INDISTINGUISHABLE SCENERIES

ELON LINDENSTRAUSS

Abstract. In this paper we give a counter example to a conjecture mentioned in Benjamini and Kesten (1996) about distinguishing sceneries by observing them along a simple random walk, giving an explicit construction of $2^{\aleph_0}$ sceneries that are all pairwise indistinguishable.

1. Introduction

The basic problem we consider is how well can we distinguish two infinite words (sceneries) by observing these words along a simple random walk. This problem was introduced independently by I. Benjamini and by F. den Hollander and M. Keane, and has stimulated a considerable amount of research (Benjamini and Kesten (1996), Howard (1996), Howard (1997), Kesten (1996), Matzinger (1997)). Most of the results proved so far show that many sceneries can be distinguished by these observations. The result presented in this paper is a negative result, and gives some bounds to just how far the positive results can be pushed. A general survey about problems related to observing sceneries along random walks can be found in Kesten (1997).

Let A be a finite or even infinite alphabet. A *scenery* is simply a bi-infinite sequence of symbols from the alphabet A. Suppose that we are given a sequence $f \in A^{\mathbb{N}}$ (*a film*) that was generated (in a random fashion) from a word $w = (\dots, w_{-1}, w_0, w_1 \dots)$ as follows: The first symbol of f is the symbol w_0, the second symbol is w_{α_1} with $\alpha_1 = -1$ or 1 with equal probability, the third is w_{α_2} where $\alpha_2 = \alpha_1 \pm 1$ (again both possibilities are equally probable), etc. Thus f is simply the symbols in w read in a random order according to a simple random walk, and the terminology alludes to the non mathematical description of this situation as a drunken tourist randomly going about in some (one dimensional) scenery, taking every step a picture of his whereabouts.

There are essentially two questions one can ask, both of them are about how much information knowing f gives us about w. One of them, which will not be of interest for us in this paper, can be roughly stated as can one, for a typical scenery w and a typical film

Date: June 20, 1998.

Key words and phrases. Random walk, sceneries, distinguishability, mutually singular measures.

f generated from w, deduce the sequence w from f? (see Matzinger (1997)). The question we consider is more modest: suppose we are given two sceneries w and w', and a film f which was generated either from w or w'. Can we figure out if f was generated from w or from w'? Clearly, for most pairs the set of possible films from w and the corresponding set for w' are very far from being disjoint. So, to make the question interesting we need to consider not only what films are a possible outcome of our drunken tourist's tour, but also the distribution this process induces on the films (naturally, this distribution depends on the scenery). We give a formal definition of this distribution below:

Definition 1.1. *For any $w \in A^{\mathbb{Z}}$ (the scenery), we can construct the map*

$$\Psi_w \colon \{\pm 1\}^{\mathbb{N}} \to A^{\mathbb{N}}$$

by

$$\Psi_w(\epsilon_0, \epsilon_1, \dots) = (w_0, w_{\epsilon_0}, w_{\epsilon_0+\epsilon 1}, \dots).$$

If ω is the 0.5, 0.5 Bernoulli measure on $\{\pm 1\}^{\mathbb{N}}$ we define a probability measure $\rho(w)$ on $A^{\mathbb{Z}}$ (the space of all films) by

$$\rho(w) = \Psi_w(\omega).$$

Intuitively, even if the space of films that correspond to w has a nonempty intersection with the space of films for w', it can still be true that from a typical film one can decide with arbitrarily high level of certainty whether it belongs to w or to w'. The rigorous way to express this is that the measures $\rho(w)$ and $\rho(w')$ are mutually singular — that is, there is a set $C \subset A^{\mathbb{N}}$ so that $\rho(w)[C] = 0$ but $\rho(w')[C] = 1$.

Definition 1.2. *Two sceneries w and w' will be said to be* **distinguishable** *if $\rho(w)$ and $\rho(w')$ are mutually singular. Two sceneries that are not distinguishable, are called* **indistinguishable**.

This notion of distinguishability is somewhat weaker than the usual one, but is more suited for our purposes. We now present a stronger notion of distinguishability, distinguishability by suffixes, that corresponds to the notion of distinguishability in most of the literature on this subject.

Let σ denote both the one sided shift

$$\sigma(x_0, x_1, x_2, \dots) = (x_1, x_2, \dots)$$

and the two sided shift

$$\sigma(\dots, x_{-1}, x_0, x_1, \dots) = (\dots, x_0, x_1, x_2, \dots)$$

It should be clear from the context which operation we use.

Definition 1.3. *For $n \in \mathbb{N}$, and any scenery w, let $\rho_n(w)$ the measure $\sigma^n(\rho(w))$, i.e. the measure corresponding to letters of the alphabet A seen along a simple random walk, after omitting the first n observations.*

Definition 1.4. *Two points w and w' will be said to be* **distinguishable by suffixes** *if for every $n > 0$, $\rho_n(w)$ and $\rho_n(w')$ are mutually singular.*

Clearly, if w is any scenery, and if $\tilde{w}$ is the reflection of w (i.e. $\tilde{w}|_n = w|_{-n}$ for all n) then the distributions $\rho(w)$ and $\rho(\tilde{w})$ are identical, and so w and $\tilde{w}$ are indistinguishable.

A somewhat more interesting example of indistinguishable sceneries can be obtained by looking at w and $\sigma^n w$ for n even, which are rather often indistinguishable (we will explain this in detail latter in this introduction). In fact, for any even n, w and $\sigma^n w$ are *always* not distinguishable by suffixes.

Almost any two sceneries can be distinguished (even only by suffixes) — this is shown in Benjamini and Kesten (1996). The conjecture we disprove is that any two sceneries w and w', such that w' is neither a translation of w nor a translation of $\tilde{w}$, are distinguishable by suffixes. In fact, we construct an example of an uncountable family of sceneries, every two of which are indistinguishable. We remark that our construction can easily be generalized to more general random walks.

To give some idea of why this example works, and some of the ideas we use in the proof, we show that that w and $\sigma^n(w)$ are indistinguishable if $w_0 = w_1 = \cdots = w_n$. Notice that $\rho(\sigma^n w)$ is the distribution on $A^{\mathbb{N}}$ one obtains by reading w along a simple random random walk starting at place n. So, essentially the situation at hand is that we have two drunken tourists, wondering around in the scenery w, one starting at place 0, the other at place n. If we find a way to synchronize the two tourists so that:

- If one looks only at one of the two tourists, the path this tourist goes is a simple random walk ,
- With positive probability, the films the two tourists generate are identical,

then clearly $\rho(\sigma^n w)$ and $\rho(w)$ cannot be mutually singular. A good way to synchronize the two tourists would be if they both went independently of one another, *until* the following event (which we will denote by Q) happens: at the nth step the tourist starting from place zero returns to place zero, having visited up to this time only the places $0, \ldots, n/2$, *and* the second tourist at the nth step also arrives to the 0th place. If Q happens, the second tourist from now on steps in the same way as the first tourist, who continues in his simple random walk. As n is even, there is a non zero probability of Q occuring, and if Q occurs, the films the two tourist generate will be identical — and so $\rho(w)$ and $\rho(\sigma^n w)$ are not singular. Such a synchronization is called a joining (or coupling) of two simple random walks, and is the technical tool we use in our proof.

Essentially, the idea of the construction is the following observation: w and $\sigma^n w$ are many times indistinguishable. We construct many sceneries that are very nearly translates of one another, but not exactly, so that one the one hand these sceneries are still indistinguishable, but on the other hand we allow ourselves enough degrees of freedom so that there is a non-countable number of these sceneries. We present this construction in the following section. In §3 we develop some technical and more or less standard machinery about joinings which we use in §4 to prove that the example we have constructed in §2 has the required properties. Finally, we give some concluding remarks in §5.

The proof presented here is an improved version of the original proof for this result, and is similar to a proof suggested to the author by Prof. Yuval Peres. I would like to thank Prof. Peres for his kind consent for using his ideas (namely using couplings of random walks to simplify the argument) in this article. I would also like to thank the referee for his (or her) helpful suggestions on how to improve the exposition of this article.

2. The example

We now turn to construct the many indistinguishable sceneries. The sceneries we construct will be taken from a shift invariant closed subset of $A^{\mathbb{Z}}$. The words in this shift invariant subset will be in almost 1-1 correspondance to elements of a monothetic group G (a compact commutative group, with an element g_0 that generates a dense subgroup of G).

The monothetic group will depend on a sequence $\{m_k\}_{k=1}^{\infty}$ of positive integers. Define $M_k = \Pi_{i=1}^{k} m_i$, and $M_0 = 1$. For $k' > k$, the group $\mathbb{Z}/M_{k'}\mathbb{Z}$ projects onto $\mathbb{Z}/M_k\mathbb{Z}$ in the natural way ($x \mapsto x \bmod M_k$), and we can define G to be the corresponding inverse limit

$$G = G(m_1, m_2, \dots) := \varprojlim{}_{k\to\infty} \mathbb{Z}/M_k\mathbb{Z}.$$

We recall the definition of an inverse limit: if we are given a sequence of groups G_i and homomorphisms h_i from G_{i+1} onto G_i, their inverse limit is the group

$$\varprojlim{}_{k\to\infty} G_k = \{(g_1, g_2, \dots) : g_i \in G_i \text{ and } h_i(g_{i+1}) = g_i \text{ for all } i\} \tag{1}$$

with the group operation being

$$(f_1, f_2, \dots) + (g_1, g_2, \dots) = (f_1 + g_1, f_2 + g_2, \dots).$$

Let $\pi_k : G \to \mathbb{Z}/M_k\mathbb{Z}$ be the mod M_k map. Define $\gamma_k \colon G \to \mathbb{Z}/m_k\mathbb{Z}$ by

$$\gamma_k(g) = \lfloor \pi_k(g)/M_{k-1} \rfloor.$$

It is possible to view G as a sequence of elements of $\{\mathbb{Z}/M_k\mathbb{Z}\}_{k=1}^{\infty}$ as in (1). An alternative view is that as a set

$$G \overset{\Gamma}{\cong} \{(\gamma_1, \gamma_2, \dots) : \gamma_i \in \{0, 1, \dots, m_i - 1\}\}$$

with the (set theoretic) isomorphism being defined by

$$\Gamma(g) = (\gamma_1(g), \gamma_2(g), \dots)$$

or equivalently by

$$\pi_k(\Gamma^{-1}(\gamma_1, \gamma_2, \dots)) = \sum_{i=1}^{k} \gamma_i M_{i-1}.$$

Essentially what we have done above is to expand the numbers in $\mathbb{Z}$ according to the variable base $\{m_k\}$ and then take a natural compactification of this space.

We can define a one-to-one function $i \colon \mathbb{Z} \to G$ by $\pi_k(i(n)) = n \bmod M_k$ for every k. The subset $i(\mathbb{Z})$ of G can be characterized as the set of g's such that $\gamma_k(g) = 0$ for k large enough. Let $\mathbf{1}$ be $i(1)$. By slight abuse of notation we will sometimes write $g - n$ ($g \in G$ and $n \in \mathbb{Z}$) for $g - n \cdot \mathbf{1} \equiv g - i(n)$.

The subgroups $A_k = \{g \in G : \pi_k(g) = 0\}$ of G form a neighbourhood basis at $\mathbf{0} \in G$. Define $A_0 = G$. We designate for $g \neq \mathbf{0}$,

$$r(g) = \max\{k : g \in A_k\} = \min\{k : \pi_k(g) \neq 0\} - 1, \tag{2}$$

and $r(\mathbf{0}) = +\infty$.

Let A be any alphabet. We are now ready to construct a closed shift invariant subset of $A^{\mathbb{Z}}$ that will be in almost 1-1 correspondence with G. This subset of $A^{\mathbb{Z}}$ will be constructed using an arbitrary sequence

$$\mathbf{a} = (a_0, a_1, \dots) \in A^{\mathbb{N}},$$

as well as the group G, and so we will denote it by $X_{\mathbf{a},G}$.

Definition 2.1. *Given* $\mathbf{a}$ *define* $\phi_{\mathbf{a},G} \colon G \setminus i(\mathbb{Z}) \to A^{\mathbb{Z}}$ *by*

$$\phi_{\mathbf{a},G}(g) = (\dots, a_{r(-g-\mathbf{1})}, a_{r(-g)}, a_{r(-g+\mathbf{1})}, \dots),$$

i.e. the nth coordinate of $\phi_{\mathbf{a},G}(g)$ *is* $a_{r(-g+n\cdot\mathbf{1})}$. *Set* $X_{\mathbf{a},G} := \mathrm{cl}(\phi_{\mathbf{a},G}(G \setminus i(\mathbb{Z})))$, *the closure (in the product topology on* $A^{\mathbb{Z}}$*) of the image of* $\phi_{\mathbf{a},G}$.

Notice that for $g \notin i(\mathbb{Z})$,

$$\phi_{\mathbf{a},G}(g-1) = (\dots, a_{r(-g)}, a_{r(-g+\mathbf{1})}, a_{r(-g+2\cdot\mathbf{1})}, \dots) = \sigma(\phi_{\mathbf{a},G}(g)).$$

The sceneries in $X_{\mathbf{a},G}$ are of the following form: if $w \in X_{\mathbf{a},G}$, then most of the symbols of w are a_0 — all except those symbols that appear at places in some arithmetic progression of the form $n_1 + M_1\mathbb{Z}$ for some $n_1 \in \{0, \dots, m_1 - 1\}$. Of these symbols that appear at places in the arithmetic progression $n_1 + M_1\mathbb{Z}$, most are a_1 — all but those that appear at places in $n_2M_1 + n_1 + M_2\mathbb{Z}$ for some $n_2 \in \{0, \dots, m_2 - 1\}$, and so on. We summarize this description below:

$$w = \dots, a_0, \underbrace{a_1, a_0, \dots, a_0}_{M_1}, \overbrace{\underbrace{a_2, a_0, \dots, a_0}_{M_1}, a_1, a_0, \dots, a_0, a_1, a_0, \dots, a_0}^{M_2}, a_2, a_0, \dots$$

We can relate this picture to the formal definition in Definition 2.1 by noticing that if w and n_1, n_2, ... are as above then

$$\phi_{\mathbf{a},G}(\Gamma^{-1}(n_1, n_2, \dots)) = w,$$

provided $\Gamma^{-1}(n_1, n_2, \dots) \notin i(\mathbb{Z})$. If $\Gamma^{-1}(n_1, n_2, \dots) = n \cdot \mathbf{1} \in i(\mathbb{Z})$, then the sequence n_1, n_2, ... need not uniquely determine w — the symbol $w|_n$ remains undetermined.

Under reasonable conditions ($\mathbf{a}$ is not eventually constant), $\phi_{\mathbf{a},G}(g)$ is one-to-one on $G \setminus i(\mathbb{Z})$. Indeed, by replacing the sequence $\{M_k\}$ with a subsequence if necessary, we can assume that $a_k \neq a_{k-1}$. Let $w \in X_{\mathbf{a},G}$. There would be exactly one arithmetic progression $n_1 + M_1\mathbb{Z}$ such that the symbols of w that appear on places in this progression are not all a_0. If $w = \phi_{\mathbf{a},G}(g)$, this n_1 must be $\gamma_1(g)$. Proceeding further in this way we can recover all digits of g from $\phi_{\mathbf{a},G}(g)$.

Let

$$\Lambda = \{\xi \in G : \gamma_k(\xi) = \pm 1\}.$$

Theorem 2.1. *If the m_k increase rapidly enough (a precise condition will be given later), and $g \in G$ satisfies $\sqrt{m_k} + 1 < \gamma_k(g) < m_k - \sqrt{m_k}$ for every k, then for any two elements ξ^1, $\xi^2 \in \Lambda$, the scenery $\phi_{\mathbf{a},G}(g + \xi^1)$ is indistinguishable from $\phi_{\mathbf{a},G}(g + \xi^2)$.*

There are uncountably many ξs in Λ, and as $\phi_{\mathbf{a},G}$ is one-to-one we get an uncountable number of indistinguishable sceneries, in stark contrast to the conjecture we wish to disprove.

Notice that $|\gamma_k(g + \xi^i) - \gamma_k(g)| \leq 2$ (less than or equal to 2 since we might have to compensate for carry from the low order digits — in fact for our g the above difference will always be ± 1), and so for all k, $\gamma_k(g + \xi^i) \neq 0$ if m_k are large enough, so $g + \xi^i \notin i(\mathbb{Z})$.

3. Preliminaries

We now introduce a sequence of progressively stronger pseudo-metrics (the last element of this sequence D_∞ will actually be a metric) on the set of (not necessarily σ-invariant) measures on $A^{\mathbb{N}}$.

Definition 3.1. *Let ρ^1, ρ^2 be two measures on $A^{\mathbb{N}}$, and denote by $J(\rho^1, \rho^2)$ the set of joinings of ρ^1 and ρ^2, i.e. the measures ν on $A^{\mathbb{N}} \times A^{\mathbb{N}}$ so that the projection of ν to the first coordinate is ρ^1, and the projection to the second coordinate is ρ^2. Define the D_N-metric of ρ^1 from ρ^2 to be*

$$D_N(\rho^1, \rho^2) := \inf_{\nu \in J(\rho^1, \rho^2)} \nu(\Delta_N^C) = 1 - \sup_{\nu \in J(\rho^1, \rho^2)} \nu(\Delta_N).$$

where $\Delta_N \subset A^{\mathbb{N}} \times A^{\mathbb{N}}$ is the set

$$\Delta_N := \left\{(x^1, x^2) \in A^{\mathbb{N}} \times A^{\mathbb{N}} : x^1|_{1\ldots N} = x^2|_{1\ldots N}\right\}$$

and $\Delta_N^C = A^{\mathbb{N}} \times A^{\mathbb{N}} \setminus \Delta_N$ is its complement.

That this is a pseudo-metric is easy to verify: trivially $D_N(\rho^1, \rho^2) = D_N(\rho^2, \rho^1)$, and $D_N(\rho, \rho) = 0$.

A standard argument gives the triangle inequality:

Proposition 3.1. *For any $\nu \in J(\rho^1, \rho^2)$ and $\nu' \in J(\rho^2, \rho^3)$, and any $N \leq \infty$, there is a $\nu'' \in J(\rho^1, \rho^3)$ such that*

$$\nu''(\Delta_N^C) \leq \nu(\Delta_N^C) + \nu'(\Delta_N^C)$$

Proof:

Let X^1, X^2 and X^3 be three copies on $A^{\mathbb{N}}$, with matching σ-algebras $\mathcal{F}^1$, $\mathcal{F}^2$ and $\mathcal{F}^3$. We consider ν as a measure on $X^1 \times X^2$ and ν' as a measure on $X^2 \times X^3$. We can construct from these the relative independent joining $\nu \times_{\rho^2} \nu'$ on $X^1 \times X^2 \times X^3$ as follows: for any continuous $f^1 \in C(X^1)$, $f^2 \in C(X^2)$ and $f^3 \in C(X^3)$ define

$$\int_{X^1 \times X^2 \times X^3} f^1(x^1) f^2(x^2) f^3(x^3) \, d\nu \times_{\rho^2} \nu' = \int_{X^2} f^2(x^2) \mathbf{E}_\nu(f^1|\mathcal{F}^2)(x^2) \cdot \mathbf{E}_{\nu'}(f^3|\mathcal{F}^2)(x^2) \, d\rho^2$$

As the linear span of such $f^1(x^1) f^2(x^2) f^3(x^3)$ is dense in $C(X^1 \times X^2 \times X^3)$ this determines $\nu \times_{\rho^2} \nu'$. We define ν'' to be the projection of the measure $\nu \times_{\rho^2} \nu'$ on $X_1 \times X_3$. Since

$$\begin{aligned}\int_{X^1 \times X^3} f^1(x^1) \, d\nu'' &= \int_{X^2} \mathbf{E}_\nu(f^1|\mathcal{F}^2)(x^2) \, d\rho^2 \\ &= \int_{X^1 \times X^2} f^1(x^1) \, d\nu = \int_{X^1} f^1(x^1) \, d\rho^1,\end{aligned}$$

ν'' projects to ρ^1 on X^1, and the same is true for ρ^3. Thus $\nu'' \in J(\rho^1, \rho^3)$. Similarly, one can verify that the projection of $\nu \times_{\rho^2} \nu'$ to $X^1 \times X^2 = \nu$, and the projection of this measure to $X^2 \times X^3$ is ν'. Finally,

$$\begin{aligned}\nu''(\Delta_N^C) &= \int_{X^1 \times X^3} 1_{\Delta_N^C}(x^1, x^3)\, d\nu'' \\ &\le \int_{X^1 \times X^2 \times X^3} (1_{\Delta_N^C}(x^1, x^2) + 1_{\Delta_N^C}(x^2, x^3))\, d\nu \times_{\rho^2} \nu' \\ &= \nu(\Delta_N^C) + \nu'(\Delta_N^C).\end{aligned}$$

□

If $N = \infty$, then D_N is actually a metric, as in this case $D_\infty(\rho^1, \rho^2) = 0$ only if $\rho^1 = \rho^2$. Another point worth noting is that since $\Delta_N \supset \Delta_{N'}$ for any $N < N'$,

$$D_N(\rho^1, \rho^2) \le D_{N'}(\rho^1, \rho^2).$$

Lemma 3.2. *Let ρ^1, ρ^2 be two measures on $A^{\mathbb{N}}$. Then*

$$D_\infty(\rho^1, \rho^2) = \lim_{N\to\infty} D_N(\rho^1, \rho^2)$$

Proof:

It follows from the monotonicity of the sequence of metrics $\{D_N\}$ that

$$D_\infty(\rho^1, \rho^2) \ge \lim_{N\to\infty} D_N(\rho^1, \rho^2);$$

we will now prove the opposite direction.

Let J_N be a joining of ρ^1 and ρ^2 such that

$$J_N(\Delta_N^C) < D_N(\rho^1, \rho^2) + \frac{1}{N}$$

Let ν be a weak limit of some subsequence J_{N_i}. As Δ_N is compact,

$$\begin{aligned}\nu(\Delta_N) &\ge \lim_{i\to\infty} J_{N_i}(\Delta_N) \ge \lim_{i\to\infty} J_{N_i}(\Delta_{N_i}) \ge \lim_{i\to\infty}(1 - D_{N_i}(\rho^1, \rho^2) - 1/N_i) \\ &= \lim_{N\to\infty}(1 - D_N(\rho^1, \rho^2)),\end{aligned}$$

and so

$$\nu(\Delta_\infty) = \nu(\cap_{N=1}^\infty \Delta_N) = \lim_{N\to\infty} \nu(\Delta_N) \ge \lim_{N\to\infty}(1 - D_N(\rho^1, \rho^2)).$$

By definition, $D_\infty(\rho^1, \rho^2) \le 1 - \nu(\Delta_\infty)$. □

Remark: Notice that ρ^1 and ρ^2 are mutually singular if and only if $D_\infty(\rho^1, \rho^2) = 1$. Even though this fact is almost self evident, it is very important and explains why the D_∞ metric is connected to the problem of distinguishing between sceneries. We will only need the "only if" direction — if ρ^1 and ρ^2 are mutually singular, there are disjoint sets A^1 and A^2 such that $\rho^i(A^j) = \delta_{i,j}$ for $i, j = 1, 2$. Then for any joining $\nu \in J(\rho^1, \rho^2)$ we have

$$1 = \nu(A^1 \times A^2) \leq \nu(\Delta_\infty^C) \leq D_\infty(\rho^1, \rho^2).$$

4. Many sceneries cannot be distinguished

Lemma 4.1. *Let $\{m_k\}$ and $G = G(m_1, m_2, \dots)$ be as above, and assume in addition that $\sqrt{m_1} < \gamma_1(g) < m_1 - \sqrt{m_1}$. Then for any $\epsilon > 0$ there is a $F(\epsilon)$ that does not depend on the m_i's and g such that if $m_1 \geq F(\epsilon)$*

$$D_\infty\left(\rho(\phi_{\mathbf{a},G}(g + \mathbf{1})), \rho(\phi_{\mathbf{a},G}(g - \mathbf{1}))\right) < \epsilon.$$

The proof of this Lemma follows along similar lines as the proof that under certain circumstances w and $\sigma^{2n}w$ are indistinguishable we have given in the introduction. This is not too surprising, given the fact that $\phi_{\mathbf{a},G}(g - \mathbf{1}) = \sigma^2(\phi_{\mathbf{a},G}(g + \mathbf{1}))$. The picture behind the proof is the following: recall that $\rho(\phi_{\mathbf{a},G}(g + \mathbf{1}))$ is the measure on the set of films, derived by observing the symbols of $\phi_{\mathbf{a},G}(g - \mathbf{1}) = \sigma^2\phi_{\mathbf{a},G}(g + \mathbf{1})$ along a random walk starting at place 2. Thus we take two independent random walks, one starting from place 0 and one from place 2, until they meet. From this moment on, the two random walk step in the same way. Unless at least one of the random walk reached a place with some symbol $\neq a_0$ in it before the two random walks met, the two films that were generated will be identical. Since both random walks start at nearly the same point, at least $\sqrt{m_1}$ steps from the nearest non a_0 symbol, if m_1 is large enough the probability that this will happen is very small.

Proof: We now describe in detail the joining $\tilde{\nu}$ of two simple random walks described above, where as before a joining of two random walks is a measure that projects to a simple random walk in each coordinate. This joining $\tilde{\nu}$ of random walks induces a joining ν between $\rho(\phi_{\mathbf{a},G}(g - \mathbf{1}))$ and $\rho(\phi_{\mathbf{a},G}(g + \mathbf{1}))$ — we generate a ν-random pair of films by observing $\phi_{\mathbf{a},G}(g - \mathbf{1})$ and $\phi_{\mathbf{a},G}(g + \mathbf{1})$ along random walks chosen according to the distribution $\tilde{\nu}$. We shall show that this ν satisfies $\nu(\Delta_\infty) \to 1$ uniformly as $m_1 \to \infty$.

We now define $\tilde{\nu}$. If α_n^1 and α_n^2 are two independent simple random walks on $\mathbb{Z}$ (i.e. $\alpha_0^i = 0,\ \alpha_n^i - \alpha_{n-1}^i = \pm 1$), we generate a $\tilde{\nu}$ random pair of simple random walks (β_n^1, β_n^2) as follows:

- First, set n' to be the smallest positive integer such that $\alpha_n^1 = \alpha_n^2 - 2$.
- Set $\beta_n^1 = \alpha_n^1$ for all n, and
- Set $\beta_n^2 = \alpha_n^2$ for $n \leq n'$, $\ \beta_n^2 = \alpha_n^1 + 2$ for $n > n'$.

Note that since $\alpha_n^1 - \alpha_n^2$ is a recurrent random walk on $2\mathbb{Z}$ (which will eventually visit every point of $2\mathbb{Z}$ infinitely many times), $n' < \infty$ almost surely. It is clear $\tilde{\nu}$ is a joining. If the n' defined above is smaller than $\sqrt{m_1} - 1$, then for $i = 1, 2$ and $n < n'$

$$\min_{k \in \mathbb{Z}} |\pi_1(g + (-1)^i - \beta_n^i) - kM_1| \geq \min_{k \in \mathbb{Z}} |\pi_1(g + (-1)^i) - kM_1| - (\sqrt{m_1} - 1) > 0,$$

i.e.

$$\phi_{\mathbf{a},G}(g + (-1)^i)\big|_{\beta_n^i} = a_{r(-g-(-1)^i+\beta_n^i)} = a_0 \qquad \text{for } n < n'.$$

If $n \geq n'$, $\beta_n^1 = \beta_n^2 - 2$, i.e.

$$\phi_{\mathbf{a},G}(g-1)\big|_{\beta_n^1} = a_{r(-g+1+\beta_n^1)} = a_{r(-g-1+\beta_n^2)} = \phi_{\mathbf{a},G}(g+1)\big|_{\beta_n^2}.$$

Thus for all n,

$$\phi_{\mathbf{a},G}(g-1)\big|_{\beta_n^1} = \phi_{\mathbf{a},G}(g+1)\big|_{\beta_n^2}.$$

and so we have demonstrated that

$$D_\infty\left(\rho\phi_{\mathbf{a},G}(g-1), \rho\phi_{\mathbf{a},G}(g+1)\right) < \mathrm{Prob}(n' > \sqrt{m_1} - 1)$$

and by recurrence $\mathrm{Prob}(n' > \sqrt{m_1} - 1) \to 0$ as $m_1 \to \infty$. $\square$

Let w, w' be any two infinite words in $A^{\mathbb{Z}}$. We know that a joining of the simple random walk with itself induces a joining of $\rho(w)$ and $\rho(w')$. The following simple technical lemma is rather standard, and shows that all joinings of $\rho(w)$ and $\rho(w')$ can be constructed in this way. Denote by ω the standard measure on the space Ω of simple random walks. Ω is a compact space that can be identified with $\{-1, 1\}^{\mathbb{N}}$: indeed to every $(\epsilon_n)_{n=1}^\infty \in \{-1, 1\}^{\mathbb{N}}$ there corresponds the random walk $\alpha_0 = 0$, $\alpha_1 = \epsilon_1$, $\alpha_2 = \epsilon_1 + \epsilon_2$, etc. Given a scenery $w \in A^{\mathbb{Z}}$, we recall the definition of $\Psi_w \colon \Omega \to A^{\mathbb{N}}$

$$\Psi_w \colon ((\alpha_n)_{n=0}^\infty) \mapsto (w_{\alpha_0}, w_{\alpha_1}, \dots).$$

$\Psi_w \times \Psi_{w'}$ clearly maps $J(\omega, \omega)$ to $J(\rho(w), \rho(w'))$.

Lemma 4.2. *$\Psi_w \times \Psi_{w'}$ maps $J(\omega, \omega)$* **onto** *$J(\rho(w), \rho(w'))$.*

Proof: As $\Psi_w \times \Psi_{w'}$ is continuous, Ω compact, $C(\Psi_w(\Omega) \times \Psi_{w'}(\Omega))$ can be viewed as a closed subspace of $C(\Omega \times \Omega)$. A joining in $J(\omega, \omega)$ is a positive linear functional with norm 1 on $C(\Omega \times \Omega)$ that gives the value zero to any function in the closed set

$$A = \Big\{ f(\alpha, \beta) : \forall \alpha, \beta\ f(\alpha, \beta) = g(\alpha) \text{ or } \forall \alpha, \beta\ f(\alpha, \beta) = g(\beta) \\ \text{with } g(\alpha) \in C(\Omega), \text{ and } \textstyle\int g(\alpha) d\omega(\alpha) = 0 \Big\}$$

Take any element $\nu \in J(\rho(w), \rho(w'))$. we must show there is some $\tilde{\nu} \in J(\omega, \omega)$ such that $\Psi_w \times \Psi_{w'}(\tilde{\nu}) = \nu$.

An elements ν of $J(\rho(w), \rho(w'))$ can be viewed as a positive functional with norm one on $C(\Psi_w(\Omega) \times \Psi_{w'}(\Omega))$, which is zero on $A \cap C(\Psi_w(\Omega) \times \Psi_{w'}(\Omega))$. By the Hahn-Banach theorem, this functional can be extended to a positive functional $\tilde{\nu}$ that acts on the full space $C(\Omega \times \Omega)$ with norm one, so that for any $f \in A$, $\tilde{\nu}(f) = 0$. By construction

$$\Psi_w \times \Psi_{w'}(\tilde{\nu}) = \nu.$$

$\square$

Definition 4.1. *Let $G = G(m_1, m_2, \dots)$, $\tilde{G} = G(m_2, m_3, \dots)$. Define $T \colon G \to \tilde{G}$ by*

$$\gamma_{k-1}(Tg) = \gamma_k(g) \qquad \text{for all } k \geq 1.$$

Thus $\Gamma(Tg) = (\gamma_2, \gamma_3, \dots)$ is the sequence $\Gamma(g) = (\gamma_1, \gamma_2, \dots)$ shifted once to the left. Let α_n be a simple random walk along a scenery $w = \phi_{\mathbf{a},G}(g)$ for $g \in G$ with $\pi_1(G) = 0$, and we consider the times t during which $\alpha_t \in m_1\mathbb{Z}$ — i.e. the times where the symbol recorded on the film is not a_0. The symbols we record at these times are a result of a slightly different random walk (there is now a positive probability of staying at exactly the same place the next step of the random walk), along a modified scenery. The modified scenery is the scenery we get from $\phi_{\mathbf{a},G}(g)$ by erasing all symbols except those at places in $m_1\mathbb{Z}$. This modified scenery is exactly the scenery that corresponds to $T(g)$ via $\phi_{\sigma\mathbf{a},\tilde{G}}$, where $\tilde{G} = G(m_2, m_3, \dots)$ and $\sigma\mathbf{a}$ is the sequence $\mathbf{a}$ shifted to the left. If we consider the symbols of $\phi_{\mathbf{a},G}(g)$ recorded on the film not for all t such that $\alpha_t \in m_1\mathbb{Z}$, but only only for those times t_k such that $\alpha_{t_k} \in m_1\mathbb{Z}$ but the last $\alpha_t \in m_1\mathbb{Z}$ for $t < t_k$ is not equal to α_{t_k}, then the distribution of these symbols is exactly the distribution we see when we walk by a simple random walk on $\phi_{\sigma\mathbf{a},\tilde{G}}(T(g))$.

The next lemma allows us to use inductive type arguments for estimating how well $\rho(\phi_{\mathbf{a},G}(g))$ and $\rho(\phi_{\mathbf{a},G}(h))$ can be coupled by showing that if we have a good coupling of $\rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Tg))$ and $\rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Th))$ (for g, $h \in G$ which are zero in their γ_1 coordinate), we can use this to obtain a good coupling of $\rho(\phi_{\mathbf{a},G}(g))$ and $\rho(\phi_{\mathbf{a},G}(h))$. The idea is to use the inverse of the procedure described above for deriving a simple random walk on $\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)$ from a random walk on $\phi_{\mathbf{a},G}(g)$ to get, from a pair of coupled random walks on $\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)$ and $\phi_{\sigma\mathbf{a},\tilde{G}}(Th)$, a pair of random walks on $\phi_{\mathbf{a},G}(g)$ and $\phi_{\mathbf{a},G}(h)$.

Lemma 4.3. *Again let $G = G(m_1, m_2, \dots)$, $\tilde{G} = G(m_2, m_3, \dots)$. If $g, h \in G$, such that $\pi_1(g) = \pi_1(h) = 0$ then*

$$D_\infty(\rho(\phi_{\mathbf{a},G}(g)), \rho(\phi_{\mathbf{a},G}(h))) \leq D_\infty(\rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)), \rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Th))).$$

Proof:

Let $\epsilon > 0$,

$$\nu \in J(\rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)), \rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Th)))$$

such that

$$\nu(\Delta_\infty) > 1 - D_\infty(\rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)), \rho(\phi_{\sigma\mathbf{a},\tilde{G}}(Th))) - \epsilon.$$

By Lemma 4.2, there is some joining $\tilde{\nu}$ of the simple random walk with itself that induces the joining ν.

We will now define a joining $\tilde{\mu}$ that will induce a joining $\mu \in J(\rho(\phi_{\mathbf{a},G}(g)), \rho(\phi_{\mathbf{a},G}(h)))$ such that $\mu(\Delta_\infty)$ will be high.

In order to define $\tilde{\mu}$ we will give an algorithm how to generate a $\tilde{\mu}$-random pair of (non independent) simple random walks $(\beta^1_n)_{n=0}^\infty$, $(\beta^2_n)_{n=0}^\infty$ from a triplet of random walks: A simple random walk $(s_n)_{n=0}^\infty$, chosen independently of the pair $(\alpha^1_n)_{n=0}^\infty$ and $(\alpha^2_n)_{n=0}^\infty$, which we chose according to $\tilde{\nu}$.

Define the sequence $0 = t_0 < t_1 < t_2 < \ldots$ inductively by

$$t_n := \min\{t > t_{n-1} : \pi_1(s_t) = 0,\ s_t \neq s_{t_{n-1}}\}.$$

Thus, t_n is the least t such that $s_t = s_{t_{n-1}} \pm m_1$. Define $\beta^1_0 = \beta^2_0 = 0$, and for all $t_k < t \leq t_{k+1}$, $i = 1,\, 2$

$$\beta^i_t = \beta^i_{t_k} + (s_t - s_{t_k})\operatorname{sgn}(s_{t_{k+1}} - s_{t_k})(\alpha^i_{k+1} - \alpha^i_k).$$

Notice that since $s_{t_{k+1}} - s_{t_k} = \pm m_1$, $\beta^i_{t_{k+1}} - \beta^i_{t_k}$ is also $\pm m_1$ — in fact, $\beta^i_{t_{k+1}} - \beta^i_{t_k} = m_1(\alpha^i_{k+1} - \alpha^i_k)$, and so $\beta^i_{t_n} = m_1\alpha^i_n$.

We must first convince ourself that β^1_t by itself is distributed like a simple random walk, and the same for β^2_t. But β^1_t depends only on s_n and α^1_n, two independent simple random walks. Essentially what happens is that as $\{\alpha^1_{k+1} - \alpha^1_k\}_{k=0}^\infty$ are ± 1 with equal probability i.i.d. irrespective of s_t, the same is true for $\{\operatorname{sgn}(s_{t_{k+1}} - s_{t_k})(\alpha^1_{k+1} - \alpha^1_k)\}_{k=0}^\infty$. And so β^1_n is obtained by reflecting the simple random walk s_k at times chosen randomly in a way that depends only on past history. By the Strong Markov Property of simple random walks this does not change the distribution - i.e. β^1_n is distributed as a simple random walk. The same argument is valid for β^2_n. Thus $\tilde{\mu} \in J(\omega, \omega)$.

We would like now to show

$$\mu(\Delta_\infty) \geq \nu(\Delta_\infty). \tag{3}$$

So let s_n be arbitrary, α_n^1, α_n^2 a pair such that

$$\phi_{\sigma\mathbf{a},\tilde{G}}(Tg)\big|_{\alpha_n^1} = \phi_{\sigma\mathbf{a},\tilde{G}}(Th)\big|_{\alpha_n^2} \qquad \text{for all } n. \tag{4}$$

The probability of this event happening is exactly $\nu(\Delta_\infty)$. We claim that if (4) holds, then

$$\phi_{\mathbf{a},G}(g)\big|_{\beta_t^1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_t^2} \qquad \text{for all } t.$$

We first prove that for all k,

$$\phi_{\mathbf{a},G}(g)\big|_{\beta_{t_k}^1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_{t_k}^2}$$

We recall that the definition of r in equation (2) depends on the group G. This has not caused any confusion up to now since the group G was fixed; now, however, since we have two groups we are working with, we will use the notation r_G and $r_{\tilde{G}}$ to designate the function r on G and $\tilde{G}$ respectively. If $t = t_k$ then by construction $\beta_{t_k}^i = m_1\alpha_k^i$, i.e.

$$\begin{aligned}
\phi_{\mathbf{a},G}(g)\big|_{\beta_{t_k}^1} &= a_{r_G(-g+m_1\alpha_k^1)} = a_{r_{\tilde{G}}(-Tg+\alpha_k^1)+1} = \phi_{\sigma\mathbf{a},\tilde{G}}(Tg)\big|_{\alpha_k^1} \\
&= \phi_{\sigma\mathbf{a},\tilde{G}}(Th)\big|_{\alpha_k^2} = a_{r_{\tilde{G}}(-Th+\alpha_k^2)+1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_{t_k}^2}.
\end{aligned}$$

where $r_G(-g+m_1\alpha_k^i) = r_{\tilde{G}}(-Tg+\alpha_k^1)+1$ since

$$\pi_{i,\,\text{in }G}(g-m_1\alpha_k^1) = m_1\pi_{i-1,\,\text{in }\tilde{G}}(Tg-\alpha_k^1),$$

thus $\pi_{i,\text{in }G}(g-m_1\alpha_k^1) \equiv 0 \pmod{m_1\cdot m_2\cdots m_i}$ — and hence $r_G(-g+m_1\alpha_k^1)\geq i$ — if and only if $\pi_{i-1,\text{in }\tilde{G}}(Tg-\alpha_k^1)\equiv 0 \pmod{m_2\cdots m_i}$.

Now suppose $t\notin\{t_0,t_1,\dots\}$. Then either $\pi_1(\beta_t^1)\neq 0$, which implies $\pi_1(\beta_t^2)\neq 0$ and so

$$\phi_{\mathbf{a},G}(g)\big|_{\beta_t^1} = a_{r_G(-g+\beta_t^1)} = a_0 = a_{r_G(-h+\beta_t^2)} = \phi_{\mathbf{a},G}(h)\big|_{\beta_t^2},$$

or $t_k < t < t_{k+1}$ for some k, and $s_{t_k} = s_t$. If this is the case then $\beta^i\big|_t = \beta^i\big|_{t_k}$ for both $i=1$ and 2 — and $\phi_{\mathbf{a},G}(g)\big|_{\beta_t^1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_t^2}$ follows from $\phi_{\mathbf{a},G}(g)\big|_{\beta_{t_k}^1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_{t_k}^2}$.

Thus

$$\begin{aligned}
&\tilde{\mu}\left\{\beta_n^1,\beta_n^2 : \phi_{\mathbf{a},G}(g)\big|_{\beta_n^1} = \phi_{\mathbf{a},G}(h)\big|_{\beta_n^2} \text{ for all } n\right\} \\
&\qquad\qquad \geq \tilde{\nu}\left\{\alpha_n^1,\alpha_n^2 : \phi_{\sigma\mathbf{a},\tilde{G}}(Tg)\big|_{\alpha_n^1} = \phi_{\sigma\mathbf{a},\tilde{G}}(Th)\big|_{\alpha_n^2} \text{ for all } n\right\}
\end{aligned}$$

proving (3). ∎

Lemma 4.4. *Let m_i, $G = g(m_1,m_2,\dots)$ be as above, g and f elements of G, with $\pi_1(g) = \pi_1(f) = p$. p is an element of $\mathbb{Z}/m_1\mathbb{Z}$, but with slight abuse of notation we can view it as an* *element of* $\mathbb{Z}$ *between* 0 *and* $m_1 - 1$. *Using this notation we claim that*

$$D_\infty(\rho\phi_{\mathbf{a},G}(g), \rho\phi_{\mathbf{a},G}(f)) \leq \max\big(D_\infty(\rho\phi_{\mathbf{a},G}(g-p), \rho\phi_{\mathbf{a},G}(f-p)), D_\infty(\rho\phi_{\mathbf{a},G}(g+m_1-p), \rho\phi_{\mathbf{a},G}(f+m_1-p))\big).$$

Proof. since the proof of this lemma is very similar to the proofs of the preceding lemmas, we omit the details.

Assume $\nu^1 \in J(\rho(\phi_{\mathbf{a},G}(g-p)), \rho(\phi_{\mathbf{a},G}(f-p)))$ and $\nu^2 \in J(\rho(\phi_{\mathbf{a},G}(g+m_1-p)), \rho(\phi_{\mathbf{a},G}(f+m_1-p)))$ having an almost maximal measure for Δ_∞, and use Lemma 4.2 to find $\tilde{\nu}^i \in J(\omega,\omega)$ joinings of simple random walks that induce ν^i. We will use a simple random walk α_n^1, two random walks (α_n^2 and α_n^3) chosen according to $\tilde{\nu}^1$, and two chosen according to $\tilde{\nu}^2$ (α_n^4 and α_n^5). We will use all these α_n^i's to construct a pair of random walks β_n^1 and β_n^2. This will give us a measure $\tilde{\mu}$ on pairs of random walks which will easily seen to be a joining of two simple random walks, which will induce a measure $\mu \in J(\rho\phi_{\mathbf{a},G}(g), \rho\phi_{\mathbf{a},G}(f))$ with high $\mu(\Delta_\infty)$.

Indeed, we take $\beta_n^1 = \beta_n^2 = \alpha_n^1$ up to the first n' such that $\pi_1(g-\alpha_n^1) = 0$ (this will also mean that $\pi_1(f-\alpha_{n'}^1) = 0$). There are two possibilities: $\alpha_{n'}^1 = p$ or $\alpha_{n'}^1 = p - m_1$. In the first case we will take for $n > n'$, and $i = 1,2$, $\beta_n^i = \alpha_{n-n'}^{1+i} + p$, in the second case we take for $n > n'$, and $i = 1,2$, $\beta_n^i = \alpha_{n-n'}^{3+i} + p - m_1$. The rest of the details are omitted. □

Theorem 4.5. *Let* $c_i > 0$ *be a sequence of positive real numbers,* $\{m_1, m_2, \ldots,\}$ *a sequence of integers such that* $m_i > F(c_i)$ *(where* F *is as in Lemma 4.1). Let* $G = G(m_1, m_2, \ldots)$*, with* $g \in G$ *satisfying* $\sqrt{m_1} < \gamma_1(g) < m_1 - \sqrt{m_1}$ *and* $\sqrt{m_k} + 1 < \gamma_k(g) < m_k - \sqrt{m_k}$ *for* $k > 1$. *Then for any* ξ^1, $\xi^2 \in \Lambda$,

$$D_\infty(\rho(\phi_{\mathbf{a},G}(g+\xi^1)), \rho(\phi_{\mathbf{a},G}(g+\xi^2))) \leq \sum_{i=1}^{\infty} c_i,$$

and hence if $\sum c_i < 1$, $\phi_{\mathbf{a},G}(g+\xi^1)$ *and* $\phi_{\mathbf{a},G}(g+\xi^2)$ *are indistinguishable (in the sense explained in the introduction)*

Proof:

Step 1: First we show by induction on k that for any k and any m_i, ξ^1, ξ^2 and g as in the statement of the Theorem,

$$D_\infty(\rho(\phi_{\mathbf{a},G}(g+\pi_k(\xi^1))), \rho(\phi_{\mathbf{a},G}(g+\pi_k(\xi^2)))) \leq \sum_{i=1}^{k} c_k \tag{5}$$

(again we treat $\pi_k(\cdot)$ as an element of $\mathbb{Z}$ between 0 and $M_k - 1$). Let $\xi(k,r) \in G$ be defined by $\gamma_i(\xi(k,r)) = \gamma_i(\xi^1)$ for $i \leq r$, $\gamma_i(\xi(k,r)) = \gamma_i(\xi^2)$ for $r < i \leq k$, and $\gamma_i(\xi(k,r)) = 0$ for $i > k$. Note that $\xi(k,0) = \pi_k(\xi^2)$, $\xi(k,k) = \pi_k(\xi^1)$.

To show (5) holds, we will use induction on k: we assume that (5) holds for $k-1$ and all $m_1, m_2, \ldots, g$, and ξ^i satisfying the above conditions, and use this to prove the same for k. For $k=0$ the result is trivial. Now assume (5) holds for $k-1$. Use Lemma 4.1 to see that

$$\begin{aligned}
D_\infty(\rho\phi_{\mathbf{a},G}(g+\xi(k,k)),&\rho\phi_{\mathbf{a},G}(g+\xi(k,0))) \\
&\le D_\infty(\rho\phi_{\mathbf{a},G}(g+\xi(k,k)),\rho\phi_{\mathbf{a},G}(g+\xi(k,1))) \\
&\quad + D_\infty(\rho\phi_{\mathbf{a},G}(g+\xi(k,1)),\rho\phi_{\mathbf{a},G}(g+\xi(k,0))) \\
&\le D_\infty(\rho\phi_{\mathbf{a},G}(g+\xi(k,k)),\rho\phi_{\mathbf{a},G}(g+\xi(k,1))) + c_1
\end{aligned} \tag{6}$$

But $\pi_1(g+\xi(k,k)) = \pi_1(g+\xi(k,1))$ and so Applying Lemma 4.4, we have

$$\begin{aligned}
&D_\infty\Big(\rho\phi_{\mathbf{a},G}(g+\xi(k,k)),\rho\phi_{\mathbf{a},G}(g+\xi(k,1))\Big) \\
&\quad\le \max\Bigg(D_\infty\Big(\rho\phi_{\mathbf{a},G}\big(g-\pi_1(g+\xi^1)+\xi(k,k)\big),\rho\phi_{\mathbf{a},G}\big(g-\pi_1(g+\xi^1)+\xi(k,1)\big)\Big), \\
&\qquad\quad D_\infty\Big(\rho\phi_{\mathbf{a},G}\big(g+m_1-\pi_1(g+\xi^1)+\xi(k,k)\big), \\
&\qquad\qquad \rho\phi_{\mathbf{a},G}\big(g+m_1-\pi_1(g+\xi^1)+\xi(k,1)\big)\Big)\Bigg) = (*).
\end{aligned}$$

We then apply Lemma 4.3 twice, to get

$$\begin{aligned}
(*) \le \max\Bigg(&D_\infty\Big(\rho\phi_{\sigma\mathbf{a},\tilde G}\big(T(g-\pi_1(g))+T(\xi(k,k)-\pi_1(\xi^1))\big), \\
&\qquad \rho\phi_{\sigma\mathbf{a},\tilde G}\big(T(g-\pi_1(g))+T(\xi(k,1)-\pi_1(\xi^1))\big)\Big), \\
&D_\infty\Big(\rho\phi_{\sigma\mathbf{a},\tilde G}\big(T(g+m_1-\pi_1(g))+T(\xi(k,k)-\pi_1(\xi^1))\big), \\
&\qquad \rho\phi_{\sigma\mathbf{a},\tilde G}\big(T(g+m_1-\pi_1(g))+T(\xi(k,1)-\pi_1(\xi^1))\big)\Big)\Bigg) = (**).
\end{aligned}$$

We now note that for $i>1$

$$\begin{aligned}
\gamma_{i,\text{in }\tilde G}(T(g-\pi_1(g))) &= \gamma_{i,\text{in }\tilde G}(T(g+m_1-\pi_1(g))) \\
&= \gamma_{i+1,\text{in }G}(g) \in [\sqrt{m_{i+1}}+1, m_{i+1}-\sqrt{m_{i+1}}].
\end{aligned}$$

For $i=1$,

$$\begin{aligned}
\gamma_{1,\text{in }\tilde G}(T(g-\pi_1(g))) &= \gamma_{1,\text{in }\tilde G}(T(g+m_1-\pi_1(g))) - 1 \\
&= \gamma_{2,\text{in }G}(g) \in [\sqrt{m_2}+1, m_2-\sqrt{m_2}],
\end{aligned}$$

hence both the first and second term are in $[\sqrt{m_2}, m_2-\sqrt{m_2}]$. Finally using the induction hypothesis twice, once for for $T(g-\pi_1(g))$ and once for $T(g+m_1-\pi_1(g))$, we see that

$$D_\infty\Big(\rho\phi_{\mathbf{a},G}(g+\xi(k,k)),\rho\phi_{\mathbf{a},G}(g+\xi(k,1))\Big) \le (**) \le \max(\sum_{i=2}^k c_i, \sum_{i=2}^k c_i) = \sum_{i=2}^k c_i \tag{7}$$

Combining (6) and (7) we get (5).

step 2:

We only need to pass to the limit as $k \to \infty$. But this is easy, since clearly if N is smaller than $M_{k-1}\sqrt{m_k}$, the sceneries $\phi_{\mathbf{a},G}(g + \pi_k(\xi^i))$ and $\phi_{\mathbf{a},G}(g + \xi^i)$ are identical in the first N coordinates in both directions from the origin. This clearly implies

$$D_N(\rho\phi_{\mathbf{a},G}(g + \xi^1), \rho\phi_{\mathbf{a},G}(g + \xi^2)) = D_N(\rho\phi_{\mathbf{a},G}(g + \pi_k(\xi^1)), \rho\phi_{\mathbf{a},G}(g + \pi_k(\xi^2)))$$

since the distribution of the first N symbols in the film cannot depend on the scenery at places of distance greater than N from the origin. The latter expression is less than $\sum_{i=1}^{\infty} c_i$ by step 1. We now use Lemma 3.2 to pass to the limit. $\square$

It is, perhaps, interesting to note that for all finite k, $\phi_{\mathbf{a},G}(g + \pi_k(\xi^1))$ is a translate of $\phi_{\mathbf{a},G}(g + \pi_k(\xi^2))$. Only by passing to the limit do we obtain a counter example for the conjecture.

5. Concluding Remarks

$X_{\mathbf{a},G}$ is shift invariant and uniquely ergodic, its invariant measure m being the image of the Haar measure on the compact group $G(m_1, m_2, \dots)$. If the m_i increases fast enough, the set

$$\{g \in G : \forall k \quad \sqrt{m_k} + 1 < \gamma_k(g) < m_k - \sqrt{m_k}\}$$

has positive measure, and from this using ergodicity one easily concludes that m-a.e. $x \in X_{\mathbf{a},G}$ there are uncountable number of points of $X_{\mathbf{a},G}$ that are not distinguishable by suffixes from x.

One can try to weaken the conjecture that every two points (except for the trivial case of points that can be derived one from the other by reflection and/or translation) be distinguishable, by asking whether there is an ergodic shift invariant measure on $A^{\mathbb{Z}}$ such that according to this measure a.e. two points are indistinguishable.

From the results in Benjamini and Kesten (1996) or Matzinger (1997) it follows that if one takes the Bernoulli measure on $k \geq 2$ symbols then a.e. two points can be distinguished. The analogous question for the measure m is not clear. It is not hard to see that if the symbols in the sequence $\mathbf{a}$ are all distinct then almost every pair of elements in $X_{\mathbf{a},G}$ are distinguishable. It might be true however that for some $\mathbf{a}$ if $m_i \to \infty$ fast enough $m \times m$-almost every two points are indistinguishable.

The measure m we have considered is rather rigid. It is conceivable that if we take a shift invariant measure μ with "enough mixing" (e.g. K-systems) a.e. pair of points can be distinguished.

References

[1] I. Benjamini and H. Kesten, *Distinguishing Sceneries by Observing the Scenery along a Random Walk Path*, J. d'Anal. Math. (**69**), pp 97–135.

[2] Howard, C. D., *Detecting defects in periodic scenery by random walks on* $\mathbb{Z}$, Random Structures and Algorithms (**1996, vol 8**), pp 59–74.

[3] Howard, C. D., *Distinguishing certain random sceneries on* $\mathbb{Z}$ *via random walks*, Statistics and Probability Letters (1997).

[4] Kesten, H., *Detecting a single defect in a scenery by observing the scenery along a random walk path*, Itô's Stochastic Calculus and Probability Theory (editors N. Ikeda, S. Watanabe, M. Fukushima and H. Kunita), Springer-Verlag (1996), pp 171-183.

[5] H. Kesten, *Distinguishing and reconstructing sceneries from observations along random walk paths*, in preparation (1997).

[6] Matzinger, H. Ph.D. Thesis Cornell University, in preparation (1997).

Institute of Mathematics, The Hebrew University, Jerusalem 91904, Israel

E-mail address: `elon@math.huji.ac.il`