ on x_{l+1}. To derive item 6, it suffices to check that $1-\theta$ belongs to I_{q-u-1} or to I_{q-1}. To do this, we use again equality **??** and and equality $up - vq = 1$.

Since $q-u-1 = h^{-1}(q-1-p)$, so we get

$$\begin{aligned} x_{q-u-1} - (1-\theta) &= \frac{q-1-p}{q} + (q-u-1)\Big(\theta - \frac{p}{q}\Big) + \theta - 1 \\ &= (q-u)\theta - (p-v) < 0. \end{aligned}$$

If $u \neq 1$, then $p \neq 1$, so $0 \leq q+1-p \leq q-1$ and $u-1 = h^{-1}(q+1-p)$. We get

$$\begin{aligned} x_{u-1} - (1-\theta) &= \frac{q+1-p}{q} + (u-1)\Big(\theta - \frac{p}{q}\Big) + \theta - 1 \\ &= u\theta - v > 0. \end{aligned}$$

Last, $q-1 = h^{-1}(q-p)$, so we get

$$\begin{aligned} x_{q-1} - (1-\theta) &= \frac{q-p}{q} + (q-1)\Big(\theta - \frac{p}{q}\Big) + \theta - 1 \\ &= q\theta - p. \end{aligned}$$

If $\theta > p/q$, we get $x_{q-u-1} < 1-\theta < x_{q-1}$, so $1-\theta \in [x_{q-u-1}, x_{q-1}[= I_{q-u-1}$ and

$$T_\theta(I_{q-u-1}) = [x_{q-u}, 1[\cup [0, x_{q-1}+\theta-1[= I_{q-u} \cup [0, q\theta - p[.$$

$$T_\theta(I_{q-1}) = [x_{q-1}+\theta-1, x_u[= [q\theta - p, x_u[= I_0 \setminus [0, q\theta - p[.$$

If $\theta \leq p/q$, we get that $1-\theta \in I_{q-1}$ since $I_{q-1} = [x_{q-1}, x_{u-1}[$ if $u \neq 1$ and $I_{q-1} = [x_{q-1}, 1[$ otherwise. As T_θ sends the upper bound of I_{q-1} on x_u, we get

$$T_\theta(I_{q-1}) = [x_{q-1}+\theta, 1[\cup [0, x_u[= [1+q\theta-p, 1[\cup I_0.$$

$$T_\theta(I_{q-u-1}) = [x_{q-u}, x_{q-1}+\theta-1[= [x_{q-u}, 1+q\theta-p[= I_{q-u} \setminus [1+q\theta-p, 1[.$$

Items 6,7 and 8 follow.

4 Proof of theorem ??

We will use repeatedly the following classical fact (see for example [**?**], chapter 10, section 14, subsection 4): given two positive integers a and b, the expected reaching time of $\{-a, b\}$ by a simple symmetric random walk in $\mathbf{Z}$ starting at 0 is ab. As a result, given two integers $\ell \geq k \geq 0$ the expected reaching time of $\overline{0}$ by a simple symmetric random walk in $\mathbf{Z}/\ell\mathbf{Z}$ starting at $\overline{k}$ is $k(\ell - k)$.

Since the integers $q > p > 0$ are fixed, we omit the superscripts p, q. We begin the proof with the second part, since it is simpler and helps us to prove the first part.

4.1 Proof of the second part

For every $t \geq 0$, set $\mathcal{F}_t = \sigma(Z_0, \eta_1, \ldots, \eta_t)$,

$$Z_t = g_{\eta_t} \circ \cdots \circ g_{\eta_1}(Z_0), \quad Z'_t = g_{\eta_t} \circ \cdots \circ g_{\eta_1}(z'_0), \quad X_t = \overline{Z_t - Z'_t},$$

where the bar indicates the equivalence class in $\mathbf{Z}/q\mathbf{Z}$. Then

$$T_{g,z'_0} = \inf\{n \geq 0 : X_t = \overline{0}\}.$$

After time T_{g,z'_0}, the processes Z and Z' coincide, so X stays at $\overline{0}$.

By construction, the processes $Z = (Z_t)_{t\geq 0}$ and $Z' = (Z'_t)_{t\geq 0}$ are Markov chains in the filtration $(\mathcal{F}_t)_{t\geq 0}$. The definition of the maps g_0 and g_1 yields for every $n \geq 1$

$$Z_t = g_{\eta t}(Z_{t-1}) = (Z_{t-1} - \xi_t) \mod q \text{ where } \xi_t = (\eta_t + \mathbf{1}_{L^c}(Z_{t-1})) \mod 2,$$

$$Z'_t = g_{\eta t}(Z'_{t-1}) = (Z'_{t-1} - \xi'_t) \mod q \text{ where } \xi'_t = (\eta_t + \mathbf{1}_{L^c}(Z'_{t-1})) \mod 2.$$

The random variables ξ_t and ξ'_t are $\mathcal{F}_t$-measurable and are uniform on $\{0, 1\}$ conditionally on $\mathcal{F}_{t-1}$; they coincide on the event $[\mathbf{1}_L(Z_{t-1}) = \mathbf{1}_L(Z'_{t-1})]$ and add up to 1 on its complement. Hence

$$\begin{array}{ll} X_t = X_{t-1} - \overline{2\xi_t - 1} & \text{if } \mathbf{1}_L(Z_{t-1}) \neq \mathbf{1}_L(Z'_{t-1}) \\ X_t = X_{t-1} & \text{otherwise.} \end{array}$$

Define stopping times $(\tau_n)_{n\geq 0}$ and $(\sigma_n)_{n\geq 1}$ by $\tau_0 = 0$ and for every $n \geq 1$,

$$\sigma_n = \inf\{t \geq \tau_{n-1} : \mathbf{1}_L(Z_t) \neq \mathbf{1}_L(Z'_t)\} \text{ and } \tau_n = \sigma_n + 1.$$

Therefore

$$\tau_n = \inf\{t > \tau_{n-1} : X_t \neq X_{\tau_{n-1}}\} \text{ on the event } [\tau_{n-1} < +\infty],$$

so

$$T_{g,z'_0} = \tau_N \text{ where } N = \inf\{n \geq 0 : Z_{\tau_n} = Z'_{\tau_n}\} = \inf\{n \geq 0 : X_{\tau_n} = \overline{0}\}.$$

In particular, $T_{g,z'_0} \geq N$. We now introduce a very crude upper bound.

Lemma 15 *Let z and z' be two distincts elements in $[\![0, q-1]\!]$. Then a deterministic walk in $[\![0, q-1]\!]^2$ starting from (z, z') and making steps equal to $(-1, -1)$ modulo q reaches the set $L \times L^c \cup L^c \times L$ in at most $q-2$ steps.*

Proof. The map $k \mapsto \mathbf{1}_L(k \bmod q)$ from $\mathbf{Z}$ to $\mathbf{Z}$ is q-periodic by construction. Call ℓ its least period. Then $q = d\ell$ for some integer $d \geq 1$, and

$$p = |L| = \sum_{k=0}^{q-1} \mathbf{1}_L(k \bmod q) = d \sum_{k=0}^{\ell-1} \mathbf{1}_L(k \bmod q).$$

Hence d divides p and q. Since p and q are relatively prime, we get $d = 1$, so $\ell = q$. Therefore, there are at least two integers $k \in [\![0, q-1]\!]$ such that $\mathbf{1}_L\big((z-k) \bmod q\big) \neq \mathbf{1}_L\big((z'-k) \bmod q\big)$. The statement follows. □

Actually, the upper bound $q-2$ above corresponds to the worst case, namely when $z' - z \equiv \pm u[q]$. We will get and use better bounds in the next section. At the moment, we continue the proof of theorem **??** with this rough estimate.

On the event $[\tau_{n-1} < T_{g,z'_0}]$ and on the time interval $[\![\tau_{n-1}, \sigma_n]\!]$, the process $(\overline{Z_t}, \overline{Z'_t})$ coincides with a random walk on $(\mathbf{Z}/q\mathbf{Z})^2$ whose steps are uniformly distributed on the pair $\{(\overline{0}, \overline{0}), (\overline{-1}, \overline{-1})\}$. By lemma **??**, we get

$$\mathbf{E}[\tau_n - \tau_{n-1} | \tau_{n-1} < T_{g,z'_0}] = \mathbf{E}[\sigma_n - \tau_{n-1} | \tau_{n-1} < T_{g,z'_0}] + 1 \leq 2(q-2) + 1 \leq 2q.$$

Therefore, $\mathbf{P}[\tau_n < +\infty | \tau_{n-1} < T_{g,z'_0}] = 1$. A recursion shows that $\tau_n < +\infty$ almost surely on the event $[n \leq N]$, whereas $\tau_n = +\infty$ on the event $[n > N]$, so the events $[\tau_{n-1} < T_{g,z'_0}]$ and $[n \leq N]$ almost surely coincide. Putting things together, we derive

$$\mathbf{E}[T_{g,z'_0}] = \sum_{n \geq 1} \mathbf{E}[(\tau_n - \tau_{n-1}) \mathbf{1}_{n \leq N}] \leq \sum_{n \geq 1} 2q \mathbf{P}[n \leq N] = 2q \mathbf{E}[N].$$

But the process $(X_{\tau_n})_{0 \leq n \leq N}$ is a simple symmetric random walk on the group $\mathbf{Z}/q\mathbf{Z}$ up to its hitting time of $\overline{0}$, whose initial position is uniform on $\mathbf{Z}/q\mathbf{Z}$. Thus

$$\mathbf{E}[N] = \frac{1}{q} \sum_{k=0}^{q-1} k(q-k) = \frac{1}{q}\Big(\frac{(q-1)q^2}{2} - \frac{(q-1)q(2q-1)}{6}\Big) = \frac{(q-1)(q+1)}{6} \leq \frac{q^2}{6}.$$

Since $T_{g,z'_0} \geq N$, we get $(q^2-1)/6 \leq \mathbf{E}[T_{g,z'_0}] \leq q^3/3$ as desired.

4.2 Proof of the first part

The proof relies on the following lemma. For every $t \geq 0$, we set $G_t = g_{\eta_t} \circ \cdots \circ g_{\eta_1}$.

Lemma 16 *Let R be a subset of $[\![0, q-1]\!]$ with size $k \geq 2$. Set*

$$T_R = \inf\{t \geq 0 : |G_t(R)| < k\}.$$

Then

$$\mathbf{E}[T_R] \leq \frac{2q^3}{k^2} \text{ if } k \text{ divides } q \text{ or } k = 2,$$
$$\mathbf{E}[T_R] \leq \frac{4q^3}{(k+1)^2} \text{ if } k \geq 3.$$

Proof. Set $R = \{z_0, \ldots, z_{k-1}\}$ with $z_0 < \ldots < z_{k-1}$ and set $z_k = z_0$. We define processes $Z^0, \ldots, Z^{k-1}$, $Z^k = Z^0$, $D^0, \ldots, D^{k-1}$ and D taking values in $[\![0, q-1]\!]$ by

$$Z_t^i = G_t(z_i), \quad D_t^i = \left(Z_t^{i+1} - Z_t^i\right) \mod q, \quad D_t = \min(D_t^0, \ldots, D_t^{k-1}).$$

Let us define a process I taking values in the collection of all non-empty subsets of $[\![0, k-1]\!]$ by

$$I_t = \{i \in [\![0, k-1]\!] : D_t^i = D_t\}.$$

All these processes are adapted to the filtration defined by $\mathcal{F}_t = \sigma(\eta_1, \ldots, \eta_t)$.

For each $i \in [\![0, k-1]\!]$, the increments of the process Z^i are 0 or -1 modulo q, so the increments of the process D^i are 1, 0 or -1 modulo q. Moreover, if $D_t^i = 0$, then $D_s^i = 0$ for all $s \geq t$.

Therefore, at each time t, the positions $Z_t^0, \ldots, Z_t^{k-1}$ are in the same cyclic order (in a large sense since there may be equalities) as the initial positions $z_0, \ldots, z_{k-1}$, and the sum $D_t^0 + \cdots + D_t^{k-1}$ remains constant equal to q, so $D_t \leq q/k$. We also deduce that

$$T_R = \inf\{t \geq 0 : D_t = 0\}.$$

We now adapt the arguments given in the last subsection to our present situation. Note that $D_{t+1}^i = D_t^i$ on the event $[\mathbf{1}_L(Z_t^i) = \mathbf{1}_L(Z_t^{i+1})]$, whereas $\mathbf{P}[D_{t+1}^i = D_t^i + 1 | \mathcal{F}_t] = \mathbf{P}[D_{t+1}^i = D_t^i - 1 | \mathcal{F}_t] = 1/2$ on the event $[\mathbf{1}_L(Z_t^i)) \neq \mathbf{1}_L(Z_t^{i+1})]$.

Define stopping times $(\tau_n)_{n \geq 0}$ and $(\sigma_n)_{n \geq 1}$ by $\tau_0 = 0$ and for every $n \geq 1$,

$$\sigma_n = \inf\{t \geq \tau_{n-1} : \exists i \in I_t, \quad \mathbf{1}_L(Z_t^i) \neq \mathbf{1}_L(Z_t^{i+1})\} \text{ and } \tau_n = \sigma_n + 1.$$

Since the process D cannot vary (although the process I may increase) during the time intervals $[\tau_{n-1}, \sigma_n]$, one has $T_R = \tau_N$ where N is some random positive index, possibly infinite, and lemma **??** yields again $\mathbf{E}[\tau_n - \tau_{n-1} | \tau_{n-1} < +\infty] \leq 2q$, so $\mathbf{E}[\tau_R] \leq 2q\mathbf{E}[N]$.

Moreover, on each event $[\sigma_n < T_R \ ; \ i \in I_{\sigma_n}]$, one has

$$\mathbf{P}[D_{\tau_n} = D_{\tau_{n-1}} - 1 | \mathcal{F}_{\sigma_n}] \geq \mathbf{P}[D_{\sigma_n + 1}^i = D_{\sigma_n}^i - 1 | \mathcal{F}_{\sigma_n}] = \frac{1}{2}.$$

Set $m = \lfloor q/k \rfloor \geq 1$. We derive a stochastic domination of the process $(D_{\tau_n})_{0 \leq n \leq N}$ by a Markov chain M on the state space $[\![0, m]\!]$, starting at m and killed immediatly after hitting 0, with transition probabilities given by

$$P(d, d-1) = 1/2 \qquad \text{if } 1 \leq d \leq m,$$
$$P(d, d+1) = 1/2 \quad \text{if } 1 \leq d \leq m-1,$$
$$P(m, m) = 1/2.$$

Therefore, $\mathbf{E}[N]$ is bounded above by the expected hitting time of 0 by M, which is also the expected hitting time of $\overline{0}$ by a simple symmetric random walk on $\mathbf{Z}/(2m+1)\mathbf{Z}$ starting at $\overline{m}$, so $\mathbf{E}[N] \leq m(m+1)$.

Case where k divides q. In this case, $q = km$, so $D_t = m$ if and only if all D_t^i are equal to m. When the process is at m, it goes necessarily to $m-1$ as soon as one of the processes D^i varies. Thus we may modify the transition probabilities of the dominating chain M by setting $P(m, m-1) = 1$, so the expected hitting time of 0 by M becomes the expected hitting time of $\overline{0}$ by a simple symmetric random walk on $\mathbf{Z}/2m\mathbf{Z}$ starting at $\overline{m}$, which is m^2. Note that if $k \geq 3$, then $m^2 = q^2/k^2 \leq 2q^2/(k+1)^2$.

Case where k does not divide q. If $k = 2$, then $q = 2m+1$, so $q^2/4 \geq m(m+1)$. If $k \geq 3$ and k does not divide q, then $q \geq km+1$, so

$$\begin{aligned}\frac{q^2}{m(m+1)} &\geq \frac{k^2m^2 + (2k-1)m + m + 1}{m(m+1)} \\ &= \frac{k^2m + (2k-1)}{m+1} + \frac{1}{m} \\ &= k^2 - \frac{(k-1)^2}{m+1} + \frac{1}{m}\end{aligned}$$

By derivating, one checks that the right hand side is an increasing function of $m \in [1, \infty[$, so

$$\frac{q^2}{m(m+1)} \geq k^2 - \frac{(k-1)^2}{2} + 1 = \frac{(k+1)^2}{2}.$$

Hence $m(m+1) \leq 2q^2/(k+1)^2$. The proof is complete.

Let us now prove the first part of theorem **??**.

For every $t \geq 0$, call R_t the range of the map G_t. For every $k \in [\![1, q]\!]$, set

$$T_k = \inf\{t \geq 1 : |R_t| \leq k\}.$$

Then $0 = T_q \leq \ldots \leq T_1 = T_c$, so

$$T_c = \sum_{k=2}^{q} (T_{k-1} - T_k) = \sum_{k=2}^{q} (T_{k-1} - T_k)\mathbf{1}_{\left[|R_{T_k}| = k\right]}.$$

Applying Markov property at time T_k and lemma **??** to the set $|R_{T_k}|$ yields

$$\mathbf{E}\big[T_1 - T_2 \big| \mathcal{F}_{T_2}\big] \leq \frac{q^3}{2} \text{ on the event } \big[|R_{T_2}| = 2\big]$$

and for every $k \in [\![3, q]\!]$,

$$\mathbf{E}\big[T_{k-1} - T_k \big| \mathcal{F}_{T_k}\big] \leq \frac{4q^3}{(k+1)^2} \text{ on the event } \big[|R_{T_k}| = k\big].$$

Hence,

$$\mathbf{E}[T_1] \leq \frac{q^3}{2} + \sum_{k=3}^{q} \frac{4q^3}{(k+1)^2} = q^3\Big(\frac{1}{2} + 4\Big(\frac{\pi^2}{6} - 1 - \frac{1}{4} - \frac{1}{9}\Big)\Big) = q^3\Big(\frac{2\pi^2}{3} - \frac{89}{18}\Big) \leq \frac{5q^3}{3}.$$

5 Proof of theorem ??

In the whole section, we assume that $\theta \in]0, 1/2[$, so $\mathrm{dist}(\theta, \mathbf{Z}) = \theta$. Therefore, we will consider rational approximations p/q, where $q > p > 0$ are relatively prime integers such that $p/q < 1/2$. These approximations will be given by convergents of the continued fraction expansion of θ.

5.1 Reminders on continued fraction expansions

Given any integer a_0 and positive integers $(a_n)_{n\geq 1}$, we set

$$[a_0; a_1, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Every irrational number θ admits a unique expansion

$$\theta = [a_0; a_1, a_2, a_3, \cdots] = \lim_{n\to+\infty} [a_0; a_1, \cdots, a_n],$$

provided by a variant of Euclidean algorithm, where we set recursively

$$a_0 := \lfloor \theta \rfloor, \quad \theta_1 := \frac{1}{\theta - a_0}, \quad a_1 := \lfloor \theta_1 \rfloor, \quad \theta_2 := \frac{1}{\theta_1 - a_1}, ...$$

The positive integers $(a_n)_{n\geq 1}$ thus defined are called the *partial quotients* of the continued fraction expansion of θ.

Define two sequences $(p_n)_{n\geq -2}$ and $(q_n)_{n\geq -2}$ of integers by $p_{-2} = 0$, $q_{-2} = 1$, $p_{-1} = 1$, $q_{-1} = 0$, and for every $n \geq 0$,

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

A recursion yields $q_n \geq F_{n+1}$ for every $n \geq 0$, where $(F_n)_{n\geq 0}$ is the Fibonacci sequence with first terms $F_0 = 0$ and $F_1 = 1$. When $\theta \in]0, 1/2[$, the stronger inequality $q_n \geq \phi^n$ holds for every $n \geq 0$, where ϕ is the golden ratio. In every cases, the sequence $(q_n)_{n\geq 0}$ is positive, non-decreasing and goes to infinity.

A recursion shows that for every $n \geq 0$, and $x > 0$,

$$\frac{x p_{n-1} + p_{n-2}}{x q_{n-1} + q_{n-2}} = [a_0, a_1, \cdots, a_{n-1}, x].$$

In particular,

$$\frac{p_n}{q_n} = [a_0; a_1, \cdots, a_n].$$

Moreover, p_n and q_n are relatively prime since $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$.

The following inequalities hold

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \theta < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

In particular, the difference $\theta - p_n/q_n$ has the same sign as $(-1)^n$ and

$$\left|\theta - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2}.$$

Hence the sequence $(p_n/q_n)_{n\geq 0}$ converges to θ.

By definition, the convergents of θ are the rational numbers $p_n/q_n = [a_0; a_1, \cdots, a_n]$ and the semiconvergents of θ are the rational numbers

$$\frac{bp_{n-1}+p_{n-2}}{bq_{n-1}+q_{n-2}} = [a_0, a_1, \cdots, a_{n-1}, b], \text{ where } n \geq 1 \text{ and } b \in [\![1, a_n - 1]\!].$$

5.2 Using extended Euclidean algorithm to get a sharper estimate

From now on, we assume that $\theta \in]0, 1/2[$, so $p_0 = a_0 = 0$ and $0 < p_n \leq q_n/2 < q_n$ for $n \geq 1$. Hence the results of subsection **??** apply when $(p, q) = (p_n, q_n)$ for some $n \geq 1$.

We fix $n \geq 1$ and $(p, q) = (p_n, q_n)$, so we omit the superscripts p, q. We now want to get a shaper estimate than the crude upper bound given by lemma **??**. Recall that $L = h^{-1}([\![0, p-1]\!])$ where h is the permutation map defined by $h(z) = (pz) \mod q$ on the set $[\![0, q-1]\!]$.

Let z and z' be two distincts elements in $[\![0, q-1]\!]$. The number of steps $(-1, -1)$ modulo q required to reach the set $L \times L^c \cup L^c \times L$ from (z, z') is also the number of steps $(-p, -p)$ modulo q required to reach the set $[\![0, p-1]\!] \times [\![p, q-1]\!] \cup [\![p, q-1]\!] \times [\![0, p-1]\!]$ from $(h(z), h(z'))$.

Denote by $d_q(z, z')$ the distance modulo q between z and z'. Then the upper bound we will give is a function of $d_q(h(z), h(z'))$, which is a function of $d_q(z, z')$, namely

$$d_q(h(z), h(z')) = \text{dist}(pd_q(z, z'), q\mathbf{Z}).$$

Indeed, if $z' - z \equiv \pm d \quad [q]$, then $h(z') - h(z) \equiv p(z' - z) \equiv \pm pd \quad [q]$.

To do this, we apply the extended euclidean algorithm to the integers p and q. Since p and q are relatively prime and $p/q = [0, a_1, \cdots, a_n]$, this algorithm yields remainders $r_{-1} = q > r_0 = p > r_1 > \ldots > r_{n-1} = 1 > r_n = 0$ such that

$$\begin{aligned}
q &= pa_1 + r_1, \\
p &= r_1 a_2 + r_2, \\
\ldots &= \ldots \\
r_{n-3} &= r_{n-2}a_{n-1} + r_{n-1}, \\
r_{n-2} &= r_{n-1}a_n + r_n,
\end{aligned}$$

Extended Euclidean algorithm provides Bezout identities: a recursion shows that

$$\forall k \in [\![0, n]\!], r_k = (-1)^k(q_k p - p_k q).$$

Indeed, $q_0 p - p_0 q = 1 \times p - 0 \times q = p = r_0$ and $q_1 p - p_1 q = a_1 p - q = -r_1$. Given $k \in [\![2, n]\!]$, the equalities $r_{k-2} = (-1)^{k-2}(q_{k-2}p - p_{k-2}q)$ and $r_{k-1} = (-1)^{k-1}(q_{k-1}p - p_{k-1}q)$ yield

$$q_k p - p_k q = a_k(q_{k-1}p - p_{k-1}q) + (q_{k-2}p - p_{k-2}q) = (-1)^k(-a_k r_{k-1} + r_{k-2}) = (-1)^k r_k.$$

As a result, given $k \in [\![0, n]\!]$, making q_k translations of $-p$ modulo q is equivalent to make one translation of $(-1)^{k+1}r_k$ modulo q. This observation yields the next lemma.

Lemma 17 *Let $k \in [\![0, n-1]\!]$ and $d \in [\![r_k, r_{k-1} - 1]\!]$. Let $J \subset [\![0, q-1]\!]$ be a subset containing exactly d elements which are consecutive modulo q. Then J can be reached from anywhere in $[\![0, q-1]\!]$ by making at most $a_1 q_0 + \cdots + a_{k+1}q_k$ translations of $-p$ modulo q.*

Proof. We argue by recursion on k.

First, assume that $k = 0$, so $d \geq r_0 = p$. Since $q = a_1 p + r_1 \leq (a_1 + 1)p$, J can be reached from anywhere in $[\![0, q-1]\!]$ by making at most $a_1 = a_1 q_0$ translations of $-p$ modulo q.

Assume that the property holds at level $k-1$. Let $k \in [\![0, n-1]\!]$ and $d \in [\![r_k, r_{k-1}-1]\!]$. Let $J \subset [\![0, q-1]\!]$ be a subset containing exactly d elements which are consecutive modulo q. Complete J by adding $r_{k-1} - d$ consecutive (modulo q) points to get a subset J' of $[\![0, n-1]\!]$ made with r_{k-1} consective (modulo q) points. These additional points should be on the right of J if k is even, and on the left of J if k is odd. The number of additional points is $r_{k-1} - d \leq r_{k-1} - r_k \leq a_{k+1} r_k$. Therefore, to reach J from anywhere, one may first reach J' by making at most $a_1 q_0 + \cdots + a_k q_{k-1}$ translations of $-p$ modulo q, and then make at most a_{k+1} translations of $(-1)^{k+1} r_k$ modulo q, provided by at most $a_{k+1} q_k$ translations of $-p$ modulo q. This yields the property at level k.

The proof is complete.

We now give the better estimate announced above.

Corollary 18 *Let z and z' be two distincts elements in $[\![0, q-1]\!]$. Assume that the distance $d_q(h(z), h(z')) = \mathrm{dist}(p d_q(z, z'), q\mathbf{Z})$ belongs to $[\![r_k, r_{k-1} - 1]\!]$ with $k \in [\![0, n-1]\!]$ Then a deterministic walk in $[\![0, q-1]\!]^2$ starting from (z, z') and making steps equal to $(-1, -1)$ modulo q reaches the set $L \times L^c \cup L^c \times L$ in at most $a_1 q_0 + \cdots + a_{k+1} q_k$ steps.*

Proof. Let $d = d_q(h(z), h(z')) = \mathrm{dist}(p d_q(z, z'), q\mathbf{Z})$, so $1 \leq d \leq q/2$. By symmetry, one may assume that $h(z') = (h(z) - d) \mod q$.

The number of steps above is also the number of steps $(-p, -p)$ modulo q required to reach the set $[\![0, p-1]\!] \times [\![p, q-1]\!] \cup [\![p, q-1]\!] \times [\![0, p-1]\!]$ from $(h(z), h(z'))$.

This is at most the number of steps $-p$ modulo q required to reach the interval $[\![0, \min(d, p) - 1]\!]$ from $h(z)$ since for every $k \in \mathbf{N}$,

$$(h(z) - kp) \mod q \in [\![0, \min(d, p) - 1]\!] \implies \begin{cases} (h(z) - kp) \mod q \in [\![0, p-1]\!], \\ (h(z') - kp) \mod q \in [\![p, q-1]\!]. \end{cases}$$

Hence lemma **??** applies, yielding the conclusion.

The upper bound provided by corollary **??** is a function of $d_q(h(z), h(z'))$ and also a function of $d_q(z, z')$. Denote by $M(d_q(h(z), h(z'))) = N(d_q(z, z'))$ this upper bound.

Corollary 19 *One has*

$$\sum_{d=1}^{\lfloor q/2 \rfloor} N(d) = \sum_{d=1}^{\lfloor q/2 \rfloor} M(d) \leq q \sum_{k=1}^{n} a_k - q.$$

Proof. For every $d \in [\![1, \lfloor q/2 \rfloor]\!]$, set $\tilde{h}(d) = \mathrm{dist}(pd, q\mathbf{Z})$. Then $N(d) = M(\tilde{h}(d))$ because $d_q(h(z), h(z')) = \tilde{h}(d_q(z, z'))$ for every z and z' in $[\![0, q-1]\!]$. Since p and q are relatively prime, the map $\tilde{h}$ is a permutation on the set $[\![1, \lfloor q/2 \rfloor]\!]$, so

$$\sum_{d=1}^{\lfloor q/2 \rfloor} N(d) = \sum_{d=1}^{\lfloor q/2 \rfloor} M(d).$$

But corollary **??** yields

$$\forall d \in [\![1, \lfloor q/2 \rfloor]\!], \quad M(d) = \sum_{k=0}^{n-1} a_{k+1} q_k \mathbf{1}_{[d \leq r_{k-1}-1]}$$

and for every $k \in [\![0, n-1]\!]$, one has $a_{k+1}q_k = q_{k+1} - q_{k-1}$ and $q_k r_{k-1} \leq q$ since

$$\begin{aligned} q - q_k r_{k-1} &= (-1)^{k-1}(q_{k-1}p_k - p_{k-1}q_k)q - (-1)^{k-1}q_k(q_{k-1}p - p_{k-1}q) \\ &= (-1)^{k-1}q_{k-1}(p_k q - p q_k) \\ &\geq 0. \end{aligned}$$

Hence, one gets

$$\begin{aligned} \sum_{d=1}^{\lfloor q/2 \rfloor} M(d) &= \sum_{k=0}^{n-1} a_{k+1} q_k (r_{k-1} - 1) \\ &= \sum_{k=0}^{n-1} a_{k+1} q_k r_{k-1} - (q_n + q_{n-1} - q_0 - q_{-1}) \\ &\leq q \sum_{k=0}^{n-1} a_{k+1} - q. \end{aligned}$$

The proof is complete.

5.3 Proof of theorem ??

We keep the notations of the last subsections, fix $n \geq 1$ and $(p, q) = (p_n, q_n)$, so we omit the superscripts p, q.

For every $t \geq 0$, set $G_t = g_{\eta_t} \circ \cdots \circ g_{\eta_1}$, $Z_t = G_t(Z_0)$, $Z'_t = G_t(z'_0)$, and $\mathcal{F}_t = \sigma(Z_0, \eta_1, \ldots, \eta_t)$. Consider the stopping time

$$\tau_1 = \inf\{t \geq 0 : (Z_t - Z'_t) \mod q \neq (Z_0 - z'_0) \mod q\}.$$

By definition of the maps g_0 and g_1, one has

$$\tau_1 = \inf\{t \geq 0 : (Z_t, Z'_t) \in L \times L^c \cup L^c \times L\} + 1.$$

Given $z_0 \in [\![0, q-1]\!]$, set $e(z_0, z'_0) = \mathbf{E}[T_{g,z'_0} | Z_0 = z_0]$, $w(z_0, z'_0) = \mathbf{E}[\tau_1 | Z_0 = z_0]$ and call $n(z_0, z'_0)$ the number of steps required to reach the set $L \times L^c \cup L^c \times L$ from (z_0, z'_0) by making steps equal to $(-1, -1)$ modulo q.

Conditionally on $\mathcal{F}_t$ and on the event $[(Z_t, Z'_t) \in L \times L \cup L^c \times L^c]$, the random variable (Z_{t+1}, Z'_{t+1}) equals (Z_t, Z'_t) or $((Z_t - 1) \mod q, (Z'_t - 1) \mod q)$, each possibility having probability $1/2$. Hence if $z_0 \neq z'_0$, then $w(z_0, z'_0) = 2n(z_0, z'_0) + 1$. Proposition **??** yields an upper bound $n(z_0, z'_0) \leq N(d_q(z_0, z'_0))$ so

$$w(z_0, z'_0) \leq W(d_q(z_0, z'_0)) := 2N(d_q(z_0, z'_0)) + 1.$$

But Markov property yields

$$e(z_0, z'_0) \leq w(z_0, z'_0) + \mathbf{E}[e(G_{\tau_1}(Z_0), G_{\tau_1}(z'_0))].$$

and $G_{\tau_1}(z_0') - G_{\tau_1}(z_0) = (z_0' - z_0 \pm 1) \mod q$, each possibility having probability $1/2$.

Let $m = \lfloor q/2 \rfloor$ be the maximum possible value for the distance $d_q(z_0, z_0')$ and set $e_d = \max\{e(z_0, z_0') : d_q(z_0, z_0') = d\}$ for every $d \in [\![0, m]\!]$. Then $e_0 = 0$ and

$$\begin{aligned} e_d &\le W(d) + \frac{1}{2}(e_{d-1} + e_{d+1}) && \text{if } d \in [\![1, m-1]\!], \\ e_m &\le W(m) + e_{m-1} && \text{if } q \text{ is even}, \\ e_m &\le W(m) + \frac{1}{2}(e_{m-1} + e_m) && \text{if } q \text{ is odd}. \end{aligned}$$

Hence $e_d - e_{d-1} \le 2W(d) + e_{d+1} - e_d$ for every $d \in [\![1, m-1]\!]$, and $e_m - e_{m-1} \le 2W(m)$, whatever the parity of q is. By addition, we get successively

$$\forall d \in [\![1, m]\!], \quad e_d - e_{d-1} \le 2\sum_{j=d}^{m} W(j) \le 2S \text{ where } S := \sum_{j=1}^{m} W(j),$$

$$\forall i \in [\![0, m]\!], \quad e_i = \sum_{d=1}^{i} (e_d - e_{d-1}) \le 2iS.$$

But Z_0 is uniform on $[\![0, q-1]\!]$, so

$$\mathbf{E}[T_{g,z_0'}] = \frac{1}{q} \sum_{z_0=0}^{q-1} e(z_0, z_0').$$

If q is even, i.e. $q = 2m$, we derive

$$\mathbf{E}[T_{g,z_0'}] \le \frac{1}{2m}(e_0 + 2e_1 + \cdots + 2e_{m-1} + e_m) \le \frac{1}{m}\Big(2\sum_{i=1}^{m-1} i + m\Big)S = mS.$$

If q is odd, i.e. $q = 2m+1$, we derive

$$\mathbf{E}[T_{g,z_0'}] \le \frac{1}{2m+1}(e_0 + 2e_1 + \cdots + 2e_m) \le \frac{4}{2m+1}\sum_{i=1}^{m} iS = \frac{2m(m+1)}{2m+1}S \le \frac{2m+1}{2}S.$$

In both cases, we get

$$\mathbf{E}[T_{g,z_0'}^{p,q}] \le \frac{q}{2}\sum_{j=1}^{m} W(j) \le \frac{q}{2}\Big(2\sum_{j=1}^{m} N(j) + m\Big) \le q^2 \sum_{k=1}^{n} a_k,$$

by lemma **??**. The proof is complete.

Acknowledgement. I thank my collegues J. Brossard and A. Coquio and the referee for their careful reading of this paper and I thank T. De la Rue and J.P. Thouvenot for stimulating conversations.

Index of notations

We recall here the notations widely used throughout the paper.

Numbers

θ fixed irrational number. By convenience, we assume that $\theta \in [0,1[$ and even that $\theta \in [0,1/2[$ in section **??**. This is not a true restriction.

$r = p/q$ denotes a good rational aproximation of θ, where p and q are relatively prime integers and $q \geq 2$. Here, good means that $-1/u < q\theta - p < 1/(q-u)$ where $u \in [\![1, q-1]\!]$ is the inverse of p modulo q. We call $v \in \mathbf{Z}_+$ the integer such that $up - vq = 1$.

Dynamical systems considered

S unilateral shift on $X = \{0,1\}^{\mathbf{Z}_+}$, endowed with the measure $\mu = \bigotimes_{n\geq 0}(\delta_0 + \delta_1)/2$.

$T_\theta : y \mapsto (y+\theta) \mod 1$ on $\mathbf{I} = [0,1[$, endowed with the Lebesgue measure ν.

$S_\theta = [T_\theta, \mathrm{Id}] : (x,y) \mapsto \big(x(0), (y + x(0)\theta) \mod 1\big)$ on $X \times [0,1[$, endowed with the measure $\mu \otimes \nu$.

$T_{p,q} : z \mapsto (z+p) \mod q$ on $[\![0, q-1]\!]$, endowed with the uniform measure ν_q.

$S_{p,q} = [T_{p,q}, \mathrm{Id}] : (x,z) \mapsto \big(x(0), (z + x(0)p) \mod q\big)$ on $X \times [\![0, q-1]\!]$, endowed with the measure $\mu \otimes \nu_q$.

Partitions

$\alpha_\theta = \{A_0^\theta, A_1^\theta\}$ the partition considered by Parry, and also the associated map from $X \times \mathbf{I}$ to $\{0,1\}$.

$\alpha_{p,q}$ discrete analogue on $X \times [\![0, q-1]\!]$.

$\Phi_\theta : (x,y) \mapsto \alpha_\theta\big((S_\theta^n(x,y))_{n\geq 0}\big)$ the associated factor map.

$\iota = \{I_0, \dots, I_{q-1}\}$ the partition of $\mathbf{I} = [0,1[$ provided by the subdivision $(x_k)_{0\leq k\leq q-1}$, where $x_k = k\theta - \lfloor k\theta \rfloor$. We also denote by ι the associated map from $X \times \mathbf{I}$ to $\{0,1\}$.

Maps

$f_0^\theta(y) = y - \theta \mathbf{1}_{[\theta,1[}(y)$ and $f_1^\theta(y) = y + (1-\theta)\mathbf{1}_{[0,\theta[}(y)$ for $y \in \mathbf{I}$.

$f_0^{p,q}(z) = z - p\mathbf{1}_{[\![p,q-1]\!]}(z)$ and $f_1^{p,q}(z) = z + (q-p)\mathbf{1}_{[\![0,p-1]\!]}(z)$ for $z \in [\![0, q-1]\!]$.

$h(z) = h_{p,q}(z) = (pz) \mod q$ for $z \in [\![0, q-1]\!]$. The map $h_{p,q}$ is a permutation and its inverse is given by $h_{p,q}^{-1}(z) = (uz) \mod q$. We set $L_{p,q} = h_{p,q}^{-1}([\![0, p-1]\!])$.

$g_0^{p,q}(z) = z - \mathbf{1}_{L_{p,q}^c}(z)$ and $g_1^{p,q}(z) = z - \mathbf{1}_{L_{p,q}}(z)$ for $z \in [\![0, q-1]\!]$.

References

[1] R.L. Adler, P.C. Shields, *Skew products of Bernoulli shifts with rotations.* Israel Journal of Mathematics **12**, 215–222 (1972).

[2] R.L. Adler, P.C. Shields, *Skew products of Bernoulli shifts with rotations.* Israel Journal of Mathematics **19**, 228–236 (1974).

[3] J. Feldman, *New K-automorphisms and a problem of Kakutani.* Israel J. Math. 24, no. 1, 16–38 (1976).

[4] J. Feldman, D. Rudolph, *Standardness of sequences of σ-fields given by certain endomorphisms*. Fundamenta Mathematicae. 157, 175–189 (1998).

[5] D. Heicklen, C Hoffman, $[T, T^{-1}]$ *is not standard*. Ergodic Theory and Dynamical Systems 18, no. 4, 875–878 (1998).

[6] C. Hoffman, D. Rudolph *Uniform endomorphisms which are isomorphic to a Bernoulli shift*. Annals of Mathematics, Second Series, Vol. 156, No. 1 (Jul., 2002), pp. 79-101 (2002).

[7] C. Hoffman, D. Rudolph *A dyadic endomorphism which is Bernoulli but not standard*. Israël Journal of Mathematics, Vol. 130, pp. 365-379 (2002).

[8] S. Kalikow, T, T^{-1} *transformation is not loosely Bernoulli.* Ann. of Math. (2) 115, no. 2, 393–409 (1982).

[9] A. Khintchine, *Metrische Kettenbruchprobleme*. Compositio Mathematica, Tome 1, 361–382 (1935).

[10] S. Laurent, *Filtrations à temps discret négatif*. PhD Thesis, Université de Strasbourg, Strasbourg (2004).

[11] C. Leuridan, *Filtration d'une marche aléatoire stationnaire sur le cercle*. Séminaire de Probabilités XXXVI, Springer Lecture Notes in Mathematics 1801, 335–347 (2002).

[12] C. Leuridan, *Filtrations associated to some two-to-one transformations*, to be published in Séminaire de Probabilités LI.

[13] C. Leuridan, *Characterizations of convergents and semi-convergents in continued fraction expansions*, in preparation. French version submited and available on https://hal.archives-ouvertes.fr/hal-02272389.

[14] J. Marklof, A. Strömbergsson, (2017), *The three gap theorem and the space of lattices*, American Mathematical Monthly **124**-8, 741–745 (2017).

[15] I. Meilijson, *Mixing properties of a class of skew-products*. Israel J. Math. 19, 266–270 (1974).

[16] W. Parry, *Automorphisms of the Bernoulli endomorphism and a class of skew-products*. Ergodic Theory and Dynamical Systems 16, 519–529 (1996).

[17] K. Petersen, *Ergodic theory*. Corrected reprint of the 1983 original. Cambridge University Press (1989).

[18] Resnick, S. I., *A probability path*, Reprint of the 2005 Edition, Birkhäuser.

[19] Sós, V. T., *On the distribution mod 1 of the sequence $n\alpha$*, Ann. Univ. Sci. Budapest, Eötvös Sect. Math., 1: 127–134 (1958).

[20] Surányi, J., *Über die Anordnung der Vielfachen einer reellen Zahl mod 1*, Ann. Univ. Sci. Budapest, Eötvös Sect. Math., 1: 107–111 (1958).

[21] Świerczkowski, S., *On successive settings of an arc on the circumference of a circle*, Fundamenta Mathematicae, 46 (2): 187–189, (1959).

[22] A.M. Vershik, *Decreasing sequences of measurable partitions, and their applications*. Dokl. Akad. Nauk SSSR, **193**, 748–751 (1970). English translation: Soviet mathematics - Doklady, **11**, 1007–1011 (1970).