



Universiteit
Leiden
The Netherlands

Matching for random systems with an application to minimal weight expansions

Dajani, K.; Kalle, C.C.C.J.; Maggioni, M.

Citation

Dajani, K., Kalle, C. C. C. J., & Maggioni, M. (2021). Matching for random systems with an application to minimal weight expansions. *Nonlinearity*, 34(6), 3676-3708.
doi:10.1088/1361-6544/abebc6

Version: Publisher's Version

License: [Licensed under Article 25fa Copyright Act/Law \(Amendment Taverne\)](#)

Downloaded from: <https://hdl.handle.net/1887/3223078>

Note: To cite this publication please use the final published version (if applicable).



PAPER

Matching for random systems with an application to minimal weight expansions

To cite this article: Karma Dajani *et al* 2021 *Nonlinearity* **34** 3676

View the [article online](#) for updates and enhancements.

You may also like

- [Effects of overlapping sources on cosmic shear estimation: Statistical sensitivity and pixel-noise bias](#)
for the LSST Dark Energy Science collaboration, Javier Sanchez, Ismael Mendoza et al.
- [Indexing moiré patterns of metal-supported graphene and related systems: strategies and pitfalls](#)
Patrick Zeller, Xinzhou Ma and Sebastian Günther
- [Entanglement Preserving in Quantum Copying of Three-Qubit Entangled State](#)
Tong Zhao-Yang and Kuang Le-Man

Matching for random systems with an application to minimal weight expansions

Karma Dajani¹ , Charlene Kalle²  and
Marta Maggioni^{2,*} 

¹ Department of Mathematics, Utrecht University, P.O. Box 80010, 3508TA Utrecht, The Netherlands

² Mathematisch Instituut, Leiden University, Niels Bohrweg 1, 2333CA Leiden, The Netherlands

E-mail: k.dajani1@uu.nl, kallecccj@math.leidenuniv.nl and
m.maggioni@math.leidenuniv.nl

Received 17 August 2020, revised 5 February 2021

Accepted for publication 3 March 2021

Published 4 June 2021



CrossMark

Abstract

We extend the notion of matching for one-dimensional dynamical systems to random matching for random dynamical systems on an interval. We prove that for a large family of piecewise affine random systems of the interval the property of random matching implies that any invariant density is piecewise constant. We further introduce a one-parameter family of random dynamical systems that produce signed binary expansions of numbers in the interval $[-1, 1]$. This family has random matching for Lebesgue almost every parameter. We use this to prove that the frequency of the digit 0 in the associated signed binary expansions never exceeds $\frac{1}{2}$.

Keywords: interval map, random dynamics, invariant measure, matching, digit frequency, signed digit expansion

Mathematics Subject Classification numbers: 37E05, 37A45, 37A05, 60G10, 11K55.

(Some figures may appear in colour only in the online journal)

1. Introduction

Optimal algorithms for the computation of powers of elements in a group are at the basis of many public key cryptosystems. Here the group is either the multiplicative group of a finite field or the group of points on an elliptic curve and the optimality refers to the ability of computing high powers in a short amount of time. One such algorithm is the *binary method*, introduced in [Knu69] and based on the binary expansion of the power. More precisely, if x is an element of a given group, and $a = \sum_{k=0}^n d_k 2^k \in \mathbb{N}$ for some digits $d_k \in \{0, 1\}$, then

*Author to whom any correspondence should be addressed.

$$x^a = \prod_{k=0}^n x^{d_k 2^k},$$

and the power x^a is computed by taking the product of repeated squarings. While the number of squarings is given by the length n of the binary expansion of a , the number of multiplications equals the number of non-zero bits d_k in the expansion or its *Hamming weight*. Clearly, a lower Hamming weight implies fewer multiplications and a faster result. To increase the number of zero bits, [Boo51] introduced a *signed binary representation*, i.e., a binary representation with digits in the set $\{-1, 0, 1\}$. This signed binary representation was later adopted in several methods in elliptic cryptosystems, see e.g. [1998, HP06] and the references therein.

The ordinary binary representation of an integer a is uniquely determined, but this is not the case for the signed one. In fact, each integer has infinitely many signed binary representations, which led to the study of algorithms that choose the ones with minimal Hamming weight (see e.g. [MO90, 1993, LK97]). Typically a number has several signed binary representations with minimal weight (see [GH06]), but already in the 1960s Reitwiesner proved in [Rei60] that the signed representation is unique when adding the constraint $d_k d_{k+1} = 0$. Such representations are known as *signed separated binary expansions*, or SSB for short. In [DKL06] it is shown how to obtain SSB expansions through the binary odometer and a three state Markov chain. Furthermore, in [DKL06] the set $K := \{d_1 d_2 \dots \in \{-1, 0, 1\}^{\mathbb{N}} : \forall k \in \mathbb{N}, d_k d_{k+1} = 0\}$ is introduced as a compactification of \mathbb{Z} . The authors identified K , endowed with the left shift σ , with the map $S(x) = 2x \bmod \mathbb{Z}$ on the interval $[-\frac{2}{3}, \frac{2}{3}]$ through the conjugation

$$\psi(d_1 d_2 \dots) = \sum_{k=1}^{\infty} \frac{d_k}{2^k}.$$

This dynamical viewpoint allowed them to obtain metric properties of the system (K, σ) , such as a σ -invariant measure, the maximal entropy and the frequency of 0 in typical expansions.

In [DK20] this dynamical approach was further developed by considering a family of *symmetric doubling maps* $\{S_\alpha : [-1, 1] \rightarrow [-1, 1]\}_{\alpha \in [1, 2]}$ defined by $S_\alpha(x) = 2x - d\alpha$ and

$$d = \begin{cases} -1, & \text{if } x \in [-1, -\frac{1}{2}), \\ 0, & \text{if } x \in [-\frac{1}{2}, \frac{1}{2}], \\ 1, & \text{if } x \in (\frac{1}{2}, 1]. \end{cases}$$

The map S from [DKL06], producing SSB expansions, is then easily identified with the map $S_{\frac{3}{2}}$. For each $\alpha \in [1, 2]$ iterations of S_α give a signed binary expansion of the form $x = \sum_{k=1}^{\infty} \frac{d_k}{2^k}$ with $d_k \in \{-1, 0, 1\}$ for each number $x \in [-1, 1]$. The authors of [DK20] showed that the frequency of 0 in such expansions depends continuously on the parameter α and takes its maximal value $\frac{2}{3}$, corresponding to the minimal Hamming weight of $\frac{1}{3}$, precisely for $\alpha \in [\frac{6}{5}, \frac{3}{2}]$. It follows that typically only $\frac{1}{3}$ of the digits in the SSB expansions of integers is different from 0. The results from [DK20] are obtained by finding a detailed description of the unique invariant probability density f_α of S_α for each value α and then explicitly computing the frequency of the digit 0 using Birkhoff's ergodic theorem. The fact that the family $\{S_\alpha\}$ exhibits the dynamical phenomenon of matching was essential for these results.

In this article we consider signed binary expansions in the framework of random dynamical systems. The advantage of random systems in this context is that a single random system

produces many more number expansions per number than a deterministic map, allowing one to study the properties of many expansions simultaneously. See e.g. [DK03, DdV05, DdV07, DK07, KKV17, DO18] for the use of random systems in the study of different types of number expansions. We will introduce a family of random systems $\{R_\alpha\}_{\alpha \in [1,2]}$, called *random symmetric doubling maps*, such that each element R_α produces for typical numbers in the interval $[-1, 1]$ infinitely many different signed binary expansions. This is contrary to the map S_α , which produces a unique signed binary expansion for each number in $[-1, 1]$. Our main result for the family $\{R_\alpha\}_{\alpha \in [1,2]}$ is that the frequency of the digit 0 in typical signed binary expansions produced by any of the maps R_α is at most $\frac{1}{2}$, and therefore the Hamming weight is at least $\frac{1}{2}$. This reinforces the result from [DK20] that the maps S_α with $\alpha \in [\frac{6}{5}, \frac{3}{2}]$ perform best in terms of minimal weight.

We obtain this result from Birkhoff's ergodic theorem after gathering detailed knowledge on the invariant probability densities of the random maps R_α . We first express these densities as infinite sums of indicator functions using the algebraic procedure from [KM20]. To compute the frequency of 0 we need to evaluate the Lebesgue integral of these densities over part of the domain and therefore we convert the infinite sums into finite sums. For this we introduce a random version of the dynamical concept of matching that is available for one-dimensional systems (see e.g. [NN08, DKS09, BCIT13, BSORG13, BCK17, BCMP19, CIT18, CM18, KLMM20]). Our definition of random matching properly extends the one-dimensional notion of matching and we illustrate the concept with examples of random continued fraction maps and random generalised β -transformations. We show that under mild certain conditions, if a random system of piecewise affine maps defined on the same interval has random matching, then any invariant probability density of the system is piecewise constant. The precise formulation of this statement and the conditions are given in the next section. Finally, we use this random matching property to show that for Lebesgue almost all parameters α the invariant density of the random systems R_α , producing signed binary expansions, is in fact a.e. piecewise constant.

The article is outlined as follows. The second section is devoted to random matching for random systems defined on an interval. We first recall some preliminaries on invariant measures for random interval maps. We then define the notion of random matching and state and prove the result about densities of random systems of piecewise affine maps with matching. We also discuss the examples of random continued fraction transformations and random generalised β -transformations. In the third section we introduce and discuss the family $\{R_\alpha\}$ of random symmetric doubling maps and the corresponding signed binary expansions. We prove that R_α has random matching for Lebesgue almost all $\alpha \in [1, 2]$. We also provide a full description of the *matching intervals*, i.e., intervals of parameters that exhibit comparable matching behaviour, and describe the invariant densities of the maps R_α . Finally we prove that typically the frequency of the digit 0 in the signed binary expansions produced by R_α does not exceed $\frac{1}{2}$ for any parameter α . Throughout the paper the statement almost every parameter α is intended with respect to Lebesgue measure.

2. Random matching

2.1. The definition of random matching

Matching is a dynamical phenomenon observed in certain families of piecewise smooth interval maps. If $T : I \rightarrow I$ is such a map (so the domain I is an interval of real numbers), then we say that T has *matching* if for every discontinuity point c of T or of the derivative T' the orbits of the left and right limits $T^k(c^-) = \lim_{x \uparrow c} T^k(x)$ and $T^k(c^+) = \lim_{x \downarrow c} T^k(x)$ eventually meet, i.e.,

if for each c there exist positive constants $M = M_c$ and $Q = Q_c$, such that

$$T^M(c^-) = T^Q(c^+). \quad (1)$$

T is then said to have *strong matching* if, moreover, the orbits of the left and right limits have equal one-sided derivatives at the moment they meet, i.e., if besides (1) it also holds that

$$(T^M)'(c^-) = (T^Q)'(c^+). \quad (2)$$

It was proven in [BCMP19, theorem 1.2] (see also remark 1.3 in [BCMP19]) that for any piecewise smooth T with strong matching, any invariant probability measure μ that is absolutely continuous with respect to the Lebesgue measure has a piecewise smooth density. For continued fraction transformations (as in [NN08, DKS09, KLMM20] for example) it seems that matching is sufficient to guarantee the existence of a piecewise smooth density (since this is sufficient to construct a natural extension with finitely many pieces). The strong matching condition then enforces some stability in the matching behaviour of certain one-parameter families of continued fraction maps, which becomes visible in the appearance of so called *matching intervals* in the parameter space: if such a family has strong matching for one parameter, then one can find an interval of parameters around it, such that all the corresponding transformations have matching in the same number of steps and with comparable orbits.

In this section we extend the above definitions of matching and strong matching to random dynamical systems. With a random map we mean a system evolving in discrete time units in which at each step one of a number of transformations is chosen at random and applied. One way to describe a random map is with a pseudo-skew product transformation as follows. Let $\Omega \subseteq \mathbb{N}$ be the index set of the available maps, so we have a collection of transformations $\{T_j : I \rightarrow I\}_{j \in \Omega}$ defined on the same interval I at our disposal. Let $\sigma : \Omega^{\mathbb{N}} \rightarrow \Omega^{\mathbb{N}}$ be the left shift on one-sided sequences. The *random map* or *pseudo-skew product* $R : \Omega^{\mathbb{N}} \times I \rightarrow \Omega^{\mathbb{N}} \times I$ is defined by

$$R(\omega, x) = (\sigma(\omega), T_{\omega_1}x).$$

So, the coordinates of ω determine which of the maps T_j is applied at each time step. Let $\mathbf{p} = (p_j)_{j \in \Omega}$ be a positive probability vector, i.e., $p_j > 0$ for all $j \in \Omega$ and $\sum_{j \in \Omega} p_j = 1$, representing the probabilities with which we choose the maps T_j . Denote by $m_{\mathbf{p}}$ the \mathbf{p} -Bernoulli measure on $\Omega^{\mathbb{N}}$, let $\mu_{\mathbf{p}}$ be a probability measure on I that is absolutely continuous with respect to the one-dimensional Lebesgue measure λ and denote its density by $f_{\mathbf{p}} := \frac{d\mu_{\mathbf{p}}}{d\lambda}$. If $\mu_{\mathbf{p}}$ satisfies for each Borel set $B \subseteq I$ that

$$\mu_{\mathbf{p}}(B) = \int_B f_{\mathbf{p}} d\lambda = \sum_{j \in \Omega} p_j \mu_{\mathbf{p}}(T_j^{-1}B), \quad (3)$$

then the product measure $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ is an invariant probability measure for R . Here we call $\mu_{\mathbf{p}}$ a *stationary measure* and $f_{\mathbf{p}}$ an *invariant density* for R .

In the literature there exist various sets of conditions under which the existence of such an invariant measure is guaranteed. See for example [Mor85, Pel84, Buz00, GB03, BG05, Ino12]. Here we explicitly mention a special case of the conditions by Inoue from [Ino12] which are simple to state and suit our purposes in the next sections. Let $\Omega \subseteq \mathbb{N}$, $I \subseteq \mathbb{R}$ an interval and $\{T_j : I \rightarrow I\}_{j \in \Omega}$ a family of transformations. Let $\mathbf{p} = (p_j)_{j \in \Omega}$ be a positive probability vector. Assume that the following three conditions hold:

- (a1) There is a finite or countable interval partition $\{I_i\}$ of I , such that each map T_j is C^1 and monotone on the interior of each interval I_i .

Let C denote the set of all boundary points of the intervals I_i that are in the interior of I . We choose the collection $\{I_i\}$ as small as possible, so that C contains precisely those points that are a critical point of T_j or T'_j for at least one $j \in \Omega$. We call elements $c \in C$ *critical points* for the corresponding random system R .

- (a2) The random system R is *expanding on average*, i.e., there exists a constant $0 < \rho < 1$, such that $\sum_{j \in \Omega} \frac{p_j}{|T'_j(x)|} \leq \rho$ holds for each $x \in I \setminus C$.
- (a3) For each $j \in \Omega$ and $c \in C$ the map

$$x \mapsto \begin{cases} \frac{p_j}{|T'_j(x)|}, & \text{if } x \neq c, \\ 0, & \text{otherwise,} \end{cases}$$

is of bounded variation.

It then follows from [Ino12, theorem 5.2] that an invariant measure for R of the form $m_p \times \mu_p$ with μ_p satisfying (3) exists. Let \mathcal{R} denote the class of random maps R that satisfy these three conditions. We will define random matching for maps in \mathcal{R} , but first we fix some notation on sequences and strings.

For each $k > 0$ the set $\Omega^k = \{\mathbf{u} = u_1 \cdots u_k : u_i \in \Omega, 1 \leq i \leq k\}$ is the set of all k -strings of elements in Ω . We let $\Omega^0 = \{\epsilon\}$, with ϵ the empty string. For a finite string \mathbf{u} let $|\mathbf{u}|$ denote its length, i.e., $|\mathbf{u}| = k$ if $\mathbf{u} \in \Omega^k$. Also, for $1 \leq n \leq k$ we let $\mathbf{u}_1^n := u_1 \cdots u_n$ and we set $\mathbf{u}_1^0 = \epsilon$. Similarly, for an infinite sequence $\omega \in \Omega^{\mathbb{N}}$ and $n \geq 1$ we use the notation $\omega_1^n := \omega_1 \cdots \omega_n$ with $\omega_1^0 = \epsilon$. Finally, we use square brackets to denote cylinder sets, so

$$[\mathbf{u}] = \{\omega \in \Omega^{\mathbb{N}} : \omega_1 \cdots \omega_{|\mathbf{u}|} = \mathbf{u}\}. \quad (4)$$

For $\mathbf{u} \in \Omega^k$ and $0 \leq n \leq k$, let

$$T_{\mathbf{u}} = T_{u_k} \circ T_{u_{k-1}} \circ \cdots \circ T_{u_1} \quad \text{and} \quad T_{\mathbf{u}}^n = T_{\mathbf{u}_1^n} = T_{u_n} \circ T_{u_{n-1}} \circ \cdots \circ T_{u_1}.$$

Note that $T_{\mathbf{u}}^0 = T_{\mathbf{u}_1^0} = T_{\epsilon} = \text{id}$. Similarly if $\omega \in \Omega^{\mathbb{N}}$, we let $T_{\omega}^n = T_{\omega_1^n} = T_{\omega_n} \circ T_{\omega_{n-1}} \circ \cdots \circ T_{\omega_1}$ for any $n \geq 0$. For $\mathbf{u} \in \Omega^k$ the left and right random orbits of the critical points $c \in C$ are

$$T_{\mathbf{u}}(c^-) = \lim_{x \uparrow c} T_{\mathbf{u}}(x) \quad \text{and} \quad T_{\mathbf{u}}(c^+) = \lim_{x \downarrow c} T_{\mathbf{u}}(x).$$

The one-sided derivatives along \mathbf{u} are given by

$$T'_{\mathbf{u}}(c^-) = \lim_{x \uparrow c} \prod_{n=1}^k T'_{u_n}(T_{\mathbf{u}_1^{n-1}}(x)) \quad \text{and} \quad T'_{\mathbf{u}}(c^+) = \lim_{x \downarrow c} \prod_{n=1}^k T'_{u_n}(T_{\mathbf{u}_1^{n-1}}(x)).$$

We use the abbreviation $p_{\mathbf{u}} := p_{u_1} \cdots p_{u_k}$ with $p_{\epsilon} = 1$.

Definition 2.1. (Random matching). A random map $R \in \mathcal{R}$ has *random matching* if for every $c \in C$ there exists an $M = M_c \in \mathbb{N}$ and a set

$$Y = Y_c \subseteq \{T_{\omega}^k(c^-) : \omega \in \Omega^{\mathbb{N}}, 1 \leq k \leq M\} \cap \{T_{\omega}^k(c^+) : \omega \in \Omega^{\mathbb{N}}, 1 \leq k \leq M\}$$

such that for every $\omega \in \Omega^{\mathbb{N}}$ there exist $k = k_c(\omega), \ell = \ell_c(\omega) \leq M$ with $T_{\omega}^k(c^-), T_{\omega}^{\ell}(c^+) \in Y$.

The main difference with one-dimensional matching as in (1) and (2) is that in a random system R the critical points have many different random orbits. Definition 2.1 states that any random orbit of the left or the right limit of any critical point c passes through the set Y_c at

the latest at time M . The indices k, ℓ are introduced to cater for the possibility that these orbits pass through the set Y_c at different moments. Since all points in Y_c are in the orbit of both c^- and c^+ , this implies that all random orbits of the left limit meet with some random orbit of the right limit and vice versa. This corresponds to the statement in (1). Note that we do not ask $T_\omega^k(c^-) = T_\omega^\ell(c^+)$.

Definition 2.2. (Strong random matching). A random map $R \in \mathcal{R}$ has *strong random matching* if it has random matching and if for each $c \in C$ and $y \in Y_c$ the following holds. Set

$$\Omega(y)^- = \left\{ \mathbf{u} \in \bigcup_{k=1}^M \Omega^k : \exists \omega \in \Omega^\mathbb{N} \text{ with } \mathbf{u} = \omega_1 \cdots \omega_{k_c(\omega)} \text{ and } T_{\mathbf{u}}(c^-) = y \right\},$$

$$\Omega(y)^+ = \left\{ \mathbf{u} \in \bigcup_{k=1}^M \Omega^k : \exists \omega \in \Omega^\mathbb{N} \text{ with } \mathbf{u} = \omega_1 \cdots \omega_{\ell_c(\omega)} \text{ and } T_{\mathbf{u}}(c^+) = y \right\}.$$

Then,

$$\sum_{\mathbf{u} \in \Omega(y)^-} \frac{p_{\mathbf{u}}}{T_{\mathbf{u}}'(c^-)} = \sum_{\mathbf{u} \in \Omega(y)^+} \frac{p_{\mathbf{u}}}{T_{\mathbf{u}}'(c^+)}. \quad (5)$$

Definition 2.2 guarantees that one can choose the times k, ℓ such that at those times orbits enter the set Y with the same weighted derivative. This is comparable to (2). Note that

$$\bigcup_{y \in Y_c} \bigcup_{\mathbf{u} \in \Omega(y)^-} [\mathbf{u}] = \Omega^\mathbb{N} = \bigcup_{y \in Y_c} \bigcup_{\mathbf{u} \in \Omega(y)^+} [\mathbf{u}],$$

where $[\mathbf{u}]$ is a cylinder as defined in (4), so we have indeed captured all random orbits of c . Note that definition 2.2 depends on the choices of $k_c(\omega)$ and $\ell_c(\omega)$ for each c in definition 2.1.

If Ω consists of one element only, then the random map is actually a deterministic map. In this case definitions 2.1 and 2.2 reduce to the definitions of one-dimensional matching and strong matching given in (1) and (2), so the random definitions extend the deterministic ones.

2.2. Two examples of families of dynamical systems with random matching

Below there are two examples of families of random interval maps depending on one parameter. We show that for each of these families there exist parameter intervals such that the systems have strong random matching for every parameter within these intervals. Moreover, within such an interval matching happens in a comparable way, i.e., with the same M and similar sets Y . As in the deterministic case, we call these intervals *matching intervals*. To ease the notation we use the symbol \star to indicate the set of strings obtained by replacing \star with any $j \in \Omega$. E.g., if $\Omega = \{0, 1, 2\}$, then $0\star = \{00, 01, 02\}$.

Example 2.3. For $\alpha \in (0, 1)$ let $T_{\alpha,0}, T_{\alpha,1} : [\alpha - 1, \alpha] \rightarrow [\alpha - 1, \alpha]$ be the Nakada and Ito–Tanaka α -continued fraction transformations, introduced in [Nak81] and in [TI81] respectively, which are given by

$$T_{\alpha,0}(x) = \frac{1}{|x|} - \left\lfloor \frac{1}{|x|} + 1 - \alpha \right\rfloor \quad \text{and} \quad T_{\alpha,1}(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} + 1 - \alpha \right\rfloor,$$

for $x \neq 0$ and $T_{\alpha,0}(0) = 0 = T_{\alpha,1}(0)$. The graphs are shown in figure 1.

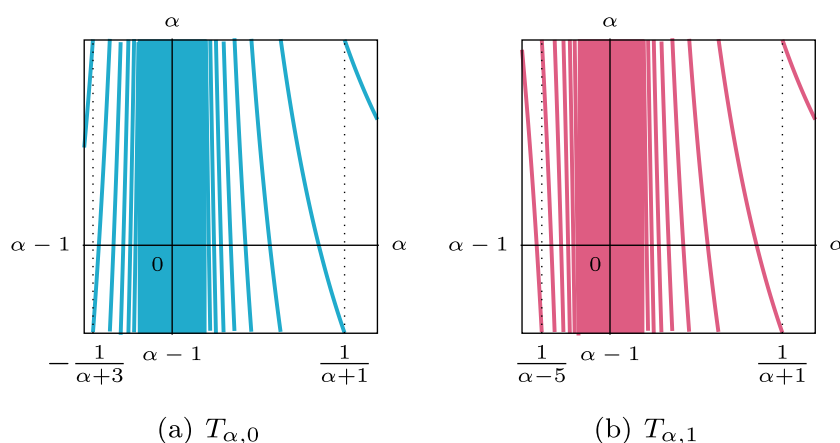


Figure 1. The Nakada α -continued fraction map $T_{\alpha,0}$ in (a) and the Ito-Tanaka α -continued fraction map $T_{\alpha,1}$ in (b) for $\alpha = \frac{7}{10} \in \left(\frac{5-\sqrt{13}}{2}, \frac{\sqrt{2}}{2}\right)$.

Let R_α denote the corresponding pseudo-skew product on $\{0, 1\}^{\mathbb{N}} \times [\alpha - 1, \alpha]$ and let $\mathbf{p} = (p_0, p_1)$ be a positive probability vector. For $x \in [0, \alpha]$, the two maps coincide and

$$T_{\alpha,0}(x) = T_{\alpha,1}(x) = \frac{1}{x} - n \quad \text{for } x \in \left(\frac{1}{\alpha+n}, \frac{1}{\alpha+n-1}\right], \quad n \in \mathbb{N}.$$

For $x \in [\alpha - 1, 0)$, we have

$$\begin{aligned} T_{\alpha,0}(x) &= -\frac{1}{x} - n \quad \text{for } x \in \left[-\frac{1}{\alpha+n-1}, -\frac{1}{\alpha+n}\right), \\ T_{\alpha,1}(x) &= \frac{1}{x} + n \quad \text{for } x \in \left[\frac{1}{\alpha-n}, \frac{1}{\alpha-(n+1)}\right). \end{aligned}$$

We first show that for any $\alpha \in \left(\frac{\sqrt{10}-2}{2}, 2 - \sqrt{2}\right)$ the map R_α has random matching. For this note that the critical points c are all in the set $\left\{\frac{1}{\alpha+n}, -\frac{1}{\alpha+n}, \frac{1}{\alpha-n} : n \in \mathbb{N}\right\}$. For any positive critical point $c > 0$ and any $j \in \{0, 1\}$, $T_j(c^-), T_j(c^+) \in \{\alpha - 1, \alpha\}$. For $c < 0$, c is either a critical point for T_0 and a continuity point for T_1 , or a critical point for T_1 and a continuity point for T_0 . Specifically, since $\alpha > \frac{1}{2}$, for $c = -\frac{1}{\alpha+n}$ we have

$$T_0(c^-) = \alpha, \quad T_0(c^+) = \alpha - 1, \quad \text{and} \quad T_1(c^-) = T_1(c^+) = 1 - \alpha,$$

and for $c = \frac{1}{\alpha-n}$

$$T_1(c^-) = \alpha - 1, \quad T_1(c^+) = \alpha, \quad \text{and} \quad T_0(c^-) = T_0(c^+) = 1 - \alpha.$$

As a consequence, to show that R_α has random matching we only need to consider the orbits of $\alpha - 1$ and α . Due to the choice of endpoints of the parameter interval $\left(\frac{\sqrt{10}-2}{2}, 2 - \sqrt{2}\right)$, the first three orbit points of α and $\alpha - 1$ are easily determined. They are given in figure 2. Hence, if we take $M = 3$ and

$$Y = \left\{ \frac{5\alpha - 3}{1 - 2\alpha}, \frac{4 - 7\alpha}{1 - 2\alpha} \right\}, \quad \text{if } c > 0$$

and

$$Y = \left\{ \frac{5\alpha - 3}{1 - 2\alpha}, \frac{4 - 7\alpha}{1 - 2\alpha}, 1 - \alpha \right\}, \quad \text{if } c < 0,$$

then R_α has random matching according to definition 2.1.

R_α does not satisfy strong random matching with this choice of Y . To see this, note that $T'_{\alpha,1}(x) = -\frac{1}{x^2}$ for all x where the derivative exists, while $T'_{\alpha,0}(x) = -\frac{1}{x^2}$ if $x > 0$ and $T'_{\alpha,0}(x) = \frac{1}{x^2}$ if $x < 0$. Now take for example $c = \frac{1}{\alpha+n} > 0$ and $y = \frac{4-7\alpha}{1-2\alpha}$. Then $\Omega(y)^- = \star 11 = \{011, 111\}$ and $\Omega(y)^+ = \star \star 1$. For the quantities from (5), we obtain

$$\sum_{\mathbf{u} \in \Omega(y)^-} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^-)} = -p_1^2 c^2 (2\alpha - 1)^2 \quad \text{and} \quad \sum_{\mathbf{u} \in \Omega(y)^+} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^+)} = -p_1 c^2 (2\alpha - 1)^2,$$

which are not equal for any $p_1 \in (0, 1)$.

We now identify a countable number of parameter intervals on which the maps R_α have strong matching with the same exponent $M = 4$, i.e., we identify a countable number of *matching intervals* for the family R_α . For $n \geq 4$ let the interval $J_n := (\ell_n, r_n)$ be defined by the left and right endpoints

$$\ell_n = \frac{n+1 - \sqrt{n^2 - 2n + 5}}{2} \quad \text{and} \quad r_n = \sqrt{\frac{n-2}{n}}, \quad (6)$$

respectively. Set $g := \frac{\sqrt{5}-1}{2}$ for the small golden mean and note that $g < \ell_n < r_n$ for all $n \geq 4$ and that $\lim_{n \rightarrow \infty} \ell_n = \lim_{n \rightarrow \infty} r_n = 1$. See figure 3 for an illustration of the location of these intervals.

The intervals J_n are chosen in such a way that we can determine the first three orbit points of α and $\alpha - 1$. Let $n \geq 4$. We further divide the interval J_n . For $k \in \{2, 3, \dots, n\}$, let

$$i_{n,k} = \frac{-4 + 2n - kn + k + \sqrt{k^2 n^2 - 2k^2 n + k^2 + 4}}{2(n-1)},$$

and note that $J_n \subseteq \cup_{k=2}^{n-1} (i_{n,k+1}, i_{n,k}]$. Therefore, for each $\alpha \in J_n$ there exists a $k \in \{2, 3, \dots, n-1\}$ such that $\alpha \in (i_{n,k+1}, i_{n,k}]$. For $\alpha \in J_n \cap (i_{n,k+1}, i_{n,k}]$ the orbits of α and $\alpha - 1$ are given in figure 4.

Definition 2.1 holds for $\alpha \in J_n \cap (i_{n,k+1}, i_{n,k}]$ with $M = 4$ and

$$Y = \left\{ \frac{1 - 2k + kn - \alpha(kn - k + 1)}{\alpha(n-1) + 2 - n} \right\}$$

for any critical point $c > 0$. For $c < 0$ we add the point $1 - \alpha$ to Y . Here the values $k_c(\omega)$ and $\ell_c(\omega)$ either equal 1, 3 or 4 according to the number of orbit points in the paths in figure 4. For definition 2.2, for $c > 0$ and $y \in Y$ we have $\Omega(y)^- = \star 0 \star \cup \star 1 \star \star$ and $\Omega(y)^+ = \star \star \star \star$, so that

$$\begin{aligned} \sum_{\mathbf{u} \in \Omega(y)^-} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^-)} &= (-c^2) p_0 (\alpha - 1)^2 \cdot \frac{(\alpha(n-1) + 2 - n)^2}{-(\alpha - 1)^2} \\ &\quad + (-c^2) p_1 (-(\alpha - 1)^2) \cdot \frac{(1 + n(\alpha - 1))^2}{-(\alpha - 1)^2} \cdot \frac{(\alpha(n-1) + 2 - n)^2}{-(1 + n(\alpha - 1))^2} \\ &= c^2 (\alpha(n-1) + 2 - n)^2. \end{aligned}$$

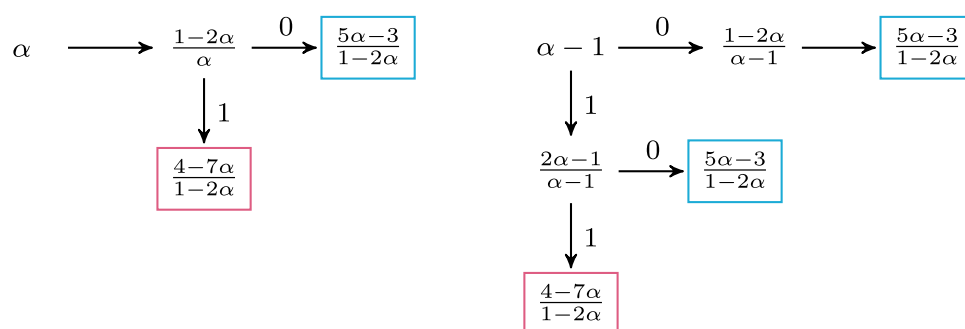


Figure 2. The first three elements in the orbits of α and $\alpha - 1$ under the random continued fraction map R_α for $\alpha \in \left(\frac{\sqrt{10}-2}{2}, 2 - \sqrt{2}\right)$. The digits above the arrows indicate which one of the maps $T_{\alpha,0}$ or $T_{\alpha,1}$ is applied. If there is no digit, then both maps yield the same orbit point. Orbit points in boxes with the same colour are equal.

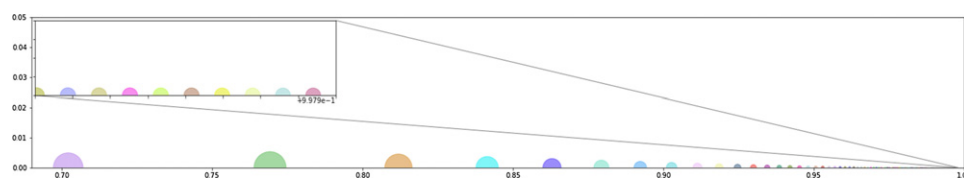


Figure 3. The semicircles indicate the locations of the intervals J_n .

and

$$\begin{aligned} \sum_{\mathbf{u} \in \Omega(y)^+} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^+)} &= (-c^2)(-\alpha^2) \frac{(1-\alpha)^2}{-\alpha^2} \cdot \frac{(\alpha(n-1) + 2 - n)^2}{-(1-\alpha)^2} \\ &= c^2(\alpha(n-1) + 2 - n)^2, \end{aligned}$$

implying that also condition (5) holds. For $c = -1/(\alpha + n)$ we get $\Omega(1 - \alpha)^- = \Omega(1 - \alpha)^+ = \{1\}$, $\Omega(y)^- = 0 \star \star \star$ and $\Omega(y)^+ = 00 \star \cup 01 \star \star$, and for $c = 1/(\alpha - n)$ we obtain $\Omega(1 - \alpha)^- = \Omega(1 - \alpha)^+ = \{0\}$, $\Omega(y)^- = 10 \star \cup 11 \star \star$ and $\Omega(y)^+ = 1 \star \star \star$. In both cases the result follows in a similar fashion. So, the random continued fraction system R_α has strong random matching for any \mathbf{p} and any $\alpha \in J_n$.

Note that in this example the orbits of α meet with some of the orbits of $\alpha - 1$ already after two time steps in the point $\frac{\alpha(n-1)+2-n}{1-\alpha}$. Hence,

$$\frac{\alpha(n-1) + 2 - n}{1 - \alpha} \in \{T_\omega^k(c^-) : \omega \in \Omega^\mathbb{N}, k \leq M\} \cap \{T_\omega^k(c^+) : \omega \in \Omega^\mathbb{N}, k \leq M\}.$$

Therefore, for a critical point $c > 0$, we could also take $Y = \left\{ \frac{\alpha(n-1)+2-n}{1-\alpha}, \frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n} \right\}$ and split the random orbits of α for example in the following way:

$$\Omega\left(\frac{\alpha(n-1) + 2 - n}{1 - \alpha}\right)^+ = \star \star 0 \quad \text{and} \quad \Omega\left(\frac{1 - 2k + kn - \alpha(kn - k + 1)}{\alpha(n-1) + 2 - n}\right)^+ = \star \star 1 \star.$$

$$\begin{array}{ccccc}
 \alpha & \longrightarrow & \frac{1-\alpha}{\alpha} & \longrightarrow & \frac{\alpha(n-1)+2-n}{1-\alpha} & \longrightarrow & \boxed{\frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n}} \\
 \\
 \alpha-1 & \xrightarrow{0} & \frac{\alpha(n-1)+2-n}{1-\alpha} & \longrightarrow & \boxed{\frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n}} \\
 \downarrow 1 & & & & & & \\
 \frac{n(\alpha-1)+1}{\alpha-1} & \longrightarrow & \frac{\alpha(n-1)+2-n}{-1-n(\alpha-1)} & \longrightarrow & \boxed{\frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n}}
 \end{array}$$

Figure 4. The first few points in the orbits of α and $\alpha - 1$ under the random continued fraction map R_α for $\alpha \in J_n \cap (i_{n,k+1}, i_{n,k}]$. For details we refer the reader to [2021].

For the orbits passing through $\alpha - 1$ we have

$$\Omega\left(\frac{\alpha(n-1)+2-n}{1-\alpha}\right)^- = *0 \quad \text{and} \quad \Omega\left(\frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n}\right)^- = *1* *.$$

One can check that condition (5) is satisfied and R_α has strong random matching with this choice of Y . Note that in this case many sequences ω have smaller values $k_c(\omega)$ and $\ell_c(\omega)$ than with $Y = \left\{\frac{1-2k+kn-\alpha(kn-k+1)}{\alpha(n-1)+2-n}\right\}$ and that for some $\omega \in \Omega^\mathbb{N}$ we do not take $k_c(\omega)$ equal to the first time that the random orbit $T_\omega^k(c^-)$ enters Y . For example, for $c > 0$ and any ω with $\omega_3 = 1$ we have $T_\omega^3(c^+) = \frac{\alpha(n-1)+2-n}{1-\alpha} \in Y$, but we take $k_c(\omega) = 4$. The flexibility in the choice of Y and the length of the paths $k_c(\omega)$ and $\ell_c(\omega)$ embedded in definition 2.1 allows one to choose the option that is computationally most convenient.

Example 2.4. Let $\beta = \frac{1+\sqrt{5}}{2}$ be the golden mean, so $\beta^2 = \beta + 1$, and for any $\alpha \in (\frac{3\beta-2}{2}, 4\beta-5)$ consider two generalised β -transformations $T_{\alpha,j}: [-\beta, \beta] \rightarrow [-\beta, \beta]$, $j = 0, 1$, defined by

$$T_{\alpha,0}(x) = \begin{cases} \beta x + \alpha, & \text{if } x \in \left[-\beta, -\frac{1}{\beta}\right), \\ \beta x, & \text{if } x \in \left[-\frac{1}{\beta}, 1\right], \\ \beta x - \alpha, & \text{if } x \in (1, \beta], \end{cases} \quad \text{and} \\
 T_{\alpha,1}(x) = \begin{cases} \beta x + \alpha, & \text{if } x \in [-\beta, -1), \\ \beta x, & \text{if } x \in \left[-1, \frac{1}{\beta}\right], \\ \beta x - \alpha, & \text{if } x \in \left(\frac{1}{\beta}, \beta\right]. \end{cases}$$

Note that it does not matter how one defines the maps at the discontinuity points. This is just a choice that we made. See figure 5 for the graphs.

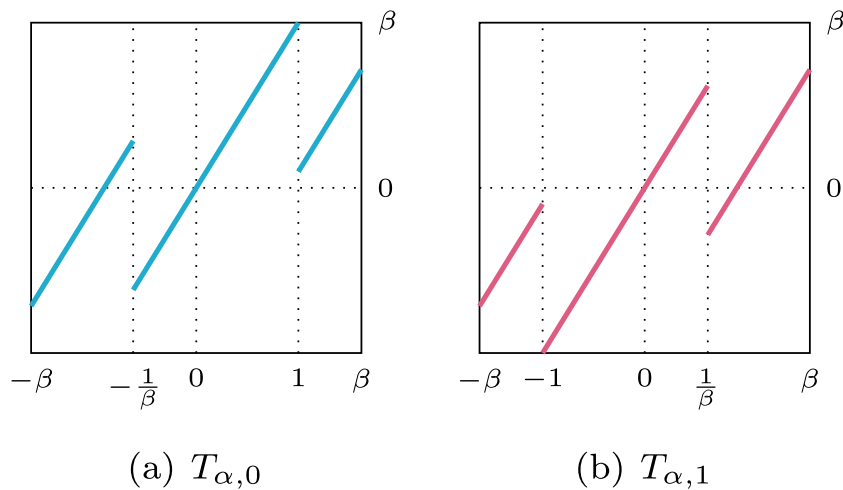


Figure 5. The maps $T_{\alpha,0}$ and $T_{\alpha,1}$ from example 2.4 for $\alpha \in (\frac{3\beta-2}{2}, 4\beta-5)$.

Let R_α denote the corresponding random system and let $\mathbf{p} = (p_0, p_1)$ be a positive probability vector. Then $C = \left\{-1, -\frac{1}{\beta}, \frac{1}{\beta}, 1\right\}$. By the symmetry in the maps to show that R_α has matching we only need to consider the points $\frac{1}{\beta}$ and 1. The parameter interval $(\frac{3\beta-2}{2}, 4\beta-5)$ is constructed in such a way that for any $\alpha \in (\frac{3\beta-2}{2}, 4\beta-5)$ the initial parts of the random orbits of the left and right limits to $\frac{1}{\beta}$ and 1 are determined in the following way. For $j = 0, 1$ and any $\omega \in \{0, 1\}^\mathbb{N}$,

$$\begin{aligned} T_{\alpha,0}(1^-) &= \beta, & T_{\alpha,\omega}(\beta) &= \beta^2 - \alpha, & T_{\alpha,\omega}^2(\beta) &= \beta^2(\beta - \alpha), \\ T_{\alpha,1}(1^-) &= T_{\alpha,j}(1^+) = \beta - \alpha, & T_{\alpha,\omega}(\beta - \alpha) &= \beta(\beta - \alpha), & T_{\alpha,\omega}^2(\beta - \alpha) &= \beta^2(\beta - \alpha). \end{aligned}$$

Hence, for $1 \in C$ we can take $M = k_1(\omega) = \ell_1(\omega) = 3$ for each ω , $Y = \{\beta^2(\beta - \alpha)\}$ and one easily checks the conditions of both definitions 2.1 and 2.2.

For $\frac{1}{\beta}$ we get $T_{\alpha,j}(\frac{1}{\beta}^-) = 1 = T_{\alpha,0}(\frac{1}{\beta}^+)$ and $T_{\alpha,1}(\frac{1}{\beta}^+) = 1 - \alpha$. We saw the orbit of 1 above and the orbit of $1 - \alpha$ is depicted in figure 6. Then straightforward computations show that R_α has strong random matching with $M = k_{\frac{1}{\beta}}(\omega) = \ell_{\frac{1}{\beta}}(\omega) = 7$ for each ω and $Y = \{\beta^5(\beta - \alpha) - \alpha, \beta^5(\beta - \alpha) - \beta\alpha = \beta^6 - 3\beta^3\alpha\}$.

Theorem 2.5 below explains the need for condition (5) in definition 2.2.

2.3. Random matching for piecewise affine systems

In case each map $T_j : I \rightarrow I$ is piecewise affine on a finite partition $c_0 < c_1 < \dots < c_N$ the conditions (a1) and (a3) are automatically satisfied and under some additional assumptions strong random matching has consequences for invariant densities. For this result we consider a subset of the collection of random maps \mathcal{R} . We define the subset $\mathcal{R}_A \subset \mathcal{R}$ to be the set of random systems in \mathcal{R} that satisfy the following additional assumptions:

- (c1) There exists a finite interval partition $\{I_i\}_{1 \leq i \leq N}$ of $I = [c_0, c_N]$ given by the points $c_0 < c_1 < \dots < c_N$, such that each map $T_j : I \rightarrow I$, $j \in \Omega$, is piecewise affine with respect to this partition. In other words, for each $j \in \Omega$ and $1 \leq i \leq N$ we can write $T_j|_{(c_{i-1}, c_i)}(x) = k_{i,j}x + d_{i,j}$ for some constants $k_{i,j}, d_{i,j}$.

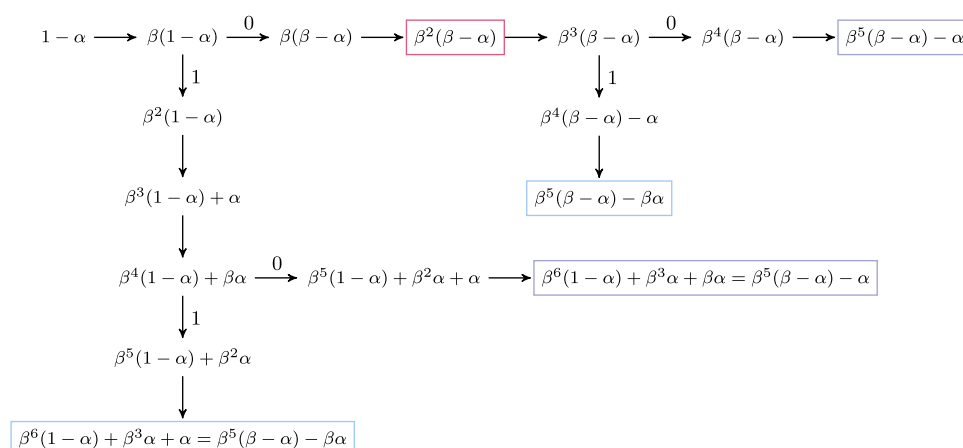


Figure 6. The first couple of points in the orbit of $1 - \alpha$ under the random generalised β -transformation from example 2.4. We have boxed $\beta^2(\beta - \alpha)$, since this point also appears in all random orbits of 1.

(c2) For each $1 \leq i \leq N$ there is an $1 \leq n \leq N$, such that

$$\frac{\sum_{j \in \Omega} \frac{p_i}{k_{i,j}} d_{i,j}}{1 - \sum_{j \in \Omega} \frac{p_i}{k_{i,j}}} \neq \frac{\sum_{j \in \Omega} \frac{p_j}{k_{n,j}} d_{n,j}}{1 - \sum_{j \in \Omega} \frac{p_j}{k_{n,j}}}. \quad (7)$$

(c3) For each $1 \leq i \leq N$, $\sum_{j \in \Omega} \frac{p_j}{k_{i,j}} \neq 0$.

Using the results from [KM20], we will show that for $R \in \mathcal{R}_A$ the following holds.

Theorem 2.5. *Let $R \in \mathcal{R}_A$. If R has strong random matching, then there exists an invariant probability measure $\mu_{\mathbf{p}} \times \mu_{\mathbf{p}}$ for R with $\mu_{\mathbf{p}}$ absolutely continuous with respect to λ and such that its density $f_{\mathbf{p}}$ is piecewise constant. If moreover every map T_j is expanding, i.e., if $|k_{i,j}| > 1$ for each $1 \leq i \leq N$ and $j \in \Omega$, then any invariant probability density $f_{\mathbf{p}}$ of R is piecewise constant.*

Assumptions (c2) and (c3) are used in [KM20] to prove that for systems in \mathcal{R}_A there exists an invariant probability density function that can be written as an infinite sum of indicator functions. More precisely, assumption (c2) states that the maps $x \mapsto k_{i,j}x + d_{i,j}$ do not have a common weighted intersection point with the diagonal, and assumption (c3) states that the weighted inverse derivatives of the maps T_j are not 0. These conditions, which are not very restrictive, guarantee that the method from [KM20] works, but they might not be necessary for the results from [KM20, theorem 4.1] and theorem 2.5. In fact, the deterministic analog of theorem 2.5, which can be found in [BCMP19, theorem 1.2], does not have a condition like (7). Their proof uses an induced system with a full branched return map instead. One could try to transfer the proof of [BCMP19, theorem 1.2] to the setting of random interval maps to avoid (c2) and (c3). Then, the recent results from Inoue in [Ino20] on first return time functions for random systems seem relevant. These results show, however, that an induced system for a random interval map will become position dependent instead of i.i.d., which might make such an extension not so straightforward.

Proof. The set of critical points of R is given by $C = \{c_1, \dots, c_{N-1}\}$. Any random map $R \in \mathcal{R}_A$ satisfies the conditions of [KM20, theorem 4.1]. Thus, there exists an invariant probability

measure $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ for R with a probability density $f_{\mathbf{p}}$ for $\mu_{\mathbf{p}}$ of the form

$$f_{\mathbf{p}} = \sum_{i=1}^{N-1} \gamma_i \sum_{k \geq 1} \sum_{\mathbf{u} \in \Omega^k} \left(\frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^-)} 1_{[c_0, T_{\mathbf{u}}(c_i^-))} - \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^+)} 1_{[c_0, T_{\mathbf{u}}(c_i^+))} \right), \quad (8)$$

for some constants γ_i depending only on the critical points c_i . Fix an i and let M, Y be such that R satisfies the conditions of definitions 2.1 and 2.2 for c_i . Then by (5)

$$\sum_{y \in Y} \left(\sum_{\mathbf{u} \in \Omega(y)^-} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^-)} 1_{[c_0, T_{\mathbf{u}}(c_i^-))} - \sum_{\mathbf{u} \in \Omega(y)^+} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^+)} 1_{[c_0, T_{\mathbf{u}}(c_i^+))} \right) = 0.$$

For each $1 \leq i \leq N-1$ and each $1 \leq k \leq M$, let

$$\Omega_-^{i,k} = \{\mathbf{u} \in \Omega^k : \exists \omega \in \Omega^{\mathbb{N}} \text{ with } \mathbf{u} = \omega_1 \cdots \omega_k \text{ and } k < k_{c_i}(\omega)\}$$

and similarly

$$\Omega_+^{i,k} = \{\mathbf{u} \in \Omega^k : \exists \omega \in \Omega^{\mathbb{N}} \text{ with } \mathbf{u} = \omega_1 \cdots \omega_k \text{ and } k < \ell_{c_i}(\omega)\}.$$

Then $f_{\mathbf{p}}$ can be written as

$$f_{\mathbf{p}} = \sum_{i=1}^{N-1} \gamma_i \sum_{k=1}^M \left(\sum_{\mathbf{u} \in \Omega_-^{i,k}} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^-)} 1_{[c_0, T_{\mathbf{u}}(c_i^-))} - \sum_{\mathbf{u} \in \Omega_+^{i,k}} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c_i^+)} 1_{[c_0, T_{\mathbf{u}}(c_i^+))} \right).$$

Hence $f_{\mathbf{p}}$ is constant on each interval in the finite partition of I specified by the orbit points in the set

$$\bigcup_{i=1}^{N-1} \bigcup_{k=1}^M (\{T_{\mathbf{u}}(c_i^-) : \mathbf{u} \in \Omega_-^{i,k}\} \cup \{T_{\mathbf{u}}(c_i^+) : \mathbf{u} \in \Omega_+^{i,k}\}).$$

This gives the first part of the result.

For the second part, note that under the additional assumption that $|k_{i,j}| > 1$ for all i, j the map R satisfies the conditions of [KM20, theorem 5.3]. As a consequence, any invariant density $f_{\mathbf{p}}$ of R can be written as in (8) for some values γ_i . This proves the theorem. \square

Example 2.6. The random generalised β -transformations R_{α} from example 2.4 satisfy all conditions of theorem 2.5. Hence, for any $\alpha \in (\frac{3\beta-2}{2}, 4\beta-5)$ any invariant density of the random system R_{α} is piecewise constant.

3. Random signed binary transformations and expansions

In the second part of this article we use strong random matching to study the frequency of the digit 0 in the signed binary expansions produced by a family of random system of piecewise affine maps. We first define this family and its relation to binary expansions.

3.1. The family of random symmetric doubling maps

A signed binary expansion of a number $x \in [-1, 1]$ can be obtained by iterating any piecewise affine map $D : [-1, 1] \rightarrow [-1, 1]$ that is given by $D(x) = 2x - d$ with $d \in \{-1, 0, 1\}$ on each

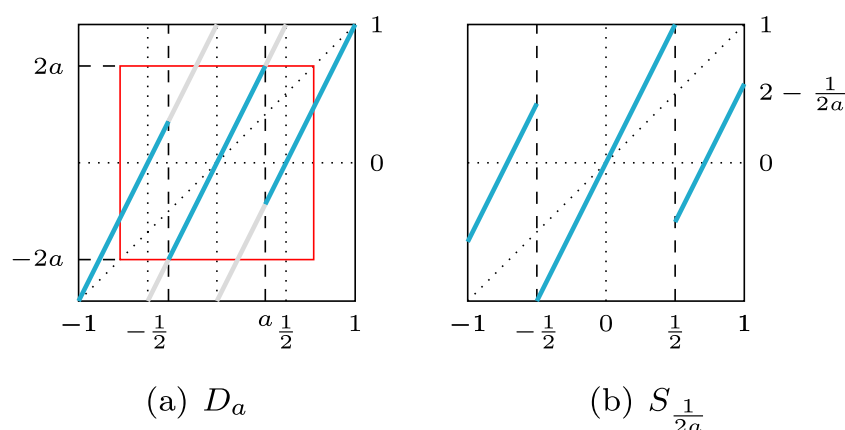


Figure 7. The maps D_a and $S_{\frac{1}{2a}}$ for $a = \frac{7}{20}$. The grey lines indicate the remainder of the maps $x \mapsto 2x + 1$, $x \mapsto 2x$ and $x \mapsto 2x - 1$. The red box in (a) shows the attractor of the map D_c . The map inside the box in (a) is a rescaled version of the map in (b).

of its intervals of monotonicity. One can for example take any $a \in [\frac{1}{4}, \frac{1}{2}]$ and then define the symmetric map

$$D_a(x) = \begin{cases} 2x + 1, & \text{if } -1 \leq x < -a, \\ 2x, & \text{if } -a \leq x \leq a, \\ 2x - 1, & \text{if } a < x \leq 1. \end{cases}$$

By setting $d_n(x) = d$, $d \in \{-1, 0, 1\}$, if $D_a^n(x) = 2D_a^{n-1}(x) - d$, one obtains

$$x = \frac{d_1(x)}{2} + \frac{D_a(x)}{2} = \cdots = \frac{d_1(x)}{2} + \cdots + \frac{d_n(x)}{2^n} + \frac{D_a^n(x)}{2^n} \rightarrow \sum_{n \geq 1} \frac{d_n(x)}{2^n},$$

so this gives a signed binary expansion of x . The family of maps $\{D_a\}_{\frac{1}{4} \leq a \leq \frac{1}{2}}$ is the object of study in [DK20]. As can be seen from figure 7(a) the interval $[-2a, 2a]$ is an attractor for the dynamics of D_a . Since this interval depends on a , in [DK20] the authors decided to work instead with the measurably isomorphic family $\{S_\alpha\}_{1 \leq \alpha \leq 2}$ given by

$$S_\alpha(x) = \begin{cases} 2x + \alpha, & \text{if } -1 \leq x < -\frac{1}{2}, \\ 2x, & \text{if } -\frac{1}{2} \leq x \leq \frac{1}{2}, \\ 2x - \alpha, & \text{if } \frac{1}{2} < x \leq 1, \end{cases} \quad (9)$$

see figure 7(b), which transfers the dependence on the parameter from the domain $[-1, 1]$ to the branches of the maps.

While each deterministic map produces for each number in its domain a single signed binary expansion, one can define random dynamical systems that produce for λ almost all numbers uncountably many different signed binary expansions. The family of random maps

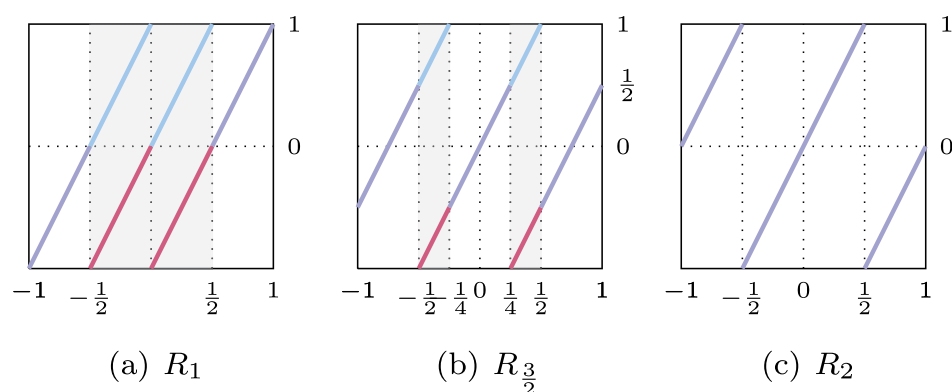


Figure 8. The maps $T_{\alpha,0}$ and $T_{\alpha,1}$ for $\alpha = 1$ in (a), $\alpha = \frac{3}{2}$ in (b), and $\alpha = 2$ in (c). The blue lines correspond to $T_{\alpha,0}$, the pink ones to $T_{\alpha,1}$ and the purple ones to both.

$\{R_\alpha\}$, which we define next, extends the family of deterministic maps $\{S_\alpha\}$. So the dependence on the parameter is visible in the branches of the maps instead of in the domains.

Let $\Omega = \{0, 1\}$ and define for $j \in \Omega$ and each parameter $\alpha \in [1, 2]$ the maps $T_j = T_{\alpha,j} : [-1, 1] \rightarrow [-1, 1]$ by

$$T_{\alpha,0}(x) = \begin{cases} 2x + \alpha, & \text{if } x \in \left[-1, \frac{1-\alpha}{2}\right], \\ 2x, & \text{if } x \in \left(\frac{1-\alpha}{2}, \frac{1}{2}\right], \\ 2x - \alpha, & \text{if } x \in \left(\frac{1}{2}, 1\right], \end{cases} \quad \text{and} \\ T_{\alpha,1}(x) = \begin{cases} 2x + \alpha, & \text{if } x \in \left[-1, -\frac{1}{2}\right), \\ 2x, & \text{if } x \in \left[-\frac{1}{2}, \frac{\alpha-1}{2}\right), \\ 2x - \alpha, & \text{if } x \in \left[\frac{\alpha-1}{2}, 1\right]. \end{cases} \quad (10)$$

See figure 8 for three examples. The maps $T_{\alpha,0}$ and $T_{\alpha,1}$ differ on the intervals $\left[-\frac{1}{2}, \frac{1-\alpha}{2}\right]$ and $\left[\frac{\alpha-1}{2}, \frac{1}{2}\right]$, which are indicated by the grey areas in the pictures. Let $R = R_\alpha : \Omega^{\mathbb{N}} \times [-1, 1] \rightarrow \Omega^{\mathbb{N}} \times [-1, 1]$ be the random system obtained from $T_{\alpha,0}$ and $T_{\alpha,1}$, i.e.,

$$R_\alpha(\omega, x) = (\sigma(\omega), T_{\alpha,\omega_1}(x)),$$

where σ is the left shift on $\Omega^{\mathbb{N}}$. We call the systems R_α *random symmetric doubling maps* and the subscript α will sometimes be suppressed if it does not lead to confusion.

Fix an $\alpha \in [1, 2]$. Recall from (4) that we use square brackets to denote the cylinder sets in $\Omega^{\mathbb{N}}$. Let $\pi : \Omega^{\mathbb{N}} \times [-1, 1] \rightarrow [-1, 1]$ denote the canonical projection onto the second coordinate and set

$$s_n(\omega, x) = \begin{cases} -1, & \text{if } R^{n-1}(\omega, x) \in \Omega^{\mathbb{N}} \times [-1, -\frac{1}{2}) \cup [0] \times [-\frac{1}{2}, \frac{1-\alpha}{2}], \\ 0, & \text{if } R^{n-1}(\omega, x) \in [1] \times [-\frac{1}{2}, \frac{1-\alpha}{2}] \\ & \cup \Omega^{\mathbb{N}} \times \left(\frac{1-\alpha}{2}, \frac{\alpha-1}{2}\right) \cup [0] \times \left[\frac{\alpha-1}{2}, \frac{1}{2}\right], \\ 1, & \text{if } R^{n-1}(\omega, x) \in [1] \times \left[\frac{\alpha-1}{2}, \frac{1}{2}\right] \cup \Omega^{\mathbb{N}} \times \left(\frac{1}{2}, 1\right]. \end{cases} \quad (11)$$

Then

$$\pi(R^n(\omega, x)) = 2\pi(R^{n-1}(\omega, x)) - s_n(\omega, x)\alpha,$$

so that just as in the deterministic case by iteration we obtain

$$x = \frac{s_1(\omega, x)\alpha}{2} + \dots + \frac{s_n(\omega, x)\alpha}{2^n} + \frac{\pi(R^n(\omega, x))}{2^n} \rightarrow \alpha \sum_{n \geq 1} \frac{s_n(\omega, x)}{2^n}.$$

In other words, iterations of the random system R give a signed binary expansion for the pair (ω, x) .

Note that for each $x \in [-1, 1]$ there is an $\omega \in \Omega^{\mathbb{N}}$, such that $\pi(R^n_\alpha(\omega, x)) = S_\alpha^n(x)$, where S_α is the map in the family $\{S_\alpha\}$ from [DK20]. In particular, the random signed binary expansions produced by the family $\{R_\alpha\}$ include, among many others, the SSB expansions. The randomness of the system allows us to choose (up to a certain degree) where and when we want to have a digit 0. Below we investigate the frequency of the digit 0 in typical expansions produced by the maps R . We do so by applying Birkhoff's ergodic theorem for invariant measures for R of the form $m \times \mu$ with m a Bernoulli measure and μ absolutely continuous with respect to λ . For that we need to investigate the density of such measures μ .

3.2. Prevalent matching for random symmetric doubling maps

For any $\alpha \in [1, 2]$ the common partition on which T_0 and T_1 are monotone is given by the points

$$c_0 = -1, \quad c_1 = -\frac{1}{2}, \quad c_2 = \frac{1-\alpha}{2}, \quad c_3 = \frac{\alpha-1}{2}, \quad c_4 = \frac{1}{2}, \quad c_5 = 1.$$

Set, in accordance with (a1),

$$I_1 = [c_0, c_1], \quad I_2 = [c_1, c_2], \quad I_3 = (c_2, c_3), \quad I_4 = [c_3, c_4], \quad I_5 = (c_4, c_5],$$

then $C = \{c_1, c_2, c_3, c_4\}$. Note that for $\alpha = 1$, $c_2 = c_3 = 0$ and I_3 vanishes. For $0 < p < 1$, use $\mathbf{p} = (p_0, p_1)$ to denote the probability vector with $p_0 = p$ and $p_1 = 1 - p$. Since T_0 and T_1 from (10) are both piecewise affine with slope 2, we have $\frac{p_j}{|T_j'(x)|} = \frac{p_j}{T_j'(x)} = \frac{p_j}{2}$, $j = 0, 1$. So the random system R satisfies conditions (a1), (a2), (a3), i.e., $R \in \mathcal{R}$. Due to the symmetry in the map, to verify whether R has strong random matching it is enough to check the conditions of definitions 2.1 and 2.2 for the points $1 = T_0(c_4)^-$ and $1 - \alpha = T_0(c_4)^+$.

Before we proceed with a description of the matching behaviour of the family of random systems $\{R_\alpha\}$, we first recall the results from [DK20, propositions 2.1 and 2.3] on matching

for the family of deterministic symmetric doubling maps $\{S_\alpha\}$, see (9). Let

$$M_\alpha = \inf \left\{ n \geq 0 : \frac{1}{2} < S_\alpha^n(1) < \alpha - \frac{1}{2} \right\} + 1, \quad (12)$$

with $M_\alpha = \infty$ if no such n exists. Then according to [DK20, propositions 2.1 and 2.3] for all $\alpha \in [1, 2]$,

$$S_\alpha^k(1 - \alpha) = S_\alpha^k(1) - \alpha \quad \text{for } k < M_\alpha \quad (13)$$

and for almost all $\alpha \in [1, 2]$ in fact $M_\alpha < \infty$ and

$$S_\alpha^{M_\alpha+1} \left(\frac{1}{2}^- \right) = S_\alpha^{M_\alpha}(1) = S_\alpha^{M_\alpha}(1 - \alpha) = S_\alpha^{M_\alpha+1} \left(\frac{1}{2}^+ \right).$$

In other words, for almost all parameters $\alpha \in [1, 2]$ the map S_α has matching with matching exponent $M = M_\alpha + 1$ that is determined by the first time the orbit of 1 enters the interval $(\frac{1}{2}, \alpha - \frac{1}{2})$. Moreover, $S_\alpha^{M_\alpha-1}(1 - \alpha) < -\frac{1}{2}$ for all α , $M_\alpha = 1$ for $\alpha \in [\frac{3}{2}, 2]$ and $M_\alpha > 1$ for $\alpha \in (1, \frac{3}{2})$. Due to the constant slope and the same matching exponent M_α of the left and right limits, in this case matching implies strong matching.

Remark 3.1. The discrepancy between $M_\alpha + 1$ here and M_α as matching exponent in [DK20] comes from the fact that in [DK20] the orbits are considered as starting from 1 and $1 - \alpha$, whereas in (1) and (2) we followed the convention in [BCMP19] and start at the critical point $c = \frac{1}{2}$ instead.

From this we deduce the following small lemma.

Lemma 3.2. For $\alpha \in [1, 2]$ and for all $k < M_\alpha - 1$, either $S_\alpha^k(1) \in I_4$ and $S_\alpha^k(1) - \alpha \in I_1$ or $S_\alpha^k(1) \in I_5$ and $S_\alpha^k(1) - \alpha \in I_2$.

Proof. From (13) it follows for all $k < M_\alpha$ that $S_\alpha^k(1) - \alpha \geq -1$, implying that

$$\frac{\alpha - 1}{2} \leq \alpha - 1 \leq S_\alpha^k(1) \leq 1 \quad \text{and} \quad -1 \leq S_\alpha^k(1) - \alpha \leq 1 - \alpha \leq \frac{1 - \alpha}{2},$$

so that $S_\alpha^k(1) \in I_4 \cup I_5$. If $S_\alpha^k(1) \in I_4$, then $S_\alpha^k(1) - \alpha \leq \frac{1}{2} - \alpha < -\frac{1}{2}$, so $S_\alpha^k(1) - \alpha \in I_1$. Suppose $S_\alpha^k(1) \in I_5$ and $k < M_\alpha - 1$. If $S_\alpha^k(1) - \alpha < -\frac{1}{2}$, this would imply that $S_\alpha^k(1) \in (\frac{1}{2}, \alpha - \frac{1}{2})$, contradicting the definition of M_α in (12). Hence, $S_\alpha^k(1) - \alpha \in I_2$. \square

The next result states that a random equivalent of (13) holds for $\alpha \in (1, \frac{3}{2})$.

Proposition 3.3. For all $\alpha \in [1, 2]$, $0 \leq k \leq M_\alpha$ and $\mathbf{u} \in \Omega^k$, it holds that $T_{\mathbf{u}}(1), T_{\mathbf{u}}(1 - \alpha) \in \{S_\alpha^k(1), S_\alpha^k(1) - \alpha\}$.

Proof. First consider $\alpha \in [\frac{3}{2}, 2]$. Then $M_\alpha = 1$ and the result trivially holds. Fix an $\alpha \in (1, \frac{3}{2})$. Since T_0 and T_1 agree on I_5 we can find a sequence $\hat{\omega} \in \Omega^{\mathbb{N}}$ with $\hat{\omega}_1 = 0$ that gives

$$T_{\hat{\omega}_1^k}(1) = S_\alpha^k(1) \quad \text{for all } k \geq 0.$$

Note that $1 \in I_5$ and from $\alpha \in (1, \frac{3}{2})$ we get $1 - \alpha \in I_2$, so

$$T_0(1 - \alpha) = T_0(1) = T_1(1) = 2 - \alpha = S_\alpha(1) \quad \text{and} \quad T_1(1 - \alpha) = 2 - 2\alpha = S_\alpha(1 - \alpha). \quad (14)$$

Hence, from the first iterate on, the orbits of 1 and $1 - \alpha$ under the deterministic map S_α are contained in the orbit of $1 - \alpha$ under the random map R . To prove the statement, we therefore only have to consider $T_\omega^n(1 - \alpha)$ for any $\omega \in \Omega^\mathbb{N}$ and $n \geq 1$. In particular (14) implies that

$$T_{\omega_1^k}(1 - \alpha) = S_\alpha^k(1)$$

for all $k \geq 1$. We prove the statement by induction.

The statement obviously holds for $k = 0$ and by (14) also for $k = 1$. Let $1 \leq n < M_\alpha$ and suppose the statement holds for all $k \leq n$. Then

$$T_{\omega_1^n}(1 - \alpha) = S_\alpha^n(1) \quad \text{and} \quad T_{\omega_1^n}(1 - \alpha) \in \{S_\alpha^n(1), S_\alpha^n(1) - \alpha\} \quad \text{for all } \omega \in \Omega^\mathbb{N}.$$

By lemma 3.2 there are three cases.

- (a) If $S_\alpha^n(1) \in I_4$, then $S_\alpha^{n+1}(1) = 2S_\alpha^n(1)$ and $S_\alpha^n(1) - \alpha \in I_1$. So for the random images we get

$$T_0(S_\alpha^n(1)) = 2S_\alpha^n(1), \quad T_1(S_\alpha^n(1)) = 2S_\alpha^n(1) - \alpha,$$

and

$$T_0(S_\alpha^n(1) - \alpha) = T_1(S_\alpha^n(1) - \alpha) = 2S_\alpha^n(1) - \alpha.$$

- (b) If $S_\alpha^n(1) \in I_5$ and $S_\alpha^n(1) - \alpha \in I_2$, then

$$T_0(S_\alpha^n(1)) = T_1(S_\alpha^n(1)) = 2S_\alpha^n(1) - \alpha = S_\alpha^{n+1}(1)$$

and

$$T_0(S_\alpha^n(1) - \alpha) = 2S_\alpha^n(1) - \alpha, \quad T_1(S_\alpha^n(1)) = 2S_\alpha^n(1) - 2\alpha.$$

- (c) If $S_\alpha^n(1) \in I_5$ and $S_\alpha^n(1) - \alpha \in I_1$ (so $n = M_\alpha - 1$), then

$$T_0(S_\alpha^n(1)) = T_1(S_\alpha^n(1)) = 2S_\alpha^n(1) - \alpha = S_\alpha^{n+1}(1)$$

and

$$T_0(S_\alpha^n(1) - \alpha) = T_1(S_\alpha^n(1) - \alpha) = 2S_\alpha^n(1) - \alpha = S_\alpha^{n+1}(1).$$

Hence, for all $\mathbf{u} \in \Omega^n$ and $j = 0, 1$, $T_{\mathbf{u}j}(1 - \alpha) \in \{S_\alpha^{n+1}(1), S_\alpha^{n+1}(1) - \alpha\}$, which gives the result. \square

From this proposition we can deduce that matching is prevalent for the family $\{R_\alpha\}$ and we can find the precise matching times. We first prove the following lemma, stating that all the orbit points $S_\alpha^n(1), S_\alpha^n(1 - \alpha)$ up to the moment of matching are different.

Lemma 3.4. *For each $k < M_\alpha$ the set $\{S_\alpha^n(1), S_\alpha^n(1 - \alpha) : 0 \leq n \leq k\}$ has $2(k + 1)$ elements.*

Proof. Since $k < M_\alpha$ it follows from (13) that $S_\alpha^n(1) \neq S_\alpha^n(1 - \alpha)$ for each n . It also cannot hold that there are $0 \leq n < k < M_\alpha$ such that $S_\alpha^n(1) = S_\alpha^k(1 - \alpha)$ or $S_\alpha^k(1) = S_\alpha^n(1 - \alpha)$, since this would imply that $|S_\alpha^k(1) - S_\alpha^n(1)| = \alpha$ and that would contradict the fact that $S_\alpha^n(1), S_\alpha^k(1) \in I_4 \cup I_5$. This leaves the possibility that there are $0 \leq n < k < M_\alpha$ such that $S_\alpha^n(1) = S_\alpha^k(1)$, i.e., that the orbit of 1 under S_α is ultimately periodic, or $S_\alpha^n(1 - \alpha) = S_\alpha^k(1 - \alpha)$. Assume $S_\alpha^n(1) = S_\alpha^k(1)$ for some $n < k$. It follows that $S_\alpha^n(1 - \alpha) = S_\alpha^n(1) - \alpha = S_\alpha^k(1) - \alpha = S_\alpha^k(1 - \alpha)$, so the

orbit of $1 - \alpha$ is also ultimately periodic and by (13) all these orbit points lie at distance α of the corresponding orbit points of 1. This contradicts the fact that α is a matching parameter. Hence, the set $\{S_\alpha^n(1), S_\alpha^n(1 - \alpha) : 0 \leq n \leq k\}$ has $2(k + 1)$ elements. \square

Theorem 3.5. *For almost all parameters $\alpha \in [1, 2]$ the map R_α has strong random matching with $M = M_\alpha + 1$, where M_α is given by (12), and $Y = \{S_\alpha^{M_\alpha}(1)\}$. Moreover, R_α does not satisfy the conditions of strong random matching for any $K < M$.*

Proof. First consider $\alpha \in [\frac{3}{2}, 2]$. Then $T_j(1 - \alpha) = 2 - \alpha = T_j(1)$ for $j = 0, 1$, so random matching occurs for R with $M = 2$ and $Y = \{2 - \alpha\}$ and both parts of the theorem hold.

Now, fix $\alpha \in [1, \frac{3}{2})$ such that S_α has matching. Then, $S_\alpha^k(1) \neq S_\alpha^k(1 - \alpha)$ for $1 \leq k < M_\alpha$ and $S_\alpha^{M_\alpha-1}(1) \in (\frac{1}{2}, \alpha - \frac{1}{2})$, so that $S_\alpha^{M_\alpha}(1) = 2S_\alpha^{M_\alpha-1}(1) - \alpha$. By proposition 3.3 for each $\mathbf{u} \in \Omega^{M_\alpha-1}$ either

$$T_{\mathbf{u}}(1 - \alpha) = S_\alpha^{M_\alpha-1}(1) > \frac{1}{2}$$

or

$$T_{\mathbf{u}}(1 - \alpha) = S_\alpha^{M_\alpha-1}(1) - \alpha < -\frac{1}{2}.$$

In both cases this leads to $T_{\mathbf{u}j}(1 - \alpha) = 2S_\alpha^{M_\alpha-1}(1) - \alpha$ for both $j = 0, 1$. The same statement holds for $T_{\mathbf{u}}(1)$, so that for $c = \frac{1}{2}$ we therefore have

$$T_{1\mathbf{u}j}\left(\frac{1}{2}\right) = T_{0\mathbf{u}j}\left(\frac{1}{2}\right) = T_{1\mathbf{u}j}\left(\frac{1}{2}\right) = T_{\mathbf{u}j}(1 - \alpha) = S_\alpha^{M_\alpha}(1)$$

and

$$T_{0\mathbf{u}j}\left(\frac{1}{2}\right) = T_{\mathbf{u}j}(1) = S_\alpha^{M_\alpha}(1).$$

Hence, we can take $Y_{\frac{1}{2}} = \{S_\alpha^{M_\alpha}(1)\}$. Since this set contains one element only and the maps T_j have the same constant slope, condition (5) from definition 2.2 follows immediately. The first part of the theorem now follows since the deterministic maps S_α have matching for almost all parameters α . For the critical points $c \neq \frac{1}{2}$ the statement follows by symmetry.

For the second part we assume for $\alpha \in [1, \frac{3}{2})$ that S_α has matching and we proceed by contradiction. Therefore, assume that R_α satisfies the conditions of definitions 2.1 and 2.2 for $c = \frac{1}{2}$ for some minimal $1 \leq K < M = M_\alpha + 1$. Suppose that $S_\alpha^n(1) \in Y_{\frac{1}{2}}$ for some $n < K - 1$.

By lemma 3.4 any \mathbf{u} for which $T_{\mathbf{u}}\left(\frac{1}{2}\right) = S_\alpha^n(1)$ has length $|\mathbf{u}| = n + 1$. Together with (5) and the fact that the maps $T_{\alpha,0}$ and $T_{\alpha,1}$ both have constant slope 2, this implies that

$$\sum_{\mathbf{u} \in \Omega(S_\alpha^n(1))^-} p_{\mathbf{u}} = \sum_{\mathbf{u} \in \Omega(S_\alpha^n(1))^+} p_{\mathbf{u}}. \quad (15)$$

For any $\mathbf{u} \in \Omega^{n+1} \setminus \Omega(S_\alpha^n(1))^-$, $\mathbf{u}' \in \Omega^{n+1} \setminus \Omega(S_\alpha^n(1))^+$ we have by proposition 3.3 that $T_{\mathbf{u}}\left(\frac{1}{2}\right) = T_{\mathbf{u}'}\left(\frac{1}{2}\right) = S_\alpha^n(1) - \alpha$. Furthermore,

$$\begin{aligned}
1 &= \sum_{\mathbf{u} \in \Omega^{n+1}} p_{\mathbf{u}} = \sum_{\mathbf{u} \in \Omega(S_{\alpha}^n(1))^-} p_{\mathbf{u}} + \sum_{\mathbf{u} \in \Omega^{n+1} \setminus \Omega(S_{\alpha}^n(1))^-} p_{\mathbf{u}} \\
&= \sum_{\mathbf{u} \in \Omega(S_{\alpha}^n(1))^+} p_{\mathbf{u}} + \sum_{\mathbf{u} \in \Omega^{n+1} \setminus \Omega(S_{\alpha}^n(1))^+} p_{\mathbf{u}}.
\end{aligned}$$

From (15) and proposition 3.3 we see that

$$\begin{aligned}
\sum_{\mathbf{u} \in \Omega(S_{\alpha}^n(1-\alpha))^-} p_{\mathbf{u}} &= \sum_{\mathbf{u} \in \Omega^{n+1} \setminus \Omega(S_{\alpha}^n(1))^-} p_{\mathbf{u}} = \sum_{\mathbf{u} \in \Omega^{n+1} \setminus \Omega(S_{\alpha}^n(1))^+} p_{\mathbf{u}} \\
p_{\mathbf{u}} &= \sum_{\mathbf{u} \in \Omega(S_{\alpha}^n(1-\alpha))^+} p_{\mathbf{u}}.
\end{aligned}$$

This implies that the conditions of definitions 2.1 and 2.2 hold with $M_{\frac{1}{2}} = n+1$ and $Y_{\frac{1}{2}} = \{S_{\alpha}^n(1), S_{\alpha}^n(1-\alpha)\}$, contradicting the minimality of K . In a similar way we can exclude the possibility that $S_{\alpha}^n(1-\alpha) \in Y$ for $n < K-1$. Since there is an $\tilde{\omega} \in \Omega^{\mathbb{N}}$ such that for each $k < M-1$, $T_{\tilde{\omega}_1^k}(1-\alpha) = S_{\alpha}^k(1-\alpha) = S_{\alpha}^k(1) - \alpha$, it must hold that

$$Y_{\frac{1}{2}} = \{S_{\alpha}^{K-1}(1), S_{\alpha}^{K-1}(1) - \alpha\}.$$

To conclude the proof we show that for this set $Y_{\frac{1}{2}}$ condition (5) cannot hold. By the constant slope, condition (5) can be rephrased as

$$\begin{cases} \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-1}(1))^-} p_{\mathbf{u}} - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-1}(1))^+} p_{\mathbf{u}} = 0, \\ \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-1}(1-\alpha))^-} p_{\mathbf{u}} - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-1}(1-\alpha))^+} p_{\mathbf{u}} = 0. \end{cases} \quad (16)$$

and by lemma 3.4 any $\mathbf{u} \in \Omega(S_{\alpha}^{K-1}(1))^{\pm} \cup \Omega(S_{\alpha}^{K-1}(1-\alpha))^{\pm}$ has length K . Since $K < M_{\alpha} + 1$, so $K-2 < M_{\alpha} - 1$, lemma 3.2 tells us that there are only two possibilities:

- (a) $S_{\alpha}^{K-2}(1) \in I_4$ and $S_{\alpha}^{K-2}(1) - \alpha \in I_1$;
- (b) $S_{\alpha}^{K-2}(1) \in I_5$ and $S_{\alpha}^{K-2}(1) - \alpha \in I_2$.

If case (a) holds, then $T_0(S_{\alpha}^{K-2}(1)) = S_{\alpha}^{K-1}(1)$ and

$$T_1(S_{\alpha}^{K-2}(1)) = T_0(S_{\alpha}^{K-2}(1) - \alpha) = T_1(S_{\alpha}^{K-2}(1) - \alpha) = S_{\alpha}^{K-1}(1) - \alpha,$$

so that (16) becomes

$$\begin{cases} \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^-} p_{\mathbf{u}} p_0 - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^+} p_{\mathbf{u}} p_0 = 0, \\ \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^-} p_{\mathbf{u}} p_1 + \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1-\alpha))^-} p_{\mathbf{u}} - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^+} p_{\mathbf{u}} p_1 - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1-\alpha))^+} p_{\mathbf{u}} = 0. \end{cases}$$

The last system of equations implies

$$\begin{cases} \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^-} p_{\mathbf{u}} - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1))^+} p_{\mathbf{u}} = 0, \\ \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1-\alpha))^-} p_{\mathbf{u}} - \sum_{\mathbf{u} \in \Omega(S_{\alpha}^{K-2}(1-\alpha))^+} p_{\mathbf{u}} = 0, \end{cases}$$

which contradicts the minimality of K . For the second case, the same contradiction is obtained in a similar way. \square

Remark 3.6. From the previous result we see that matching occurs for the random systems R_α for the same parameters α and at the same time as for the deterministic systems S_α . [DK20] contains a complete description of the matching intervals of the maps S_α . The interval $[1, 2]$ can be divided into intervals of parameters for which matching of the maps S_α occurs after the same number of steps. By the above, these matching intervals also apply to the systems R_α .

3.3. An expression for the invariant density

The existence of an invariant measure of the form $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ with $\mu_{\mathbf{p}} \ll \lambda$ for the random symmetric doubling maps R_α is guaranteed by the results of [Pel84, Mor85]. Furthermore, since T_0 is expanding and has a unique absolutely continuous invariant measure, it follows from [Pel84, corollary 7] that also for R_α there is a unique measure $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ and that R_α is ergodic with respect to this measure. To show that $R_\alpha \in \mathcal{R}_A$, we check conditions (c1)–(c3). (c1) is immediate and (c3) follows from the constant slope 2 of the maps $T_{\alpha,0}$ and $T_{\alpha,1}$. We check condition (7). Note that for any $\alpha \neq 2$,

$$\frac{\sum_{j \in \Omega} \frac{p_j}{k_{3,j}} d_{3,j}}{1 - \sum_{j \in \Omega} \frac{p_j}{k_{3,j}}} = \frac{\sum_{j \in \Omega} \frac{p_j}{2} 0}{1 - \sum_{j \in \Omega} \frac{p_j}{2}} = 0$$

and

$$\frac{\sum_{j \in \Omega} \frac{p_j}{k_{1,j}} d_{1,j}}{1 - \sum_{j \in \Omega} \frac{p_j}{k_{1,j}}} = \frac{\sum_{j \in \Omega} \frac{p_j}{2} \alpha}{1 - \sum_{j \in \Omega} \frac{p_j}{2}} = 2\alpha \neq 0.$$

Then [KM20, theorem 5.3] implies that an explicit formula for the density of this measure can be found via the algebraic procedure in [KM20] and from theorems 2.5 and 3.5 we know that for almost all parameters α this density is piecewise constant. We will execute the procedure from [KM20] and start by introducing the same notation as in [KM20]. Since Ω consists of two elements only, from now on we will just use p as an index instead of \mathbf{p} whenever appropriate.

Denote by $a_{i,j}$ and $b_{i,j}$ the left and right limits at each critical point $c_i \in C$, i.e., for $1 \leq i \leq 4$ and $j \in \Omega$:

$$a_{i,j} = T_j(c_i^-) = \lim_{x \uparrow c_i} T_j(x), \quad \text{and} \quad b_{i,j} = T_j(c_i^+) = \lim_{x \downarrow c_i} T_j(x).$$

The images of the critical points are then given by

$$\begin{aligned} a_{1,0} &= a_{1,1} = b_{1,0} = \alpha - 1, & b_{1,1} &= -1, \\ a_{2,0} &= 1, & a_{2,1} &= b_{2,0} = b_{2,1} = 1 - \alpha, \\ a_{3,0} &= a_{3,1} = b_{3,0} = \alpha - 1, & b_{3,1} &= -1, \\ a_{4,0} &= 1, & a_{4,1} &= b_{4,0} = b_{4,1} = 1 - \alpha. \end{aligned}$$

For $y \in [-1, 1]$ and $1 \leq n \leq 4$ set

$$\text{KI}_n(y) = \sum_{k \geq 1} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} 1_{I_n}(T_{\mathbf{u}_1^{k-1}}(y)). \quad (17)$$

The quantity $\text{KI}_n(y)$ weighs the number of times the random orbits of y enters the interval I_n . The weight depends on the length and probability of each path $\omega \in \Omega^{\mathbb{N}}$ leading the point y to I_n . The *fundamental matrix* $A = (A_{n,i})$ of R is the 5×4 matrix with entries

$$A_{n,i} = \begin{cases} \sum_{j \in \Omega} p_j (1 + \text{KI}_n(a_{i,j}) - \text{KI}_n(b_{i,j})), & \text{for } n = i, \\ \sum_{j \in \Omega} p_j (\text{KI}_n(a_{i,j}) - \text{KI}_n(b_{i,j}) - 1), & \text{for } n = i + 1, \\ \sum_{j \in \Omega} p_j (\text{KI}_n(a_{i,j}) - \text{KI}_n(b_{i,j})), & \text{else.} \end{cases}$$

Since for R there is a unique invariant probability measure $m_p \times \mu_p$ with $\mu_p \ll \lambda$, [KM20, theorem 5.3] implies that the null space of the matrix A is one-dimensional. According to [KM20, theorem 4.1] there is a unique vector $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4) \in \mathbb{R}^4 \setminus \{\mathbf{0}\}$ with $A\gamma = \mathbf{0}$ and such that the probability density f_p of μ_p has the form (8). Using the values of $a_{i,j}$ and $b_{i,j}$ computed above, we can reduce this to

$$\begin{aligned} f_p = (\gamma_1 + \gamma_3) \sum_{k \geq 0} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{1\mathbf{u}}}{2^{k+1}} (1_{[-1, T_{\mathbf{u}}(\alpha-1))} - 1_{[-1, T_{\mathbf{u}}(-1))}) \\ + (\gamma_2 + \gamma_4) \sum_{k \geq 0} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{0\mathbf{u}}}{2^{k+1}} (1_{[-1, T_{\mathbf{u}}(1))} - 1_{[-1, T_{\mathbf{u}}(1-\alpha))}). \end{aligned} \quad (18)$$

By symmetry to determine f_p it is enough to know the random orbits of 1 and $1 - \alpha$ only. From (18) we see that the density is piecewise constant when the orbits of 1 and $1 - \alpha$ are finite or when they merge with the same weight. In the former case the map admits a Markov partition, the latter case happens if R exhibits strong random matching. We focus on the second situation, since we know from theorem 3.5 that this holds for almost all parameters.

Fix an $\alpha \in [1, 2]$ such that R presents strong random matching. Let M be as in theorem 3.5. Then for each i, j, n ,

$$\text{KI}_n(a_{i,j}) - \text{KI}_n(b_{i,j}) = \sum_{k=1}^{M-1} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} (1_{I_n}(T_{\mathbf{u}_1^{k-1}}(a_{i,j})) - 1_{I_n}(T_{\mathbf{u}_1^{k-1}}(b_{i,j}))).$$

From lemma 3.2 and the symmetry of the map we get

$$\text{KI}_3(1) - \text{KI}_3(1 - \alpha) = 0 = \text{KI}_3(-1) - \text{KI}_3(\alpha - 1),$$

implying that $A_{3,1} = A_{3,4} = 0$, $A_{3,2} = -1$ and $A_{3,3} = 1$. Hence, any solution vector $\hat{\gamma}$ for $A\hat{\gamma} = \mathbf{0}$ has the form $\hat{\gamma} = (\hat{\gamma}_1, \hat{\gamma}_2, \hat{\gamma}_2, \hat{\gamma}_3)$ and (18) becomes

$$\begin{aligned} f_p = (\gamma_1 + \gamma_2) \frac{p_1}{2} \sum_{k=0}^{M-2} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} (1_{[-1, T_{\mathbf{u}}(\alpha-1))} - 1_{[-1, T_{\mathbf{u}}(-1))}) \\ + (\gamma_2 + \gamma_3) \frac{p_0}{2} \sum_{k=0}^{M-2} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} (1_{[-1, T_{\mathbf{u}}(1))} - 1_{[-1, T_{\mathbf{u}}(1-\alpha))}), \end{aligned} \quad (19)$$

where $\gamma = (\gamma_1, \gamma_2, \gamma_2, \gamma_3)$ is the unique non-trivial vector in the null space of the fundamental matrix A that makes f_p into a probability density function. In the next section we will derive a number of properties of f_p with the goal of determining the frequency of the digit 0 in the signed binary expansions of $m_p \times \mu_p$ typical points.

3.4. The frequency of the digit 0 in random signed binary expansions

Recall from (11) that the random signed binary expansion of a point (ω, x) has a digit 0 in the n -th position precisely if

$$R^{n-1}(\omega, x) \in [1] \times I_2 \cup \Omega^{\mathbb{N}} \times I_3 \cup [0] \times I_4 =: D_0.$$

Since R is ergodic with respect to $m_p \times \mu_p$, it follows from Birkhoff's ergodic theorem that the frequency of the digit 0 in $m_p \times \mu_p$ -almost all (ω, x) equals

$$\pi_0(\alpha, p) := \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=0}^{n-1} 1_{D_0}(R^k(\omega, x)) = (1-p)\mu_p(I_2) + \mu_p(I_3) + p\mu_p(I_4). \quad (20)$$

To give an example, consider $\alpha = 1$, see figure 8(a). It is straightforward to check that the probability density $f_p = (1-p)1_{[-1,0]} + p1_{[0,1]}$ is invariant. This gives

$$\pi_0(1, p) = p\mu_p\left(\left[0, \frac{1}{2}\right]\right) + (1-p)\mu_p\left(\left[-\frac{1}{2}, 0\right]\right) = \frac{p^2 + (1-p)^2}{2} \leq \frac{1}{2} \quad (21)$$

with equality only for $p = 0$ or $p = 1$.

For any $\alpha \in [\frac{3}{2}, 2]$ it is also easy to see that $M_\alpha = 2$, and a quick computation leads to the following expression for the invariant probability density function

$$f_p = \frac{1-p}{\alpha} 1_{[-1, 1-\alpha]} + \frac{1}{\alpha} 1_{[1-\alpha, \alpha-1]} + \frac{p}{\alpha} 1_{(\alpha-1, 1]}.$$

With this information we can easily compute $\pi_0(\alpha, p)$ and obtain

$$\pi_0(\alpha, p) = \frac{\alpha-1}{\alpha} + \frac{2-\alpha}{2\alpha} = \frac{1}{2}. \quad (22)$$

That is, for $2 \geq \alpha \geq \frac{3}{2}$, and any $0 < p < 1$, the frequency of the digit 0 is equal to $\frac{1}{2}$ in the signed binary expansion of $m_p \times \mu_p$ -almost all (ω, x) . For the other values of α we need to do some more work.

So in the following, consider $\alpha \in (1, \frac{3}{2})$ only. For $k \geq 1$ set $E_k = \{\mathbf{u} \in \Omega^k : T_{\mathbf{u}}(1) = S_\alpha^k(1)\}$ and $F_k = \{\mathbf{u} \in \Omega^k : T_{\mathbf{u}}(1-\alpha) = S_\alpha^k(1)\}$. Also, use $(b_n)_{n \geq 1}$ to denote the digits in the signed binary expansion of 1 generated by S_α , i.e.,

$$b_n = \begin{cases} -1, & \text{if } S_\alpha^{n-1}(1) < -\frac{1}{2}, \\ 0, & \text{if } -\frac{1}{2} \leq S_\alpha^{n-1}(1) \leq \frac{1}{2}, \\ 1, & \text{if } S_\alpha^{n-1}(1) > \frac{1}{2}. \end{cases}$$

Write $\mathbf{b}_k = b_1 \cdots b_k$ for any $k \geq 1$.

Lemma 3.7. For all $1 \leq k < M-1$, $F_k \subseteq E_k$ and $E_k \setminus F_k = \{\mathbf{b}_k\}$.

Proof. First note that the n th signed binary digit of 1 generated by S_α , $n < M - 1$, equals 0 if $S_\alpha^{n-1}(1) \in I_4$ and 1 if $S_\alpha^{n-1}(1) \in I_5$. We prove the statement by induction. For $k = 1$ we have $E_1 = \{0, 1\}$ and $F_1 = \{0\}$. Assume the statement holds for some $1 \leq k < M - 2$. If $S_\alpha^k(1) = T_{\mathbf{b}_k}(1) \in I_4$, then $b_{k+1} = 0$ and we know from the assumptions, proposition 3.3 and since $S_\alpha^k(1) - \alpha \in I_1$ that

$$T_{\mathbf{b}_k 0}(1) = S_\alpha^{k+1}(1), \quad T_{\mathbf{b}_k 1}(1) = T_{\mathbf{b}_k 0}(1 - \alpha) = T_{\mathbf{b}_k 1}(1 - \alpha) = S_\alpha^{k+1}(1) - \alpha.$$

Hence, $\mathbf{b}_k 0 \in E_{k+1} \setminus F_{k+1}$ and $\mathbf{b}_k 1 \notin E_{k+1} \cup F_{k+1}$. If $S_\alpha^k(1) = T_{\mathbf{b}_k}(1) \in I_5$, then $b_{k+1} = 1$ and

$$T_{\mathbf{b}_k 0}(1) = T_{\mathbf{b}_k 1}(1) = T_{\mathbf{b}_k 0}(1 - \alpha) = S_\alpha^{k+1}(1), \quad T_{\mathbf{b}_k 1}(1 - \alpha) = S_\alpha^{k+1}(1) - \alpha.$$

So, $\mathbf{b}_k 1 \in E_{k+1} \setminus F_{k+1}$ and $\mathbf{b}_k 0 \in E_{k+1} \cap F_{k+1}$. For any other $\mathbf{u} \in \Omega^k$ it holds that $T_{\mathbf{u}}(1) = T_{\mathbf{u}}(1 - \alpha)$, so that either $\mathbf{u}j \in E_{k+1} \cap F_{k+1}$ or $\mathbf{u}j \notin E_{k+1} \cup F_{k+1}$, $j = 0, 1$. This gives the statement. \square

Lemma 3.8. The density f_p is constant and equal to $\frac{1}{\alpha}$ on the interval $[1 - \alpha, \alpha - 1]$.

Proof. For any $\mathbf{u} \in \Omega^k$, write $\bar{\mathbf{u}} = (1 - u_1) \cdots (1 - u_k)$ and for a subset $E \subseteq \Omega^k$ write $\bar{E} = \{\mathbf{u} \in \Omega^k : \bar{\mathbf{u}} \in E\}$. By lemma 3.7 we have for each $k < M$,

$$\delta_k := \sum_{\mathbf{u} \in E_k} \frac{p_{\mathbf{u}}}{2^k} - \sum_{\mathbf{u} \in F_k} \frac{p_{\mathbf{u}}}{2^k} = \frac{p_{\mathbf{b}_k}}{2^k}, \quad \bar{\delta}_k := \sum_{\mathbf{u} \in E_k^c} \frac{p_{\mathbf{u}}}{2^k} - \sum_{\mathbf{u} \in F_k^c} \frac{p_{\mathbf{u}}}{2^k} = \frac{p_{\bar{\mathbf{b}}_k}}{2^k},$$

Recall the formula for the density f_p from (19). Using proposition 3.3 we get

$$\begin{aligned} & \frac{p_0}{2} \sum_{k=0}^{M-2} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} (1_{[-1, T_{\mathbf{u}}(1))} - 1_{[-1, T_{\mathbf{u}}(1-\alpha))}) \\ &= \frac{p_0}{2} \sum_{k=0}^{M-2} \sum_{\substack{\mathbf{u} \in \Omega^k: \\ T_{\mathbf{u}}(1) = S_\alpha^k(1), \\ T_{\mathbf{u}}(1-\alpha) = S_\alpha^k(1) - \alpha}} \frac{p_{\mathbf{u}}}{2^k} 1_{[T_{\mathbf{u}}(1-\alpha), T_{\mathbf{u}}(1))} - \frac{p_0}{2} \sum_{k=0}^{M-2} \sum_{\substack{\mathbf{u} \in \Omega^k: \\ T_{\mathbf{u}}(1) = S_\alpha^k(1) - \alpha, \\ T_{\mathbf{u}}(1-\alpha) = S_\alpha^k(1)}} \frac{p_{\mathbf{u}}}{2^k} 1_{[T_{\mathbf{u}}(1), T_{\mathbf{u}}(1-\alpha))}) \\ &= \frac{p_0}{2} \sum_{k=0}^{M-2} \delta_k 1_{[S_\alpha^k(1) - \alpha, S_\alpha^k(1))}. \end{aligned}$$

For the other side it holds similarly using the symmetry of the system that

$$\frac{p_1}{2} \sum_{k=0}^{M-2} \sum_{\mathbf{u} \in \Omega^k} \frac{p_{\mathbf{u}}}{2^k} (1_{[-1, T_{\mathbf{u}}(\alpha-1))} - 1_{[-1, T_{\mathbf{u}}(-1))}) = \frac{p_1}{2} \sum_{k=0}^{M-2} \bar{\delta}_k 1_{[-S_\alpha^k(1), \alpha - S_\alpha^k(1))}.$$

By (13) we have for all $k < M - 1$,

$$S_\alpha^k(1), \alpha - S_\alpha^k(1) \in [\alpha - 1, 1] \quad \text{and} \quad S_\alpha^k(-1), S_\alpha^k(\alpha - 1) \in [-1, 1 - \alpha],$$

so that on $[1 - \alpha, \alpha - 1]$ we obtain

$$f_p|_{[1-\alpha, \alpha-1]}(x) = (\gamma_1 + \gamma_2) \frac{p_1}{2} \sum_{k=0}^{M-2} \bar{\delta}_k + (\gamma_2 + \gamma_3) \frac{p_0}{2} \sum_{k=0}^{M-2} \delta_k.$$

Since f_p is a probability density it follows that

$$1 = \int_{[-1,1]} f_p d\lambda = (\gamma_1 + \gamma_2) \frac{p_1}{2} \sum_{k=0}^{M-2} \bar{\delta}_k \alpha + (\gamma_2 + \gamma_3) \frac{p_0}{2} \sum_{k=0}^{M-2} \delta_k \alpha. \quad (23)$$

Hence,

$$f_p|_{[1-\alpha, \alpha-1]}(x) = \frac{1}{\alpha},$$

which gives the result. \square

Lemma 3.9. Let $\gamma = (\gamma_1, \gamma_2, \gamma_2, \gamma_3)$ be the unique vector in the null space of A that makes f_p into a probability density function. Then $\gamma_2 = \frac{1}{\alpha}$.

Proof. Since $S_\alpha^k(1) \in I_4 \cup I_5$ for all $k < M-1$ it follows from the definition of the function KI_n in (17) and proposition 3.3 that for $y = 1, 1 - \alpha$,

$$\text{KI}_4(y) + \text{KI}_5(y) = \sum_{k=0}^{M-2} \sum_{j \in \Omega} \sum_{\mathbf{u} \in \Omega^k} \frac{p_j}{2} \frac{p_{\mathbf{u}}}{2^k} 1_{I_4 \cup I_5}(T_{\mathbf{u}}(y)) = \frac{1}{2} \sum_{k=0}^{M-2} \sum_{\substack{\mathbf{u} \in \Omega^k; \\ T_{\mathbf{u}}(y) = S_\alpha^k(1)}} \frac{p_{\mathbf{u}}}{2^k},$$

so that

$$\frac{1}{2} \sum_{k=0}^{M-2} \delta_k = \text{KI}_4(1) - \text{KI}_4(1 - \alpha) + \text{KI}_5(1) - \text{KI}_5(1 - \alpha).$$

A similar statement holds for -1 and $\alpha - 1$. The fourth and fifth line of the linear system $A\gamma = \mathbf{0}$ read

$$p_1(\text{KI}_4(\alpha - 1) - \text{KI}_4(-1))(\gamma_1 + \gamma_2) + p_0(\text{KI}_4(1) - \text{KI}_4(1 - \alpha))(\gamma_2 + \gamma_3) - \gamma_2 + \gamma_3 = 0,$$

and

$$p_1(\text{KI}_5(\alpha - 1) - \text{KI}_5(-1))(\gamma_1 + \gamma_2) + p_0(\text{KI}_5(1) - \text{KI}_5(1 - \alpha))(\gamma_2 + \gamma_3) - \gamma_2 + \gamma_3 = 0,$$

respectively, where we have used that $\gamma = (\gamma_1, \gamma_2, \gamma_2, \gamma_3)$. Adding them up gives

$$\begin{aligned} \gamma_2 &= p_1(\gamma_1 + \gamma_2)(\text{KI}_4(\alpha - 1) - \text{KI}_4(-1) + \text{KI}_5(\alpha - 1) - \text{KI}_5(-1)) \\ &\quad + p_0(\gamma_2 + \gamma_3)(\text{KI}_4(1) - \text{KI}_4(1 - \alpha) + \text{KI}_5(1) - \text{KI}_5(1 - \alpha)) \\ &= \frac{p_1}{2}(\gamma_1 + \gamma_2) \sum_{k=0}^{M-2} \bar{\delta}_k + \frac{p_0}{2}(\gamma_2 + \gamma_3) \sum_{k=0}^{M-2} \delta_k. \end{aligned}$$

The result then follows from (23). \square

Combining lemmas 3.8 and 3.9 gives the following expression for the density f_p :

$$f_p = \left(\gamma_1 + \frac{1}{\alpha} \right) \frac{p_1}{2} \sum_{k=0}^{M-2} \frac{p_{\bar{\mathbf{b}}_k}}{2^k} 1_{[-S_\alpha^k(1), \alpha - S_\alpha^k(1)]} + \left(\frac{1}{\alpha} + \gamma_3 \right) \frac{p_0}{2} \sum_{k=0}^{M-2} \frac{p_{\mathbf{b}_k}}{2^k} 1_{[S_\alpha^k(1) - \alpha, S_\alpha^k(1)]}, \quad (24)$$

where $\mathbf{b}_k = b_1 \cdots b_k$ denote the first k digits in the signed binary expansion of 1 given by S_α .

Lemma 3.10. *Let $\alpha \in (1, \frac{3}{2})$ be a parameter for which the random system R has strong random matching. Then both $\gamma_1, \gamma_3 \geq 0$. As a consequence, $f_p > 0$ and μ_p is equivalent to λ .*

Proof. Let $\gamma = (\gamma_1, \gamma_2, \gamma_2, \gamma_3)$ be the unique vector in the null space of A that makes f_p into a probability density. Set

$$y = \max_{k \in \{1, 2, \dots, M-2\}} \{S_\alpha^k(1), \alpha - S_\alpha^k(1)\}.$$

By lemma 3.4 we can assume that $y \neq 1$. Furthermore, $T_0(1 - \alpha) = 2 - \alpha$ and $T_1(1 - \alpha) = 2 - 2\alpha$, so in particular $y \geq \max\{2 - \alpha, 2\alpha - 2\} > \alpha - 1$. Then

$$\mu_p([y, 1]) = m_p \times \mu_p(R^{-1}(\Omega \times [y, 1])) = p\mu_p\left(\left[\frac{y - \alpha}{2}, \frac{1 - \alpha}{2}\right] \cup \left[\frac{y}{2}, \frac{1}{2}\right]\right).$$

By the definition of y one can see from (24) that

$$\mu_p([y, 1]) = \frac{p(\gamma_2 + \gamma_3)}{2}(1 - y).$$

It follows that $1 - \alpha \leq \frac{y - \alpha}{2} < \frac{1 - \alpha}{2}$. Thus by lemmas 3.8 and 3.9, $f_p|_{[\frac{y - \alpha}{2}, \frac{1 - \alpha}{2}]} = \gamma_2$. We proceed by showing that none of the points $S_\alpha^k(1)$ or $\alpha - S_\alpha^k(1)$, $1 \leq k \leq M - 2$, lie in the interval $[\frac{y}{2}, \frac{1}{2}]$, which then by (24) implies that the density f_p is also constant on the interval $[\frac{y}{2}, \frac{1}{2}]$. For $k = M - 2 = M_\alpha - 1$, matching for S_α implies that $\frac{1}{2} < S_\alpha^{M-2}(1) < \alpha - \frac{1}{2}$ and $\alpha - S_\alpha^{M-2}(1) > \frac{1}{2}$. Suppose there exists a $k \in \{1, 2, \dots, M - 3\}$ such that $\frac{y}{2} < S_\alpha^k(1) < \frac{1}{2}$ (or $\frac{y}{2} < \alpha - S_\alpha^k(1) < \frac{1}{2}$). Then $S_\alpha^{k+1}(1) > y$ (or $\alpha - S_\alpha^{k+1}(1) > y$), which gives a contradiction with the definition of y . The same holds for $\alpha - S_\alpha^k(1)$. Hence, there is a constant $c \geq 0$ such that

$$\frac{p(\gamma_2 + \gamma_3)}{2}(1 - y) = \mu_p([y, 1]) = p\left(\gamma_2 \frac{(1 - y)}{2} + c \frac{(1 - y)}{2}\right).$$

So, $0 \leq \mu_p([\frac{y}{2}, \frac{1}{2}]) = c = \gamma_3$. The proof that $\gamma_1 \geq 0$ goes similarly. The fact that f_p is strictly positive and the equivalence of μ_p and λ now follow from (24). \square

The following result can be proven in essentially the same way as [DK20, theorem 4.1]. We include a proof here for convenience.

Lemma 3.11 (cf theorem 4.1 of [DK20]). *Fix $0 < p < 1$. The map $\alpha \mapsto \pi_0(\alpha, p)$ is continuous on $(1, \frac{3}{2})$.*

Proof. In this proof we use $f_\alpha = f_{\alpha, p}$ to denote the unique density from (24). By (20), for the continuity of $\alpha \mapsto \pi_0(\alpha, p)$ it is sufficient to prove L^1 -convergence of the densities f_α ; i.e., for any sequence $\{\alpha_k\}_{k \geq 1} \subseteq (1, \frac{3}{2})$ converging to a fixed $\hat{\alpha} \in (1, \frac{3}{2})$, there is convergence $f_{\alpha_k} \rightarrow f_{\hat{\alpha}}$ in $L^1(\lambda)$. The proof of this fact goes along the following lines:

- First we show that there is a uniform bound, i.e., independent of k , on the total variation and supremum norm of the densities f_{α_k} . It then follows from Helly's selection theorem that there is some subsequence of (f_{α_k}) for which an a.e. and L^1 limit \hat{f} exist.
- We show that $\hat{f} = f_{\hat{\alpha}}$, which by the same proof implies that any subsequence of (f_{α_k}) has a further subsequence converging a.e. to the same limit $f_{\hat{\alpha}}$. Hence, (f_{α_k}) converges to $f_{\hat{\alpha}}$ in measure.

(c) By the uniform integrability of (f_{α_k}) it then follows from Vitali's convergence theorem that the convergence of (f_{α_k}) to $f_{\hat{\alpha}}$ is in L^1 .

Steps (a) and (b) use Perron–Frobenius operators. For $j = 0, 1$ the Perron–Frobenius operator $P_{\alpha,j}$ of $T_{\alpha,j}$ is uniquely defined by the equation

$$\int (P_{\alpha,j}f)g d\lambda = \int f(g \circ T_{\alpha,j}) d\lambda \quad \forall f \in L^1(\lambda), g \in L^\infty(\lambda)$$

and the Perron–Frobenius operator P_α of R_α is then defined by $P_\alpha f = pP_{\alpha,0}f + (1-p)P_{\alpha,1}f$. Equivalently, P_α is uniquely defined by the equation

$$\int (P_\alpha f)g d\lambda = p \int f(g \circ T_{\alpha,0}) d\lambda + (1-p) \int f(g \circ T_{\alpha,1}) d\lambda \quad \forall f \in L^1(\lambda), g \in L^\infty(\lambda). \quad (25)$$

Since each R_α has a unique probability density f_α it follows from [Pel84, theorem 1] that f_α is the L^1 limit of $(\frac{1}{n} \sum_{j=0}^{n-1} P_\alpha^j 1)_{n \geq 1}$ and it is the unique probability density that satisfies $P_\alpha f_\alpha = f_\alpha$. From [Ino12, theorem 5.2] each f_α is a function of bounded variation. We proceed by finding uniform bounds on the total variation and supremum norm of these densities.

Fix $\hat{\alpha} \in (1, \frac{3}{2})$. For the second iterates of the Perron–Frobenius operators we have

$$P_\alpha^2 f = \sum_{i,j=0}^1 p_i p_j P_{\alpha,j}(P_{\alpha,i}f).$$

Since the intervals of monotonicity of any of the maps $T_{\alpha,\mathbf{u}}$ for $\mathbf{u} \in \Omega^2$, only become arbitrarily small for α approaching 1 and $\frac{3}{2}$, we can find a uniform lower bound δ on the length of the intervals of monotonicity of any map $T_{\alpha,\mathbf{u}}$, $\mathbf{u} \in \Omega^2$, for all values α that are close enough to $\hat{\alpha}$. Applying [BG97, lemma 5.2.1] to $T_{\alpha,j}$, $j = 0, 1$, and any of the second iterates $T_{\alpha,\mathbf{u}}$, $\mathbf{u} \in \Omega^2$, gives that

$$\text{Var}(P_{\alpha,j}f) \leq \text{Var}(f) + \frac{1}{\delta} \|f\|_1 \quad \text{and} \quad \text{Var}(P_{\alpha,\mathbf{u}}f) \leq \frac{1}{2} \text{Var}(f) + \frac{1}{2\delta} \|f\|_1,$$

where Var denotes the total variation over the interval $[-1, 1]$. Since these bounds do not depend on α, j, \mathbf{u} , the same estimates hold for P_α , so that for any function $f : [-1, 1] \rightarrow \mathbb{R}$ of bounded variation and any $n \geq 1$,

$$\text{Var}(P_\alpha^n f) \leq \frac{1}{2^{[n/2]}} \text{Var}(f) + \left(2 + \frac{1}{\delta}\right) \|f\|_1. \quad (26)$$

Let $\{\alpha_k\}_{k \geq 1}$ with $\alpha_k \rightarrow \hat{\alpha}$ be a sequence for which the lower bound δ holds for each k . For each k and n , write $f_{k,n} = \frac{1}{n} \sum_{i=0}^{n-1} P_{\alpha_k}^i 1$. Since

$$\sup |f_{k,n}| \leq \text{Var}(f_{k,n}) + \int f_{k,n} d\lambda,$$

it follows from (26) that there is a uniform constant $C > 0$ (independent of k, n) such that $\text{Var}(f_{k,n}), \sup |f_{k,n}| < C$. The same then holds for the limits f_{α_k} . Helly's selection theorem then gives the existence of a subsequence $\{k_i\}$ and a function \hat{f} of bounded variation, such that $f_{\alpha_{k_i}} \rightarrow \hat{f}$ in $L^1(\lambda)$ and λ -a.e. and with $\text{Var}(\hat{f}), \sup |\hat{f}| < C$. This finishes (a).

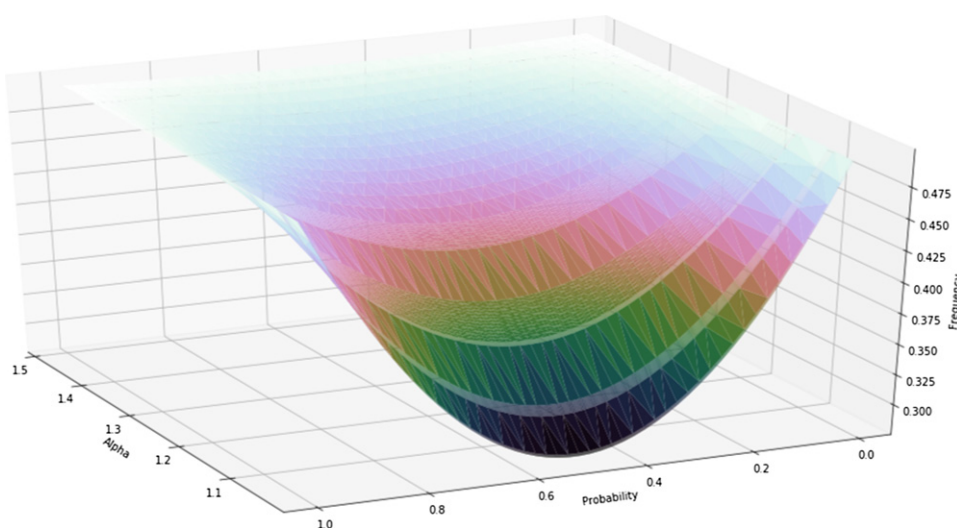


Figure 9. The graph of $(\alpha, p) \mapsto \pi_0(\alpha, p)$.

By (b) and (c) above, what remains to finish the proof is to show that $P_{\hat{\alpha}}\hat{f} = \hat{f}$. By (25) it is enough to show that for any compactly supported C^1 function $g : [-1, 1] \rightarrow \mathbb{R}$ it holds that

$$\left| \int (P_{\hat{\alpha}}\hat{f})g d\lambda - \int \hat{f}g d\lambda \right| = 0.$$

Note that

$$\begin{aligned} \left| \int (P_{\hat{\alpha}}\hat{f})g d\lambda - \int \hat{f}g d\lambda \right| &\leq p \left| \int \hat{f}(g \circ T_{\hat{\alpha},0})d\lambda - \int \hat{f}g d\lambda \right| \\ &\quad + (1-p) \left| \int \hat{f}(g \circ T_{\hat{\alpha},1})d\lambda - \int \hat{f}g d\lambda \right|. \end{aligned}$$

For $j = 0, 1$ we can write

$$\begin{aligned} \left| \int \hat{f}(g \circ T_{\hat{\alpha},j})d\lambda - \int \hat{f}g d\lambda \right| &\leq \left| \int \hat{f}(g \circ T_{\hat{\alpha},j})d\lambda - \int f_{\alpha_{k_j}}(g \circ T_{\hat{\alpha},j})d\lambda \right| \\ &\quad + \left| \int f_{\alpha_{k_j}}(g \circ T_{\hat{\alpha},j})d\lambda - \int f_{\alpha_{k_j}}(g \circ T_{\alpha_{k_j},j})d\lambda \right| \\ &\quad + \left| \int f_{\alpha_{k_j}}(g \circ T_{\alpha_{k_j},j})d\lambda - \int \hat{f}g d\lambda \right|. \end{aligned}$$

The first and third integral on the right-hand side can be bounded by $\|g\|_{\infty}\|\hat{f} - f_{\alpha_{k_j}}\|_1 \rightarrow 0$. For the second integral, $\|f_{\alpha_{k_j}}\|_{\infty} < C$ and $\int |g \circ T_{\hat{\alpha},j} - g \circ T_{\alpha_{k_j},j}|d\lambda \rightarrow 0$ by the dominated convergence theorem. Hence, $\hat{f} = f_{\hat{\alpha}}$ and $f_{\alpha_k} \rightarrow f_{\hat{\alpha}}$ in L^1 . \square

Figure 9 shows a numerical approximation of the graph of the function $(\alpha, p) \mapsto \pi_0(\alpha, p)$. We can now prove that the maximal value of the frequency of the digit 0 is in fact $\frac{1}{2}$.

Theorem 3.12. For any $0 < p < 1$ and any $\alpha \in [1, 2]$ the frequency $\pi_0(\alpha, p)$ is at most $\frac{1}{2}$ for $m_p \times \lambda$ -a.e. $(\omega, x) \in \Omega^{\mathbb{N}} \times [-1, 1]$.

Proof. For $\alpha \in [\frac{3}{2}, 2]$ the statement follows from (22) and for $\alpha = 1$ from (21). Let $\alpha \in (1, \frac{3}{2})$. The deterministic map $T_{\alpha,0}$ has density $f_0 = \frac{1}{\alpha} 1_{[1-\alpha, 1]}$ and $T_{\alpha,1}$ has $f_1 = \frac{1}{\alpha} 1_{[-1, \alpha-1]}$. Hence $\pi_0(\alpha, p) = \frac{1}{2}$ for $p = 0, 1$. Let $0 < p < 1$ and let α be a parameter satisfying the conditions of lemma 3.10. We know that f_p is constant and equal to $\frac{1}{\alpha}$ on $[1-\alpha, \alpha-1]$. For $x > \alpha-1$ the density can be written as

$$\begin{aligned} f_p(x) &= \frac{1}{\alpha} - \left(\frac{(1-p)(\gamma_1 + \gamma_2)}{2} \sum_{k=0}^{M-2} \frac{p\mathbf{b}_k}{2^k} 1_{[\alpha-1, x]}(\alpha - S_\alpha^k(1)) \right. \\ &\quad \left. + \frac{p(\gamma_2 + \gamma_3)}{2} \sum_{k=0}^{M-2} \frac{p\mathbf{b}_k}{2^k} 1_{[\alpha-1, x]}(S_\alpha^k(1)) \right) \\ &= \frac{1}{\alpha} - \frac{(1-p)(\gamma_1 + \gamma_2)}{2} - \left(\frac{(1-p)(\gamma_1 + \gamma_2)}{2} \sum_{k=1}^{M-2} \frac{p\mathbf{b}_k}{2^k} 1_{[\alpha-1, x]}(\alpha - S_\alpha^k(1)) \right. \\ &\quad \left. + \frac{p(\gamma_2 + \gamma_3)}{2} \sum_{k=1}^{M-2} \frac{p\mathbf{b}_k}{2^k} 1_{[\alpha-1, x]}(S_\alpha^k(1)) \right) \\ &\leq \frac{1}{\alpha} - \frac{(1-p)(\gamma_1 + \gamma_2)}{2}. \end{aligned}$$

Similarly, for $x < 1-\alpha$ we get $f_p(x) \leq \frac{1}{\alpha} - \frac{p(\gamma_2 + \gamma_3)}{2}$. By (20) and lemma 3.10,

$$\begin{aligned} \pi_0(\alpha, p) &= \frac{\alpha-1}{\alpha} + \frac{\alpha-1}{2\alpha} + p\mu_{\alpha,p} \left(\left[\alpha-1, \frac{1}{2} \right] \right) + (1-p)\mu_{\alpha,p} \left(\left[-\frac{1}{2}, 1-\alpha \right] \right) \\ &\leq \frac{3(\alpha-1)}{2\alpha} + \frac{3-2\alpha}{2\alpha} \left(1 - \frac{p(1-p)\alpha}{2} \min\{\gamma_1 + \gamma_2, \gamma_2 + \gamma_3\} \right) \\ &= \frac{1}{2} - \frac{3-2\alpha}{2} \frac{p(1-p)}{2} \min\{\gamma_1 + \gamma_2, \gamma_2 + \gamma_3\} \\ &< \frac{1}{2}. \end{aligned}$$

Since matching holds for almost all parameters α , the statement now follows from lemma 3.11 and the equivalence of μ_p and λ . \square

4. Final remarks

4.1. Remarks on the symmetric doubling maps

The numerical approximation of the graph of $(\alpha, p) \mapsto \pi_0(\alpha, p)$ shown in figure 9 seems to suggest some other features of the map that we have not proved. Firstly, it suggests some symmetry. In fact it can be shown that for each fixed α and any $x \in [0, 1]$, it holds that $f_p(x) = f_{1-p}(-x)$. For this one needs to consider the fundamental matrix \tilde{A} corresponding to the random system \tilde{R}_α obtained by switching the roles of p and $1-p$. Then using the permutation (12)(45), one can relate various of the quantities involved for \tilde{A} to the fundamental matrix A of R_α .

Secondly, for any matching parameter α and any $0 < p < 1$ the density $f_{\alpha,p}$ is a finite combination of indicator functions, whose supports depend on the position of the points in the set $\{S_\alpha^k(1), \alpha - S_\alpha^k(1)\}_{k=0}^{M-2}$ and whose coefficients are polynomials in p . So, for such a fixed α and any $x \in [-1, 1]$, the map $p \mapsto f_{\alpha,p}(x)$ is continuous in p .

Thirdly, the graph also suggests that the map presents a minimum at $p = \frac{1}{2}$. Using the above two facts we were only able to show the following:

Proposition 4.1. *Let $\alpha \in [1, 2]$ be such that R has strong random matching. Then the map $p \mapsto \pi_0(\alpha, p)$ has an extremal value at $p = \frac{1}{2}$.*

Proof. By combining (20) and the fact that $f_p(x) = f_{1-p}(-x)$ we obtain

$$\pi_0(\alpha, p) = (1-p)\mu_{1-p}(I_4) + \mu_p(I_3) + p\mu_p(I_4).$$

Computing the derivative with respect to p then gives

$$\partial_p \pi_0(\alpha, p) = -\mu_{1-p}(I_4) - (1-p)\partial_p(\mu_{1-p}(I_4)) + \partial_p(\mu_p(I_3)) + \mu_p(I_4) + \partial_p(\mu_p(I_4)). \quad (27)$$

From lemma 3.8 it follows that $\partial_p(\mu_p(I_3)) = -\partial_p(\mu_{1-p}(I_3))$, implying that $\partial_p(\mu_p(I_3)) = 0$ at $p = \frac{1}{2}$. Therefore, by (27) $\partial_p \pi_0(\alpha, p) = 0$ at $p = \frac{1}{2}$. \square

4.2. Remarks on random continued fractions

Theorem 2.5 states that for random piecewise affine maps of the interval satisfying (c1)–(c3) strong random matching implies that there exists a piecewise constant invariant density. Condition (5) was sufficient for the theorem to work, which was one of the main motivations for definition 2.2.

Theorem 2.5 is a random analogue of [BCMP19, theorem 1.2], except that there the statement has less assumptions. The authors mention in [BCMP19, remark 1.3] that for piecewise smooth interval maps with strong matching the corresponding invariant probability densities are piecewise smooth. On the other hand, as we noted before, the natural extension construction which for continued fraction transformations is often used to find invariant densities, seems to suggest that matching alone is sufficient to guarantee the existence of a piecewise smooth density. It would be interesting to investigate this further for the random continued fraction transformation.

In a first attempt to investigate to what extent theorem 2.5 can be generalised to piecewise smooth random systems on an interval, we include some numerical simulations. Recall from example 2.3 that the random continued fraction maps R_α have strong random matching for α in the intervals J_n with endpoints as in (6), see also figure 3. Figure 10 shows two simulations of the invariant densities for such systems R_α . The densities seem to be piecewise smooth with discontinuities precisely at the orbit points of α and $\alpha - 1$ before matching. This seems to support the claim that strong random matching is sufficient to guarantee the existence of a piecewise smooth invariant density.

In example 2.3 we also considered the maps R_α for $\alpha \in \left(\frac{\sqrt{10}-2}{2}, 2 - \sqrt{2}\right)$. We showed that R_α has random matching with $M = 3$, but no strong matching at that moment. With a similar approach it can be shown that R_α has random matching for various other intervals in $\left[\frac{1}{2}, \frac{\sqrt{5}-1}{2}\right]$. For $\alpha \in \left[\frac{1}{2}, 2 - \sqrt{2}\right]$ both deterministic maps $T_{\alpha,0}$ and $T_{\alpha,1}$ have strong matching with

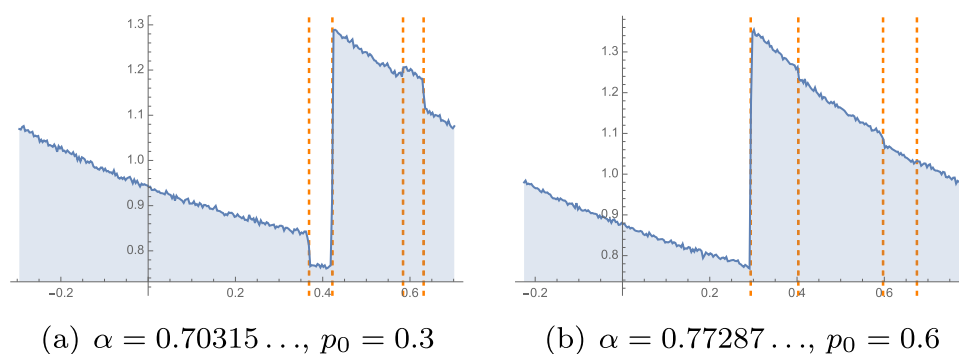


Figure 10. Numerical simulations of the invariant probability densities of the random continued fraction maps R_α from example 2.3. In (a) we take $\alpha \in J_4$ and $p_0 = 0.3$ and in (b) we have $\alpha \in J_5$ and $p_0 = 0.6$. The dashed lines indicate the positions of the *pre-matching points*, i.e., the points in the orbits of α and $\alpha - 1$ before the moment of matching.

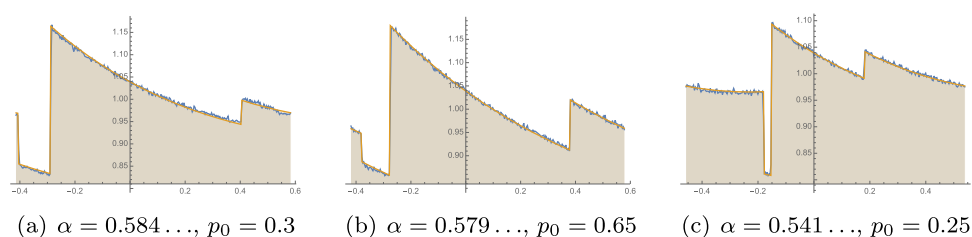


Figure 11. Numerical simulations of the invariant probability densities of the random continued fraction maps R_α from example 2.3 for three values of α between $\frac{1}{2}$ and $2 - \sqrt{2}$. The map in (a) has $\alpha \in \left(\frac{\sqrt{10}-2}{2}, 2 - \sqrt{2}\right)$, which is the matching interval considered in example 2.3. The orange graph is the graph of the weighted average of the densities of $T_{\alpha,0}$ and $T_{\alpha,1}$ with the appropriate values of p .

$M, Q \leq 2$, as was shown in [Nak81] and [TI81], and moreover, for both of them the invariant densities are known. In figure 11 we have plotted the weighted average of these densities together with numerical simulations of the densities for various values of $\alpha \in \left[\frac{1}{2}, 2 - \sqrt{2}\right]$ and $0 < p < 1$. This makes us wonder whether we need strong random matching to guarantee the existence of a piecewise smooth invariant density for these random systems or whether random matching is sufficient.

Acknowledgments

The third author is supported by the NWO TOP-Grant No. 614.001.509.

ORCID iDs

Karma Dajani  <https://orcid.org/0000-0001-8013-1729>
 Charlene Kalle  <https://orcid.org/0000-0002-3178-996X>
 Marta Maggioni  <https://orcid.org/0000-0002-9331-5217>

References

- [BG05] Bahsoun W and Góra P 2005 Position dependent random maps in one and higher dimensions *Stud. Math.* **166** 271–86
- [BCIT13] Bonanno C, Carminati C, Isola S and Tiozzo G 2013 Dynamics of continued fractions and kneading sequences of unimodal maps *Discrete Contin. Dyn. Syst.* **33** 1313–32
- [Boo51] Booth A D 1951 A signed binary multiplication technique *Q. J. Mech. Appl. Math.* **4** 236–40
- [BSORG13] Botella-Soler V, Oteo J A, Ros J and Glendinning P 2013 Lyapunov exponent and topological entropy plateaus in piecewise linear maps *J. Phys. A: Math. Theor.* **46** 125101
- [BG97] Boyarsky A and Góra P 1997 *Laws of chaos (Probability and its Applications)* Invariant Measures and Dynamical Systems in One Dimension (Boston, MA: Birkhäuser)
- [BCK17] Bruin H, Carminati C and Kalle C 2017 Matching for generalised β -transformations *Indagat. Math.* **28** 55–73
- [BCMP19] Bruin H, Carminati C, Marmi S and Profeti A 2019 Matching in a family of piecewise affine maps *Nonlinearity* **32** 172–208
- [Buz00] Buzzi J 2000 Absolutely continuous S.R.B. measures for random Lasota–Yorke maps *Trans. Am. Math. Soc.* **352** 3289–303
- [CIT18] Carminati C, Isola S and Tiozzo G 2018 Continued fractions with $SL(2, \mathbb{Z})$ -branches: combinatorics and entropy *Trans. Am. Math. Soc.* **370** 4927–73
- [CMO98] Cohen H, Miyaji A and Ono T 1998 *Advances in Cryptology — ASIACRYPT'98* Efficient elliptic curve exponentiation using mixed coordinates (Berlin: Springer) pp 51–65
- [CM18] Cosper D and Misiurewicz M 2018 Entropy locking *Fund. Math.* **241** 83–96
- [DdV05] Dajani K and de Vries M 2005 Measures of maximal entropy for random β -expansions *J. Eur. Math. Soc.* **7** 51–68
- [DdV07] Dajani K and de Vries M 2007 Invariant densities for random β -expansions *J. Eur. Math. Soc.* **9** 157–76
- [DK07] Dajani K and Kalle C 2007 Random β -expansions with deleted digits *Discrete Contin. Dyn. Syst.* **18** 199–217
- [DK20] Dajani K and Kalle C 2020 Invariant measures, matching and the frequency of 0 for signed binary expansions *Publ. Res. Inst. Math. Sci.* **56** 701–42
- [DK03] Dajani K and Kraaikamp C 2003 Random β -expansions *Ergod. Theory Dyn. Syst.* **23** 461–79
- [DKL06] Dajani K, Kraaikamp C and Liardet P 2006 Ergodic properties of signed binary expansions *Discrete Contin. Dyn. Syst.* **15** 87–119
- [DKS09] Dajani K, Kraaikamp C and Steiner W 2009 Metrical theory for α -Rosen fractions *J. Eur. Math. Soc.* **11** 1259–83
- [DO18] Dajani K and Oomen M 2018 Random N -continued fraction expansions *J. Approx. Theor.* **227** 1–26
- [GB03] Góra P and Boyarsky A 2003 Absolutely continuous invariant measures for random maps with position dependent probabilities *J. Math. Anal. Appl.* **278** 225–42
- [GH06] Grabner P J and Heuberger C 2006 On the number of optimal base 2 representations of integers *Des. Codes Cryptogr.* **40** 25–39
- [HP06] Heuberger C and Prodinger H 2006 Analysis of alternative digit sets for nonadjacent representations *Monatsh. Math.* **147** 219–48
- [Ino12] Inoue T 2012 Invariant measures for position dependent random maps with continuous random parameters *Stud. Math.* **208** 11–29
- [Ino20] Inoue T 2020 First return maps of random maps and invariant measures *Nonlinearity* **33** 249–75
- [KKV17] Kalle C, Kempton T and Verbitskiy E 2017 The random continued fraction transformation *Nonlinearity* **30** 1182–203
- [KLMM20] Kalle C, Langeveld N, Maggioni M and Munday S 2020 Matching for a family of infinite measure continued fraction transformations *Discrete Contin. Dyn. Syst.* **40** 6309–30
- [KM20] Kalle C and Maggioni M 2020 Invariant densities for random systems of the interval *Ergod. Theory Dyn. Syst.* 1–39

- [Knu69] Knuth D E 1969 *The Art of Computer Programming* 1st edn (Reading, MA: Addison-Wesley)
- [KT93] Koyama K and Tsuruoka Y 1993 *Advances in Cryptology — CRYPTO'92* Speeding up elliptic cryptosystems by using a signed binary window method (Berlin: Springer) pp 345–57
- [LK97] Lai C-S and Kuo W-C 1997 Speeding up the computations of elliptic curves cryptoschemes *Comput. Math. Appl.* **33** 29–36
- [Mag21] Maggioni M 2021 Measures and matching for number systems *PhD Thesis* Leiden University
- [MO90] Morain F and Olivos J 1990 Speeding up the computations on an elliptic curve using addition–subtraction chains *Theor. Inf. Appl.* **24** 531–43
- [Mor85] Morita T 1985 Random iteration of one-dimensional transformations *Osaka J. Math.* **22** 489–518
- [Nak81] Nakada H 1981 Metrical theory for a class of continued fraction transformations and their natural extensions *Tokyo J. Math.* **04** 399–426
- [NN08] Nakada H and Natsui R 2008 The non-monotonicity of the entropy of α -continued fraction transformations *Nonlinearity* **21** 1207–25
- [Pel84] Pelikan S 1984 Invariant densities for random maps of the interval *Trans. Am. Math. Soc.* **281** 813
- [Rei60] Reitwiesner G W 1960 Binary arithmetic *Advances in Computers* vol 1 (Amsterdam: Elsevier) pp 231–308
- [TI81] Tanaka S and Ito S 1981 On a family of continued-fraction transformations and their ergodic properties *Tokyo J. Math.* **04** 153–75