

The generic transformation has roots of all orders

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082
squash@ufl.edu
Webpage <http://squash.1gainesville.com/>
16 August, 2016 (at 18:06)

Dedicated to the memory of Anzelm Iwanik.

ABSTRACT: In the sense of the Baire Category Theorem we show that the generic transformation T has roots of all orders (RAO theorem). The argument appears novel in that it proceeds by establishing that the set of such T is *not meager* —and then appeals to a Zero-One Law. (Lemma ??.)

On the group Ω of (invertible measure-preserving) transformations, §?? shows that the squaring map $\varphi : S \mapsto S^2$ is topologically complex in that both the *locally-dense* and *locally-lacunary* points of φ are dense. (Theorem ??.)

The last section, §??, discusses the relation between RAO and a recent example of Blair Madore. Answering a question of the author’s, Madore constructs a transformation with a square-root chain of each finite length, yet possessing no infinite square-root chain.

§A History

A transformation T might have a *cartesian* square root, $T = S^{\times 2} := S \times S$, or a *composition* square root, $T = R^2 := R \circ R$; I will henceforth call composition roots just roots. In a paper which had a significant impact on Ergodic theory in the 1970’s and 1980’s, “*On the root problem in ergodic theory*”, [?], Don Ornstein constructed a remarkable transformation T with no roots. Then Dan Rudolph showed, in [?], that the parameters

AMS Subject Classification: Primary: 28D05. Secondary: 54E52.

of Ornstein’s construction could be tuned to insure that T was prime –no factors– and therefore had no cartesian roots. (This was shown independently by Ken Berg in [?].) Indeed, Rudolph constructed a T with the stronger property of *minimal self-joinings*, and showed that MSJ implies primeness and trivial commutant. Later work, [?], showed that MSJ followed automatically from T being both mixing and rank-1. The MSJ property, and the more general property of *simplicity*, have been fruitful for the study of classes of zero-entropy maps, [?, ?].

Ornstein’s map has no roots “because” it commutes only with its powers. An entirely different type of rootless T was constructed in [?] via an algebraic automorphism-extension; the commutant of this T is uncountable.

The following overview uses topological terms *almost-open*, *meager*, *residual* (=generic), *coarse topology* and *BaireCat space*. These will be defined further below.

Genericity. What happens generically for transformations on a Lebesgue probability space (\mathbb{I}, μ) ? We ask this question with respect to the standard coarse topology on Ω , where Ω is the group –under composition– of (invertible measure-preserving) transformations on \mathbb{I} .

It follows from the **Weak-Closure theorem** of [?] that no rank-1 map has a cartesian square root. Since RANK-1 is generic,^{♥1} only a meager set of transformations in Ω can have a cartesian square root.

In contrast, the goal of this article is to show that possessing *composition* roots is generic. To this end, let $\varphi_e : \Omega \rightarrow \Omega$ denote the e^{th} -power map $S \mapsto S^e$.

1: RAO Theorem (Roots of All Orders). *The set of*

^{♥1}This is implicit in [?, P.65–68], and also follows from the Rohlin lemma. Several equivalent definitions of *rank-1* appear in the introduction of [?].

transformations with roots of all orders,

$$\text{RAO} := \bigcap_{e=2}^{\infty} \wp_e(\Omega),$$

is Ω -residual. \diamond

It suffices to show that $\wp_e(\Omega)$ is residual, for each exponent e . Most of the ideas appear in the $e = 2$ case, so we henceforth let \wp be the squaring map \wp_2 , and endeavor to show that

$\zeta 1$: $\text{SQUARES} := \wp(\Omega)$, *is residual.*

The sequel will reduce this ($\zeta 1$), in a series of steps, to an assertion ($\zeta 4$). Here is a roadmap.

§Outline

A tool that we need is the following special case of the **Zero-One Law** for genericity. In the terminology of [?], a subset $\mathbf{P} \subset \Omega$ is **dynamical** if

- i: It is isomorphism-invariant:* Whenever a transformation T' is isomorphic to a $T \in \mathbf{P}$, then T' itself is in \mathbf{P} .
- ii: It is sufficiently measurable:* \mathbf{P} is an almost-open subset of Ω .

2: Zero-One Lemma ([?, P.232]). *Each dynamical property $\mathbf{P} \subset \Omega$ is either meager or residual.* \diamond

Miscellany. Use “ $x := \text{foo}$ ” or “ $\text{foo} =: x$ ” to mean that *foo* is the definition of symbol x . When defining a term, we use a **bold-face italic font**, whereas just *italics* indicates emphasis. We use the small-caps font to indicate the *set* of objects satisfying a property, e.g, **RAO**, **RANK-1**, **SQUARES** —and, later, **WEAKMIXING** and **LOC DEN**.

Use $A \setminus B$ for the difference of two sets. Use $A \triangle B$ for the symmetric difference $[A \setminus B] \cup [B \setminus A]$. For real numbers a and b , let $[a .. b)$ denote the “interval of integers” $[a, b) \cap \mathbb{Z}$.

Employ $K \blacklozenge L$ for “ K divides L ”, and use $L \blacklozenge K$ for “ L is a multiple of K ”.

To indicate a map from a set to *itself*, we may write $f: X \circlearrowright$ instead of $f: X \rightarrow X$.

Topological Preliminaries

On a set X , a family $\{\mathcal{W}_n\}_{n=1}^{\infty}$ of topologies engenders the coarsest (fewest open sets) topology, \mathcal{X} , such that each $\mathcal{W}_n \subset \mathcal{X}$. This \mathcal{X} is generated by finite intersections $U_{n_1} \cap \dots \cap U_{n_K}$, where each $U_n \in \mathcal{W}_n$.

Suppose further, for each \mathcal{X} -open set X' and point $z \in X'$, that the following holds.

- 3: *For all sufficiently large n , there is a \mathcal{W}_n -open set U_n for which $z \in U_n \subset X'$.*

If so, say that “sequence $(\mathcal{W}_n)_{n=1}^{\infty}$ **tends to \mathcal{X}** ” and write $\mathcal{W}_n \nearrow \mathcal{X}$.

For a pseudo-metric \mathbf{d} (a symmetric mapping $\mathbf{d}: X \times X \rightarrow [0, \infty)$ satisfying the triangle inequality, but allowing $\mathbf{d}(x, z) = 0$) and point $z \in X$, use $\mathbf{d}\text{-Ball}_{\varepsilon}(z)$ to mean the set of x for which $\mathbf{d}(x, z) < \varepsilon$.

Now suppose that \mathbf{d}_n is a pseudo-metric on X , with \mathcal{W}_n its topology comprising all unions of \mathbf{d}_n -balls. If each \mathbf{d}_n is bounded by 1, then topology \mathcal{X} is realized by pseudo-metric

4:
$$\mathbf{m} := \sum_{n=1}^{\infty} \frac{1}{2^n} \mathbf{d}_n .$$

The next two headings will develop the requisite topological notions to prove ($\zeta 1$).

The Coarse Topology, \mathcal{C} , on Ω

Since each two non-atomic Lebesgue probability spaces are isomorphic, henceforth take \mathbb{I} to be the half-open interval $[0, 1)$ with Lebesgue measure μ .

The **coarse topology** on Ω , call it \mathcal{C} , is the topology in which transformations τ_j approach T iff:

$$\text{For each measurable set } E \subset \mathbb{I}: \\ \mu(\tau_j^{-1}(E) \triangle T^{-1}(E)) \rightarrow 0, \text{ as } j \nearrow \infty.$$

Said differently, the coarse topology on Ω is simply the strong operator topology with each transformation $T \in \Omega$ regarded as a unitary operator on $\ell^2(\mu)$.

A metric m realizing C

In the sequel, let **interval** mean a non-void half-open set $[a, b) \subset \mathbb{I}$. A **partition** Q decomposes \mathbb{I} into equal-length subintervals,

$$Q = Q_k := \left\{ \left[0, \frac{1}{k}\right), \left[\frac{1}{k}, \frac{2}{k}\right), \dots, \left[\frac{k-1}{k}, 1\right) \right\},$$

called the **atoms** of Q . A partition P **refines** Q if each Q -atom $A \in Q$ is some union of P -atoms. The formula

$$5: \quad d_Q(S, T) := \sum_{A \in Q} \frac{1}{2} \mu(S^{-1}(A) \triangle T^{-1}(A))$$

shows that a partition Q gives rise to a bounded-by-1 pseudo-metric on Ω . Let \mathcal{W}_Q denote the d_Q -topology on Ω .

A given finite list $E_1, \dots, E_L \subset \mathbb{I}$ of (measurable) sets can be ε -approximated, taking a k sufficiently large, by various unions of Q_k -atoms. Consequently:

??': Sequence $(\mathcal{W}_{Q_n})_{n=1}^\infty$ tends to \mathcal{C} .

Letting d_n denote d_{Q_n} in (??), the resulting pseudo-metric m is a *metric* which realizes the coarse topology on Ω .

6: Lemma. *Our space (Ω, \mathcal{C}) is a **Polish** (non-void, and homeomorphic to a complete separable metric space) topological group. In particular, each power map \wp_e is continuous.* \diamond

Sketch of proof. It is not difficult to show that Ω is complete with respect to the metric

$$T, S \mapsto m(T, S) + m(T^{-1}, S^{-1}).$$

And this metric still realizes \mathcal{C} , since the mapping $S \mapsto S^{-1}$ is continuous, as now shown: It suffices to take transformations $\sigma_j \rightarrow S$ and fix a set E , then establish that $\sigma_j(E)$ tends to $S(E)$. But letting $A := S(E)$, note that

$$\begin{aligned} \mu(\sigma_j(E) \triangle S(E)) &= \mu(E \triangle \sigma_j^{-1}S(E)) \\ &= \mu(S^{-1}(A) \triangle \sigma_j^{-1}(A)), \end{aligned}$$

which certainly goes to zero as $j \rightarrow \infty$.

To show that the group-multiplication is continuous, we need only measure convergence on a fixed set A . To this end, let $[\tau, \sigma]$ abbreviate

$$\mu(\tau^{-1}(A) \triangle \sigma^{-1}(A)).$$

Fix maps T and S , let $E := T^{-1}(A)$, and consider transformations $\tau_j \rightarrow T$ and $\sigma_j \rightarrow S$. Evidently

$$\begin{aligned} [[\tau_j \sigma_j, TS]] &\leq [[\tau_j \sigma_j, T \sigma_j]] + [[T \sigma_j, TS]] \\ &= [[\tau_j, T]] + \mu(\sigma_j^{-1}(E) \triangle S^{-1}(E)). \end{aligned}$$

And these two terms go to zero, as $j \rightarrow \infty$.

Finally, as detailed in Proposition ??, below, those transformations which permute the atoms of some partition form a set which is Ω -dense and countable. Hence Ω is separable. (For further discussion, see [?, pp.62–68].) \blacklozenge

The Baire Necessities

Recall that a subset $B \subset X$ of a topological space is nowhere-dense if its closure has no interior. Less stringent, B is **meager** if it equals some countable union of nowhere-dense sets. Finally, a subset $E \subset X$ is **residual** if its complement $X \setminus E$ is meager.

Say that X is a **BaireCat space** if the conclusion of the Baire Category Theorem holds in this form:

Each residual subset of X is dense.

Since Ω is completely metrizable, it is BaireCat.^{♡2}

For the Zero-One Law to apply to SQUARES, we need to know that SQUARES fulfills the stated measurability condition. Say that a subset $B \subset X$ is **almost-open** if it is “almost” equal to some open set U —in the sense that the symmetric difference $B \triangle U$ is meager. It is straightforward to show that the almost-open sets form a sigma-algebra. *A fortiori* the open sets are almost-open, so ALMOSTOPEN includes^{♡3} the Borel sigma-algebra. Here is the non-trivial fact that we need.

7: Theorem. *Each analytic set (the forward image of a Borel set, under a continuous map between Polish spaces) is almost-open.* ♦

Proof. See [?, pp. 482, 92]. ♦

This result comes into play as follows. Since \wp is continuous, the set of pairs (R, T) with $R^2 = T$ is a closed subset of Polish space $\Omega \times \Omega$. And SQUARES is its continuous image under

$$\Omega \times \Omega \rightarrow \Omega: (S, T) \mapsto T,$$

the projection map. Thus SQUARES is analytic, hence almost-open. So by Zero-One, we need but establish that

ζ2: SQUARES is non-meager.

^{♡2}A standard term is *Baire*, rather than *BaireCat*; alas, the modifier “Baire” is used inconsistently. It has three distinct meanings in these usages: “a Baire space”, “a Baire set”, “a set with the property of Baire”. Unfortunately a *Baire set* is not —with the standard terminology— a *Baire space* in the induced topology.

^{♡3}This inclusion is proper: Computing cardinalities shows that

$$\#\text{ALMOSTOPEN} = \#\text{MEAGER} = 2^{\mathbb{R}},$$

whereas #BOREL only equals \mathbb{R} .

Our next step is to develop a condition which guarantees non-meagerness of a continuous image.

Local density. Suppose that $f: X \rightarrow \Lambda$ is a map between topological spaces. A point $z \in X$ is **locally-dense** (with respect to f) if:

Each neighborhood of z has f -image which is dense in some neighborhood of $f(z)$.

Let $\text{LOCDEN}(f)$ denote the set of locally-dense points. The following neat observation is due to Randall Dougherty.

8: Dougherty’s Lemma. *Consider $f: X \rightarrow \Lambda$, a continuous map from a BaireCat space to a topological space. If $\text{LOCDEN}(f)$ is X -dense, then $f(X)$ is not Λ -meager.* ♦

Proof. Were $f(X)$ meager, then we could cover it by a union $\bigcup_1^\infty \Gamma_n$ of closed sets, each without interior. Thus each $C_n := f^{-1}(\Gamma_n)$ is closed, and $\bigcup_1^\infty C_n$ covers X .

The interior, U , of a C_n , has its f -image inside the closed interiorless set Γ_n , so no point of U is locally-dense. Thus C_n has no interior, hence is meager. Consequently X is not BaireCat. ♦

Remark. The same argument shows that the f -image of each X -residual set is not Λ -meager. □

Setting up property $\alpha(z, K)$

Topologically, the last tool we need is the lemma below. The baroqueness of its formulation is adapted to its use in §???

Consider a map between topological spaces,

$$f: (X, \mathcal{X}) \rightarrow (\Lambda, \mathcal{L}),$$

as well as topologies $\mathcal{W}_n \nearrow \mathcal{X}$ and topologies $\mathcal{K}_n \subset \mathcal{L}$. For a point $z \in X$ and positive integer K , define this property.

§B Combinatorics

PROPERTY $\alpha(z, K)$: Given a \mathcal{W}_K -open set $U \ni z$ there exists an \mathcal{L} -dense set $\Delta \subset \Lambda$ and a \mathcal{K}_K -open set $\Upsilon \ni f(z)$ so that:

$$\alpha': \quad f(U) \supset \Upsilon \cap \Delta.$$

9: Baroque lemma. *With notation from immediately above, suppose that $\alpha(z, n)$ holds for infinitely many n . Then z is locally-dense for f . \diamond*

Proof. Fix an arbitrary \mathcal{X} -open set $Z \ni z$.

Among those n fulfilling $\alpha(z, n)$, take n large enough to produce a \mathcal{W}_n -open set U for which $z \in U \subset Z$. Then take subsets $\Delta, \Upsilon \subset \Lambda$ as $\alpha(z, n)$ provides. *A fortiori* Υ is \mathcal{L} -open, so $\Upsilon \cap \Delta$ is \mathcal{L} -dense in Υ . Taking \mathcal{L} -closures, then,

$$\overline{f(Z)} \supset \overline{f(U)} \supset \overline{\Upsilon \cap \Delta} \supset \Upsilon \ni f(z),$$

as was desired. \diamond

The foregoing discussion will allow us to make “local-density” a purely combinatorial matter. Henceforth, d_k denotes pseudo-metric d_{Q_k} from (??).

Permutations

A permutation of $[0 .. K)$ will be called a ***K-perm.*** If a K -perm $\pi: [0 .. K) \rightarrow [0 .. K)$ happens to comprise a single cycle –necessarily of length K – then we call π a ***K-cycle.*** Each K -perm π has an associated interval-exchange map $G_\pi \in \Omega$ which rigidly permutes the atoms of partition Q_K according to π . Specifically, letting A_ℓ be the atom $[\frac{\ell}{K}, \frac{\ell+1}{K})$:

$$G_\pi(x) := \frac{\pi(\ell)}{K} + [x - \frac{\ell}{K}], \quad \text{for } x \in A_\ell.$$

Call transformation G_π a ***K-shuffle***, or just a ***shuffle.*** Evidently if T is a K -shuffle and K divides L , then T is also an L -shuffle.

As an example, take $K = 5$ and $T := G_\pi$, where π maps 2 to 0 to 4 to 2, and π exchanges 1 and 3. Then

$$*: \quad (2 \ 0 \ 4) (1 \ 3)$$

is the cycle structure of π . Call $(*)$ also “the 5-***structure*** of T ”. In contrast, the 10-structure of T splits each cycle into two copies:

$$(4 \ 0 \ 8)(5 \ 1 \ 9) (2 \ 6)(3 \ 7) .$$

If the K -structure of T is a single cycle then we call T a ***K-solo.*** The Rohlin lemma or [?, P.65] implies the following.

10: Proposition. *The set of K -solos, with K ranging over an infinite set of positive integers, is \mathcal{C} -dense in Ω . \diamond*

Creating combinatorial roots

Given an L -perm λ , say that an L' -perm ρ is a “**combinatorial n^{th} root** of λ ” if $L' \bullet L$ and, for the corresponding transformations, $[G_\rho]^n$ equals G_λ .

We now construct combinatorial square-roots. Consider an L -sequence $\mathbf{c} = c_0 \dots c_{L-1}$ of numbers. Let $\lfloor \mathbf{c} \rfloor^3$ be the sequence *rotated* by 3 positions. Thus

$$\lfloor \mathbf{c} \rfloor^3 := c_3 c_4 c_5 \dots c_{L-1} c_0 c_1 c_2 .$$

For $r \in \mathbb{Z}$, define the rotation $\lfloor \mathbf{c} \rfloor^r$ analogously; so $\lfloor \mathbf{c} \rfloor^0 = \mathbf{c}$.

A linear expression such as “ $2\mathbf{c} + 5$ ” shall mean the L -sequence \mathbf{d} , where each $d_\ell := 2c_\ell + 5$.

Given two L -sequences \mathbf{a} and \mathbf{c} , let

$$\mathbf{a} : \mathbf{c} := a_0 c_0 a_1 c_1 a_2 c_2 \dots a_{L-1} c_{L-1}$$

denote their *alternation*.

The Weave operation. From an L -cycle λ , we can produce a square root of the corresponding L -solo G_λ by cutting its Rohlin stack into left/right halves, rotating one half (perhaps), and then zig-zagging. We now describe this operation directly on λ .

Arbitrarily cut cycle λ to produce

- 11: *an L -sequence $c_0 c_1 c_2 \dots c_{L-1}$, with each $c_\ell \in [0 .. L)$; here $\lambda(c_\ell) = c_{\ell \oplus 1}$, where \oplus denotes addition mod L .*

For a “rotation number” $r \in \mathbb{Z}$, define this cycle,

$$\text{Weave}_\lambda(r) := (2\mathbf{c} : \lfloor 2\mathbf{c} + 1 \rfloor^r) .$$

The resulting cycle has length $2L$, and does not depend on where λ was cut.

- 12: *Example.* Suppose that $L = 7$ and sequence \mathbf{c} is 0246135. Zig-zagging gives this 14-cycle

$$\text{Weave}_\lambda(0) = (\underline{0} \ \dot{0} \ \underline{2} \ \dot{2} \ \underline{4} \ \dot{4} \ \underline{6} \ \dot{6} \ \underline{1} \ \dot{1} \ \underline{3} \ \dot{3} \ \underline{5} \ \dot{5}) ,$$

where \underline{c} denotes $2c$, and \dot{c} means $2c + 1$. Rotating the dotted numbers by 4 places produces

$$\begin{aligned} \text{Weave}_\lambda(4) &= (\underline{0} \ \dot{1} \ \underline{2} \ \dot{3} \ \underline{4} \ \dot{5} \ \underline{6} \ \dot{0} \ \underline{1} \ \dot{2} \ \underline{3} \ \dot{4} \ \underline{5} \ \dot{6}) \\ &= (0 \ 3 \ 4 \ 7 \ 8 \ 11 \ 12 \ 1 \ 2 \ 5 \ 6 \ 9 \ 10 \ 13) . \end{aligned}$$

For $\rho := \text{Weave}_\lambda(r)$, observe that the cycle structure of ρ^2 is $(2\mathbf{c})(2\mathbf{c} + 1)$; this, regardless of what r equals. And since the ℓ^{nd} atom of partition Q_L is the union of atoms 2ℓ and $2\ell + 1$ of Q_{2L} , we see that transformation $[G_\rho]^2$ equals G_λ .

- 13: **Root Lemma.** *For an L -cycle λ and rotation number $r \in \mathbb{Z}$, the $2L$ -cycle $\text{Weave}_\lambda(r)$ is a combinatorial square-root of λ .* \diamond

Computing d_K -distance

We now convert distance between shuffles to a computation directly with permutations. The notation for the following lemma appears anon.

- 14: **Frequency Lemma.** *Suppose that π is an K -perm and ρ is an L -perm, where $L \bullet K$. Then*

$$d_K(G_\pi, G_\rho) = D_\pi(\rho) .$$

Atoms of partitions. Enumerate the atoms of Q_K as A_0, \dots, A_{K-1} and the atoms of Q_L as C_0, \dots, C_{L-1} . For the nonce letting V denote the ratio $\frac{L}{K}$, remark that each atom A_k is the disjoint union

$$*: \quad A_k = \bigsqcup_{\ell=V_k}^{V_k+[V-1]} C_\ell ,$$

of V consecutive Q_L -atoms. For an index ℓ , let $\hat{\ell}$ be the corresponding value of k in (*). That is,

$$\hat{\ell} := \left\lfloor \ell \cdot \frac{K}{L} \right\rfloor ,$$

where $\lfloor \cdot \rfloor$ is the floor (greatest integer) function.

Measuring disagreement. Use $D_\pi(\rho)$ to measure the frequency of discord between π and ρ , as measured on the partition, Q_K , that π permutes:

??':

$$D_\pi(\rho) := \frac{1}{L} \cdot \# \left\{ \ell \in [0..L) \mid \widehat{\rho(\ell)} \neq \pi(\widehat{\ell}) \right\}.$$

Example ??, revisited. Let permutation π be the 7-cycle (0123456). Its square is $\lambda = (0246135)$ of Example ??. The 14-structure of G_π is

$$\pi = (0\ 2\ 4\ 6\ 8\ 10\ 12)(1\ 3\ 5\ 7\ 9\ 11\ 13).$$

The cycle $\rho := \text{Weave}_\lambda(4)$ of Example ?? is

$$\rho = (0\ 3\ 4\ 7\ 8\ 11\ 12\ 1\ 2\ 5\ 6\ 9\ 10\ 13).$$

Evidently, $G_\rho \neq G_\pi$. Although $d_{14}(G_\rho, G_\pi)$ is positive, the d_7 distance is *zero*. To see this, apply the reduction $\ell \mapsto \widehat{\ell} = \lfloor \ell \cdot \frac{7}{14} \rfloor$ to the preceding two displays. This results in:

$$\begin{aligned} \pi &: (0\ 1\ 2\ 3\ 4\ 5\ 6)(0\ 1\ 2\ 3\ 4\ 5\ 6) \\ \rho &: (0\ 1\ 2\ 3\ 4\ 5\ 6\ 0\ 1\ 2\ 3\ 4\ 5\ 6) \end{aligned}$$

Thus $D_\pi(\rho) = 0$.

When we apply this observation, in (ζ4), our cycle λ will not be π^2 , but rather will be a *perturbation* of π^2 . \square

Proof of (??), the Frequency Lemma. For specificity, take $K = 21$. Define transformations

$$T := G_\pi \quad \text{and} \quad R := G_\rho,$$

and have P denote partition Q_{21} .

Given two P -atoms, say, A_8 and A_{17} , let \mathcal{F} be the set of $\ell \in [0..L)$ with $\ell = 8$. Enumerating the Q_L -atoms as C_0, \dots, C_{L-1} , then, A_8 is the disjoint union $\bigsqcup_{\ell \in \mathcal{F}} C_\ell$. Thus

$$\begin{aligned} \mu(R(A_8) \cap A_{17}) &= \sum_{\ell \in \mathcal{F}} \mu(R(C_\ell) \cap A_{17}) \\ &= \frac{1}{L} \cdot \# \left\{ \ell \in \mathcal{F} \mid \widehat{\rho(\ell)} = 17 \right\}. \end{aligned}$$

Replacing “17” by $\pi(8)$ and “ A_{17} ” by $T(A_8)$ gives this:

$$\mu(R(A_8) \cap T(A_8)) = \frac{1}{L} \cdot \# \left\{ \ell \in \mathcal{F} \mid \widehat{\rho(\ell)} = \pi(\widehat{\ell}) \right\}.$$

Substituting k for “8”, then summing over all k in $[0..21)$ yields that

$$\begin{aligned} * : \quad \sum_{A \in P} \mu(R(A) \cap T(A)) \\ = \frac{1}{L} \cdot \# \left\{ \ell \in [0..L) \mid \widehat{\rho(\ell)} = \pi(\widehat{\ell}) \right\}. \end{aligned}$$

With B denoting $T(A)$, subtract each side of (*) from 1 to arrive at this:

$$\begin{aligned} D_\pi(\rho) &= 1 - \sum_{B \in P} \mu(R(A) \cap B) \\ &= \sum_B \left[\mu(B) - \mu(R(A) \cap B) \right] \\ &= \sum_B \frac{1}{2} \mu(R(A) \triangle B); \end{aligned}$$

this last, since $R(A)$ and B have the same μ -mass. The denouement, by applying R^{-1} , is that

$$D_\pi(\rho) = \sum_{B \in P} \frac{1}{2} \mu(T^{-1}(B) \triangle R^{-1}(B)),$$

which is indeed the definition of $d_K(T, R)$. \blacklozenge

Reduction to Combinatorics

Here is the standing condition which is in force for the remainder of §??.

We have integers $K \mid J$, with J odd, and have a J -solo T . Necessarily, T equals some shuffle G_π , where $\pi: [0..K) \circlearrowright$ is a permutation comprising $\frac{K}{J}$ many J -cycles. Define

$$16: \quad \begin{aligned} \sigma &:= \pi^2 = \pi \circ \pi \quad \text{and} \\ S &:= T^2 \stackrel{\text{note}}{=} G_\sigma, \end{aligned}$$

the corresponding squares.

Since J is odd, note that permutation σ , like π , is made up of $\frac{K}{J}$ many cycles, each of length J .

Courtesy of (??), the collection of odd-solos is Ω -dense. Consequently:

ζ3: *If each odd-solo is locally-dense for \wp , then SQUARES is Ω -residual.*

This follows from (??) and (ζ2).

Describing property $\beta(\pi, K)$. Let $(\times K)$ -cycles be the infinite family of cyclic permutations $\lambda: [0..L) \circlearrowright$ taken over all lengths $L = K, 2K, 3K, 4K, \dots$

Here is a combinatorial property that the π, K pair might have.

PROPERTY $\beta(\pi, K)$: Given ε there is a $\delta > 0$ so that for each $(\times K)$ -cycle λ :

There is a combinatorial square-root ρ , of λ , for which $D_\sigma(\lambda) < \delta \implies D_\pi(\rho) < \varepsilon$.

Roughly: “Each perturbation λ of the square of π , has a combinatorial square root close to π .”

17: LOC DEN Combinatorial Lemma. *If each pair π and K has property $\beta(\pi, K)$, then SQUARES is residual in Ω .* ◇

Proof. Letting T denote G_π , we will first show that

$$??': \quad \beta(\pi, K) \implies \alpha(T, K),$$

by letting \mathbf{d} mean \mathbf{d}_K , and then applying Property α to the squaring map via the correspondence below.

General: $f: X \rightarrow \Lambda$	Squaring: $\wp: \Omega \rightarrow \Omega$
$\mathcal{W}_n \nearrow \mathcal{X}$	\mathbf{d}_n -topologies $\nearrow \mathcal{C}$
$\mathcal{K}_n \subset \mathcal{L}$	\mathbf{d}_n -topology $\subset \mathcal{C}$
U, Υ	$\mathbf{d}\text{-Ball}_\varepsilon(T), \mathbf{d}\text{-Ball}_\delta(S)$

Establishing (??'). A \mathbf{d} -open set $U \ni T$ may freely be shrunk to some $\mathbf{d}\text{-Ball}_\varepsilon(T)$, for a sufficiently Lilliputian ε . Property $\beta(\pi, K)$ produces a number δ for which (β') holds. Happily,

$$\Delta := \{G_\lambda \mid \lambda \text{ is a } (\times K)\text{-cycle}\}$$

is \mathcal{C} -dense, thanks to (??). By definition,

$$\Upsilon := \mathbf{d}\text{-Ball}_\delta(S)$$

is a \mathbf{d} -open neighborhood of $\wp(T)$.

Using the Frequency lemma twice, (β') says that for each $(\times K)$ -cycle λ ,

$$G_\lambda \in \Upsilon \implies G_\rho \in \mathbf{d}\text{-Ball}_\varepsilon(T).$$

Thus $\Delta \cap \Upsilon \subset \wp(U)$, as required by (α') . ◇

Second step. Given that each $\beta(\pi, K)$ holds, we now know that each $\alpha(T, K)$ holds. Fixing T and varying K over the multiples of J , the Baroque lemma guarantees that T is locally-dense for \wp . Courtesy of (ζ3) then, SQUARES is Ω -residual. ◆

The upshot, (ζ4). We have navigated from (ζ1) to this becoming our goal:

Given ε there is a δ so that for each $L \blacktriangleright K$ and each L -cycle λ :

$\zeta 4$:

$$\mathbf{D}_\sigma(\lambda) < \delta \implies \mathbf{D}_\pi(\rho) < 2\varepsilon$$

where ρ is the $2L$ -cycle $\text{Weave}_\lambda\left(\frac{J+1}{2}\right)$.

The above assertion is a specification of property $\beta(\pi, K)$, since for an arbitrary integer r , the cycle $\rho := \text{Weave}_\lambda(r)$ is a combinatorial square root of λ .

Establishing ($\zeta 4$)

Given a K -perm σ and an L -cycle λ , with $L \blacktriangleright K$, we ask: *How does frequency-of-disagreement behave relative to the Weave operation?*

The results that we need, (??) and (??), arise from substrings of λ which look like pieces of σ .

The σ -blocking of a cycle λ

Cut λ to produce a sequence \mathbf{b} , with each number $b_\ell \in [0..L)$ and with $\lambda(b_\ell) = b_{\ell \oplus 1}$; here, \oplus means addition mod L . Note that from its definition, (??'), computing $\mathbf{D}_\sigma(\lambda)$ does not require all the information in \mathbf{b} . Indeed

$$\mathbf{D}_\sigma(\lambda) \stackrel{\text{note}}{=} \frac{1}{L} \cdot \#\left\{ \ell \in [0..L) \mid c_{\ell \oplus 1} \neq \sigma(c_\ell) \right\}$$

where \mathbf{c} is the Q_K -*name* of \mathbf{b} ; that is,

$$18: \quad c_\ell := \widehat{b}_\ell \stackrel{\text{note}}{=} \left\lfloor c_\ell \cdot \frac{K}{L} \right\rfloor.$$

At this juncture, let $\mathbf{A} \subset [0..L)$ denote the *positions of agreement* —the set of indices ℓ such that $c_{\ell \oplus 1} = \sigma(c_\ell)$; thus $\#\mathbf{A}/L$ equals $1 - \mathbf{D}_\sigma(\lambda)$. Decompose \mathbf{A} into a disjoint union,

$$\mathbf{A} = \bigsqcup_{n=1}^N [\ell_n .. r_n),$$

of half-open intervals (of integers), satisfying $0 \leq \ell_1 < r_1 < \ell_2 < r_2 < \dots < r_N \leq L$. Each interval

$[\ell .. r)$ is called a σ -**block** of λ . This decomposition is unique.^{♥4}

Given a positive integer M , call a σ -block $[\ell .. r)$ a σ - M -**block** if its length dominates M ; that is, if $r - \ell \geq M$. Thus the “ σ - M -blocking of λ ” comprises all the σ - M -blocks. Let

$$\mu(\sigma\text{-}M\text{-blocks on } \lambda)$$

denote the probability that an index in $[0..L)$ is in some σ - M -block. Evidently $M = 0$ yields the full σ -blocking, and so

$$\mu(\sigma\text{-}0\text{-blocks on } \lambda) = 1 - \mathbf{D}_\sigma(\lambda),$$

by definition.

19: Blocking Lemma. *With σ, λ, L and M as above,*

$$a: 1 - \mathbf{D}_\sigma(\lambda) \geq \mu(\sigma\text{-}M\text{-blocks on } \lambda).$$

$$b: \mu(\sigma\text{-}M\text{-blocks on } \lambda) \geq 1 - M\mathbf{D}_\sigma(\lambda).$$

Proof of (b). A miracle occurs: Suppose that *every* position $r \in [0..L)$ of disagreement, $c_{r \oplus 1} \neq \sigma(c_r)$, happens to be the end of a σ -block $[\ell .. r)$ whose length, $r - \ell$, is *exactly* $M - 1$. In this one case, the quantity $1 - \mu(\sigma\text{-}M\text{-blocks})$ is just large enough to equal M times the probability of a disagreement. So

$$1 - \mu(\sigma\text{-}M\text{-blocks on } \lambda) \leq M \cdot \mathbf{D}_\sigma(\lambda),$$

is the general non-miraculous assertion. ♦

^{♥4}There is an exceptional case: When $\mathbf{D}_\sigma(\lambda)$ is zero, \mathbf{A} is the entire cycle $[0..L)$ and so \mathbf{A} does not break into intervals. Since this exceptional case makes the subsequent estimate even better, we can safely ignore it.

With $\mathbf{D}_\sigma(\lambda)$ positive, we can have chosen to cut λ so that no σ -block “wraps around” the end of \mathbf{c} ; that is, so that $c_0 \neq \sigma(c_{L-1})$. Once \mathbf{c} has been so chosen, the decomposition is unique.

Upper-bounding disagreement

To establish (ζ4), there is no loss of generality in taking particular values for the parameters of our standing condition (??) and so we fix

$$J = 7 \text{ and } K = 21 .$$

In consequence, π comprises three 7-cycles.

For specificity, take one of the 7-cycles to be

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6$$

(and 6 → 0). The corresponding 7-cycle of σ is

$$20: \quad 0 \rightarrow 2 \rightarrow 4 \rightarrow 6 \rightarrow 1 \rightarrow 3 \rightarrow 5 .$$

Given an L-cycle λ with Dσ(λ) small, define its QK-name c as we did in the (??) paragraph.

σ-M-blocking λ. Having frozen a value for M, there are three “types” of σ-M-block on λ; one for each of the three 7-cycles of σ. Suppose that [ℓ .. ℓ+M) is a σ-M-block of type (??). That means, letting s denote the sequence 0246135, that

$$c_{[\ell .. \ell+M)} = \underbrace{\text{sssssss} \cdots \text{sss}}_{M \text{ positions}},$$

where this s...s represents a concatenation of copies of s, possibly ending (starting) with an initial (terminal) segment of s. Such segments have no effect on the observation below and so, for simplicity, the notation below presumes that “s...s” is exactly a concatenation of copies of s.

Thanks to this presumption, the last position of s...s is occupied by ‘5’. This is a “position of agreement”, so ‘5’ must be followed by ‘0’. We will write this trailing zero in slanted and enlarged font. Thus, along the name c, we witness occurrences of

$$\underbrace{? \text{sssssss} \cdots \text{sss} \mathbf{0}}_{M+2 \text{ positions}},$$

where ‘?’ indicates an unknown symbol in [0 .. 21).

π-M'-blocking ρ. Since $\frac{J+1}{2} = \frac{7+1}{2} = 4$, we consider $\rho := \text{Weave}_\lambda(4)$. How does the M-block s...s appear on the ρ cycle?

Figure ?? shows part of the Weaveλ(4) cycle. The σ-M-block upstairs zips together with the σ-M-block downstairs to form a π-block of length at least 2M - J.

The upshot is that for M an arbitrary positive integer,

$$22: \quad \mu(\pi\text{-}M'\text{-blocks on } \rho) \geq \frac{M'}{2M} \cdot \mu(\sigma\text{-}M\text{-blocks on } \lambda),$$

where M' is 2M - J.

Completing the proof of (ζ4): Picking δ

Since J, K and ε are known in advance, we can take M sufficiently Brobdingnagian that

$$23: \quad \frac{J}{2M} < \varepsilon; \quad \text{then let } \delta := \frac{\varepsilon}{M} .$$

Consider now an L-cycle λ, with L • K and with Dσ(λ) < δ. Courtesy of (??,??) above,

$$\mu(\pi\text{-blocks on } \rho) \geq [1 - \varepsilon] \cdot \mu(\sigma\text{-}M\text{-blocks on } \lambda) .$$

Furthermore,

$$\begin{aligned} \mu(\sigma\text{-}M\text{-blocks on } \lambda) &\geq 1 - M D_\sigma(\lambda) \\ &\geq 1 - \varepsilon , \end{aligned}$$

by (??b) and (??). Together, the two preceding displayed inequalities yield that

$$1 - D_\pi(\rho) \geq [1 - \varepsilon][1 - \varepsilon] \geq 1 - 2\varepsilon .$$

Consequently $2\varepsilon \geq D_\pi(\rho)$, which establishes (ζ4) and completes the proof that SQUARES is residual in Ω.

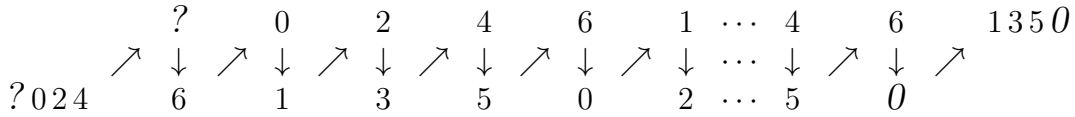


FIG. 21: Part of the Q_{21} -name of ρ : The upper line of shows the $M + 2$ string $?s \dots s0$ which, in the lower line, is shifted left by 4 positions. The arrows show how ρ weaves between the two lines.

§C Handling a general exponent e

We sketch, for a general exponent $2 \leq e < \infty$, the argument that $\wp_e(\Omega)$ is residual. For simplicity of notation, however, we will take $e = 17$; so each “16”, below, represents “ $e - 1$ ”.

Say that a positive integer J is **good** if $J \equiv -1$, modulo 17. Here, the good-cycles will play the role that the odd-cycles played in §??.

Creating combinatorial roots [bis]

Handed 17 sequences, $\mathbf{a}, \mathbf{b}, \dots, \mathbf{c}$, each of length L , define their alternation $\mathbf{a} : \mathbf{b} : \dots : \mathbf{c}$ to be the sequence

$$a_0 b_0 \dots c_0 a_1 b_1 \dots c_1 a_2 b_2 \dots c_2 \dots a_{L-1} b_{L-1} \dots c_{L-1},$$

whose length is $17L$.

Given an L -cycle λ , cut it to produce an L -sequence \mathbf{c} , as in (??). As before, a linear expression such as “ $17\mathbf{c} + 5$ ” means the L -sequence whose ℓ^{nd} number is $17c_\ell + 5$. For arbitrary rotation numbers r_1, \dots, r_{16} , define

$$\rho := \text{Weave}_\lambda(r_1, r_2, \dots, r_{16})$$

to be the cycle

$$(17\mathbf{c} : |17\mathbf{c} + 1|^{r_1} : |17\mathbf{c} + 2|^{r_2} : \dots : |17\mathbf{c} + 16|^{r_{16}}),$$

whose length is $17L$. Independent of what the rotation numbers are, the cycle structure of the composition ρ^{17} is

$$(17\mathbf{c})(17\mathbf{c} + 1)(17\mathbf{c} + 2) \dots (17\mathbf{c} + 16).$$

Thus transformation $[G_\rho]^{17}$ indeed equals G_λ , so permutation ρ is a combinatorial 17^{th} root of λ .

Standing Condition (??[bis]). We set $\sigma := \pi^{17}$ and $S := T^{17}$. As before, π comprises $\frac{K}{J}$ many J -cycles; and so does σ , since J is relatively prime to 17. We need but establish this version of ($\zeta 4$):

Given ε there is a δ so that for each $L \bullet K$ and each L -cycle λ :

$$D_\sigma(\lambda) < \delta \implies D_\pi(\rho) < 2\varepsilon$$

$\zeta 4$ [bis]:

where ρ is the $17L$ -cycle

$$\text{Weave}_\lambda(r, r, r, \dots, r)$$

$$\text{with } r := \frac{J+1}{17}.$$

With this value of r , the Reader may convince himself that the following analog of inequality (??) succeeds: For M arbitrary:

$$\mu(\pi\text{-}M'\text{-blocks on } \rho) \geq \frac{M'}{17M} \cdot \mu(\sigma\text{-}M\text{-blocks on } \lambda),$$

with $M' := 17M - F$, where F is some number which depends neither on L nor M . A straightforward estimate^{♥5} allows $F = [J + 1] \cdot 17$.

The final step is to grab an M sufficiently large that

$$\frac{F}{17M} < \varepsilon; \quad \text{then let } \delta := \frac{\varepsilon}{M}.$$

As before $1 - D_\pi(\rho) \geq 1 - 2\varepsilon$, which delivers the goods on ($\zeta 4$ [bis]).

^{♥5}In general, $F = [J + 1]e$ works. A fastidious analysis would justify $F = [J - 2][e - 1]$, once $M > J + 1$.

Reflections on the argument

The combinatorics used to show $\wp_2(\Omega)$ residual are elementary. The one non-elementary tool was (??), that analytic sets are almost-open. We could do without this theorem if we had a “yes” to this question.

Q1: Question. *Is $\wp_2(\Omega)$, the set of SQUARES, a Borel subset of Ω ?* \square

In the more general setting of a Polish semigroup, there is an example where the answer is known to be “no”. Humke and Laczkovich showed, in the Polish semigroup (under composition) of continuous functions from $[0, 1]^\circ$, that the set of composition squares $g \circ g$ is *not* Borel. (See [?]. Also see Beleznyay, [?].)

§D The power map is locally complex

Having shown that $\text{LOC DEN}(\wp_e)$ is dense in Ω , one would be singularly incurious to not inquire about density of its complement.

It turns out that the tools already developed are sufficient to show that \wp_e is “locally complex” in the sense of (??ab), below. Part (??a) is simply an embellishment of what we already know.

Use $\sqrt[e]{T}$ to denote the *collection* of e^{th} roots of T , i.e, the closed set $\wp_e^{-1}(T)$.

Locally lacunary. With respect to a mapping $f: X \rightarrow \Lambda$, a point $z \in X$ is **locally-lacunary** if it is not locally-dense. Equivalently: *There exists a neighborhood of z whose f -image is dense in no neighborhood of $f(z)$.* Let $\text{LOCLAC}(f)$ denote the set of locally-lacunary points of f .

24: Complexity Theorem. *For each integer $e \in [2.. \infty)$ and transformation T , the set $\sqrt[e]{T}$ is closed and nowhere-dense in Ω . Furthermore*

a: $\text{LOC DEN}(\wp_e)$ is residual. *Indeed, it is a dense \mathcal{G}_δ -subcollection of Ω .*

b: $\text{LOCLAC}(\wp_e)$, while meager, is dense.

Remark. Since $\sqrt[e]{T}$ is closed, that it is nowhere-dense follows immediately from noting that WEAK MIXING and ROTATIONS are disjoint families, each of which is Ω -dense and is sealed under taking e^{th} roots. (With \oplus meaning addition mod 1, the set ROTATIONS comprises all transformations isomorphic to some rotation $x \mapsto x \oplus r$, for some rotation number $r \in \mathbb{R}$.) \square

Since $\text{LOC DEN}(\wp_e)$ is Ω -dense, (??a) follows from this general assertion:

25: Lemma. *Suppose that $f: X \rightarrow \Lambda$ is continuous map from a metrizable space X (not necessarily separable) to a topological space Λ . Then $\text{LOC DEN}(f)$ is a \mathcal{G}_δ -subset of X .* \diamond

Proof. For a number $\alpha > 0$, let U_α comprise those points $z \in X$ such that: *There exists a positive $\varepsilon < \alpha$ for which $f(\text{Ball}_\varepsilon(z))$ is dense in some neighborhood of $f(z)$.*

Since $\text{LOC DEN}(f) = \bigcap_{\alpha \searrow 0} U_\alpha$, it will do to simply show that U_α is open. For demonstrating openness at a point $z \in U_\alpha$, take an $\varepsilon < \alpha$, then an open set $\Upsilon \ni f(z)$ such that $f(\text{Ball}_\varepsilon(z))$ is dense in Υ . Necessarily, the intersection

$$I := \text{Ball}_{\alpha-\varepsilon}(z) \cap f^{-1}(\Upsilon)$$

is an open neighborhood of z . We need but show that $I \subset U_\alpha$, as follows.

Fix a point $y \in I$ and let $r := \text{dist}(y, z)$. Then

$$\text{Ball}_{r+\varepsilon}(y) \supset \text{Ball}_\varepsilon(z),$$

and so the f -image of $\text{Ball}_{r+\varepsilon}(y)$ is dense in Υ . Therefore $y \in U_\alpha$, since $r + \varepsilon < \alpha$. ◆

Transmogrifying (??b) into Combinatorics

Following the strategy of §??, let us find a statement about permutations that will imply (??b). Also as earlier, since all the ideas appear in the $e = 2$ case we let \wp mean \wp_2 from now on,

It was essential in §?? that J was odd. Here, in §?? it is essential that J be even. Fix a large even number J and a J -cycle π . Let $\sigma := \pi^2$ and have U denote this ball:

$$26: \quad U := \text{Ball}_{\frac{1}{3}}(G_\pi), \quad \text{where the pseudo-metric used is } d_J.$$

We will show that

???: *The \wp -image of U fails to be dense in each and every neighborhood, Υ , of G_σ .*

Using $H := J/2$ to denote half of J , write our J -cycle π as

$$\underbrace{(\mathbf{a}_1 \mathbf{b}_1 \mathbf{a}_2 \mathbf{b}_2 \mathbf{a}_3 \mathbf{b}_3 \cdots \mathbf{a}_H \mathbf{b}_H)}_{\text{Some reordering of the numbers } [0..J].}$$

Its square, σ , has cycle structure $(\boldsymbol{\alpha})(\boldsymbol{\beta})$, two H -cycles, where

$$\begin{aligned} \boldsymbol{\alpha} &:= \mathbf{a}_1 \mathbf{a}_2 \mathbf{a}_3 \dots \mathbf{a}_H \quad \text{and} \\ \boldsymbol{\beta} &:= \mathbf{b}_1 \mathbf{b}_2 \mathbf{b}_3 \dots \mathbf{b}_H. \end{aligned}$$

We now *perturb* permutation σ to a nearby cycle, σ_K .

For each integer $K \blacktriangleright J$, define a K -cycle σ_K to be (\mathbf{AB}) , where

$$???: \quad \mathbf{A} := \underbrace{\boldsymbol{\alpha} \boldsymbol{\alpha} \boldsymbol{\alpha} \cdots \boldsymbol{\alpha}}_{\frac{K}{J} \text{ copies}} \quad \text{and} \quad \mathbf{B} := \underbrace{\boldsymbol{\beta} \boldsymbol{\beta} \boldsymbol{\beta} \cdots \boldsymbol{\beta}}_{\frac{K}{J} \text{ copies}}.$$

27: Lemma. *In the coarse topology, $G_{\sigma_K} \rightarrow G_\sigma$ as $K \nearrow \infty$.* ◆

Sketch of proof. Since the d_N -topologies $\nearrow \mathcal{C}$, we need but establish that

$$*: \quad \lim_{K \rightarrow \infty} d_N(G_{\sigma_K}, G_\sigma) = 0$$

for each N in some sequence $N \rightarrow \infty$; so fix an $N \blacktriangleright J$. Since $d_K \nearrow \mathcal{C}$, we only need prove (*) for, say, those values $K \blacktriangleright N$. Writing $K = kN$, then,

$$d_N(G_{\sigma_K}, G_\sigma) \leq \frac{1}{k \cdot \text{Length}(\boldsymbol{\alpha})} = \frac{1}{kH},$$

courtesy the Frequency Lemma argument. ◆

Defining property $\gamma(\pi, K)$. In what follows, parameters J , π and K are implicit. We write σ for π^2 . Phrases such as “For each/every/all $\rho \dots$ ” shall mean:

“For each $L \blacktriangleright K$ and each L -cycle $\rho \dots$ ”.

Lastly, λ is another name for ρ^2 .

PROPERTY $\gamma(\pi, K)$: There exists a positive δ so that, for each ρ :

$$\begin{aligned} \text{If } \mathbf{D}_{\sigma_K}(\lambda) < \delta, \\ \text{then } \mathbf{D}_\pi(\rho) \geq \frac{1}{3}. \end{aligned}$$

Remark. The value $\frac{1}{3}$, here and in (??), is conceptually $\frac{1}{2}$. We use $\frac{1}{3}$ to allow room for edge effects in the estimate to follow. \square

28: LocLAC Combinatorial Lemma. *If $\gamma(\pi, K)$ holds for all large (or just infinitely many) $K \blacklozenge J$, then transformation G_π is locally-lacunary for the squaring map.* \diamond

Proof. We verify (??'). Let $\delta(\cdot)$ be a function going to zero sufficiently eagerly that $\delta < \frac{1}{K}$ and $\gamma(\pi, K)$ holds, where –here and henceforth– we abbreviate $\delta = \delta(K)$.

Centered at G_{σ_K} , we would like to have a ball Γ_K of transformations so that for each λ :

$$**:\quad G_\lambda \in \Gamma_K \implies \mathbf{D}_{\sigma_K}(\lambda) < \delta.$$

So, courtesy the Frequency Lemma (??), letting

$$\Gamma_K := \mathbf{d}_K\text{-Ball}_{\delta(K)}(G_{\sigma_K}).$$

does the trick.

Handed an arbitrary \mathcal{C} -open set $\Upsilon \ni G_\sigma$, lemma ?? assures us that the Γ_K ball lies within Υ , once K is Brobdingnagian. (This uses that the \mathbf{d}_n -topologies tend to \mathcal{C} .) So establishing that $\wp(U)$ misses Γ_K is enough to confirm (??'). In consequence, this statement,

The intersection $U' := \wp^{-1}(\Gamma_K) \cap U$ is empty,

is what we wish to substantiate.

Restating (**), if $G_\rho \in \wp^{-1}(\Gamma_K)$ then $\mathbf{D}_{\sigma_K}(\lambda) < \delta$. So property $\gamma(\pi, K)$ delivers that $G_\rho \notin U$. Thus the \mathcal{C} -dense set

$$\left\{ G_\rho \mid \begin{array}{l} \rho \text{ is an } L\text{-cycle, for} \\ \text{some } L \blacklozenge K \end{array} \right\}$$

is disjoint from U' . In light of the fact that U' is \mathcal{C} -open, it must of needs be empty. \diamond

Demonstrating $\gamma(\pi, K)$ for large K

Choose an $L \blacklozenge K$ and an L -cycle ρ . Similar to the paragraph of (??), cut ρ to produce a Q_J -name

$$\mathbf{c} = c_0 c_1 c_2 c_3 \cdots c_{L-1},$$

and let \oplus mean addition modulo L . Recall that $1 - \mathbf{D}_\pi(\rho)$ is the probability that an index $\ell \in [0..L)$ satisfies

$$\pi(c_\ell) = c_{\ell \oplus 1},$$

that is, is a position of agreement of the Q_J -structures of ρ and π .

Here now is the idea behind the proof of $\gamma(\pi, K)$.

29: Lemma. *For each ε positive, for all large K , for each cycle ρ with $\mathbf{D}_{\sigma_K}(\rho) < \delta$, the following holds:*

With probability exceeding $1 - \varepsilon$, if an index ℓ is a position of agreement of ρ with π , then $\ell \oplus K$ is a position of disagreement.

In particular, property $\gamma(\pi, K)$ holds once ε is small enough. \diamond

Proof of (??). Call a word \mathbf{w} an “**AB**-block” if, using the words from (??'), it is a concatenation

$$\mathbf{w} = \mathbf{ABABAB} \cdots \mathbf{AB}$$

of consecutive copies of **AB**, possibly starting or ending with a partial copy.

Recall that **A** is a concatenation of copies of word $\mathbf{a}_1 \cdots \mathbf{a}_H$, as **B** is of $\mathbf{b}_1 \cdots \mathbf{b}_H$. Let a prime, $'$, flip a letter to the opposite letter having the same index; so \mathbf{a}'_5 means \mathbf{b}_5 , and \mathbf{b}'_5 means \mathbf{a}_5 .

Since words **A** and **B** each have length $K/2$, every **AB**-block \mathbf{w} is *anti*-periodic with period $K/2$, in this sense:

$$w_{i+\frac{K}{2}} = w'_i,$$

whenever both indices i and $i + \frac{K}{2}$ are in \mathbf{w} .

σ_K -blocking the cycle λ

The Q_J -structure of $\lambda = \rho^2$ is $(\mathbf{c}^{\text{Even}})(\mathbf{c}^{\text{Odd}})$, where

$$\begin{aligned}\mathbf{c}^{\text{Even}} &:= c_0 c_2 c_4 c_6 \cdots c_{L-2} \\ \mathbf{c}^{\text{Odd}} &:= c_1 c_3 c_5 c_7 \cdots c_{L-1}.\end{aligned}$$

Let the symbol $\mathbf{c}_{[7..13]}^{\text{Even}}$ mean the subsequence of \mathbf{c}^{Even} with indices in the interval $[7..13]$. In this example,

$$\mathbf{c}_{[7..15]}^{\text{Even}} = c_8 c_{10} c_{12} c_{14} \quad \text{and} \quad \mathbf{c}_{[7..15]}^{\text{Odd}} = c_7 c_9 c_{11} c_{13} c_{15},$$

where, for $\mathbf{c}_{[7..15]}^{\text{Odd}}$, we have made the analogous definition.

Now suppose $K = 6$. Then walking $\frac{K}{2} = 3$ steps along \mathbf{c}^{Odd} brings us from c_7 to c_{13} , i.e, to c_{7+K} . So the above antiperiodicity give this generalization, for every $\ell \in [0..L)$:

*If $\mathbf{c}_{[\ell.. \ell+K]}^{\text{Even}}$ and $\mathbf{c}_{[\ell.. \ell+K]}^{\text{Odd}}$ are each **AB**-blocks, then*

$$c_{\ell+K} = c'_\ell.$$

Lower-bounding disagreement

Since ε and K are known in advance, we can take δ small enough^{♥6} that inequality $\mathbf{D}_{\sigma_K}(\lambda) < \delta$ implies the following:

With probability exceeding $1 - \varepsilon$, an index ℓ in $[0..L)$ satisfies the following:

: Sequences $\mathbf{c}_{[\ell.. \ell+1+K]}^{\text{Even}}$ and $\mathbf{c}_{[\ell.. \ell+1+K]}^{\text{Odd}}$ are each **AB-blocks.*

Finally, suppose that such an ℓ is a position of agreement of ρ with π . If c_ℓ is in **A**, say $c_\ell = \mathbf{a}_5$, then $c_{\ell+1} = \pi(\mathbf{a}_5) = \mathbf{b}_5$. Consequently, by (*),

$$\begin{aligned}c_{\ell+K} &= \mathbf{a}'_5 = \mathbf{b}_5 \quad \text{and} \\ c_{\ell+1+K} &= \mathbf{b}'_5 = \mathbf{a}_5.\end{aligned}$$

But $\pi(c_{\ell+K}) = \pi(\mathbf{b}_5) = \mathbf{a}_6$ (well... the 6 is actually to be taken modulo H). Consequently,

$$\pi(c_{\ell+K}) \neq \mathbf{a}_5 = c_{\ell+1+K}.$$

Thus position $\ell + K$ is a position of disagreement between ρ and π .

A similar argument goes through if c_ℓ is in **B**. Thus we have established (??'). This wraps up the proof of (??a) of the Complexity theorem. \blacklozenge

^{♥6}Letting δ be $[\varepsilon/[20K]]^4$ works. This uses the argument of the Blocking lemma, (??b).

§E Egress

Questions in Newtonian mechanics lead to dynamical systems in which “time is real”; the systems are \mathbb{R} -actions (flows $\varphi: \mathbb{I} \times \mathbb{R} \rightarrow \mathbb{I}$) rather than the \mathbb{Z} -actions studied in the current article.

Q2: Question. *Does the generic transformation embed in a flow? Is this set*

$$\left\{ T \mid T(\cdot) = \varphi(\cdot, 1) \text{ for some flow } \varphi \text{ on } \mathbb{I} \right\}$$

of transformations, a residual subset of Ω ? □

For such a T , the set of those transformations S which commute with T , the **commutant** of T , includes a copy of \mathbb{R} . So an inexpensive “no” to (Q2) would follow from showing that only a meager set of T have an uncountable commutant.

Alas, the generic T is rank-1 and rigid, thus necessarily has commutant which is uncountable. ♥7

Q3: *Does the generic T embed in a (measure-preserving) \mathbb{Q} -action?* □

For a $T \in \text{RAO}$, how close does the RAO Theorem come to answering (Q3)? Certainly, for each n , we can pick an n^{th} root R_n of T , then fix a set $\mathcal{S} \subset [2.. \infty)$ and look at the group $G_{\mathcal{S}} \subset \Omega$ which is generated by $\{R_n\}_{n \in \mathcal{S}}$. However, the RAO theorem gives no guarantee that R_n goes to the identity, as $n \rightarrow \infty$. So RAO does not give us control, in terms of \mathcal{S} solely, on the topology of $G_{\mathcal{S}}$. This is the reason that the groups below are equipped with the “no restriction” (i.e, discrete) topology.

Fixing K , let \mathbb{Q}_K be the additive subgroup of the rationals generated by $1/p^K$ as p ranges over all the primes; equip \mathbb{Q}_K with the discrete topology. Call each p^K a “ **K -prime**”.

Evidently \mathbb{Q}_K comprises all ratios

$$n / [p_1^{k_1} p_2^{k_2} \cdots p_J^{k_J}],$$

♥7 Katok and Stepin showed, in [?], that “rank-1 and rigid” is generic, although using a different language. Definitions of *rank-1* and of *rigid* appear in [?]. That rigidity implies uncountable commutant appears in [?] and [?].

where n is an arbitrary integer and each $k_j \in [0.. K]$.

30: Theorem. *The generic T extends to a \mathbb{Q}_K -action.* ♦

Proof. It suffices to fix a T in

$$31: \quad \text{WEAKMIXING} \cap \text{RANK-1} \cap \text{RAO}$$

and extend it to a \mathbb{Q}_K -action.

For each K -prime γ , let R_γ be a γ^{th} root of T . Let G_K be the subgroup of (Ω, \circ) generated by the R_γ transformations. Since T is rank-1, its commutant is abelian^{♥8} and thus G_K is abelian.

To show that G_K is isomorphic to \mathbb{Q}_K , define a map ψ from (G_K, \circ) to $(\mathbb{Q}_K, +)$ as follows. For each finite set of K -primes $\{\alpha, \beta, \dots, \gamma\}$, and of integers a, b, \dots, c , let

$$\psi(R_\alpha^a \circ R_\beta^b \circ \dots \circ R_\gamma^c) := \frac{a}{\alpha} + \frac{b}{\beta} + \dots + \frac{c}{\gamma}.$$

That this ψ is a group isomorphism will follow immediately once ψ is shown to be well defined.

To address this latter aim, suppose that exponents a, \dots, c cause $S := R_\alpha^a \circ \dots \circ R_\gamma^c$ to be the identity transformation. Letting L be the product $\alpha \cdots \gamma$, then $S^L = T^k$, where

$$k := a \frac{L}{\alpha} + \dots + c \frac{L}{\gamma} \stackrel{\text{note}}{=} L \cdot \left[\frac{a}{\alpha} + \dots + \frac{c}{\gamma} \right].$$

Since T is weak-mixing it cannot be periodic, so k must be zero. Thus $\frac{a}{\alpha} + \dots + \frac{c}{\gamma}$ is zero. ♦

Root chains. Related to (Q3) is this: *Does the generic T extend to a \mathbb{Q}_∞ -action?* Here, \mathbb{Q}_∞ is the group of rationals $(\mathbb{Q}, +)$, but equipped with the discrete topology.

In light of the foregoing theorem, what is the obstruction to fabricating a \mathbb{Q}_∞ -action? If, for

♥8 Although this follows from the Weak-Closure theorem, [?], there is a generic subset of RANK-1 –the maps with “flat stacks”– where abelianness of the commutant follows by an elementary argument.

each prime p , we can produce an infinite length “ p -chain”

$$T =: S_0 \xleftarrow{p} S_1 \xleftarrow{p} S_2 \xleftarrow{p} \dots$$

where each S_{k+1} is a p^{th} root of S_k , then a \mathbb{Q}_∞ -action can be build as above. Thus one is led to ask:

Q4: *Does there exist a weak-mixing T which has square-root chains of each finite length, but no infinite square-root chain?* \square

I raised this question at the Ergodic Theory seminar while on sabbatical at U. of Toronto, in 1996-1997. The menagerie of examples and techniques from the 1960&70’s suggested a “yes” to (Q4). One natural approach, harking back to Ornstein’s construction, is the “counterexample machine” built by Dan Rudolph, which uses the rank-1 mixing map of Ornstein.

Vaguely, Rudolph’s machine takes a permutation of \mathbb{Z} , and produces a weak-mixing transformation with analogous properties. A standard approach to (Q4), then, would be to search the group of \mathbb{Z} -permutations for:

A permutation π of \mathbb{Z} which has arbitrarily long square-root chains, but no infinite chains.

Alas, the Reader can verify that no such π exists.

Techniques of del Junco and others.

Nonetheless, ideas of the counterexample machine can be used. Andrés del Junco developed machinery, for certain abelian groups G , which produces a G -action $\varphi: \mathbb{I} \times G \rightarrow \mathbb{I}$ for which the commutant of certain transformations in the action is limited to the G -action itself.

This suggested first constructing a denumerable abelian group (M, \boxplus, e) and element $\eta \in M$ such that η has square-root chains of each finite length, but has no infinite chain. Here is one such group, the **Madore group**:

Let M be the free abelian group on symbols (generators) $\eta, \gamma_1, \gamma_2, \dots$, where the generating relations are

$$32: \quad \underbrace{\gamma_j \boxplus \gamma_j \boxplus \dots \boxplus \gamma_j}_{2^j \text{ copies}} = \eta, \quad \text{for } j = 1, 2, \dots$$

We now describe M in an alternative way.

Let G_j be the additive cyclic group $[0 .. 2^j)$; that is, $\mathbb{Z}/2^j\mathbb{Z}$. As a set, define M to be the *direct sum*

$$33: \quad M := \mathbb{Z} \oplus G_1 \oplus G_2 \oplus \dots$$

So M comprises all tuples $\langle a \mid g_1, g_2, \dots \rangle$ where $a \in \mathbb{Z}$ and $g_j \in G_j$, and only finitely many of the g_j are non-zero. Given $\alpha := \langle a \mid g_1, g_2, \dots \rangle$ and $\beta := \langle b \mid h_1, h_2, \dots \rangle$, let N be smallest natural number with $g_n = h_n = 0$, for all $n > N$. Define addition in M by

$$\alpha \boxplus \beta := \left\langle a + b + \sum_{j=1}^N c_j \mid r_1, r_2, \dots \right\rangle,$$

where c_j is the j^{th} “carry” in group $[0 .. 2^j)$, and r_j is the remainder. That is

$$g_j + h_j = r_j + 2^j c_j, \quad \text{where } r_j \in [0 .. 2^j) \text{ and } c_j \text{ is either 0 or 1.}$$

Thus \boxplus is component-wise addition, with a carry from the j^{th} component into the $(j+1)^{\text{th}}$ component. Evidently M is abelian with $e := \langle 0 \mid 0, \dots \rangle$ its neutral element.

To write down an additive inverse, $\boxminus \alpha$, let J be the number of indices j with $g_j \neq 0$. Then

$$\boxminus \alpha = \left\langle -[a + J] \mid f_1, f_2, f_3, \dots \right\rangle,$$

where f_j is the G_j -inverse of g_j . So f_j is $2^j - g_j$, if $g_j \neq 0$, and is zero otherwise.

Identify $\langle k \mid 0, \dots \rangle$ with the integer k , thus exhibiting a copy of $(\mathbb{Z}, +)$ inside of (M, \boxplus) . Our M is generated by the collection $\{\eta, \gamma_1, \gamma_2, \dots\}$, where

$\eta := \langle 1 \mid 0, 0, 0, 0, 0, 0, \dots \rangle$	The 1 is in the zeroth position.
$\gamma_j := \langle 0 \mid 0, \dots, 0, 1, 0, \dots \rangle$	This 1 is in j^{th} position.

Since γ_j is a 2^j -th root of η , one sees that (??) with operation \boxplus is the same group as defined by (??).

Fixing j , there is a square-root chain

$$\eta \leftarrow 2^{j-1}\gamma_j \leftarrow 2^{j-2}\gamma_j \leftarrow \dots \leftarrow 4\gamma_j \leftarrow 2\gamma_j \leftarrow \gamma_j$$

of length j . Yet one can check that no element in $M \setminus \{e\}$ has an infinite chain.

Answering “yes” to (Q4). Blair Madore, a student of del Junco, proved the following theorem as part of his doctoral travails.

34: Madore’s Theorem (Theorem 1.1 in [?]). *Let G be a countable abelian group with subgroup \mathbb{Z}^d , for some $d \geq 1$, where each element of the quotient group G/\mathbb{Z}^d has finite order. Then there exists a rank-one action of G so that the transformation T corresponding to $(1, 0, 0, \dots, 0)$ in \mathbb{Z}^d is mixing, simple, and only commutes with the other transformations in G .* \diamond

In particular, there is such an action φ of the Madore group. With η meaning $\langle 1 \mid 0, 0, \dots \rangle$, then, $T := \varphi^\eta$ is a mixing transformation having no infinite square-root chain.

Conditions implying a \mathbb{Q}_∞ extension. Various general results would imply that the generic \mathbb{Z} -action extends to an action of the discrete rationals.

Q5: *Generically, does T have at most one square-root?* \square

If a map T in (??) had, for each j , at most one j^{th} root, then the proof of (??) would extend T to a unique \mathbb{Q}_∞ -action.

Note that (Q5) is equivalent to this query: *For the generic rank-1 map T , is the identity map the only involution commuting with T ?*

Closing thoughts. The RAO theorem was proved under the aegis of the coarse topology on Ω . Because the set of maps with RAO is an analytic set, the Equivalence Theorem of [?, thm.7] applies to say that RAO is also residual in another standard setting, the Polish space of shift-invariant Borel probability measures on the Hilbert cube $[0, 1]^{\mathbb{Z}}$.

It may well turn out that there are more general equivalence theorems, and that settings whose topology is more natural for the transformations arising in physics nonetheless have the same abstract genericity properties.

§F Questions File

(This are additional questions and are not part of the “Roots” article.)

Question Q1. Is there a trn T which has a square-root chain,

$$T \leftarrow T_1 \leftarrow \dots \leftarrow T_N,$$

for each N , but has *no* infinite square-root chain? \square

Question Q2. Does there exist a permutation π of \mathbb{N} which has square-root chains of all finite lengths, but no infinite chain? (Almost certainly, “No” –simple details need to be checked.) \square

Example 2. Here is a denumerable group M , and element η , so that η has all finite square-root chains, but no infinite chain. The only infinite chain is $e \leftarrow e \leftarrow \dots$, where e is the identity element,

Let M be the free abelian group on symbols (generators) $\eta, \gamma_1, \gamma_2, \dots$, where the generating relations are

$$35: \quad [\gamma_j]^{2^j} = \eta, \quad \text{for } j = 1, 2, \dots$$

We now describe M in an alternative way.

Let G_j be the additive cyclic group $[0..2^j]$; that is, $\mathbb{Z}/2^j\mathbb{Z}$. As a set, let M be the *direct sum*

$$36: \quad M := \mathbb{Z} \oplus G_1 \oplus G_2 \oplus \dots$$

So M comprises all tuples $\langle a \mid g_1, g_2, \dots \rangle$ where $a \in \mathbb{Z}$ and $g_j \in G_j$, and only finitely many of the g_j are non-zero. Given $\alpha := \langle a \mid g_1, g_2, \dots \rangle$ and $\beta := \langle b \mid h_1, h_2, \dots \rangle$, let N be smallest natural so that $g_n = h_n = 0$, for all $n > N$. Define addition in M by

$$\alpha \boxplus \beta := \left\langle a + b + \sum_{j=1}^N c_j \mid r_1, r_2, \dots \right\rangle,$$

where c_j is the j^{th} “carry” in group $[0..2^j]$. That is

$$g_j + h_j = r_j + c_j \cdot 2^j, \quad \text{with } r_j \in [0..2^j].$$

Thus \boxplus is component-wise addition, with a carry from the j^{th} component into the $(j+1)^{\text{th}}$ component. Evidently M is abelian with $e := \langle 0 \mid 0, \dots \rangle$ its neutral element.

To write down an additive inverse, $\boxminus \alpha$, let J be the number of indices j with $g_j \neq 0$. Then

$$\boxminus \alpha = \left\langle -[a + J] \mid f_1, f_2, f_3, \dots \right\rangle,$$

where f_j is the G_j -inverse of g_j . So f_j is $2^j - g_j$, if $g_j \neq 0$, and is zero otherwise.

Identify $\langle n \mid 0, \dots \rangle$ with the integer n ; this is a copy of $(\mathbb{Z}, +)$ in (M, \boxplus) . Our M is generated by the collection $\{\eta, \gamma_1, \gamma_2, \dots\}$, where

$\eta := \langle 1 \mid 0, 0, 0, 0, \dots \rangle$	This 1 is in the zero-th position.
$\gamma_j := \langle 0 \mid 0, \dots, 0, 1, 0, \dots \rangle$	The 1 is in j^{th} position.

Since γ_j is a 2^j -th root of η , one sees that (??) with \boxplus is the same group as defined by (??).

Fixing j , there is a square-root chain

$$\eta \leftarrow 2^{j-1}\gamma_j \leftarrow 2^{j-2}\gamma_j \leftarrow \dots \leftarrow 2\gamma_j \leftarrow \gamma_j$$

of length j . Yet one can check that no element in $M \setminus \{e\}$ has an infinite chain.

For an arbitrary element $\gamma \in M$, for each j , note that γ^{2^j} has a j^{th} component of zero. Thus

If an element δ has a non-zero j^{th} component, then this element has no 2^j -th root. Hence it has no square-root j -chain.

Consequently, no (non-identity) element of M has an infinite chain. After all, from a non-zero integer n , the longest an *integer*-chain can be is k , where $2^k \parallel n$. And once a square-root chain enters the non-integers, say at δ , its length has a fixed bound (which depends on δ). □

Question Q3. How does the squaring map on Ω interact with RANK-1?

A generic T is rank-1 and, if the later argument is correct, has roots of all orders. Since $C(T)$ is necessarily abelian, all of T 's roots commute. If we could show that T had infinite chains, then T would live inside a \mathbb{Q} -action. □

Observation 4. Let \mathbb{Q}_K be the (additive) subgroup of the rationals generated by $1/p^K$, as p ranges over the primes; call p^K a “ K -prime”. \mathbb{Q}_K comprises fractions $n/[p_1^{k_1} \cdots p_j^{k_j}]$, where each k_j is in $[0..K]$.

For each K ,

The generic T lives inside a \mathbb{Q}_K -action.

To see this, fix a rank-1 T which has roots of all orders. For each K -prime p , let S_p be a p^{th} root of T . Let G_K be the abelian (T is rank-1) group generated by all the S_p . Define a mapping $\varphi: G_K \rightarrow \mathbb{Q}_K$ by

$$S_p^a S_q^b \cdots S_r^c \mapsto \frac{a}{p} + \frac{b}{q} + \cdots + \frac{c}{r} = \frac{\gamma}{pq \cdots r}$$

where $\gamma := aN_p + bN_q + \cdots + cN_r$.

In the last expression, N_p is the product of all the K -primes *except* p . To show this well defined,

suppose φ sends $S_p^a \cdots S_r^c$ to zero, i.e., $\gamma = 0$. Now p divides 0 and $bN_q + \cdots + cN_r$, yet p is co-prime to N_p . So we can write $a = Ap$, for some integer A . Similarly we write $b = Bq, \dots$ and $c = Cr$. In consequence,

$$S_p^a \cdots S_r^c = T^A \cdots T^C.$$

But this last transformation equals Id , since

$$A + \cdots + C = \frac{a}{p} + \cdots + \frac{c}{r}$$

which is zero. Lastly, since φ is well-defined, it trivially is a homomorphism from (G_K, \circ) onto $(\mathbb{Q}_K, +)$. \square

Question Q4. Does the generic T have a **unique** square-root? Since generically $C(T)$ is abelian, if S_i are distinct square-roots of T , then $S_0 S_1^{-1}$ is a non-trivial involution. So the question above is equivalent to:

Does the generic rank-1 have no involutions in its commutant?

If so, then since T has dyadic roots of all orders, in has an infinite square-root chain. If $C(T)$ had *no* e -periodic members, then T has infinite e^{th} -root chain, for $e = 2, 3, \dots$. Then the above argument would show that T lives inside a \mathbb{Q} -action; indeed, a unique \mathbb{Q} -action. \square

Question Q5. Does the generic T live in a flow?

Is the generic flow Φ determined by its time-1 map? \square

Question Q6. Suppose that T and R are arbitrary maps. For the squaring map \wp : If $\wp(\text{Ball}_r(R))$ misses $\text{Ball}_{2\epsilon}(T)$, does a sufficiently small δ force $\wp(\text{Ball}_{r+\delta}(R))$ to miss $\text{Ball}_\epsilon(T)$? \square

Question Q7. For a weak-mixing T , under what circumstances is $\sqrt[e]{T}$ compact? \square