Random matching for Random interval maps

Joint work with K. Dajani and C. Kalle

Marta Maggioni, Leiden University

One World Numeration Seminar

September 24, 2020

Outline

- Matching for deterministic interval maps
- Random matching for random interval maps
- Examples: random continued fractions, β-transformations and signed binary representations with minimal weight

Deterministic context

A piecewise smooth interval map T has **strong matching**, or synchronisation, if for any discontinuity point c of T or T' there exist $M, N \in \mathbb{N}$ such that

$$T^M(c^-) = T^N(c^+) \quad \text{and} \quad (T^M)'(c^-) = (T^N)'(c^+),$$

for $c^+ = \lim_{x \downarrow c} x$ and $c^- = \lim_{x \uparrow c} x$.

M, N are called **matching exponents**.

Some results for specific families:

- The family of shift β-**transformations** $\{T_\alpha(x) = \beta x + \alpha \mod 1\}_\alpha$ shows matching λ-a.e. parameter α but only for specific values of β.
- The family of **symmetric doubling maps** $\{S_\eta(x) = 2x - d\eta\}_\eta$ does not present matching on a set of full Hausdorff dimension.
- The α-**continued fraction maps** $\{T_\alpha\}$ have matching on a full Lebesgue set, and the difference of the matching exponents determines the behaviour of the entropy.
- For specific maps, matching causes the associated invariant densities to be piecewise smooth (or constant).

Consequence of strong matching on the structure of the density function:

Thm. '19 [Bruin, Carminati, Marmi, Profeti]

For a piecewise affine eventually expanding interval map T with strong matching, the density of its absolutely continuous invariant probability measure is constant on elements of the prematching partition,

$$\bigcup_c \left(\bigcup_{i=1}^{M-1} T^i(c^-) \cup \bigcup_{i=1}^{N-1} T^i(c^+) \right).$$

Random context

Random maps describe systems that evolve in discrete time in which at each time step one of a number of transformations is chosen according to an i.i.d. process and applied.

Let $\{T_j : I \to I\}_{j \in \Omega}$ be a collection of interval maps, for $\Omega \subseteq \mathbb{N}$ the index set. Let $\sigma : \Omega^{\mathbb{N}} \to \Omega^{\mathbb{N}}$ be the left shift on one-sided sequences. The pseudo-skew product or **random map** $R : \Omega^{\mathbb{N}} \times I \to \Omega^{\mathbb{N}} \times I$ is defined by

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

Measures for pseudo-skew products:

Let $\mathbf{p} = (p_j)_{j\in\Omega}$ be a positive probability vector representing the probabilities we apply the map T_j. Let $m_{\mathbf{p}}$ be the $\mathbf{p}$-Bernoulli measure on $\Omega^{\mathbb{N}}$ and $\mu_{\mathbf{p}}$ be an absolutely continuous wrt λ measure on I such that for each measurable set B

$$\mu_{\mathbf{p}}(B) = \sum_{j\in\Omega} p_j \mu_{\mathbf{p}}(T_j^{-1}(B)).$$

Then $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ is an invariant probability measure for R. We call $\mu_{\mathbf{p}}$ a **stationary measure** for R.

We make assumptions on R to guarantee the existence of $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$.

1. There exists a finite or countable interval partition $\{I_i\}_i$, such that each $T_j \mid_{I_i}$ is C^1 and monotone.
2. R is expanding on average, i.e., for each $x \in I$

$$\sum_{j \in \Omega} \frac{p_j}{|T_j'(x)|} < 1.$$

3. For each $j \in \Omega$ 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 for $c \in C$, the set of critical points.

Random matching

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

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

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

Idea: any random orbit of the left/right limit of any critical point c passes through the set Y_c at the latest at time M.

Strong random matching

A random map 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. For

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

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

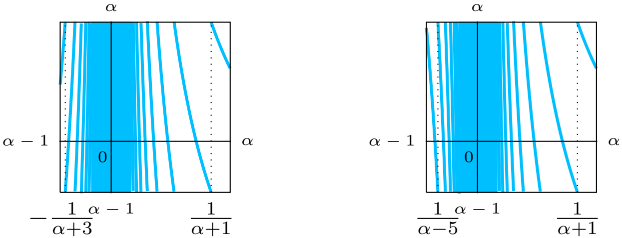
it holds

$$\sum_{\mathbf{u} \in \Omega(y)^-} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^-)} = \sum_{\mathbf{u} \in \Omega(y)^+} \frac{p_{\mathbf{u}}}{T'_{\mathbf{u}}(c^+)}.$$

Example 1: random continued fraction maps

Let CF_α be defined on $\{0,1\}^{\mathbb{N}} \times [\alpha-1,\alpha]$ as the random map given by α-continued fraction maps:

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



(a) $T_{\alpha,0}$ (b) $T_{\alpha,1}$

Note that $T_{j,\alpha}(c^{\pm}) \in \{\alpha - 1, \alpha\}$, so that strong random matching occurs if the random weighted orbits of $\alpha - 1$ and α eventually meet.

For any $\alpha \in \left(\frac{\sqrt{85}-5}{6}, \frac{\sqrt{2}}{2}\right) \subseteq J_4$ strong random matching holds for $M = 3$ and $Y = \left\{\frac{5-7\alpha}{3\alpha-2}\right\}$:

$$\begin{tikzcd}
\alpha \arrow[r] & \frac{1-\alpha}{\alpha} \arrow[r] & \boxed{\frac{3\alpha-2}{1-\alpha}} \arrow[r] & \boxed{\frac{5-7\alpha}{3\alpha-2}}
\end{tikzcd}$$

$$\begin{tikzcd}
\alpha - 1 \arrow[r, "{1,p}"] \arrow[d, "{0,\ 1-p}"] & \frac{4\alpha-3}{\alpha-1} \arrow[r] & \frac{2-3\alpha}{4\alpha-3} \arrow[r] & \boxed{\frac{5-7\alpha}{3\alpha-2}} \\
\boxed{\frac{3\alpha-2}{1-\alpha}} \arrow[d] & & & \\
\boxed{\frac{5-7\alpha}{3\alpha-2}} & & &
\end{tikzcd}$$

For $n \geq 4$ let $J_n = (\ell_n, r_n)$ be defined by the left and right endpoints

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

respectively. For any n and $\alpha \in J_n$ the system CF_α has strong random matching with the same exponent $M = 3$, identifying a countable number of *matching intervals* for the family CF_α.

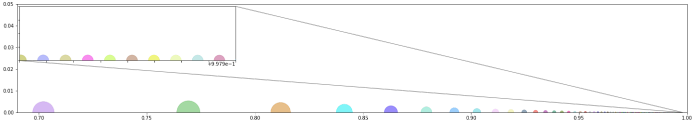
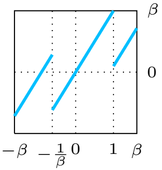


Figure: The semicircles indicate the locations of the intervals J_n.

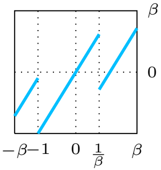
Example 2: random β-transformations

$$\beta = \frac{1+\sqrt{5}}{2},\ \alpha \in \left(\frac{3\beta-2}{2}, 4\beta - 5\right) \text{ and } T_{\alpha,j} : [-\beta,\beta] \to [-\beta,\beta]$$

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



(a) $T_{\alpha,0}$



(b) $T_{\alpha,1}$

For $R_\alpha = \{T_{\alpha,0}, T_{\alpha,0}\}$, $C = \Big\{ -1, -\frac{1}{\beta}, \frac{1}{\beta}, 1 \Big\}$.

For $1 \in C$: $M = 3$ and $Y = \{\beta^2(\beta - \alpha)\}$:

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

For $1/\beta \in C$: $M = 7$ and $Y = \{\beta^5(\beta - \alpha) - \alpha, \beta^6 - 3\beta^3\alpha\}$:

$$T_{\alpha,j}\big(\tfrac{1}{\beta}^-\big) = 1 = T_{\alpha,0}\big(\tfrac{1}{\beta}^+\big) \quad T_{\alpha,1}\big(\tfrac{1}{\beta}^+\big) = 1 - \alpha.$$

$$
\begin{tikzcd}
1-\alpha \arrow[r] & \beta(1-\alpha) \arrow[r, "0"] \arrow[d, "1"] & \beta(\beta-\alpha) \arrow[r] & \boxed{\beta^2(\beta-\alpha)} \arrow[r] & \beta^3(\beta-\alpha) \arrow[r, "0"] \arrow[d, "1"] & \beta^4(\beta-\alpha) \arrow[r] & \boxed{\beta^5(\beta-\alpha)-\alpha} \\
 & \beta^2(1-\alpha) \arrow[d] & & & \beta^4(\beta-\alpha)-\alpha \arrow[d] & & \\
 & \beta^3(1-\alpha)+\alpha \arrow[d] & & & \boxed{\beta^5(\beta-\alpha)-\beta\alpha} & & \\
 & \beta^4(1-\alpha)+\beta\alpha \arrow[r, "0"] \arrow[d, "1"] & \beta^5(1-\alpha)+\beta^2\alpha+\alpha \arrow[r] & \boxed{\beta^6(1-\alpha)+\beta^3\alpha+\beta\alpha=\beta^5(\beta-\alpha)-\alpha} & & & \\
 & \beta^5(1-\alpha)+\beta^2\alpha \arrow[d] & & & & & \\
 & \boxed{\beta^6(1-\alpha)+\beta^3\alpha+\alpha=\beta^5(\beta-\alpha)-\beta\alpha} & & & & &
\end{tikzcd}
$$

Figure: The first couple of points in the orbit of $1-\alpha$ under the random generalised β-transformation. $\beta^2(\beta-\alpha)$ is boxed since this point also appears in all random orbits of 1.

Consequences of strong random matching

On the structure of the density:

Thm. '20 [Dajani, Kalle, M.]

Let R as before. Assume furthermore that each map $\{T_j\}_j$ is defined on a finite interval partition, and for each subinterval I_i not all straight lines have a common weighted intersection point on the diagonal. If R has strong random matching, then there exists an invariant probability measure of the form $m_{\mathbf{p}} \times \mu_{\mathbf{p}}$ such that its density is piecewise constant on the random prematching set.

Proof(ish)

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

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

for some constants γ_i depending only on the discontinuity points c_i. We use random matching to rewrite $f_{\mathbf{p}}$ as

$$f_{\mathbf{p}} = \sum_{i=1}^{N-1} \gamma_i \sum_{k=1}^{M} \Bigg(\sum_{\substack{\omega \in \Omega^k: \\ \forall n \leq k, T_{\omega_1^n}(c_i^-) \notin Y}} \frac{p_\omega}{T'_\omega(c_i^-)} 1_{[c_0, T_\omega(c_i^-))} - \sum_{\substack{\omega \in \Omega^k: \\ \forall n \leq k, T_{\omega_1^n}(c_i^+) \notin Y}} \frac{p_\omega}{T'_\omega(c_i^+)} 1_{[c_0, T_\omega(c_i^+))} \Bigg).$$

Example 3: minimal weight expansions

Many public key cryptosystems deal with the problem of raising elements of a group into some power, x^a. In binary representation,

$$x^a = \prod_{i=0}^{n} x^{d_i 2^i},$$

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 digits d_i in the expansion, which is called **Hamming weight**. One way to reduce the time complexity is given by lowering the Hamming weight.

For any fixed integer a, its ordinary binary representation with digits $\{0, 1\}$ is uniquely determined, but this is not the case for the signed one, with digits in $\{-1, 0, 1\}$.
We consider a family of random maps R_α on $\{0, 1\}^{\mathbb{N}} \times [-1, 1]$ that generate **random signed binary expansions** with digits in $\{-1, 0, 1\}$. The randomness of the system allows us to choose (up to a certain degree) where and when we want to have a digit 0, and to study for each typical number its infinitely many different signed binary expansions simultaneously:

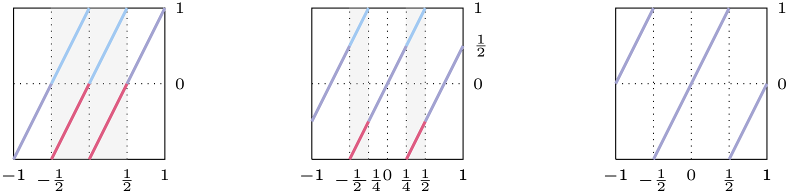
$$x = \alpha \sum_{n \geq 1} \frac{d_n(\omega, x)}{2^n}.$$

The **random symmetric doubling maps** $R_\alpha = \{T_{\alpha,0}, T_{\alpha,1}\}$ for $\alpha \in [1,2]$ and

$$T_{\alpha,0}(x) = \begin{cases} 2x+\alpha & \text{if } x \in \big[-1, \frac{1-\alpha}{2}\big), \\ 2x & \text{if } x \in \big[\frac{1-\alpha}{2}, \frac{1}{2}\big), \\ 2x-\alpha & \text{if } x \in \big[\frac{1}{2}, 1\big], \end{cases}$$

and

$$T_{\alpha,1}(x) = \begin{cases} 2x+\alpha & \text{if } x \in \big[-1, -\frac{1}{2}\big], \\ 2x & \text{if } x \in \big(-\frac{1}{2}, \frac{\alpha-1}{2}\big], \\ 2x-\alpha & \text{if } x \in \big(\frac{\alpha-1}{2}, 1\big]. \end{cases}$$



(a) R_1 (b) $R_{\frac{3}{2}}$ (c) R_2

Figure: 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 violet ones to both.

1. Let

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

and let

$$M = \inf\left\{n \ge 1 \, : \, \frac{1}{2} < S_\alpha^n(1) < \alpha - \frac{1}{2}\right\} + 1.$$

For all $k < M$ and $\omega \in \Omega^k$,

$$T_{\alpha,\omega}(1), \quad T_{\alpha,\omega}(1-\alpha) \in \{S_\alpha^k(1), S_\alpha^k(1-\alpha)\}.$$

Strong random matching holds for Lebesgue almost every $\alpha \in [1,2]$, for the time M and the set $Y = \{S_\alpha^M(1)\}$.

2. From

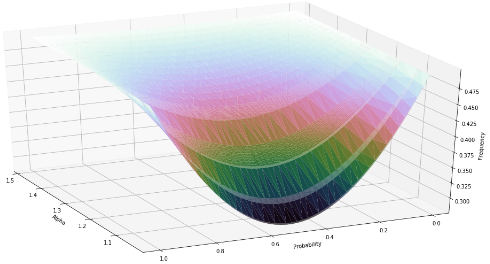
$$S_\alpha^k(1-\alpha) = S_\alpha^k(1) - \alpha \quad \text{for } k < M$$

and random matching it follows that an explicit formula for the **piecewise constant density function** is given by:

$$f_{\mathbf{p}} = (\gamma_1+\gamma_2)\frac{p_1}{2}\sum_{k=0}^{M-1}\sum_{\omega\in\Omega^k}\frac{p_\omega}{2^k}\big(\mathbf{1}_{[-1,T_\omega(\alpha-1))} - \mathbf{1}_{[-1,T_\omega(-1))}\big)$$
$$+ (\gamma_2+\gamma_3)\frac{p_0}{2}\sum_{k=0}^{M-1}\sum_{\omega\in\Omega^k}\frac{p_\omega}{2^k}\big(\mathbf{1}_{[-1,T_\omega(1))} - \mathbf{1}_{[-1,T_\omega(1-\alpha))}\big).$$

Thm. '20 [Dajani, Kalle, M.]

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



More on the **matching intervals**:

Let $a = [0; a_1, a_2, \ldots, a_{2j+1}] \in \mathbb{Q} \cap [0,1]$ such that I_a is a maximal quadratic interval for the α-CF map $T_{0,\alpha}$. Then

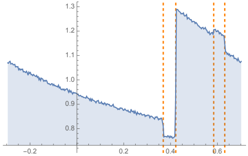
$$\left(\frac{2^M + 1}{2^M \varphi(a) + 1}, \frac{2^M - 1}{2^M \varphi(a) - 1} \right)$$

is a matching interval for R_α, for $M = \sum_{i=1}^{2j+1} a_i$, and

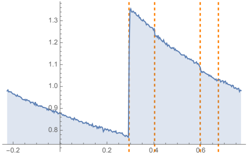
$$\varphi(a) = \eta((1 \circ a_1)(0 \circ a_2) \ldots) \text{ and } \eta((b_n)_{n \geq 1}) = \sum_{n \geq 1} \frac{b_n}{2^n}.$$

Future plans

Do piecewise smooth random interval maps with random matching have piecewise smooth densities?



(a) $\alpha = 0.70315\ldots$, $p_0 = 0.3$



(b) $\alpha = 0.77287\ldots$, $p_0 = 0.6$

Figure: Numerical simulations of $f_{\mathbf{p}}$ for the random continued fraction maps CF_α. In (a) $\alpha \in J_4$ and $p_0 = 0.3$ and in (b) $\alpha \in J_5$ and $p_0 = 0.6$. The dashed lines indicate the position of the *prematching set*, i.e., the points in the orbits of α and $\alpha - 1$ before the moment of matching.

Thank you for listening.