Gödel Diffeomorphisms

Matthew Foreman[*][†]

November 11, 2020

Abstract

A basic problem in smooth dynamics is determining if a system can be distinguished from its inverse, i.e., whether a smooth diffeomorphism T is isomorphic to T^{-1}. We show that this problem is sufficiently general that asking it for particular choices of T is equivalent to the validity of well-known number theoretic conjectures including the Riemann Hypothesis and Goldbach's conjecture. Further one can produce computable diffeomorphisms T such that the question of whether T is isomorphic to T^{-1} is independent of ZFC.

Contents

[*]University of California, Irvine.

[†]Foreman's research was supported by the National Science foundation grant DMS-1700143

1 Introduction

When is forward time isomorphic to backward time for a given dynamical system? When the acting group is $\mathbb{Z}$, this asks when a transformation T is isomorphic to its inverse. It was not until 1951, that Anzai [2] refuted a conjecture of Halmos and von Neumann ([19]) by exhibiting the first example of a transformation where T is not measure theoretically isomorphic to its inverse.[1] In fact the general problem is so complex that it cannot be be resolved using an arbitrary countable amount of information: in [14], it was shown that the collection of ergodic Lebesgue measure preserving diffeomorphisms of the 2-torus isomorphic to their inverse is complete analytic and hence not Borel.

In this paper we show that for a broad class of problems there is a one-to-one computable method of associating a Lebesgue measure preserving diffeomorphism T_P of the two-torus to each problem P in this class so that:

- P is true

if and only if

- T_P is measure theoretically isomorphic to T_P^{-1}.

The class of problems is large enough to include the *Riemann Hypothesis*, *Goldbach's Conjecture* and statements such as "*Zermelo-Frankel Set Theory (***ZFC***) is consistent.*" In consequence, each of these problems is equivalent to the question of whether $T \cong T^{-1}$ for the diffeomorphism T of 2-torus canonically associated to that problem.

Restating this, there is an ergodic diffeomorphism of the two-torus $T_{\mathbf{RH}}$ such that $T_{\mathbf{RH}} \cong {T_{\mathbf{RH}}}^{-1}$ if and only if the Riemann Hypothesis holds, and a different, non-isomorphic ergodic diffeomorphism $T_{\mathbf{GC}}$ such that $T_{\mathbf{GC}} \cong {T_{\mathbf{GC}}}^{-1}$ if and only if Goldbach's conjecture holds, and so forth.

Gödel's Second Incompleteness Theorem states that for any recursively axiomatizable theory Σ that is sufficiently strong to prove basic arithmetic facts, if Σ proves the statement "Σ *is consistent*", then Σ is in fact *inconsistent*. The statement "Σ is consistent" can be formalized in the manner of the problems we consider. Consider the most standard axiomatization for mathematics: Zermelo-Frankel Set Theory with the Axiom of Choice and the formalization of its consistency, the statement Con(ZFC).

If $T_{\mathbf{ZFC}}$ is the diffeomorphism associated with Con(ZFC) then (assuming the consistency of conventional mathematics) the question of whether $T_{\mathbf{ZFC}} \cong {T_{\mathbf{ZFC}}}^{-1}$ is independent of Zermelo-Frankel Set Theory—that is, it cannot be settled with the usual assumptions of mathematics.

One can compare this with more standard independence results, the most prominent being the Continuum Hypothesis. Those independence results inherently involve comparisons between and

[1] See for example Math Review MR0047742 where Halmos states "By constructing an example of the type described in the title the author solves (negatively) a problem proposed by the reviewer and von Neumann [Ann. of Math. (2) 63, 332–350 (1942); MR0006617]."

properties of uncountable objects. The results in this paper are about the relationships between finite computable objects.

We now give precise statements of the main theorem and its corollaries. The machinery for proving these results combines ergodic theory and descriptive set theory with logical and meta-mathematical techniques originally developed by Gödel. While the statements use only standard terminology, it is combined from several fields. In an arXiv preprint of this paper ([9]) there are several appendices in an attempt to convey this background to non-experts.

There are several standard references for connections between non-computable sets and analysis and PDE's. We note one in particular with results of Marian Pour-El and Ian Richards that give an example of a wave equation with computable initial data but no computable solution [25].

1.1 The Main Theorem

As an informal guide to reading the theorem, we say a couple of words. More formal definitions appear in later sections.

- A function F being computable means that there is a computer program that on input N outputs $F(N)$.
- The diffeomorphisms in the paper are taken to be C^∞ and Lebesgue measure preserving. A diffeomorphism $T : \mathbb{T}^2 \to \mathbb{T}^2$ is computable if there is a computer program that when serially fed the decimal expansions of a pair $(x, y) \in \mathbb{T}^2$ outputs the decimal expansions of $T(x, y)$ and for each n there is a computable function computing the decimal expansion of the modulus of continuity of the n-th differential.[2] Since computable functions have codes, computable diffeomorphisms also can be coded by natural numbers.
- By isomorphism, it is meant *measure isomorphism*. Measure preserving transformations $S : X \to X$ and $T : Y \to Y$ are measure theoretically isomorphic if there is a measure isomorphism $\varphi : X \to Y$ such that
$$S \circ \varphi = T \circ S$$
up to a sets of measure zero.
- We use the notation $\text{Diff}^\infty(\mathbb{T}, \lambda)$ for the collection of C^∞ measure-preserving diffeomorphisms of $\mathbb{T}^2$.
- Π^0_1 statements are those number-theoretic statements that start with a block of universal quantifiers and are followed by Boolean combinations of equalities and inequalities of polynomials with natural number coefficients.
- We fix Gödel numberings: computable ways of enumerating Π^0_1 statements $\langle \varphi_n : n \in \mathbb{N} \rangle$ and computer programs $\langle C_m : m \in \mathbb{N} \rangle$. The *code* of φ_n is n, the *code* of C_m is m.
- Older literature uses the word *recursive* and more recent literature uses the word *computable* as a synonym. We use the latter in this paper. Indeed, since none of the phenomenon discussed here involve recursive behavior that is not primitive recursive we use *effective*, and *computable* as synonyms for *primitive recursive.*

[2] Recent work of Banerjee and Kunde in [3] allow Theorem 1 to be extended to real analytic functions by improving the realization results in [13].

Here is the statement of the main theorem.

Theorem 1. (Main Theorem) *There is a computable function*

$$F : \{\textit{Codes for } \Pi^0_1\textit{-sentences}\} \to \{\textit{Codes for computable diffeomorphisms of } \mathbb{T}^2\}$$

such that:

1. *N is the code for a true statement if and only if $F(N)$ is the code for T, where T is measure theoretically isomorphic to T^{-1};*
2. *For $M \neq N$, $F(M)$ is not isomorphic to $F(N)$.*

The diffeomorphisms in the range of F are Lebesgue measure preserving and ergodic.

We now explicitly draw corollaries.

Corollary 2. *There is an ergodic diffeomorphism of the two-torus $T_{\mathbf{RH}}$ such that $T_{\mathbf{RH}} \cong T^{-1}_{\mathbf{RH}}$ if and only if the Riemann Hypothesis holds.*

Similarly:

Corollary 3. *There is an ergodic diffeomorphism of the two-torus $T_{\mathbf{GC}}$ such that $T_{\mathbf{GC}} \cong T^{-1}_{\mathbf{GC}}$ if and only if Goldbach's Conjecture holds.*

There are at least two reasons that this theorem is not trivial. The first is that the function F is computable, hence the association of the diffeomorphism to the Π^0_1 statement is canonical. Secondly the function is one-to-one; $T_{\mathbf{RH}}$ encodes the Riemann hypothesis and $T_{\mathbf{GC}}$ encodes Goldbach's conjecture and $T_{\mathbf{RH}} \not\cong T_{\mathbf{GC}}$.

Corollary 4. *Assume that* **ZFC** *is consistent. Then there is a computable ergodic diffeomorphism T of the torus such that T is measure theoretically isomorphic to T^{-1}, but this is unprovable in Zermelo-Frankel set theory together with the Axiom of Choice.*

We note again that there is nothing particularly distinctive about Zermelo-Frankel set theory with the Axiom of Choice. We choose it for the corollary because it forms the usual axiom system for mathematics. Thus Corollary 4 states an independence result in a classical form. Similar results can be drawn for theories of the form "**ZFC** + there is a large cardinal" or simply ZF without the Axiom of Choice.

Finally, these results can be modified quite easily to produce diffeomorphisms of (e.g.) the unit disc with the analogous properties. Moreover techniques from the thesis of Banerjee ([4]) and Banerjee-Kunde ([3]) can be used to improve the reduction F so that the range consists of real analytic maps of the 2-torus.

We finish this section by thanking Tim Carlson for asking whether Theorem 1 can be extended to lightface Σ^1_1 statements, which it can in a straightforward way. This increases the collection of statements encoded into diffeomorphisms to include virtually all standard mathematical statements.

Primitive recursion Informally, primitive recursive functions are those that can be computed by a program that uses only *for* statements and not *while* statements. This means that the computational time can be bounded constructively using iterated exponential maps. In the statements of the results we discuss "computable functions" but in fact all of the functions constructed are primitive recursive. In particular the functions and computable diffeomorphisms asserted to exist in Theorem 1 are primitive recursive.

1.2 Hilbert's 10th problem

Hilbert's 10th problem asks for a general algorithm for deciding whether Diophantine equations have integer solutions. The existence of such an algorithm was shown to be impossible by a succession of results of Davis, Putnam and Robinson culminating a complete solution by Matijasevič in 1970 ([21, 6]).

Their solution can be recast as a statement very similar to Theorem 1:

> There is a computable function
>
> $$F : \{\text{Codes for } \Pi^0_1\text{-sentences}\} \to \{\text{Diophantine Polynomials}\}$$
>
> such that N is the code for a true statement if and only if $F(N)$ has no integer solutions.

Thus their theorem reduces general questions about the truth of Π^0_1 statements to questions about zeros of polynomials. Theorem 1 states that there is an effective reduction of the true Π^0_1 statements to C^∞ transformations isomorphic to their inverse.

1.3 Why $\mathbb{Z}$? Why $\mathbb{T}^2$? Why C^∞?

The short answer is that we want to work in the simplest, best behaved and most classical context.

Physical systems are often modeled by ordinary differential equations on a smooth compact manifold M. Solutions are formalized as dynamical systems:

$$\varphi : \mathbb{R} \times M \to M$$

such that $\varphi(s, \varphi(t, x_0)) = \varphi(s+t, x_0)$ and $\varphi(s, \cdot) : M \to M$ is measure preserving.

Doing repeated experiments in a physical realization of such a system—say to measure a constant of interest such as the average value of an L^1 function on M—is viewed as measuring $\varphi(t_0, x_0), \varphi(t_0 + t_0, x_0), \ldots \varphi((N-1)t_0, x_0)$ and averaging: $\frac{1}{N}\sum_i f(\varphi(i * t_0, x_0))$. Provided that the system is sufficiently mixing ("ergodic"), the Ergodic Theorem implies that for almost every x_0 the averages along trajectories converge to the integral of f over N.

Thus empirical experiments are construed as sampling along portions of a $\mathbb{Z}$-action given by:

$$\psi(n, x_0) = \varphi(nt_0, x_0).$$

The manifold is required to be compact to avoid wild behavior and asked to be of the smallest possible dimension. Dimension one is impossible because there are very few conjugacy classes of measure preserving diffeomorphisms on one dimensional manifolds. On the unit circle there are exactly two.

Thus we move to two dimensional compact manifolds. The most convenient choice is $\mathbb{T}^2$, the two torus.

As k increases, the behavior of C^k diffeomorphisms becomes more regular–the behavior of C^1-diffeomorphisms can be quite wild. Thus the theorem involves C^∞-diffeomorphisms because it illustrates that the basic issue is not how wild the diffeomorphism is.

It could be argued that the tamest situation of all involves real analytic transformations of the 2-torus. The results in this paper can be extended to real-analytic maps using the work of Banerjee and Kunde [3].

In Summary We are proving that the question of forward vs. backward time encodes some of the most complex problems in mathematics. This claim is made stronger by taking the simples possible context: time is given by a $\mathbb{Z}$-action, $\mathbb{T}^2$ is the simplest, most concrete manifold possible, and the diffeomorphisms in question are the most regular possible.

1.4 Π^0_1-sets and Gödel numberings

While the interesting corollaries of Theorem 1 are about the Riemann Hypothesis, other number theoretic statements, and independence results for dynamical systems, it is actually a theorem about subsets of $\mathbb{N}$. In order to prove it, one has to provide a way of translating between the interesting mathematical objects as they are usually constructed and the natural numbers that encode them. This is done by means of *Gödel numberings*, natural numbers which *code* the structure of familiar mathematical objects.

The arithmetization of syntax via *Gödel Numbers* is one of the main insights in the proofs of the Incompleteness Theorems. It is used to state "Σ is consistent" (where Σ is an enumerable set of axioms) as a Π^0_1 statement. Gödel numberings originally appear in [17], but are covered in any standard logic text such as [7].

The idea behind Gödel numberings is very simple: let $\langle p_n : n \in \mathbb{N}\rangle$ be an enumeration of the prime numbers. Associate a positive integer to each symbol: "x" might be 1, "0" might be 2, "$\forall$" might be 3 and so on. Then a sequence of symbols of length k can be coded as $c = 2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdots p_k^{n_k}$.

Example 5. *Suppose we use the following coding scheme:*

Symbol	x	0	$\forall$	$*$	$=$	(	)
Integer	*1*	*2*	*3*	*4*	5	*6*	*7*

Then the Gödel number associated with the sentence:

$$\forall x(x * 0 = 0)$$

is $c = 2^3 * 3^1 * 5^6 * 7^1 * 11^4 * 13^2 * 17^5 * 19^2 * 23^7$.

Clearly the sentence can be uniquely recovered from its code. With more work, one can also use natural numbers to effectively code computer programs and their computations, sequences of formulas that constitute a proof and many other objects. The methods use the Chinese Remainder Theorem.

We now turn to Π^0_1 sentences.

Definition 6. *A sentence φ in the language $\mathcal{L}_{\mathbf{PA}} = \{+, *, 0, 1, <\}$ is Π^0_1 if it can be written in the form $(\forall x_0)(\forall x_1)\ldots(\forall x_m)\psi$, where ψ is a Boolean combination of equalities and inequalities of polynomials in the variables $x_0, \ldots x_m$ and the constants $0, 1$. (We do not allow unquantified—i.e.,* free*—variables to appear in φ.)*

It is not difficult to show that

$$\{n : n \text{ is the Gödel number of a } \Pi^0_1 \text{ sentence in a finite language}\}$$

is a computable set.

It is however, non-trivial to show that some statements such as the Riemann Hypothesis and the consistency of **ZFC** are provably equivalent to Π^0_1-statements. The Riemann Hypothesis was shown to be Π^0_1 by Davis, Matijasevič and Robinson ([6]) and a particularly elegant version of such a statement is due to Lagarias ([20]). Appendix B.1.4 of [9] exhibits Π^0_1-statements that are equivalent to the Riemann Hypothesis (using [20]) and Goldbach's Conjecture.

Truth: We say a sentence φ in the language $\mathcal{L}_{PA}$ is *true* if it holds in the structure $(\mathbb{N}, +, *, 0, 1, <)$.

Definition 7. *Fix a computable enumeration of all m-tuples $\langle \vec{z}_n = (z_0, \ldots z_m)_n : n \in \mathbb{N}\rangle$ of natural numbers. Let $\varphi = (\forall x_0)(\forall x_1)\ldots(\forall x_m)\psi$ be a Π^0_1 sentence. Define $\Omega = \Omega(\varphi)$ to be the least n such that $\psi(\vec{z}_n)$ is false, or, if no such n exists, set $\Omega = \infty$.*

Note that $\Omega = \infty$ if and only if φ is true.

1.5 Effectively computable diffeomorphisms

Since $\mathbb{T}^2$ is compact, a C^∞-diffeomorphism T is uniformly continuous, as are its differentials. Thus, it makes sense to view their moduli of continuity as functions $d : \mathbb{N} \to \mathbb{N}$ which say, informally, that if one wishes to specify the map $(x, y) \mapsto T(x, y)$ to within 2^{-n}, then the original point (x, y) must be specified to within a tolerance of $2^{-d(n)}$. With better and better information about (x, y), one can produce better and better information about $T(x, y)$. This intuitive notion is formalized by the definitions given below, and in more detail in Appendix B.2.2 of [9].[3] We note in passing that the moduli of continuity and approximations are not uniquely defined.

Definition 8 (Effective Uniform Continuity)**.** *We say that a map $T : \mathbb{T}^2 \to \mathbb{T}^2$ is* effectively uniformly continuous *if and only if the following two computable functions exist:*

- ***A computable Modulus of Continuity:*** *A computable function $d : \mathbb{N} \to \mathbb{N}$ which, given a target accuracy ϵ finds the δ within which the source must be known to approximate the function within ϵ.*

  More concretely, suppose $T : [0, 1) \times [0, 1) \to [0, 1) \times [0, 1)$. View elements in $[0, 1)$ as their binary expansions. Then the first $d(n)$ digits of each of (x, y) determine the first n digits of the two entries of $T(x, y)$.

- ***A Computable Approximation:*** *A computable function $f : (\{0, 1\} \times \{0, 1\})^{<\mathbb{N}} \to (\{0, 1\} \times \{0, 1\})^{<\mathbb{N}}$, which, given the first $d(n)$ digits of the binary expansion of (x, y)—or, equivalently, the dyadic rational numbers $(k_x \cdot 2^{-d(n)}, k_y \cdot 2^{-d(n)})$ for $0 \le k_x, k_y \le 2^{d(n)}$ closest to (x, y)—outputs the first n digits of the binary expansion of the coordinates of $T(x, y)$.*

The diffeomorphisms T we build are C^∞ and map from $\mathbb{T}^2$ to $\mathbb{T}^2$. Because we are working on $\mathbb{T}^2$ we can view T as a map from $\mathbb{R}^2$ to $\mathbb{R}^2$. The k^{th} differential is determined by the collection of k^{th} partial derivatives $\{\frac{\partial^k}{\partial^i x \partial^{k-i} y} : 0 \le i \le k\}$ of T with respect to the standard coordinate system for $\mathbb{R}^2$. For $k < \infty$, T is effectively C^k provided that for each $n < k$ there are computable $d(n, -)$ and $f(n, -)$ that give the moduli of continuity and approximations to the partial n^{th} derivatives. Being C^∞ requires that the $d(n, -)$ and $f(n, -)$ exist and are uniformly computable; that is that there is a single algorithm that on every input $n \in \mathbb{N}$ computes $d(n, -)$ and $f(n, -)$.

For clarity, in these definitions we discussed functions with domain and range $\mathbb{T}^2$. There is no difficulty generalizing effective uniform continuity to effectively presented metric spaces. The notion of a computable C^k diffeomorphism also easily generalized to smooth manifolds M and their diffeomorphisms, using atlases.

We note that computable diffeomorphisms are uniquely determined by the procedures for computing d and f and hence they too may be coded using Gödel numbers. The elements of the range of the function F in Theorem 1 code diffeomorphisms in this manner.

Inverses of recursive diffeomorphisms It is not true that the inverse of a primitive recursive function $f : \mathbb{N} \to \mathbb{N}$ is primitive recursive. However for primitive recursive diffeomorphisms of compact manifolds it is. Suppose that M is a smooth compact manifold and T is a C^∞-diffeomorphism. Then T is a diffeomorphism and hence has uniformly Lipschitz differentials of all orders. Since T is invertible and M is compact, T^{-1} also has uniformly Lipschitz differentials of all orders. Moreover the Lipschitz constants for T^{-1} are "one over" the Lipschitz constants for T. It follows in a straightforward way that the inverse of a primitive recursive diffeomorphism on M is a primitive recursive diffeomorphism.

[3] Since diffeomorphisms are Lipshitz, we could have worked with computable Lipshitz constants rather then computable moduli of continuity. The methods give the same collections of computable diffeomorphisms.

1.6 Reductions

The key idea for proving Theorem 1 is that of a *reduction*.

Definition 9. *Suppose that $A \subseteq X$ and $B \subseteq Y$ and $f : X \to Y$. Then f reduces A to B if*

$$x \in A \text{ iff } f(x) \in B.$$

The idea behind a reduction is that to determine whether a point x belongs to A one looks at $f(x)$ and asks whether it belongs to B: f reduces the question "$x \in A$" to "$f(x) \in B$.

For this to be interesting the function f must be relatively simple. In many cases the spaces X and Y are Polish spaces and f is taken to be a Borel map. In this paper $X = Y = \mathbb{N}$ and F is primitive recursive.

In [14] the function f has domain the space of trees (equivalently, acyclic countable graphs) and has range the space of measure preserving diffeomorphisms of the two-torus. It reduces the collection of ill-founded trees (those with an infinite branch or, respectively, acyclic graphs with a non-trivial end) to diffeomorphisms isomorphic to their inverse.

The function f is a Borel map. The point there is that if $\{T : T \cong T^{-1}\}$ were Borel then its inverse by the Borel function f would also have to be Borel. But the set of ill-founded trees is known not to be Borel. Hence the isomorphism relation of diffeomorphisms is not Borel.

In the current context the function F in Theorem 1 maps from a computable subset of $\mathbb{N}$ (the collection of Gödel numbers of Π^0_1 statements) to $\mathbb{N}$. It takes values in the collection of codes for diffeomorphisms of the two-torus.

Theorem 1 can be restated as saying that F is a primitive recursive reduction of the collection A of Gödel numbers for true Π^0_1 statements to the collection B of codes for computable measure preserving diffeomorphisms of the torus that are isomorphic to their inverses. For $N \neq M$ the transformation $F(N)$ is not isomorphic to $F(M)$.

Thus Theorem 1 can be restated as saying that the collection of true Π^0_1 statements is computably reducible to the collection of measure preserving diffeomorphisms that are isomorphic to their inverses. In the jargon: the collection of diffeomorphisms isomorphic to their inverses is "Π^0_1-hard."

1.7 Structure of the paper

The proof of the main theorem in this paper depends on background in two subjects, requiring the quotation of key results that would be prohibitive to prove. The actual construction itself—that is, the reduction F of the main theorem—is described in its entirety, along with the intuition behind these results.

The paper heavily uses results proved in [10], [14], [12] and [13]. When used, the results are quoted, and informal intuition is given for the proofs. When specific numbered lemmas, theorems and equations from [14] are referred to, the numbers correspond to the arXiv version cited in the bibliography.

Structure of the paper The logical background required for the proof of Theorem 1 is minimal and the exposition is aimed at an audience with a basic working knowledge of ergodic theory, in particular the Anosov-Katok method.

Section 2 defines the odometer-based transformations, a large class of measure preserving symbolic systems. These are built by iteratively concatenating words without spacers. We then construct the reduction $F_{\mathcal{O}}$ from the true Π^0_1 statements to the ergodic odometer-based transformations isomorphic to their inverse.

Section 3 moves from symbolic dynamics to smooth dynamics. This proceeds in two steps. The first step is to define a class of symbolic systems, the *circular systems* that are realizable as measure preserving diffeomorphisms of the two-torus. The second step uses the *Global Structure Theorem* of [12], which shows that the category whose objects are odometer-based systems and whose morphisms are synchronous and anti-synchronous joinings is canonically isomorphic with the category whose objects are circular systems and whose objects are synchronous and anti-synchronous joinings. Thus the odometer-based systems in the range of $F_{\mathcal{O}}$ can be canonically associated with symbolic shifts that are isomorphic to diffeomorphisms.

Section 3.2 shows that different elements of the range of $\mathcal{F} \circ F_{\mathcal{O}}$ are not isomorphic, by showing that their Kronecker factors are different. Sections 3.3 discusses diffeomorphisms of the torus and how to realize circular systems using method of *Approximation by Conjugacy* due to Anosov and Katok. Section 3.3 builds a primitive recursive map R from circular construction sequences to measure preserving diffeomorphisms of $\mathbb{T}^2$ such that $\mathbb{K}^c \cong R(\mathbb{K}^c)$.

In section 3.4 we argue that the functor $\mathcal{F}$ defined in the Global Structure Theorem is itself a reduction when composed with $F_{\mathcal{O}}$. Hence composing R, $\mathcal{F}$ and $F_{\mathcal{O}}$ gives a reduction F from the collection of true Π^0_1 statements to the collection of ergodic diffeomorphisms of the torus that are isomorphic to their inverse. This completes the proof of Theorem 1.

The overall content of the paper is summarized by Figure 1. The reduction to odometer-based systems is $F_{\mathcal{O}}$, $\mathcal{F}$ is the functorial isomorphism, the realization as smooth transformations is R and the composition F is the reduction in Theorem 1.

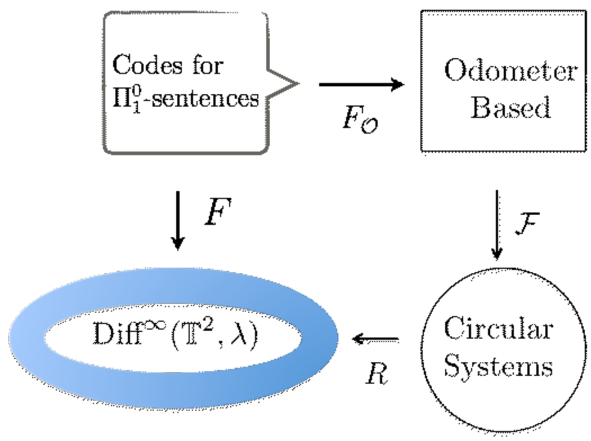

Figure 1: The reduction F.

The Appendix In the course of the proof of Theorem 1 various numerical parameters are chosen with complex relationships. The are collected, explicated and shown to be coherent in Appendix A. The numerical parameters are base on those in [14] with minor modifications and extensions. The discussion in section 11 of that paper is solely concerned with the consistency of the requirements in that paper. In this paper we give small variations of those arguments to verify, in addition, that they can be realized in a primitive recursive way.

Sections 2 and 3 of the body of the paper use certain standard notions and constructions in ergodic theory and computability theory. A complete presentation is impossible, but for readers who want an general overview we present basic well-known ideas from each subject as well exhibit explicit formulations of certain techniques in the appendices of he arXiv preprint of this paper [9]. **Those appendices contain only known background information for this paper.**

Appendix B of [9] is an overview of the logical background necessary for the proof of the theorem. It includes a basic description of Π^0_1 formulas, a discussion of bounded quantifiers, how to express Goldbach's conjecture as a Π^0_1 formula and the definition of "truth." Appendix B.2 gives basic background on recursion theory, computable functions, and primitive recursion. Appendices B.2.2 and B.2.3 give background on effectively computable functions. Readers wishing for a more complete discussion of computation/recursion theory, recursive analysis and related fields can see [23] and [5].

Appendix C of [9] gives background about ergodic theory and measure theory. It includes the notion of a measurable dynamical system, the Koopman operator, and the ergodic theorem. Appendix C.3 describes symbolic systems and gives the notation and basic definitions and conventions used in this paper. Appendix C.4 gives basic facts about odometers and odometer-based systems. These include the eigenvalues of the Koopman Operator associated to an odometer transformation and the canonical odometer factor associated with an odometer-based system. Appendix C.5 gives basic definitions including the relationship between joinings and isomorphisms. It discusses disintegrations and relatively independent products. For readers wishing for a more complete discussion of various aspects of ergodic theory we suggest [16], [18], [24], [26] and for an overview of its relationship to descriptive set theory [8].

Appendix D of [9] gives basic definitions of the space of C^∞ diffeomorphisms and gives an explicit construction of a smooth measure preserving near-transposition of adjacent rectangles. The latter is a tool used in constructing the smooth permutations of subrectangles of the unit square. These permutations are the basic building blocks of the approximations to the diffeomorphisms in the reduction. The section verifies that these are recursive diffeomorphisms with recursive moduli of continuity and that they can be given primitively recursively.

Gaebler's Theorem The writing of this paper began as a collaboration between J. Gaebler and the author with the goal of recording Foreman's results that established Theorem 1 and its corollaries. Mathematically, Gaebler was concerned with understanding the foundational significance of Theorem 1. Though unable to finish this writing project, Gaebler established the following theorem in Reverse Mathematics:

Theorem (Gaebler's Theorem)**.** *Theorem 1 can be proven in the system* ACA_0.

This result will appear in a future paper [15].

Acknowledgements The author has benefited from conversations with a large number of people. These include J. Avigad, T. Carlson, S. Friedman, M. Magidor, A. Nies, T. Slaman (who pointed out the analogy with Hilbert's 10th problem), J. Steel, H. Towsner, B. Velickovic and others. B. Kra was generous with suggestions for the emphases of the paper and with help editing the introduction. B. Weiss, was always available and as helpful as usual. Finally my colleague A. Gorodetski was indispensable for providing suggestions about how to edit the paper to make it more accessible to dynamicists.

2 Odometer-Based Systems and Reductions

In this section we prove the existence of the preliminary reduction $F_{\mathcal{O}}$.

Theorem 10. *There is a primitive recursive function* $F_{\mathcal{O}}$ *from the codes for* Π^0_1*-sentences to primitive recursive construction sequences for ergodic odometer based transformations such that:*

1. *N is the code for a true statement if and only if $F_{\mathcal{O}}(N)$ is the code for a construction sequence with limit T, where T is measure theoretically isomorphic to T^{-1}.*

2. *For $M \neq N$, $F_{\mathcal{O}}(M)$ is not isomorphic to $F_{\mathcal{O}}(N)$.*

Remark 11. *When discussing the construction of $F_{\mathcal{O}}$ and F we will always have the unstated assumption that the input N is a Gödel number of a Π^0_1-statement.*

This is justified by remarking that, though formally the domain of $F_{\mathcal{O}}$ (and so of F) is the collection of N that are Gödel numbers of Π^0_1-statements, the collection of Gödel numbers of Π^0_1-statements is primitive recursive. Theorem 1 is equivalent to constructing an F that is defined on all of $\mathbb{N}$ and outputs a code for the identity map when the input is an N that is not a Gödel number of a Π^0_1-statement as well as satisfying clauses 1, 2.

2.1 Basic Definitions

Both Odometer Based and Circular symbolic systems are built using *construction sequences*, a tool we now describe. They code cut-and-stack constructions and give a collection of words that constitute a clopen basis for the support of an invariant measure.

Fix a non-empty alphabet Σ. If $\mathcal{W}$ is a collection of words in Σ, we will say that $\mathcal{W}$ is *uniquely readable* if and only if whenever $u, v, w \in \mathcal{W}$ and $uv = pws$ then either:

- $p = \emptyset$ and $u = w$ or
- $s = \emptyset$ and $v = w$.

A consequence of unique readability is that an arbitrary infinite concatenation of words from $\mathcal{W}$ can be *uniquely* parsed into elements of $\mathcal{W}$.

Fix an alphabet Σ. A *Construction Sequence* is a sequence of collections of uniquely readable words $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$ with the properties that:

1. Each word in $\mathcal{W}_n$ is in the alphabet Σ.
2. For each n all of the words in $\mathcal{W}_n$ have the same length q_n. The number of words in $\mathcal{W}_n$ will be denoted s_n.
3. Each $w \in \mathcal{W}_n$ occurs at least once as a subword of every $w' \in \mathcal{W}_{n+1}$.
4. There is a summable sequence $\langle \epsilon_n : n \in \mathbb{N}\rangle$ of positive numbers such that for each n, every word $w \in \mathcal{W}_{n+1}$ can be uniquely parsed into segments
$$u_0 w_0 u_1 w_1 \dots w_l u_{l+1} \tag{1}$$
such that each $w_i \in \mathcal{W}_n$, $u_i \in \Sigma^{<q_n}$ and for this parsing
$$\frac{\sum_i |u_i|}{q_{n+1}} < \epsilon_{n+1}. \tag{2}$$

The segments u_i in condition 1 are called the *spacer* or *boundary* portions of w. The uniqueness requirement in clause 4 implies unique readability of each word in every $\mathcal{W}_n$.

Let $\mathbb{K}$ be the collection of $x \in \Sigma^{\mathbb{Z}}$ such that every finite contiguous subword of x occurs inside some $w \in \mathcal{W}_n$. Then $\mathbb{K}$ is a closed shift-invariant subset of $\Sigma^{\mathbb{Z}}$ that is compact if Σ is finite. The symbolic shift $(\mathbb{K}, sh)$ will be called the *limit* of $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$.

Definition 12. *Let $f \in \mathbb{K}$ where $\mathbb{K}$ is built from a construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N} \rangle$. Then by unique readability, for all n there is a unique $w \in \mathcal{W}_n$ and $a_n \leq 0 < b_n$ such that $f \upharpoonright [a_n, b_n) \in \mathcal{W}_n$. This w is called the* principal n-subword *of f. If the principal n-subword of f lies on $[a_n, b_n)$ we define $r_n(f) = -a_n$, the location of $f(0)$ relative to the interval $[a_n, b_n)$.*

The construction sequences built in this paper are strongly uniform *in that for each n there is a number f_n such that each word $w \in \mathcal{W}_n$ occurs exactly f_n times in each word $w' \in \mathcal{W}_{n+1}$. It follows that $(\mathbb{K}, sh)$ is uniquely ergodic.*

We note that in definition 12 we must have $b_n - a_n = q_n$.

Notation For a word $w \in \Sigma^{<\mathbb{N}}$ we will write $|w|$ for the length of w.

Inverses and reversals If $\mathbb{K}$ is a symbolic shift built from a construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N} \rangle$ then we can consider its inverse in two ways. The first is $(\mathbb{K}, \text{Sh}^{-1})$. The second, which we call $\text{Rev}(\mathbb{K})$ is the system built from the construction sequence $\langle \text{Rev}(\mathcal{W}_n) : n \in \mathbb{N} \rangle$ where $\text{Rev}(\mathcal{W}_n)$ is the collection of reversed words from $\mathcal{W}_n$: if $w \in \mathcal{W}_n$ then w written backwards belongs to $\text{Rev}(\mathcal{W}_n)$. Clearly $(\mathbb{K}, \text{Sh}^{-1})$ is isomorphic to $(\text{Rev}(\mathbb{K}), sh)$ and we will use both conventions depending on context.

Odometer Based construction sequences A construction sequence with $\mathcal{W}_0 = \Sigma$ and built without spacers is called an *odometer-based* construction sequence. For odometer-based sequences, Clause 3 of the definition of *Construction Sequence* implies that for odometer based systems $\mathcal{W}_{n+1} \subseteq \mathcal{W}_n^{k_n}$ for some sequence $\langle k_n : n \in \mathbb{N} \rangle$ of natural numbers with $k_n \geq 2$. Hence $|\mathcal{W}_{n+1}| \leq |\mathcal{W}_n|^{k_n}$. In the special case of odometer sequences we write the length of words in $\mathcal{W}_n$ as K_n. We note that $K_n = \prod_{m=0}^{n-1} k_m$.

The sequence $\langle k_n : n \in \mathbb{N} \rangle$ determines an *odometer* transformation with domain the compact space

$$O =_{def} \prod_n \mathbb{Z}_{k_n}.$$

The space O is naturally a monothetic compact abelian group. We will denote the group element $(1, 0, 0, 0, \dots)$ by $\bar{1}$, and the result of adding $\bar{1}$ to itself j times by $\bar{j}$. There is a natural map of O given by $\mathcal{O}(x) = x + \bar{1}$. Then $\mathcal{O}$ is a topologically minimal, uniquely ergodic invertible homeomorphism of O that preserves Haar measure. The map $x \mapsto -x$ is an isomorphism of $\mathcal{O}$ with $\mathcal{O}^{-1}$. (See Appendix C.4 of [9] and [10] for more background.)

Odometer transformations are characterized by their Koopman operators. They are discrete spectrum and the group of eigenvalues is generated by the K_n-th roots of unity.

The odometer factor If $\mathbb{K}$ is built from an odometer-based construction sequence and the principal n-subword of f sits at $[-a_n, b_n)$ then the sequence $\langle a_n : n \in \mathbb{N} \rangle$ gives a well defined member $\pi_{\mathcal{O}}(f)$ of $O = \prod_i \mathbb{Z}_{k_i}$. It is easy to verify that the map $f \mapsto \pi_{\mathcal{O}}(f)$ is a factor map.

A measure preserving transformation is *odometer-based* if it is finite entropy, ergodic and has an odometer factor. It is shown in [11] that every odometer-based transformation is isomorphic to a symbolic shift with an odometer-based construction sequence.

2.2 Inverses and factors induced by equivalence relations

Fix an odometer based construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N} \rangle$. If $\mathcal{Q}$ is an equivalence relation on $\mathcal{W}_n$, then elements of $\mathbb{K}$ can be viewed as determining sequences of equivalence classes. More precisely if Σ^* is the alphabet consisting of classes $\mathcal{W}_n/\mathcal{Q}$ we can consider the collection $\mathcal{W}_n^*$ of words of length K_n that are constantly equal to an element of Σ^*. Let $m > n$. Then for some K, the words in $\mathcal{W}_m$ are concatenations of sequences of words from $\mathcal{W}_n$ of length K. Viewed this way, the words in $\mathcal{W}_m$ determine a sequence of K many elements of $\mathcal{W}_n^*$. Concatenating them we get a word of length K_m that is constant on contiguous blocks of length K_n. Let $\mathcal{W}_m^*$ be the collection of words in the alphabet Σ^* arising this way. There is a clear projection map $\pi : \mathcal{W}_m \to \mathcal{W}_m^*$ that sends two words in $\mathcal{W}_m$ to the same word in $\mathcal{W}_m^*$ if they induce the same sequence of $\mathcal{Q}$-classes.

Equivalently define the *diagonal* equivalence relation $\mathcal{Q}^K$ on $\mathcal{W}_n^K$ by setting

$$w_0 w_1 \dots w_{K-1} \sim w_0' w_1' \dots w_{K-1}'$$

if and only if for all $i, w_i \sim_{\mathcal{Q}} w_i'$. Then for two words $w, w' \in \mathcal{W}_m, \pi(w) = \pi(w')$ if and only if $w \sim_{\mathcal{Q}^K} w'$. Similarly let $w \in (\mathcal{W}_n/Q)^K$ and $w' \in \mathcal{W}_m^K$. Then w' is a *substitution instance* of w if and only if

$$w' = w_0 w_1 \cdots w_{K-1} \text{ and } w = [w_0]_Q [w_1]_Q \cdots [w_{K-1}]_Q.$$

The sequence $\langle \mathcal{W}_m^* : m \geq n \rangle$ determines a well-defined odometer-based construction sequence in the alphabet Σ^*. If we define $\mathbb{K}_{\mathcal{Q}}$ to be the limit of $\langle \mathcal{W}_m^* : m \geq n \rangle$ then there is a canonical factor map $\pi_{\mathcal{Q}} : \mathbb{K} \to \mathbb{K}_{\mathcal{Q}}$.

We now discuss how this factor map behaves with inverse transformation. Suppose that $\mathbb{Z}_2$ acts freely on $\Sigma^* = \mathcal{W}_n/\mathcal{Q}$. Then for all K we can extend this action to $(\Sigma^*)^K$ by the *skew-diagonal* action. Suppose that g is the generator of $\mathbb{Z}_2$. Define

$$g \cdot ([w_0]_{\mathcal{Q}} [w_1]_{\mathcal{Q}} \dots [w_{K-1}]_{\mathcal{Q}}) = g \cdot [w_{K-1}]_{\mathcal{Q}} g \cdot [w_{K-2}] \dots g \cdot [w_0].$$

Assume that $\mathcal{W}_m^*$ is closed under the skew-diagonal action. Let

$$w = [w_0][w_1][w_{K-1}] \in \mathcal{W}_m^*.$$

Then we can apply g pointwise to the $[w_i]$; i.e. the diagonal action. Since $\mathcal{W}_m^*$ is closed under the skew-diagonal action, the word $g[w_0]g[w_1] \dots g[w_{K-1}] \in \textsc{Rev}(\mathcal{W}_m^*)$.[4]

Lemma 13. *Suppose for all $m > n, \mathcal{W}_m^*$ is closed under the skew-diagonal action of g. Then $\mathbb{K}_{\mathcal{Q}} \cong \textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ and the isomorphism takes an $f \in \mathbb{K}_{\mathcal{Q}}$ with associated odometer sequence x to an element of $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ determined by the diagonal action that has associated odometer sequence $-x$.*

$\vdash$ The sequence $\langle \textsc{Rev}(\mathcal{W}_m^*) : m \geq n \rangle$ is a construction sequence for $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$. The map

$$[w_0][w_1] \dots [w_{K-1}] \mapsto g[w_0]g[w_1] \dots g[w_{K-1}] \in \textsc{Rev}(\mathcal{W}_m^*)$$

is an invertible shift-equivariant map defined on the construction sequences for $\mathbb{K}_{\mathcal{Q}}$ and $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ and hence defines an invertible graph joining η_g from $\mathbb{K}_{\mathcal{Q}}$ to $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ $\dashv$

We note that the graph joining η_g does not depend on which elements of $\mathcal{W}_n$ are identified by $\mathcal{Q}$. Moreover to recover $\textsc{Rev}(\mathbb{K})$ from $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ one substitutes the appropriate *reverse* words $\textsc{Rev}(w)$ into a $\mathcal{Q}$-class $\mathcal{C}$. Frequently the graph joining η_g of $\mathbb{K}_{\mathcal{Q}}$ with $\textsc{Rev}(\mathbb{K}_{\mathcal{Q}})$ does not come from a graph joining of $\mathbb{K}$ with $\textsc{Rev}(\mathbb{K})$.

In the construction in [10], which we modify in this paper, this process is iterated: there is an equivalence relation $\mathcal{Q}_1$ on $\mathcal{W}_{n_1}$ and another equivalence relation $\mathcal{Q}_2$ on $\mathcal{W}_{n_2}$ with $n_1 < n_2$ and

[4]We note in passing that being closed under the skew diagonal action does not imply that $\mathcal{W}_m/\mathcal{Q}_n$ is closed under reverses.

$\mathcal{Q}_2$ a refinement of the product equivalence relation $\mathcal{Q}_1^K$ (for the appropriate K). There will be two copies of $\mathbb{Z}_2$ generated by g_1 and g_2 with g_1 acting freely on $\mathcal{W}_{n_1}/\mathcal{Q}_1$ and g_2 acting freely on $\mathcal{W}_{n_2}/\mathcal{Q}_2$.

For $i = 1, 2$ denote $\mathcal{W}_m/(\mathcal{Q}_i)^K$ by $(\mathcal{W}_m^*)_i$. We build two construction sequences consisting of collections of words made up of equivalence classes $\langle(\mathcal{W}_m^*)_1 : m \geq n_1\rangle$ and $\langle(\mathcal{W}_m^*)_2 : m \geq n_2\rangle$ which we assume are closed under the skew-diagonal actions of g_1 and g_2 respectively. Let $\mathbb{K}_1$ be the limit of $\langle(\mathcal{W}_m^*)_1 : m \geq n_1\rangle$ and $\mathbb{K}_2$ the limit of $\langle(\mathcal{W}_m^*)_2 : m \geq n_2\rangle$.

Then we get a tower

$$\begin{array}{c} \mathbb{K} \\ \big\downarrow \\ \mathbb{K}_2 \\ \big\downarrow \\ \mathbb{K}_1 \end{array}$$

Suppose the g_2 action on $\mathcal{Q}_2$ is *subordinate* to the g_1 action on $\mathcal{W}_{n_2}/(\mathcal{Q}_1)^K$; that is, whenever $\mathcal{C}_1$ and $\mathcal{C}_2$ are classes of $\mathcal{W}_{n_2}/(\mathcal{Q}_1)^K$ and $\mathcal{W}_{n_2}/\mathcal{Q}_2$ and $\mathcal{C}_2 \subseteq \mathcal{C}_1$, then $g_2\mathcal{C}_2 \subseteq g_1\mathcal{C}_1$.

Then the various projection maps between $\mathbb{K}$, $\mathbb{K}_{\mathcal{Q}_2}$ and $\mathbb{K}_{\mathcal{Q}_1}$ commute with the shift and the joining η_{g_2} of $\mathbb{K}_{\mathcal{Q}_2} \times \text{Rev}(\mathbb{K}_{\mathcal{Q}_2})$ extends the joining η_{g_1} of $\mathbb{K}_{\mathcal{Q}_1} \times \text{Rev}(\mathbb{K}_{\mathcal{Q}_1})$. Given an infinite sequence of equivalence relations $\mathcal{Q}_i$, the associated joinings cohere into an invertible graph joining of $\mathbb{K}$ with $\text{Rev}(\mathbb{K})$ if and only if the σ-algebras associated with the $\mathbb{K}_{\mathcal{Q}_i}$ generate the measure algebra on $\mathbb{K}$.

Diagonal vs Skew-diagonal actions. Since $\curvearrowright_n$ extends to both the diagonal and skew-diagonal actions, we summarize the distinct roles:

- The skew-diagonal actions give closure properties on $\mathcal{W}_m/\mathcal{Q}_n^m = (\mathcal{W}_m^*)_n$.
- This closure under the diagonal action gives an isomorphism between $\mathbb{K}_n$ and $\text{Rev}(\mathbb{K})_n$ that approximates a potential isomorphism from $\mathbb{K}$ to $\text{Rev}(\mathbb{K})$.

2.3 Elements of the construction

The construction of the first reduction $F_{\mathcal{O}}$ closely parallels the construction in [10] and we refer the reader to that paper for details of claims made here. For each N the routine $F_{\mathcal{O}}(N)$ inductively builds an odometer construction sequence $\langle\mathcal{W}_n : n \in \mathbb{N}\rangle$ in the alphabet $\Sigma = \{0, 1\}$ with $\mathcal{W}_{n+1} \subseteq \mathcal{W}_n^{k_n}$. During the construction we will accumulate inductive numerical requirements. Some, such as the ϵ_n's and the ε_n's are positive numbers that go to zero rapidly. Some, such as the k_n's and l_n's are sequences of natural numbers that go to infinity. These numbers depend on N, so when necessary we will write $\mathcal{W}_n(N)$, $\epsilon_n(N)$, $k_n(N)$, $l_n(N)$ and so forth. However for notational simplicity we will drop the N whenever it is clear from context. At stage n in the algorithm $F(N)$ for building $\mathcal{W}_n(N)$, for $M < N$ F can recursively refer to objects build by $F(M)$ at stages $\leq n$. For example $F(N)$ can assume that $k_n(N-1)$ is known.

These sequences of numbers are defined inductively and have complex relationships, requiring some verification that they are consistent and can be chosen primitively recursively. That they are consistent is the content of section 11 of [14]. That they can be chosen primitively recursively involves a routine review of the arguments in that paper. For completeness this is done in Appendix A.

Numerical Requirement A There is an increasings sequence of natural numbers $\leq e(n) : n \geq 1\rangle$ such that for all $n \geq 1, s_n = 2^{(n+1)e(n)}$

The construction will use the following auxiliary objects and their properties:

1. A sequence of equivalence relations $\langle \mathcal{Q}_n : n \in \mathbb{N}\rangle$. Each $\mathcal{Q}_n$ is an equivalence relation on $\mathcal{W}_n$, hence gives a factor $\mathbb{K}_n$ of $\mathbb{K}$. The equivalence relation $\mathcal{Q}_0$ is the trivial relation where any two elements of $\mathcal{W}_0$ are equivalent.

2. The equivalence relation $\mathcal{Q}_{n+1}$ refines the product equivalence relation $(\mathcal{Q}_n)^{k_n}$ on $\mathcal{W}_n^{k_n}$.

3. The sub-σ-algebra $\mathcal{H}_n$ of $\mathcal{B}(\mathbb{K})$ corresponding to $\mathbb{K}_n$. In the construction here, as with the original construction in [10], $\bigcup_n \mathcal{H}_n$ will generate $\mathcal{B}(\mathbb{K})$ modulo the sets of measure zero with respect to the unique shift-invariant measure μ. (This is Lemma 15 which uses specification Q4.)

   We denote the sub-σ-algebra of $\mathcal{B}(\mathbb{K})$ corresponding to the odometer fact by $\mathcal{H}_0$. Because the odometer factor sits in side each $\mathbb{K}_n$, $\mathcal{H}_0 \subseteq \mathcal{H}_n$ for all n.

4. A system of free $\mathbb{Z}_2$ actions $\curvearrowright_n$ on $\mathcal{W}_n/\mathcal{Q}_n$ for $n < \Omega$. (See definition 7 for the definition of Ω.) Denote the generator of $\mathbb{Z}_2$ corresponding to $\curvearrowright_n$ as g_n.

Suppose that $n < m$. As in section 2.2, the words in $\mathcal{W}_m$ are concatenations of $K = K_m/K_n$-many words from $\mathcal{W}_n$. Hence the product equivalence relation $(\mathcal{Q}_n)^K$ gives an equivalence relation on $\mathcal{W}_m$, which we call $\mathcal{Q}_n^m$. We will denote $\mathcal{W}_m/\mathcal{Q}_n^m$ by $(\mathcal{W}_m^*)_n$. The $\mathbb{Z}_2$ actions have the following properties:

- $(\mathcal{W}_m^*)_n$ is closed under the skew-diagonal action of g_n.
- If $n+1 < \Omega$, then the g_{n+1} action is subordinate to the g_n action.
- We let $\curvearrowright_n$ be the diagonal action of g_n on $\mathbb{K}_n$. Since $(\mathcal{W}_m^*)_n$ is closed under the skew-diagonal action, $\curvearrowright_n$ can be viewed as mapping $(\mathcal{W}_m^*)_n$ to $\text{Rev}((\mathcal{W}_m^*)_n)$. As described in section 2.2, for $n < \Omega$, $\curvearrowright_n$ canonically creates an isomorphism between $\mathbb{K}_n$ and $\mathbb{K}_n^{-1}$ that induces the map $x \mapsto -x$ on the odometer factor.

Restating this: if the action $\curvearrowright_n$ is non-trivial, then it induces a graph joining η_n of $\mathcal{H}_n$ with $(\mathcal{H}_n)^{-1}$ that projects to the map $x \mapsto -x$ on the odometer factor. Assuming $n+1 < \Omega$, and so the action $\curvearrowright_{n+1}$ is subordinate to $\curvearrowright_n$, the joining η_{n+1} projects to the joining η_n. If $\Omega = \infty$, since the $\bigcup_n \mathcal{H}_n$ will generate $\mathcal{B}(\mathbb{K})$, the η_n's will consequently cohere into a conjugacy of T with T^{-1}.

Lemmas 26 and 27 of [10] formalize this and show the following conclusion.

Lemma 14. *Suppose $\Omega = \infty$. Then there is a measure isomorphism η of $\mathbb{K}$ with $\mathbb{K}^{-1}$ such that for all $n \in \mathbb{N}$, η induces an isomorphism $\eta_n : \mathbb{K}_n \to \mathbb{K}_n$ that coincides with the graph joining determined by the action of the generator for $\curvearrowright_n$ on $\mathbb{K}_n$.*

The construction is arranged so that if the number Ω is finite, then $\mathbb{K} \not\cong \mathbb{K}^{-1}$. This is done by making the sequences of equivalence classes of elements of $(\mathcal{W}_m^*)_n = \mathcal{W}_m/\mathcal{Q}_n^m$ essentially independent of their reversals subject to the conditions described above. The specifications given later in this section make this precise.

2.4 An overview of $F_{\mathcal{O}}$.

The algorithm for the reduction $F_{\mathcal{O}}$ is diagrammed in Figure 2.

Given N, $F_{\mathcal{O}}$ determines the Π^0_1 formula coded by N:

$$\varphi_N = \forall z_0 \forall z_1 \dots \forall z_m \varphi(z_0, z_1, \dots z_m).$$

The function F then uses the formula to generate a computational routine R_φ that recursively computes the objects $\mathcal{W}_n(N), \mathcal{Q}_n(N)$ and $\curvearrowright_n (N)$ (as well as the various numerical parameters that are involved in the construction). Here is what R_φ does.

The routine R_φ

1. Fixes a computable enumeration of all m-tuples $\langle \vec{z}_n = (z_0, \dots z_m)_n : n \in \mathbb{N}\rangle$ of natural numbers.
2. On input n, R_φ initializes $i = 0$, sets $\mathcal{W}_0 = \{0, 1\}$, $\mathcal{Q}_0$ the trivial equivalence relation with one class and the action $\curvearrowright_0$ the trivial action.
3. For $i < n$, R_φ:
   (a) builds $\mathcal{W}_{i+1}, \mathcal{Q}_{i+1}$,
   (b) computes $\langle \vec{z}_j : 0 \leq j \leq i\rangle$,
   (c) Asks:
   "Is $\varphi_N(\vec{z}_j)$ true for all $0 \leq j \leq i$?"
   Since φ_N has no unbounded quantifiers, this question is primitive recursive.
   (d) If *yes*, R_φ builds the action $\curvearrowright_{i+1}$
   (e) If *no*, R_φ makes the $\curvearrowright_{i+1}$ trivial. (Note that if i is the first integer in this case, then Ω will equal $i + 1$.)
4. When $i = n$, R_φ returns $\mathcal{W}_n$.

2.5 Properties of the words and actions.

We describe the construction sequence, the equivalence relations and the actions. To start we choose a prime number $P_0 > 2$ sufficiently large, and let $\langle P_N : N > 0\rangle$ enumerate the prime numbers bigger than P_0.

For the construction sequence corresponding to $F_{\mathcal{O}}(N)$, words in $\mathcal{W}_1$ have length P_N. The words in $\mathcal{W}_n$ will have length $K_n = P_N 2^\ell$ for some ℓ chosen large enough as specified below. The K_n's will be increasing and K_m divides K_n for $m < n$. Let $k_n = K_{n+1}/K_n$. Thus k_n is a large power of 2 and each word in $\mathcal{W}_{n+1}$ is a concatenation of k_n many words from $\mathcal{W}_n$. The number of words in $\mathcal{W}_n$ is s_n. We require that s_n divides s_{n+1} and s_n is a power of 2 that goes to goes to infinity quickly. Since $\mathcal{W}_{n+1} \subseteq \mathcal{W}_n^{k_n}$ this induces lower bounds on the growth of the k_n's.

The requirements described here are simpler than those in [10] as modified in [14], and the "specifications" used there are appropriately simplified *or omitted* if not relevant to this proof. The construction carries along numerical parameters $\langle \epsilon_n\rangle$, $\langle k_n\rangle$, $\langle K_n\rangle$, $\langle s_n\rangle$, $\langle Q_n\rangle$, $\langle C_n\rangle$, and $\langle e(n)\rangle$. (Showing that the various coefficients are compatible and primitively recursively computable appears in Appends A.)

As an aid to the reader we use the analogous labels for the simplified specifications as those that appear in [14].

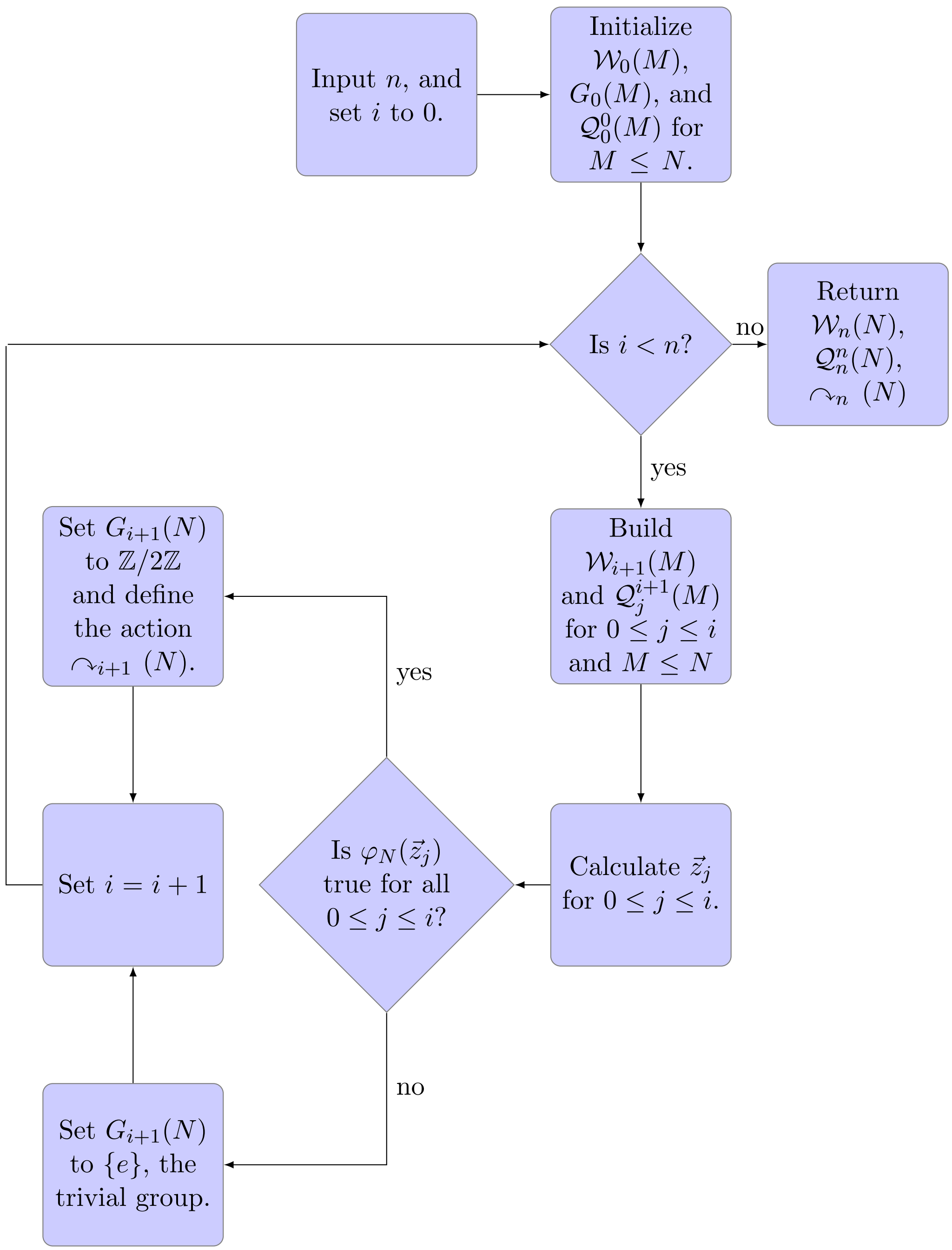

Figure 2: The algorithm $R_\varphi = F_{\mathcal{O}}(N)$.

Q4 For $n \geq 1$, any two $\mathcal{W}_n$-words in the same $\mathcal{Q}_n$ class agree on an initial segment of proportion at least $(1 - \epsilon_n)$.

Q6. As a relation on $\mathcal{W}_{n+1}$, for $1 \leq s \leq n+1$, $\mathcal{Q}_s^{n+1}$ refines $\mathcal{Q}_{s-1}^{n+1}$ and each $\mathcal{Q}_{s-1}^{n+1}$ class contains $2^{e(n+1)}$ many $\mathcal{Q}_s^{n+1}$ classes.

The point of **Q4** is that the $\mathcal{Q}_n$ classes approximate words in $\mathcal{W}_n$ by specifying arbitrarily long proportions of the words. A consequence of this is:

Lemma 15. *$\bigcup_n \mathcal{H}_n$ generates the measure algebra of $\mathbb{K}$.*

$\vdash$ This is proved in Proposition 23 of [10]. $\dashv$

Thus **Q4** is the justification for Assertion 3 of Section 2.3.

We now turn to the joining specifications. These are counting requirements that determine the joining structure. The joining specifications we present here are more complicated than strictly necessary for the simplified construction in this paper, but we present them as appear in [10] in order to be able to directly quote the theorems proved there. We note that specification J10.1 is a strengthening of J10 in [10].

Suppose that u and v are elements of $\mathcal{W}_{n+1} \cup \text{Rev}(\mathcal{W}_{n+1})$ and (u', v') an ordered pair from $\mathcal{W}_n \cup \text{Rev}(\mathcal{W}_n)$. Suppose that u and v are in positions shifted relative to each other by t units. Then an *occurrence* of (u', v') in $(sh^t(u), v)$ is a t' such that u' occurs in u starting at $t + t'$ and in v starting at t'. If X is an alphabet and $\mathcal{W}$ is a collection of words in X, and $u \in \mathcal{W} \cup \text{Rev}(\mathcal{W})$ we say that u has *forward parity* if $u \in \mathcal{W}$ and *reverse* parity if $u \in \text{Rev}(\mathcal{W})$.

By specification Q4 no word in $\mathcal{W}_{n+1}$ belongs to $\text{Rev}(\mathcal{W}_{n+1})$, so parity is well-defined and unique. However the words in $(\mathcal{W}_n^*)_i$ may belong to $\text{Rev}((\mathcal{W}_n^*)_i)$ and we view those words as having both parities.

J10.1 Let u and v be elements of $\mathcal{W}_{n+1} \cup \text{Rev}(\mathcal{W}_{n+1})$. Let $1 \leq t < (1 - \epsilon_n)(k_n)$. Let j_0 be a number between $\epsilon_n k_n$ and $k_n - t$. Then for each pair $u', v' \in \mathcal{W}_n \cup \text{Rev}(\mathcal{W}_n)$ such that u' has the same parity as u and v' has the same parity as v, let $r(u', v')$ be the number of $j < j_0$ such that (u', v') occurs in $(sh^{tK_n}(u), v)$ in the $j \cdot K_n$-th position in their overlap. Then

$$\left| \frac{r(u', v')}{j_0} - \frac{1}{s_n^2} \right| < \epsilon_n.$$

For fixed n and s, let $Q_s^n = |(\mathcal{W}_n^*)_s|$ and C_s^n be the number of equivalent elements in each block of the partition $\mathcal{W}_n / \mathcal{Q}_s^n$.

J11 Suppose that $u \in \mathcal{W}_{n+1}$ and $v \in \mathcal{W}_{n+1} \cup \text{Rev}(\mathcal{W}_{n+1})$. We let $s = s(u, v)$ be the maximal $i < \Omega$ such that $[u]_i$ and $[v]_i$ are in the same $\curvearrowright_i$-orbit. Let $g = g_i$ and $(u', v') \in \mathcal{W}_n \times (\mathcal{W}_n \cup \text{Rev}(\mathcal{W}_n))$ be such that $g[u']_s = [v']_s$. Let $r(u', v')$ be the number of occurrences of (u', v') in (u, v). Then:

$$\left| \frac{r(u', v')}{k_n} - \frac{1}{Q_s^n} \left(\frac{1}{C_s^n} \right)^2 \right| < \epsilon_n.$$

The next assumption is a strengthening of a special case of J11.

J11.1 Suppose that $u \in \mathcal{W}_{n+1}$ and $v \in \mathcal{W}_{n+1} \cup \text{Rev}(\mathcal{W}_{n+1})$ and $[u]_1$ not in the $\curvearrowright_1$-orbit of $[v]_1$.[5] Let j_0 be a number between $\epsilon_n k_n$ and k_n. Suppose that I is either an initial or a tail segment of the interval $\{0, 1, \ldots K_{n+1}-1\}$ having length $j_0 K_n$. Then for each pair $u', v' \in \mathcal{W}_n \cup \text{Rev}(\mathcal{W}_n)$ such that u' has the same parity as u and v' has the same parity as v, let $r(u', v')$ be the number of occurrences of (u', v') in $(u \upharpoonright I, v \upharpoonright I)$. Then:

$$\left| \frac{r(u', v')}{j_0} - \frac{1}{s_n^2} \right| < \epsilon_n.$$

The properties and specifications described above imply the specifications in [10] as well as J10.1 and J11.1 from [14].

Remark 16. *We note that specification J10.1 implies unique readability of the words in $\mathcal{W}_{n+1}$. This follows by induction on n. If the words in $\mathcal{W}_{n+1}$ were not uniquely readable then we would have $u, v, w \in \mathcal{W}_n$ with $uv = pws$ and neither p nor s empty. But the one of u or v would have to overlap either an initial segment or a tail segment of w of length $K_{n+1}/2$. Suppose it is an initial segment of w and a tail segment u. On this tail segment the n-subwords would have to agree exactly with the n-subwords of an initial segment of w. But this contradicts J10.1.*

Suppose we have built a collection of words $\langle \mathcal{W}_n : n \in \mathbb{N} \rangle$, equivalence relations $\langle \mathcal{Q}_n : n \in \mathbb{N} \rangle$ and actions $\langle \curvearrowright_n : n \in \mathbb{N} \rangle$ satisfying the properties described then we can cite the following results occurring in [10]. Fix a transformation T built with the construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N} \rangle$. Recall that if $\curvearrowright_n$ is non-trivial then the generator $g_n \neq 0$ induces an invertible graph joining η_n of $\mathbb{K}_n$ with $\mathbb{K}_n^{-1}$. We quote the following results of [10], referencing their numbers in that paper.

Theorem 13 and Proposition 32 Suppose that η is an ergodic joining of T with T^{-1} that is not a relatively independent joining over the odometer factor. Then $\eta \upharpoonright \mathcal{H}_0 \times \mathcal{H}_0$ is supported on the graph of some $\bar{j}$-shift of the odometer factor.

Proposition 37 If η is an ergodic joining of $\mathbb{K}$ with $\mathbb{K}^{-1}$, then exactly one of the following holds:

1. $\Omega < \infty$ and for some $n \leq \Omega$, $j \in \mathbb{Z}$ and some η_n, η is the relatively independent joining of $\mathbb{K}$ with $\mathbb{K}^{-1}$ over the joining $\eta_n \circ (1, sh^{-j})$ of $\mathbb{K}_n \times \mathbb{K}_n^{-1}$.
2. $\Omega = \infty$ and for some j, all n the projection of η to a joining on $\mathbb{K}_n \times \mathbb{K}_n^{-1}$ is of the form $\eta_n \circ (1, sh^{-j})$

If $\Omega = \infty$, since the $\mathcal{H}_n$'s generate, η is an invertible graph joining of $\mathbb{K}$ with $\mathbb{K}^{-1}$. In both cases the projection of η_n to a joining of the odometer factor with itself concentrates on the map $x \mapsto -x$.

Thus it follows that:

1. If $\mathbb{K} \cong \mathbb{K}^{-1}$ then $\Omega = \infty$. In particular if $\mathbb{K} \cong \mathbb{K}^{-1}$, then the Π^0_1 statement φ_N is true.
2. The projection of $\eta_n \circ (1, sh^{-j})$ to the odometer is of the form $x \mapsto -x - j$.
3. Similarly the projection of $\eta \circ (1, sh^{-j})$ to the odometer is of the form $x \mapsto -x - j$.

[5] In the language of J11: $s(u, v) = 0$, $Q_0^n = 1$ and $C_0^n = s_n$.

Clause 2 of Theorem 10 requires that if $M \neq N$ are different codes for Π^0_1 sentences then the transformation $F_{\mathcal{O}}(M)$ is not isomorphic to $F_{\mathcal{O}}(N)$. This is clear because the odometer sequence for $F_{\mathcal{O}}(M)$ consists of k's whose prime factors are 2 and P_M, while the odometer sequence for $F_{\mathcal{O}}(N)$ has k's whose prime factors are 2 and P_N. Since $P_M \neq P_N$, the odometer factors are not isomorphic.

Corollary 33 of [10] implies that the Kronecker factor of each $F_{\mathcal{O}}(N)$ is the odometer factor. Since any isomorphism φ between $F_{\mathcal{O}}(M)$ with $F_{\mathcal{O}}(N)$ must induce an isomorphism of the Kronecker factors, φ has to induce an isomorphism of the corresponding odometer factors, yielding a contradiction. (See Corollary 57 in Appendix C of [9] for background about Kronecker factors.)

To finish the proof of Theorem 10 we must show that the words, equivalence relations and actions can be built primitively recursively.

2.6 Building the words, equivalence relations and actions

To finish the proof of Theorem 10 the words $\mathcal{W}_n(N)$, the equivalence relations $\mathcal{Q}_n(N)$ and actions $\curvearrowright_n (N)$ must be constructed and it must be verified that the construction is primitive recursive.

Note: Formally we are just constructing actions $\curvearrowright_n$ for $n < \Omega$. However for notational convenience, when constructing the words at stage $n+1$, we will write $\curvearrowright_i$ when $\Omega \leq i < n+1$ with the understanding that it is the trivial identity action.

The collections of words $\mathcal{W}_n$ are built probabilistically. A finitary version of law of large numbers shows that there are primitive recursive upper bounds on the length of the words in a collection with the necessary properties. The actual collection of words can then be found with an exhaustive search of collections of words of that length, showing that the entire construction is primitive recursive.

Structure of the induction. The collections of words $\mathcal{W}_n$ are built by induction on n. For $n \geq 1$ the words in $\mathcal{W}_{n+1}$ are built by iteratively substituting words into k_n-sequences of classes $\mathcal{Q}^n_i$, by induction on $i \leq n$. We will adapt the notation of section 2.2.

The length K_1 of words in $\mathcal{W}_1$ will be a large prime number P_N. To pass from stage n to $n+1$, one is required to build the words $\mathcal{W}_{n+1}$, the equivalence relation $\mathcal{Q}_{n+1}$ and, if $n+1 < \Omega$ the action $\curvearrowright_{n+1}$. The length K_{n+1} of the words will be $2^\ell \cdot K_n$ for an ℓ taken large enough.

Suppose we have already chosen k_n and it is a large power of 2. Then $(\mathcal{Q}^n_i)^{k_n}$ for $0 \leq i \leq n$ give us a hierarchy of equivalence relations of potential words as described in Section 2.2 as well as the diagonal and skew-diagonal actions of $\curvearrowright_i$ for $i < \min(n, \Omega)$.

Remark 17. *The construction of $\mathcal{W}_{n+1}$ is top-down. We construct the $(\mathcal{W}^*_{n+1})_i = \mathcal{W}_{n+1}/\mathcal{Q}^{n+1}_i$ by induction on* i before *we construct $\mathcal{W}_{n+1}$. The equivalence relations get more refined as i increases, so each step gives more information about $\mathcal{W}_{n+1}$. Having built $(\mathcal{W}^*_{n+1})_n$, an additional step constructs creates both $\mathcal{W}_{n+1}$ and the equivalence relation $\mathcal{Q}^{n+1}_{n+1}$.*

Start with $i = 0$. Then $\mathcal{W}_n/\mathcal{Q}^n_0$ has one element, a string of length K_n with a single letter. Let $(\mathcal{W}^*_{n+1})_0$ be the single element consisting of strings of length $k_n \cdot K_n$ in that single letter.

Each element of $(\mathcal{W}^*_{n+1})_1$ is built by substituting k_n elements of $(\mathcal{W}^*_n)_1$—each of which is a contiguous block of length K_n—into $(\mathcal{W}^*_{n+1})_0$. We continue this process inductively, ultimately arriving at $(\mathcal{W}^*_{n+1})_n$.

The elements X being substituted into previous words	The result of the substitution
	$(\mathcal{W}^*_{n+1})_0$
$(\mathcal{W}^*_n)_1$	$(\mathcal{W}^*_{n+1})_1$
$(\mathcal{W}^*_n)_2$	$(\mathcal{W}^*_{n+1})_2$
$\vdots$	$\vdots$
$(\mathcal{W}^*_n)_n$	$(\mathcal{W}^*_{n+1})_n$

The result of this induction is a sequence of elements of $\mathcal{W}_n/\mathcal{Q}_n$ of length $k_n * K_n$, that is constant on blocks of length K_n. We must finish by substituting elements of $\mathcal{W}_n$ into the $\mathcal{W}_n/\mathcal{Q}_n$-classes to get $\mathcal{W}_{n+1}$ and defining $\mathcal{Q}_{n+1}$.

A step in the induction on i. Fix an i and view elements $(\mathcal{W}^*_{n+1})_i$ as k_n-sequences $C_0C_1\dots C_{k_n-1}$ of elements of $(\mathcal{W}^*_n)_i$. Since $\mathcal{Q}_{i+1}$ refines the diagonal equivalence relation $(\mathcal{Q}_i)^{K_{i+1}/K_i}$, $(\mathcal{Q}^n_{i+1})^{k_n}$ refines $(\mathcal{Q}^n_i)^{k_n}$. Inside each $\mathcal{Q}^n_i$ class C_j, one can choose a $\mathcal{Q}^n_{i+1}$ class $C'_j \in (\mathcal{W}^*_n)_{i+1}$. Concatenating these to get $C'_0C'_1\dots C'_{k_n-1}$ we create an element of $(\mathcal{W}^*_{n+1})_{i+1}$. We do the construction so that result is closed under the skew diagonal action of $\curvearrowright_{i+1}$.

Remark 18. *Following section 2.2, elements of $(\mathcal{W}^*_{i+1})_{i+1}$ are constant sequences of length K_{i+1}. Thus the concatenation $C'_0C'_1\dots C'_{k_n-1}$ is a sequence of $k_n * (K_n/K_{i+1})$ many contiguous constant blocks of length K_{i+1}.*

We now describe how these choices are made. Our discussion is aimed at the case where $n+1 < \Omega$, for $n+1 \geq \Omega$ take $\curvearrowright_{n+1}$ to be the trivial action. Fix a candidate k for k_n. View $\{rev\}$ as acting on $(\mathcal{W}_n/\mathcal{Q}^n_i)^k = ((\mathcal{W}^*_n)_i)^k$. Together, the skew-diagonal action of $\curvearrowright_i$ and $\{rev\}$ generate an action on $(\mathcal{W}_n/\mathcal{Q}^n_i)^k$. Let R_i be a set of representatives of each orbit of this action. Fix the number E of $i+1$-classes desired inside each i-class. Consider

$$\mathbb{X}_i = \prod_{r\in R_i}\prod_{q=0}^{E-1} S(r,q), \tag{3}$$

where $S(r,q)$ is the collection of all substitution instances of $\mathcal{Q}^n_{i+1}$ classes into r.[6] More explicitly, if $r = C_0C_2\dots C_{k-1}$ where $C_j \in \mathcal{W}_n/\mathcal{Q}^n_i$. Let $C^*_j = \{C' : C' \subseteq C_j \text{ and } C' \in \mathcal{W}_n/\mathcal{Q}^n_{i+1}\}$. For each $0 \leq q \leq E-1$, let

$$S(r,q) = \prod_{j=0}^{k-1} C^*_j.$$

Fix an $r \in R_i$. The every element $\mathcal{W}$ of $\prod_{q=0}^{E-1} S(r,q)$ can be viewed as a collection of E many words of length k in the language $(\mathcal{W}^*_n)_{i+1}$ whose $\mathcal{Q}^n_i$ classes form r. Each of these E many words can be copied by the $\curvearrowright_{i+1}$ action. If w is such a word, and is a substitution instance of r then $\curvearrowright_{i+1}(w)$ is a substitution instance of $\curvearrowright_i(r)$.

So comparing elements of $\mathcal{W}$ (and their shifts) is the same as comparing potential words in $(\mathcal{W}^*_{n+1})_{i+1}$. The action of $\curvearrowright_{i+1}$ preserves the frequencies of occurrences of words in

We work with $\mathbb{X}_i$ because it can be viewed as a discrete measure space with the counting measure. The objects being counted in the various specifications correspond to random variables on this measure space.

[6] Note that q is a dummy index variable here.

Definition 19. *If $\langle w_{r,q} : r \in R_i, 0 \le q < E\rangle$ is the collection of words built using the Substitution Lemma passing from stage i to stage $i+1$, the $(\mathcal{W}^*_{n+1})_{i+1}$ is the closure of $\{w_{r,q} : r \in R_i, 0 \le q < E\}$ under the skew-diagonal action of $\curvearrowright_i$.*

Example 20. *If $C \subseteq C_j, D \subseteq C_{j'}$ are substitution instances, we have the independent random variables $X_{r,q,j}, X_{r',q',j'}$ taking value 1 at points $\vec{x} \in \mathbb{X}_i$ where $x(r,q,j) = C$ and $x(r',q',j') = D$, respectively. The event that C occurs in $\mathbb{X}_i$ in the q^{th} word in position j and D occurs in r' in the $(q')^{th}$ word in position j' is the event that both $X_{r',q',j'} = 1$ and $X_{r,q,j} = 1$. If each i-class has p elements then the probability that both $X_{r',q',j'} = 1$ and $X_{r,q,j} = 1$ is $1/p^2$.*

The strong law of large numbers tells us that the collection of points in each $\mathbb{X}_i$ that do *not* satisfy the specifications (as they are coded in the conclusion of the Substitution Lemma) goes to zero exponentially fast in k. As k grows, the number of requirements to satisfy the Substitution Lemma grows linearly. Hoeffding's inequality (Theorem 22 below) says that the probabilities stabilize exponentially fast. The Substitution Lemma follows.

In more detail: The word construction proceeds by first getting a very close approximation to what is desired and then *finishing* the approximations to exactly satisfy the requirements. These two steps correspond to Proposition 43 and Lemma 41 of [10].

The general setup for the Substitution Lemma (Proposition 21) at stage $n+1$ is as follows:

- An alphabet X and an equivalence relation $\mathcal{Q}$ on X, with Q classes each of cardinality C.
- A collection of words $\mathcal{W} \subseteq (X/\mathcal{Q})^k$ for some k.
- Groups G, H with generators g, h that are either $\mathbb{Z}_2$ or the trivial group. If $H = \mathbb{Z}_2$ then $G = \mathbb{Z}_2$.
- If $G = \mathbb{Z}_2$ then we have a free action $G \curvearrowright X/Q$ and if $H = \mathbb{Z}_2$ we also have a free action $H \curvearrowright X$. Thus the skew-diagonal actions of G on $(X/Q)^k$ and H on X^k are well-defined. If either group is trivial, then the corresponding actions are trivial.
- The $H \curvearrowright X$ action is subordinate to $G \curvearrowright X/Q$ action via ρ.
- Constants $\epsilon_a, \epsilon_b \in (0,1)$ such that $\epsilon_b < \epsilon_a^2/5|X|$.
- A constant E determining the number of substitution instances desired for each $\mathcal{Q}$ class.
- If u, v, w, w' are words in the alphabet X, then $r(u, v, sh^i(w), w')$ is the number of j such that u occurs in w starting at $j+i$ and v occurs in w' starting at j. Similarly if u, w are words in the alphabet X, the $r(u, w)$ is the number of occurrences of u in w.

A special case of the Substitution Lemma (Proposition 63 in [10]) is:

Proposition 21 (Substitution Lemma)**.** *Let $E > 0$ be an even number. There is a lower bound k_{LB} depending on $(\epsilon_b, \epsilon_a, Q, C, W, E)$ such that for all numbers $k \ge k_{\text{LB}}$ and all symmetric $\mathcal{W} \subseteq (X/\mathcal{Q})^k$ with cardinality W that are closed under the skew-diagonal action of G and* Rev()*,* **if** *for all i with $1 \le i \le (1-\epsilon_b)k$, $u, v \in X/\mathcal{Q}$ and $w, w' \in \mathcal{W}$:*

$$\left| \frac{r(u, v, sh^i(w), w')}{k - i} - \frac{1}{Q^2} \right| < \epsilon_b \tag{4}$$

and each $u \in X/\mathcal{Q}$ occurs with frequency $1/Q$ in each $w \in \mathcal{W}$,

then *there is a collection of words* $S \subseteq X^k$ *consisting of substitution instances of* $\mathcal{W}^k$ *such that if* $\mathcal{W}' = HS \cup \textsc{Rev}(HS)$ *we have:*[7]

1. *Every element of* $\mathcal{W}'$ *is a substitution instance of an element of* $\mathcal{W}$ *and each element of* $\mathcal{W}$ *has exactly* E *many substitution instances of words from* HS.

2. *For each* $x \in X$ *and each* $w \in \mathcal{W}'$

$$\left| \frac{r(x,w)}{k} - \frac{1}{|X|} \right| < \epsilon_a \tag{5}$$

   i.e., the frequency of x *in* w *is within* ϵ_a *of* $1/|X|$.

3. *If* $w_1, w_2 \in S \cup \textsc{Rev}(S)$ *with* $[w_1]_\mathcal{Q} = [w_2]_\mathcal{Q}$ *and* $w_2 \notin H_0 w_1$ *and* $x, y \in X$ *with* $[x] = [y]$. *Then for* $h \in H_0$:[8]

$$\left| \frac{r(x,y,w_1,hw_2)}{k} - \frac{1}{Q \cdot C^2} \right| < \epsilon_a. \tag{6}$$

4. *Let* i *be a number with* $1 \leq i \leq (1-\epsilon_a)k$ *and* j_0 *be a number between* $\epsilon_a k/2$ *and* $k - i$, $x, y \in X$, $w_1, w_2 \in \mathcal{W}' \cup \textsc{Rev}(\mathcal{W}')$, *let* $r(x,y)$ *be the number of* $j < j_0$ *such that* (x,y) *occurs in* $(sh^i(w_1), w_2)$ *in the* j^{th} *position. Then*

$$\left| \frac{r(x,y)}{j_0} - \frac{1}{|X|^2} \right| < \epsilon_a. \tag{7}$$

5. *For all* $x, y \in X$ *and all* $w_1, w_2 \in \mathcal{W}' \cup \textsc{Rev}(\mathcal{W}')$ *with different* H *orbits,*

$$\left| \frac{r([x]_\mathcal{Q}, [y]_\mathcal{Q}, [w_1]_\mathcal{Q}, [w_2]_\mathcal{Q})}{k} - c \right| < \epsilon_b \tag{8}$$

   implies that,

$$\left| \frac{r(x,y,w_1,w_2)}{k} - \frac{c}{C^2} \right| < \epsilon_a. \tag{9}$$

We remark again that the Law of Large numbers implies that conclusions 1-5 hold for almost all infinite sequences. For example if you perform i.i.d. substitutions of elements of X to create a typical infinite sequence $\vec{w}$, then the density of occurrences of a given x in $\vec{w}$ will be $1/|x|$. The Hoeffding inequality says that the finitary approximations to this conclusion converge exponentially fast. As a result, for large enough k it is possible to satisfy conclusions 1-5 with very high probability.

Another remark is that at each stage we start with a collection of words $\mathcal{W}$ closed under reversals and produce another collection of words $\mathcal{W}'$ closed under reversals. However the words we keep at each stage are the results of the skew diagonal actions on the actual substitutions, not the closure under reversals.

[7] H is acting on X^k by the skew-diagonal action.

[8] While there are typographical errors in the statement of this item in [10], the proof given there yields the correct statement of the count of substitution instances in item 1 and the inequality 6. Similarly, conclusion 4 has been strengthened slightly here in a way that does not materially change the proof.

The sequence $e(n)$. We will have a sequence $e(n)$ such that for $n \geq 0$, $s_{n+1} = 2^{(n+2)e(n+1)}$. The sequence satisfies some growth conditions. (See *Inherited Requirement 2* and *Inherited Requirement 3* in Appendix A and Figure 5 for an explicit statement of these conditions.) To initialize the construction we take $e(1) = 2$.

Finding k_n We now use Proposition 21 to build the collections of words. We will apply it with $E = 2^{e(n+1)}$ except in one instance where we apply it with $E = 2^{2e(n+1)}$. To start the inductive construction, we take P_0 to be large enough to apply the Substitution Lemma with $\mathcal{Q}_0$ the trivial equivalence relation and $\mathcal{W}_0 = \Sigma = \{0, 1\}$. For $N > 0$, since $P_N \geq P_0$, P_N can also be used for $k_0(N)$ to initialize the construction as described below with $n = 0$.

We then choose k_n large enough to allow $n + 2$ successive Lemma 21-style substitutions for $E = 2^{2e(n+1)}$ corresponding to the equivalence relations $\mathcal{Q}_i^n$ for $1 \leq i \leq n$ together with a final substitution of the letters in the base alphabet Σ to produce $\mathcal{W}_{n+1}$. (This is a total of $n + 1$ substitutions.)

More explicitly, note that each of the $n + 2$ applications of the Substitution Lemma for the various $\mathcal{Q}_i$ with $E = 2^{2e(n+1)}$ and $\epsilon_a = \epsilon_n/100$ and the finishing lemma produces a lower bound k^i_{LB}. We use these lower bounds to determine k_n.

The following will be important later in the paper:

Numerical Requirement B Let $k_n(N-1)$ be the k_n corresponding to the reduction $F_{\mathcal{O}}(N-1)$ and $k_n(N)$ be the k_n corresponding to the reduction $F_{\mathcal{O}}(N)$ and $k_n(N)$. Then

$$k_n(N) \geq k_n(N-1) \tag{10}$$

Choose a large power of two

$$k_{\text{MAX}} > \max\{k^0_{\text{LB}}, k^1_{\text{LB}}, \dots, k^n_{\text{LB}}, k_n(N-1)\},$$

ensuring that it be sufficiently large that $2^{-k_{\text{MAX}}} < \epsilon_n$. Then, set

$$k_n = k^2_{\text{MAX}} * s_n. \tag{11}$$

Since k_n is of this form and s_n is a power of 2, this ensures that $K_{n+1} = P_N \cdot 2^\ell$ for a large ℓ. By increasing k_{MAX} if necessary we can also assume

1. $1/k_n < \epsilon_n^3/4$.
2. $s_{n+1} \leq s_n^{k_n}$.

Building $\mathcal{W}_{n+1}/\mathcal{Q}_i^{n+1}$ for $i \leq n$: This is done by applying the Substitution Lemma n times to pass from $(\mathcal{W}^*_{n+1})_0$ successively to $(\mathcal{W}^*_{n+1})_n$. At each $i < n$ we substitute $2^{e(n+1)}$ many elements of $(\mathcal{W}^*_{n+1})_{i+1}$ into each element of $(\mathcal{W}^*_{n+1})_i$.

Completing $\mathcal{W}_{n+1}$: Having constructed $\mathcal{W}_{n+1}/\mathcal{Q}_n$ it remains to construct $\mathcal{W}_{n+1}$, $\mathcal{Q}_{n+1}$ and the action $\frown_{n+1}$. The latter is only relevant if $n + 1 < \Omega$.

We must ensure that the resulting collection of words satisfy Q4 and Q6. This is accomplished by constructing *two* collections of words, the stems and the tails.[9]

Start by rewriting k^2_{MAX} as $(k^2_{\text{MAX}} - k_{\text{MAX}}) + k_{\text{MAX}}$.

[9] Cf. Propositions 66 and 65, and Section 8.3, in [10].

- **The tails:** To build the tails, which have length $k_{\text{MAX}}s_nK_n$, we use Lemma 21, with $X = \mathcal{W}_n$ and $\mathcal{Q} = \mathcal{Q}_n$ to build $2^{2e(n+1)}$ many substitution instances in each $\mathcal{Q}_n^{n+1}$-class C of the final $k_{\text{MAX}}s_n$ portion of each word in $(\mathcal{W}^*_{n+1})_n$. We call these the *tails* corresponding to C.

- **The stems:** The stems have length $(k_{\text{MAX}}^2 - k_{\text{MAX}})s_nK_n$. We use Lemma 21, again with $X = \mathcal{W}_n$ and $\mathcal{Q} = \mathcal{Q}_n$, to create $2^{e(n+1)}$ many substitution instances in each initial segment of a $(\mathcal{W}^*_{n+1})_n$-word of length $k_{\text{MAX}}^2 - k_{\text{MAX}}$. We call these the *stems* corresponding to the initial segments of all of the words in the $\mathcal{Q}_n^{n+1}$-class C of this word.

The words in $\mathcal{W}_{n+1}$ are built one $\mathcal{Q}_n^{n+1}$ class at a time. Fix such a class C. Then C has $2^{e(n+1)}$ many stems in the first $k_{\text{MAX}}^2 - k_{\text{MAX}}$ and $2^{2e(n+1)}$ many tails in the final segment of length k_{MAX}. Pair each stem with $2^{e(n+1)}$ many tails to create the words in $\mathcal{W}_{n+1}$ that belong to C. This puts $2^{2e(n+1)}$ words into each C.

Each equivalence class in $\mathcal{Q}_{n+1}^{n+1}$ consists of taking all words starting with a single fixed stem. It is immediate that there are $2^{e(n+1)}$ many $\mathcal{Q}_{n+1}^{n+1}$-classes in each $\mathcal{Q}_n^{n+1}$ class and that each $\mathcal{Q}_{n+1}^{n+1}$ class has $2^{e(n+1)}$ many words in it. Moreover each class is associated with a fixed stem of length $k_{\text{MAX}}^2 - k_{\text{MAX}}$ followed by many short tails. Thus specifications Q4 and Q6 are satisfied.

Finally we note that $\mathcal{W}_{n+1}$ was built by $n+2$ many successive substitutions of size $2^{e(n+1)}$ into equivalence classes. Thus $s_{n+1} = 2^{(n+2)e(n+1)}$.

Why does this work? Though it appears in detail in [10], for the reader's edification it may be appropriate to say a few things about how the stems/tails construction affects the statistics. This issue is most cogent in J10.1, where $sh^{tK_n}(u)$ and v are being compared on small portions of their overlaps. By the manner of construction of the stems, where the stem of $sh^{tK_n}(u)$ overlaps with the stem of v conclusion 4 of Proposition 21 holds with $\epsilon_a = \epsilon_n/100$.

Since $j_0 \geq \epsilon_n k_n$ the total length of the overlap is at least $\epsilon_n k_n K_n$. The tails have length $k_{\text{MAX}}s_nK_n$, so the proportion of the overlap taken up by the tails is at most

$$\begin{aligned} \frac{2k_{\text{MAX}}s_n}{j_0} \leq \frac{2k_{\text{MAX}}s_n}{\epsilon_n k_n} &< \frac{2k_{\text{MAX}}\epsilon_n^3}{100\epsilon_n} \\ &< \frac{k_{\text{MAX}}\epsilon_n^2}{50} < \epsilon_n/50. \end{aligned}$$

The specification J10.1 approximates the proportion of $j < j_0$ where (u', v') occur. This proportion is the weighted average of the proportion P_S of $j < j_0$ where (u', v') occur in the overlaps of the stems and the proportion P_T of $j < j_0$ where (u', v') occur in an overlap of a stem with a tail. Let α be the proportion of the overlap of $sh^{tK_n}(u)$ and v that occurs on the stems. By the above, $\alpha > 1 - \epsilon_n/50$. Then

$$\left|\frac{r(u', v')}{j_0} - \frac{1}{s_n^2}\right| = \left|(\alpha P_S + (1-\alpha)P_T) - \frac{1}{s_n^2}\right|$$

On the overlap of the stems $|P_S - \frac{1}{s_n^2}| < \epsilon_n/100$. Since $P_T \in [0, 1]$ and $(1-\alpha) < \epsilon_n/50$, we see that

$$\left|\frac{r(u', v')}{j_0} - \frac{1}{s_n^2}\right| < \epsilon_n.$$

Hence J10.1 holds.

The action $\curvearrowright_{n+1}$.

Case 1 ($n+1 \geq \Omega$): In this case, the action of $\curvearrowright_{n+1}$ is trivial, so there is nothing further to be done.

Case 2 ($n+1 < \Omega$): In this case, we need to define $\curvearrowright_{n+1}$ to be subordinate to $\curvearrowright_n$. Fix a $\mathcal{Q}_n^{n+1}$-class C and suppose that C gets sent to D by $\curvearrowright_n$. Since each $\mathcal{Q}_n^{n+1}$ class has the same number of elements we can define $\curvearrowright_{n+1}$ so that it induces a bijection between the $\mathcal{Q}_{n+1}$ subclasses of C and D.

The construction of the $\mathcal{W}_n, \mathcal{Q}_n$ and $\curvearrowright_n$ is primitive recursive Here is a standard theorem:

Theorem 22 (Hoeffding's Inequality)**.** *Let $\langle X_n : n \in \mathbb{N}\rangle$ be a sequence of i.i.d. Bernoulli random variables with probability of success p. Then,*

$$\mathbb{P}\left(\left|\frac{1}{n}\sum_{k=0}^{n-1} X_k - p\right| > \delta\right) < \exp\left(-\frac{n\delta^2}{6}\right).$$

Lemma 23. *The construction of the sequence $\langle \mathcal{W}_n, \mathcal{Q}_n, \curvearrowright_n : n \in \mathbb{N}\rangle$ is primitive recursive.*

Proof. The only part of the construction that is not a completely explicit induction is finding the collection of words satisfying the conclusions of the Substitution Lemma. For each candidate fixed k one can primitively recursively search *all* substitution instances to see if there is a collection of words of length $k * K_N$ that works. Using Hoeffding's inequality can give an explicit upper bound for a k that works. The algorithm first computes a k_n that works and then does the search. ⊣

This completes the proof of Theorem 10.

Remark 24. *Two remarks are in order.*

- *The asymmetry of the words in the last step of the construction of $\mathcal{W}_{n+1}$ appears problematic. How can the words all be oriented left-to-right stem and tail if they are supposed to be closed under all the various skew-diagonal actions at stage $n+1$ and later?*

  The answer is that the asymmetries are covered up by the equivalence classes. For example, the words in $\mathcal{W}_{n+1}/\mathcal{Q}_{n+1}^{n+1}$ are all constant sequences of length K_{n+1}. If $w \in \mathcal{W}_{n+1}$ and C is the $\mathcal{Q}_{n+1}^{n+1}$-class corresponding to w then the word in $\mathcal{W}_{n+1}/\mathcal{Q}_{n+1}^{n+1}$ corresponding to w is simply a string of K_{n+1} C's. Suppose that $\curvearrowright_{n+1}(C) = D$. When the action $\curvearrowright_{n+1}$ is extended to the skew-diagonal action at a later stage m, it simply takes this string of C's to a string of D's in a different place in a reverse word in the alphabet $\mathcal{W}_{n+1}/\mathcal{Q}_{n+1}^{n+1}$. It is completely opaque whether the elements of D have tails on the same side or the opposite side as the tails of words in C.

- *Roughly speaking, Cases 1 and 2 above correspond to Cases 1 and 2 in section 8.3 of [10], albeit with several differences. A key one is that here, once the construction falls into Case 1, it remains in Case 1.*

We note that we have created inductive lower bounds on the size of k_n.

Numerical Requirement C *k_n is large enough that $s_{n+1} \leq s_n^{k_n}$.*

Numerical Requirement D *k_n is large enough to satisfy the use of the Substitution Lemma 21 to construct the words in $\mathcal{W}_{n+1}$. In particular $1/k_n < \epsilon_n^3/4$.*

The data for numerical requirement D comes from the coefficients and words and equivalence relations at stages $n-1$ and before.

3 Circular Systems and Diffeomorphisms of the Torus

By Theorem 10, we have a primitive recursive reduction $F_{\mathcal{O}}$ from Gödel numbers of Π_1^0 sets to uniquely ergodic odometer-based systems. However the main theorem is about diffeomorphisms of the torus and it is an open problem whether there is any smooth ergodic transformation of a compact manifold that has an odometer as a factor. Rather than attack this problem directly, we follow [14] and do a second transformation of odometer-based systems into *circular systems*, which can be realized as diffeomorphisms. This is the downward vertical arrow $\mathcal{F}$ on the right of figure 1.

Subsection 3.1 covers circular systems and their construction. The primitive recursive map $\mathcal{F}$ maps from the odometer-based systems to circular systems and preserves *synchronous* and *antisynchronous* factors and conjugacies. In particular, for those odometer-based systems $\mathbb{K}$ in the range of $F_{\mathcal{O}}$, $\mathbb{K}$ is or is not isomorphic to its inverse, if and only if $\mathcal{F}(\mathbb{K})$ is or is not isomorphic to its inverse. We use the language of category theory to describe the structure that is preserved and define the categorical isomorphism.

In Subsection 3.3, the circular systems produced are realized as smooth diffeomorphisms of the torus. This is done in two steps: first, a given circular system is realized as a discontinuous map of the torus; second, it is shown that how to smooth the toral map into a diffeomorphisms that is measure theoretically isomorphic to the circular system.

3.1 Circular Systems

Like odometer-based systems, circular systems are symbolic systems characterized by construction sequences $\langle \mathcal{W}_n^c : n \in \mathbb{N} \rangle$ of a certain form. The basic tool for constructing circular systems is the *$\mathcal{C}$-operator.*

3.1.1 Preliminaries

Let $k, l, q \in \mathbb{N}$ be arbitrary integers greater than 1, and p be coprime to q. Let $0 \leq j_i < q$ indicate the unique integer such that

$$j_i \cdot p = i \pmod{q}. \tag{12}$$

We can rewrite j_i as $p^{-1}i \pmod{q}$, and reserve the subscript notation for this use.

Definition 25 (The $\mathcal{C}$-Operator)**.** *Let Σ be a non-empty finite alphabet and let b and e be two new symbols not contained in Σ. Let $w_0, \ldots, w_{k-1}$ be words in $\Sigma \cup \{b, e\}$. The $\mathcal{C}$-*operator *is given by:*

$$\mathcal{C}(w_0, \ldots, w_{k-1}) = \prod_{i=0}^{k-1} \prod_{j=0}^{q-1} b^{q-j_i} \cdot w_j^{l-1} \cdot e^{j_i},$$

where "$\prod$" indicates concatenation.

Fix a sequence $\langle k_n, l_n : n \in \mathbb{N} \rangle$ of positive integers with $k_n \geq 2$ and l_n increasing and $\sum_n 1/l_n < \infty$. We follow Anosov-Katok ([1]) and define auxiliary sequences of integers $\langle p_n : n \in \mathbb{N} \rangle$ and $\langle q_n : n \in \mathbb{N} \rangle$. Set $q_0 = 1$, $p_0 = 0$. Inductively define

$$q_{n+1} = k_n l_n q_n^2 \tag{13}$$

and

$$p_{n+1} = k_n l_n p_n q_n + 1. \tag{14}$$

Note that p_n and q_n are coprime for $n \geq 1$.

Let $\alpha_n = p_n/q_n$. Then

$$\alpha_{n+1} = \alpha_n + 1/q_{n+1}. \tag{15}$$

Since $q_n > l_n$ and $\sum_n 1/l_n < \infty$, we have $\sum_n 1/q_n < \infty$. Thus the α_n converge to a Liouvillean irrational $\alpha \in [0, 1)$:

$$\begin{aligned}\alpha &= \lim_{n\to\infty} \alpha_n \\ &= \sum_{n\geq 1} \frac{1}{q_n}.\end{aligned} \tag{16}$$

Circular Construction sequences We first define the notion of a circular construction sequence. Fix a non-empty finite alphabet $\Sigma \cup \{b, e\}$ as above as well as positive natural number sequences $\langle k_n : n \in \mathbb{N}\rangle$ and $\langle l_n : n \in \mathbb{N}\rangle$, with $k_n \geq 2$ and $\langle l_n\rangle$ strictly increasing such that $\sum_{n=1}^{\infty} 1/l_n < \infty$. We take $l_0 = 1$.

Let $\mathcal{W}_0^c = \Sigma$. For every n, choose a set $P_{n+1} \subseteq (\mathcal{W}_n^c)^{k_n}$ of *prewords*. Then $\mathcal{W}_{n+1}^c$ is given by all words of the form

$$\mathcal{C}(w_0, \ldots, w_{k_n-1}) = \prod_{i=0}^{k_n-1} \prod_{j=0}^{q_n-1} b^{q_n-j_i} \cdot w_j^{l_n-1} \cdot e^{j_i} \tag{17}$$

where $(w_0, \ldots, w_{k_n-1}) \in P_{n+1}$ is a preword. We call $\mathcal{C}$ the *$\mathcal{C}$-operator.*

The words created by the $\mathcal{C}$-operator are necessarily uniquely readable. However, we further demand that the collections of prewords $\langle P_n : n \in \mathbb{N}\rangle$ are uniquely readable in the sense that each k_n-tuple of words $p \in P_{n+1}$, considered a word in the alphabet $\mathcal{W}_n^c$, is uniquely readable. (Unique readability is discussed in Appendix C3 in definition 49 of [9] and in [13] which has more details.)

Definition 26 (Circular system)**.** *Let $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ be a circular construction sequence. Then the limit, which we denote $\mathbb{K}^c$ is a* circular system*.*

To emphasize that a given construction sequence is circular we denote it $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$.

In this paper the circular construction sequences will be strongly uniform. As a consequence the resulting symbolic shift is uniquely ergodic and we can write $\mathbb{K}^c = ((\Sigma \cup \{b, e\})^{\mathbb{Z}}, \mathcal{B}, \mu, \text{Sh})$ where μ is the unique shift invariant measure on $\mathbb{K}^c$.

Example 27. *Let $\Sigma = \{*\}$. Then $|\mathcal{W}_0^c| = 1$. Passing from from $\mathcal{W}_n^c$ to $\mathcal{W}_{n+1}^c$ one inductively shows that for all $n, |\mathcal{W}_n^c| = 1$. Define $\mathcal{K}_\alpha$ to be the limit of the resulting construction sequence.*

Suppose that $\langle \mathcal{U}_n^c : n \in \mathbb{N}\rangle$ is another circular construction sequence in an alphabet Λ with the same coefficients $\langle k_n, l_n : n \in \mathbb{N}\rangle$ having a limit $\mathbb{L}^c$. Define a map $\pi : \mathbb{L}^c \to \mathcal{K}_\alpha$ by setting

$$\pi(f)(n) = \begin{cases} * & \textit{if } f(n) \in \Lambda \\ b & \textit{if } f(n) = b, \\ e & \textit{if } f(n) = e. \end{cases}$$

Then π is a factor map of symbolic systems. Hence $\mathcal{K}_\alpha$ is a factor of every circular system with coefficients $\langle k_n, l_n : n \in \mathbb{N}\rangle$.

3.1.2 Rotation Factors

For $\alpha \in [0,1]$, let $\mathcal{R}_\alpha : S^1 \to S^1$ be rotation by $2\pi\alpha$ radians. Equivalently we view $\mathcal{R}_\alpha : [0,1) \to [0,1)$ as given by $x \mapsto x + \alpha \pmod 1$. This rotation $\mathcal{R}_\alpha$ plays the same role with respect to circular systems as the canonical odometer factor plays with respect to the odometer-based systems of Section 2.

Lemma 28 (The Rotation Factor)**.** *Let $\alpha = \lim \alpha_n$ be defined from a sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$ from equation 16. Then $\mathcal{K}_\alpha \cong \mathcal{R}_\alpha$. In particular if $(\mathbb{K}^c, \mathcal{B}, \nu, \text{Sh})$ is a circular system in the alphabet $\Sigma \cup \{b, e\}$ with parameters $\langle k_n, l_n : n \in \mathbb{N}\rangle$, then there is a canonical factor map $\rho : \mathbb{K}^c \to \mathcal{R}_\alpha$.*

Proof sketch. For almost every $x \in \mathbb{K}_\alpha$, there is an N for all $n \geq N$ there are $a_n, b_n \geq 0$ such that $x \restriction [-a_n, b_n)$ is some word in $\mathcal{W}_n^c$. All words in $\mathcal{W}_n^c$ have the same length, q_n, so we can define the following quantity:

$$\rho_n(x) = a_n \left(\frac{p_n}{q_n}\right).$$

Straightforward algebraic manipulations give that

$$\left|\rho_{n+1}(x) - \rho_n(x) < \frac{2}{q_n}\right|$$

whence it is clear that $\rho_n(x) \to \rho(x) \in [0,1)$. Since

$$\rho_n(\text{Sh}(x)) = \rho_n(x) + \frac{p_n}{q_n}$$

taking limits shows that $\rho(\text{Sh}(x)) = \rho(x) + \alpha$, as desired. $\dashv$

See Theorem 52 in [14] for a complete proof.

Distinguishing α's Theorem 1 demands that if $M \neq N$, then $F(M) \ncong F(N)$. This is achieved by arranging that the Kronecker factors of $F(M)$ and $F(N)$ are non-isomorphic rotations of the circle. This requires that $\alpha(N) \neq \alpha(M)$ and that $\mathcal{K}_{\alpha(N)}$ is the Kronecker factor of the limit sequence $\mathbb{K}^c(N)$. Recall that for each N we have a prime number P_N which we take for k_0 and and we build sequences $\langle k_n(N), l_n(N) : n \in \mathbb{N}\rangle$, which in turn, yield sequences $\langle p_n, q_n, k_n, l_n : n \in \mathbb{N}\rangle(N)$ and $\langle \alpha_n(N) : n \in \mathbb{N}\rangle$ which converge to an irrational $\alpha(N)$.

For each N we take $l_0(N) = 1$, so $\alpha_1(N) = \frac{1}{P_N}$. The sequence $\langle k_n(N) : n \in \mathbb{N}\rangle$ is defined in the construction of the odometer construction sequences as described after Lemma 21. The l_n's are chosen in the construction of the circular sequences and diffeomorphisms. They must satisfy some lower bounds on their growth, which we describe later.

To ensure different rotation factors correspond to different Π_1^0 sentences, we also put the following growth requirement on the $\langle l_n(N) : n \in \mathbb{N}\rangle$ sequences:

Numerical Requirement E Growth Requirement on the l_n's:

$$l_n(N) \geq l_n(N-1).$$

Lemma 29. *Suppose that the $k_n(N-1), k_n(N), l_n(N-1)$ and $l_n(N)$ satisfy Requirements B and E. Then $\alpha(N-1) > \alpha(N)$.*

$\vdash$ Note that $k_0(N-1) = P_{N-1} < P_N = k_0(N)$, so $q_1(N-1) < q_1(N)$ Since $q_{n+1} = k_n l_n q_n^2$, $k_n(N) \geq k_n(N-1)$ and $l_n(N) \geq l_n(N-1)$ one sees inductively that for all n $q_n(N-1) \leq q_n(N)$.

By equation 16 we see that

$$\begin{aligned}\alpha(N-1) &= \sum_{n\geq 1} \frac{1}{q_n(N-1)} \\ &> \sum_{n\geq 1} \frac{1}{q_n(N)} = \alpha(N).\end{aligned}$$

$\dashv$

Synchronous and Anti-synchronous joinings The system $\mathcal{K}_\alpha$ gives a symbolic representation of the rotation $\mathcal{R}_\alpha$ by $2\pi\alpha$ radians. The inverse transform $\text{Rev}(\mathcal{K}_\alpha)$ is therefore a representation of rotation by $2\pi(1-\alpha) \equiv 2\pi(-\alpha)$ radians. Moreover the conjugacies $\varphi : S^1 \to S^1$ between $\mathcal{R}_\alpha$ and $\mathcal{R}_\alpha^{-1} = \mathcal{R}_{-\alpha}$ are of the form $z \mapsto \bar{z} * e^{2\pi i\delta}$ for some δ. For combinatorial reasons we fix a particular conjugacy $\natural : \mathcal{K}_\alpha \to \text{Rev}(\mathcal{K}_\alpha)$ that is described explicitly in [12]. Thus $\natural$ corresponds to the map defined on S^1 by $z \mapsto \bar{z} * e^{2\pi i\gamma}$ for some particular γ. In additive notation on $[0,1)$ this becomes $x \mapsto -x + \gamma$ $(mod\ 1)$ for some γ.

The importance of rotation factors and odometer factors in the sequel is their function as "timing mechanisms." Joinings between odometer-based systems induce joinings on the underlying odometers; the same holds true of circular systems.

Definition 30 (Synchronous and Anti-synchronous Joinings)**.** *We define two kinds of joinings,* synchronous *and* anti-synchronous*.*

- *Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be odometer-based systems sharing the same parameter sequence $\langle k_n : n \in \mathbb{N}\rangle$. Let η be a joining between $\mathbb{K}_1$ and $\mathbb{K}_2$. Then η induces a joining η_π between $\mathbb{K}_1$ and $\mathbb{K}_2$'s copies of the underlying odometer $\mathcal{O}$. The joining η is* synchronous *if η_π is the graph joining corresponding to the identity map from $\mathcal{O}$ to $\mathcal{O}$. A joining η between $\mathbb{K}_1$ and $\mathbb{K}_2$ is* anti-synchronous *if η_π is the graph joining corresponding to the map $x \mapsto -x$ from $\mathcal{O}$ to $\mathcal{O}^{-1}$.*

- *Let $\mathbb{K}_1^c$ and $\mathbb{K}_2^c$ be circular systems sharing the same parameter sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$. Let η be a joining between $\mathbb{K}_1^c$ and $\mathbb{K}_2^c$. Then η induces a joining η_π between $\mathbb{K}_1^c$ and $\mathbb{K}_2^c$'s copies of the rotation factor, $\mathcal{K}_\alpha$. The joining η is* synchronous *if η_π is the graph joining corresponding to the identity on $\mathcal{K}_\alpha \times \mathcal{K}_\alpha$. A joining η between $\mathbb{K}_1^c$ and $(\mathbb{K}_2^c)^{-1}$ is* antisynchronous *if η_π restricts to the graph joining corresponding to $\natural : \mathcal{K}_\alpha \to (\mathcal{K}_\alpha)^{-1}$.*

3.1.3 Global Structure Theorem

Odometer-based systems and Circular systems that share the same parameter sequence $\langle k_n : n \in \mathbb{N}\rangle$ have similar joining structures. We begin by defining two categories.

Fix a parameter sequences $\langle k_n : n \in \mathbb{N}\rangle$ and $\langle l_n : n \in \mathbb{N}\rangle$ with $\sum 1/l_n < \infty$. Let $\mathcal{O}B$ be the category whose objects consist of all ergodic odometer-based systems with coefficients $\langle k_n : n \in \mathbb{N}\rangle$. A morphism of $\mathcal{O}B$ is either a synchronous graph joining between $\mathbb{K}$ and $\mathbb{L}$ or an anti-synchronous graph joining between $\mathbb{K}$ and $\mathbb{L}^{-1}$. Let $\mathcal{C}B$ be the category whose objects consist of ergodic circular systems built with coefficients $\langle k_n, l_n : n \in \mathbb{N}\rangle$ and whose morphisms consist of synchronous and anti-synchronous graph joinings from $\mathbb{K}^c$ with $(\mathbb{L}^c)^{\pm 1}$.

The main result of [12] is the following:

Theorem 31 (Global Structure Theorem)**.** *The categories $\mathcal{OB}$ and $\mathcal{CB}$ are isomorphic by a functor $\mathcal{F}$ that takes synchronous joinings to synchronous joinings, anti-synchronous joinings to anti-synchronous joinings and isomorphisms to isomorphisms.*

To prove Theorem 31 one must define the map $\mathcal{F}$ on objects, and on morphisms and then show that it is a bijection and preserves composition. Since we will only be concerned here with how effective $\mathcal{F}$ is we confine ourselves to defining it and refer the reader to [12] for complete proofs. In [15], the proof is discussed to understand the strength of the assumptions needed to prove it.

We begin by defining $\mathcal{F}$ on the objects.

Defining $\mathcal{F}$ on objects. Let an $\mathbb{K}$ be an odometer-based system with associated construction and parameter sequences $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$ and $\langle k_n : n \in \mathbb{N}\rangle$. Let $\langle l_n : n \in \mathbb{N}\rangle$ be an arbitrary sequence of positive integers growing fast enough that $\sum_n 1/l_n < \infty$. Inductively define a map $\mathcal{F}$ taking the construction sequence for an odometer-based system $\mathbb{K}$ to a construction sequence for a circular system $\mathbb{K}^c$ by applying the $\mathcal{C}$-operator. Define maps $c_n : \mathcal{W}_n \to \mathcal{W}_n^c$ as follows:

- Let $\mathcal{W}_0^c = \Sigma$ and c_0 be the identity.
- Suppose that c_n and $\mathcal{W}_n^c$ have been defined. Let

  $$\mathcal{W}_{n+1}^c = \{\mathcal{C}(c_n(w_0), \ldots, c_n(w_{k_n-1})) : w_0 w_1 \cdots w_{k_n-1} \in \mathcal{W}_{n+1}\}$$

  and $w_i \in \mathcal{W}_n$. Define $c_{n+1} : \mathcal{W}_{n+1} \to \mathcal{W}_{n+1}^c$ by setting

  $$c_{n+1}(w_0 \cdots w_{k_n-1}) = \mathcal{C}(c_n(w_0),\ \ldots,\ c_n(w_{k_n-1})).$$

  where $w_i \in \mathcal{W}_n$ with $w_0 \cdots w_{k_n-1} \in \mathcal{W}_{n+1}$.

The construction sequence $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ then gives rise to a circular system $\mathbb{K}^c$. The functor $\mathcal{F}$ will associate $\mathbb{K}^c$ with $\mathbb{K}$.

Lifting measures and joinings We need to lift measures on odometer based systems to measures on circular systems for two reasons:

1. To complete the definition of $\mathcal{F}$ on objects, given an odometer based system $(\mathbb{K}, \mu)$ we need to canonically associate a measure μ^c to $\mathbb{K}^c$. Then $\mathcal{F}(\mathbb{K}, \mu) = (\mathbb{K}^c, \mu^c)$.

   In the context of this paper this first reason is not pressing: the construction sequences in the range of $F_{\mathcal{O}}$ are strongly uniform, hence uniquely ergodic. Thus there is only one candidate for μ^c. However to complete the definition of F we need to understand what happens for arbitrary ergodic μ.

2. To define $\mathcal{F}$ on morphisms, given a joining $\mathcal{J}$ between $(\mathbb{K}, \mu)$ and $(\mathbb{L}, \nu)$ we need to associate a joining $\mathcal{J}^c$ between $(\mathbb{K}^c, \mu^c)$ with $(\mathbb{L}^c, \nu^c)$.

   For the second issue, and to deal with general odometer based systems $(\mathbb{K}, \mu)$, we review the notion of *generic sequences* of words. These were introduced in [29] and used in the proof of Theorem 31 [12].

Let $k, l > 0$ and $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$ be an arbitrary construction sequence. Using the unique readability of words in $\mathcal{W}_k$ a word w in $\Sigma^{q_{k+l}}$ determines a unique sequence of words w_j in $\mathcal{W}_k$ such that ,

$$w = u_0 w_0 u_1 w_1 \ldots w_J u_{J+1}.$$

When $w \in \mathcal{W}_{k+l}$, each u_j is in the region of spacers added in $\mathcal{W}_{k+l'}$, for $l' \leq l$. We will denote the *empirical distribution* of $\mathcal{W}_k$-words in w by $\mathrm{EmpDist}_k(w)$. Formally:

$$\mathrm{EmpDist}_k(w)(w') = \frac{|\{0 \leq j \leq J : w_j = w'\}|}{J+1},\ w' \in \mathcal{W}_k.$$

Then *EmpDist* extends to a measure on $\mathcal{P}(\mathcal{W}_k)$ in the obvious way.

To finitize the idea of a generic point for a system $(\mathbb{K}, \mu)$ we introduce the notion of a generic sequence of words. By μ_m we will denote the discrete measure on the finite set Σ^m given by $\mu_m(u) = \mu(\langle u \rangle)$. Then μ_m is not a probability measure so we normalize it. Let $\hat{\mu}_n(w)$ denote the discrete probability measure on $\mathcal{W}_n$ defined by

$$\hat{\mu}_n(w) = \frac{\mu_{q_n}(\langle w \rangle)}{\sum_{w' \in \mathcal{W}_n} \mu_{q_n}(\langle w' \rangle)}.$$

Thus $\hat{\mu}_n(w)$ is the relative measure of $\langle w \rangle$ among all $\langle w' \rangle, w' \in \mathcal{W}_n$. The denominator is a normalizing constant to account for spacers at stages $m > n$ and for shifts of size less than q_n.

Definition 32. *A sequence $\langle v_n \in \mathcal{W}_n : n \in \mathbb{N} \rangle$ is a* generic sequence of words *if and only if for all k and $\epsilon > 0$ there is an N for all $m, n > N$,*

$$\|EmpDist_k(v_m) - EmpDist_k(v_n)\|_{var} < \epsilon.$$

The sequence is generic for a measure μ if for all k:

$$\lim_{n \to \infty} \|EmpDist_k(v_n) - \hat{\mu}_k\|_{var} = 0$$

where $\| \ \|_{var}$ is the variation norm on probability distributions.

The point here is that the ergodic theorem gives infinite generic sequences for measures μ. These infinite generic sequences in turn, create generic sequences of finite words. A generic sequence of finite words determines a measure. If the generic sequence is built from the measure then the measure it determines is the original measure

We now deal with the first issue above for arbitrary $(\mathbb{K}, \nu)$ (and not just those that are strongly uniform). Given an odometer based system $(\mathbb{K}, \nu)$ we must specify the measure ν^c we associate with ν. Section 2.6 of [12] gives a canonical method of constructing a *generic* sequence of words $\langle v_n : n \in \mathbb{N} \rangle$ that encode any ergodic measure on $\mathbb{K}$. The corresponding sequence of words $v_n^c = c_n(v_n)$ is also generic and determines an ergodic measure on $\mathbb{K}^c$. The map $\mathcal{F}$ then takes $(\mathbb{K}, \nu)$ to $(\mathbb{K}^c, \nu^c)$

Defining $\mathcal{F}$ on morphisms Given an arbitrary synchronous or anti-synchronous joining $\mathcal{J}$ between odometer based systems $\mathbb{K}$ and $\mathbb{L}^{\pm 1}$ we can view $(\mathbb{K} \times \mathbb{L}, \mathcal{J})$ as an odometer based system. Taking a generic sequence of pairs of words $\langle (u_n, v_n) : n \in \mathbb{N} \rangle$ for $\mathcal{J}$ as in [12] and lifting it with the sequence of c_n's (and adjusting appropriately for reversing the circular operation with a mechanism denoted $\natural$ in [12]), one gets a joining $\mathcal{J}^c$ between $\mathbb{K}^c$ and $\mathbb{L}^c$.

Define $\mathcal{F}(\mathcal{J}) = \mathcal{J}^c$.

Is $\mathcal{F}$ primitive recursive? Clearly the maps c_n are primitive recursive so the map taking a construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$ to $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ is primitive recursive. For the same reason the map taking a joining $\mathcal{J}$ specified by a given generic sequence to $\mathcal{J}^c$ is primitive recursive. Thus, assuming that joinings $\mathcal{J}$ are presented in a manner that one can compute the generic sequences of words, the map $\mathcal{J} \mapsto \mathcal{J}^c$ is primitive recursive.

In the context of the systems in the range of $F_{\mathcal{O}}$, the relevant joinings between $\mathbb{K}$ and $\mathbb{K}^{-1}$ are given by limits of η_n's, and the generic word sequences are easily seen to be primitive recursive and can thus be translated to the joinings of $\mathbb{K}^c$ with $(\mathbb{K}^c)^{-1}$.

Remark 33. *We have shown that if φ_N is true then $\mathcal{F} \circ F_{\mathcal{O}}(N)$ is isomorphic to $\mathcal{F} \circ F_{\mathcal{O}}(N)^{-1}$ and the isomorphism is primitive recursive. In section 3.3 we build a primitive recursive realization function R which maps from strongly uniform circular systems to measure preserving diffeomorphisms of the torus. Since $F = R \circ \mathcal{F} \circ F_{\mathcal{O}}$, the result we prove is something stronger than claimed in Theorem 1. Namely we show that if φ_N is true then there is a measure isomorphism between $F(N)$ and $F(N)^{-1}$ coded by a primitive recursive generic sequence of words.*

3.2 The Kronecker Factors

The second clause of the Main Theorem (Theorem 1) says that if M and N are distinct natural numbers than the corresponding diffeomorphisms T_M and T_N are not isomorphic. To distinguish between them we use their Kronecker factors. (For more information on the Kronecker factors, see e.g. [28]. The use of operator theoretic methods dates to [27].) For this purpose we prove the following proposition. This section is otherwise independent of the other sections. Readers who find the proposition and corollary obvious can skip to the next section.

Proposition 34. *Let $\mathbb{K}^c$ be circular system in the range of $\mathcal{F} \circ F_{\mathcal{O}}$, built with coefficients $\langle k_n, l_n : n \in \mathbb{N}\rangle$ and $\alpha = \lim_n \alpha_n$ then the Kronecker factor of $\mathbb{K}^c$ is measure theoretically isomorphic to the rotation $\mathcal{R}_\alpha$.*

An immediate corollary of this is:[10]

Corollary 35. *Suppose that $M < N$ are natural numbers. Then:*

1. *$\alpha(N) < \alpha(M)$, where $\alpha(N)$ and $\alpha(M)$ are the irrationals associated with the rotation factors of $F(N)$ and $F(M)$.*
2. *$(\mathbb{K}^c)^M \not\cong (\mathbb{K}^c)^N$.*

$\vdash$ This follows immediately from Lemma 29 and the fact that the Kronecker factor $(\mathbb{K}^c)^M$ is isomorphic to $\mathcal{R}_{\alpha(M)}$ and the Kronecker factor of $(\mathbb{K}^c)^N$ is isomorphic to $\mathcal{R}_{\alpha(N)}$. $\dashv$

After Proposition 34 is shown we will have proved the following intermediate step in the proof of Theorem 1:

Proposition 36. *For N a code of a Π^0_1 sentence, then $\mathcal{F} \circ F_{\mathcal{O}}(N)$ is a primitive recursive circular construction sequence and*

1. *N is the code for a true statement if and only if the circular system T determined by $\mathcal{F} \circ F_{\mathcal{O}}(N)$ is measure theoretically conjugate to T^{-1};*
2. *$\mathcal{F} \circ F_{\mathcal{O}}(N)$ is ergodic–in fact strongly uniform; and*
3. *For $M \neq N$, $\mathcal{F} \circ F_{\mathcal{O}}(M)$ is not conjugate to $\mathcal{F} \circ F_{\mathcal{O}}(N)$.*

[10] See section 2.3 for an explanation of the (N)-notation.

Review of the Kronecker factor Let $\vec{\gamma} = \langle \gamma_m : m \in \mathbb{Z} \rangle$ be an enumeration of the eigenvalues of the Koopman operator of a measure preserving transformation $(X, \mathcal{B}, \mu, T)$. Then $\vec{\gamma}$ determines a measure preserving action on $((S^1)^{\mathbb{Z}}, \lambda^{\mathbb{Z}})$ (where $\lambda^{\mathbb{Z}}$ is the product measure on $(S^1)^{\mathbb{Z}}$) by coordinatewise multiplication. The action is ergodic, discrete spectrum and isomorphic to the Kronecker factor of $(X, \mathcal{B}, \mu, T)$.

If α is an eigenvalue of the shift operator then the powers of α, $\vec{\alpha} = \langle \alpha^n : n \in \mathbb{Z} \rangle$ are also eigenvalues corresponding to a subsequence of $\vec{\gamma}$ and hence the coordinatewise multiplication of $\vec{\alpha}$ on $(S^1)^{\mathbb{Z}}$ determines a factor of the Kronecker factor. This is a proper factor if and only if there is an eigenvalue of the Koopman operator that is not a power of α. In particular there is a non-trivial projection map from the Kronecker factor to the dual of the countable group $\{\alpha^n : n \in \mathbb{Z}\}$

The proof of Proposition 34 follows the outline of the proof of Corollary 33 of [10]. Working in the context of odometer based systems built with coefficients $\langle k_n : n \in \mathbb{N} \rangle$, it says that the Kronecker factor $\mathcal{K}r$ of each system $\mathbb{K}$ in the range of $F_{\mathcal{O}}$ is the odometer transformation $\mathcal{O}$ based on $\langle k_n : n \in \mathbb{N} \rangle$. Note that the odometer $\mathcal{O}$ is a subgroup of the Kronecker factor since rotation by the k_n^{th} root of unity is an eigenvalue of the Koopman operator. The steps there are:

1. Any joining $\mathcal{J}$ of $\mathbb{K}$ with $\mathbb{K}$ projects to a joining $\mathcal{J}_{\mathcal{O}}$ of $\mathcal{O}$ with itself. If $\mathcal{J}_{\mathcal{O}}$ is not given by the graph joining coming from a finite shift of the odometer then $\mathcal{J}$ must be the relatively independent joining of $\mathbb{K}$ with itself over $\mathcal{J}_{\mathcal{O}}$. (This is Proposition 32 of [10].)

2. If there is an eigenvalue of the unitary operator associated with $\mathbb{K}$ that is not a power of α there is a non-identity element t in the Kronecker factor whose projection to the odometer $\mathcal{O}$ is the identity.

3. Multiplying t by an element $h \in \mathcal{O}$ which is not a finite shift gives an element t' of the Kronecker factor $\mathcal{K}r$ that is not in $\mathcal{O}$ and projects to an element of $\mathcal{O}$ that is not a finite shift.

4. Let $\mathcal{H}^*$ be the sub-σ-algebra of the measurable subsets of $\mathbb{K}$ generated by $\mathcal{K}r$. Then multiplication by t' gives a graph joining $\mathcal{J}^*$ of $\mathcal{H}^*$ with itself that projects to the joining of $\mathcal{O}$ given by multiplication by h. Extend $\mathcal{J}^*$ to a joining $\mathcal{J}$ of $\mathbb{K}$ with $\mathbb{K}$. Then $\mathcal{J}$ does not project to a finite shift of the odometer but it is also not the relatively independent joining of $\mathbb{K}$ with itself over the joining of $\mathcal{O}$ with itself given by h. This is a contradiction.

To imitate this argument we first note that for circular systems, the analogue of the odometer is the rotation $\mathcal{K}_\alpha$, and that every element $\beta \in S^1$ determines an invertible graph joining $\mathcal{S}_\beta$ of $\mathcal{K}_\alpha$ with itself, corresponding to multiplication by β in the group S^1. We need to identify the analogue of the "finite shifts on the odometer" in the case of circular systems. The appropriate notion is given in Definition 78 in [14], namely the *central values*. The central values form a subgroup of the unit circle.

To prove Proposition 34, fix a circular system $\mathbb{K}^c$ in the range of $\mathcal{F} \circ F_{\mathcal{O}}$. We first show that there is a $\beta \in S^1$ that is *not* a central value. This β plays the roll of h in the outline given above. Then the analogue of Proposition 32 is proved: any joining of $\mathbb{K}^c$ with itself that does not project to the joining given by multiplication on S^1 by a central value is the relatively independent joining over its projection.

Suppose now that there is an eigenvalue of the Koopman operator that is not a power of α. Then the action of $\vec{\alpha}$ on $(S^1)^{\mathbb{Z}}$ is a non-trivial projection of the Kronecker factor $\mathcal{K}r^c$ of $\mathbb{K}^c$. Hence we can fix a non-identity element t of the Kronecker factor whose projection to the factor determined by the powers of α is the identity. As in step 3 above we multiply t by a non-central β to get a t' in the Kronecker factor which:

a.) induces a joining $\mathcal{J}^*$ of $\mathcal{H}^*$ with itself that projects to the graph joining of $\mathcal{K}_\alpha$ with itself induced by $\mathcal{S}_\beta$.

Extending $\mathcal{J}^*$ to a joining $\mathcal{J}$ of $\mathbb{K}^c$ with itself we see that:

b.) $\mathcal{J}$ is not the relatively independent joining over the joining of $\mathcal{K}_\alpha$ given by $\mathcal{S}_\beta$.

After the details are filled in, this contradiction establishes Proposition 34.

Notation As in previous sections we identify the unit interval $[0,1)$ with the unit circle via the map $x \mapsto e^{2\pi i * x}$, which identifies "addition mod one" on the unit interval with multiplication on the unit circle. When we write "+" in this section it means addition mod one, interpreted in this manner.

We use the following numerical requirement in explicit proof of Proposition 34:

Numerical Requirement F The k_n's must grow fast enough that $\sum \frac{6^n}{k_n} < \infty$.

To finish the proof of Proposition 34, we fix a circular system $\mathbb{K}^c$ in the range of $\mathcal{F} \circ F_{\mathcal{O}}$ and prove the following two lemmas.

Lemma 37. *There is a non-central value β.*

Lemma 38. *Suppose that β is not a central value. Let $\mathcal{J}$ be a joining of $\mathbb{K}^c \times \mathbb{K}^c$ whose projection to $\mathcal{K}_\alpha \times \mathcal{K}_\alpha$ is the graph joining of $\mathcal{K}_\alpha$ with itself given by multiplication by $\mathcal{S}_\beta$. Then $\mathcal{J}$ is the relatively independent joining of $\mathbb{K}^c \times \mathbb{K}^c$ over the joining of $\mathcal{K}_\alpha$ with itself given by $\mathcal{S}_\beta$.*

$\vdash$ [Lemma 37] While it seems very likely that there is a measure one set of examples we just need one. The example will be of the form $\beta = \sum_{n=1}^{\infty} \frac{a_n}{k_n q_n}$ for an inductively chosen sequence of natural numbers $\langle a_n : n \in \mathbb{N}\rangle$ with $0 \le a_n < 6^n$.

To describe β completely and verify it is non-central we need several facts from sections 5, 6 and 7 in [14], which discuss the relationship between the geometric and the symbolic representations of $\mathcal{K}_\alpha$.

The geometric construction builds a sequence of periodic approximations of lengths $\langle q_n : n \in \mathbb{N}\rangle$ with the resulting limit being the rotation of the circle by $\mathcal{R}_\alpha$. Expanding on Lemma 28, these approximations are given by the towers of intervals $\mathcal{T}_n = \{[0, 1/q_n), [p_n/q_n, p_n/q_n + 1/q_n), [2p_n/q_n, 2p_n/q_n + 1/q_n), \dots [kp_n/q_n, kp_n/q_n + 1/q_n), \dots\}$ viewed as a periodic system.

The symbolic representation uses the $\mathcal{C}$ operation to build the construction sequence for the symbolic system. The latter is described in Example 27. We give the geometric description of the periodic approximations presently.

We use the following notions and notation from [14]:

1. $\varphi_0 : (\mathcal{K}_\alpha, sh) \to ([0,1), +)$ is the measure theoretic isomorphism between the shift on $\mathcal{K}_\alpha$ and the rotation $\mathcal{R}_\alpha$ given in Lemma 28. We use s's to refer to elements of $\mathcal{K}_\alpha$ and x's to refer to elements of $[0,1)$ and s *corresponds* to x if $\varphi_0(s) = x$.

2. The notion of $s \in \mathcal{K}_\alpha$ being *mature* implies that s has a principal n-subword and it is repeated multiple times both before and after $s(0)$.

3. $\mathcal{S}_\beta = \varphi_0^{-1}\mathcal{R}_\beta\varphi_0$ is the symbolic conjugate of the rotation $\mathcal{R}_\beta$, via the map φ_0. If s corresponds to x then $\mathcal{S}_\beta(s)$ corresponds to $x + \beta$ (mod 1). We will occasionally be sloppy and use the language $s + \beta$ for $s \in \mathcal{K}_\alpha$ when we mean $\mathcal{S}_\beta(s)$.

4. In [14], a set S is defined as the collection of elements $s \in \mathcal{K}_\alpha$ such that the left and right endpoints of the principal n-subwords of s go to minus and plus infinity respectively. Explicitly suppose that $s \in \mathcal{K}_\alpha$ is such that for all large enough n, the principal n-subword exists and lives on an interval $[-a_n, b_n] \subseteq \mathbb{Z}$. The point $s \in S$ if $\lim_n a_n = \lim_n b_n = \infty$.

   The set S_β is $\bigcap_{n\in\mathbb{Z}} \mathcal{S}_\beta(S)$, the maximal $\mathcal{S}_\beta$ invariant subset of S. It is of measure one for the unique invariant measure on $\mathcal{K}_\alpha$. Since $\mathcal{K}_\alpha$ is a factor of every circular system $\mathbb{K}^c$ with the same coefficient sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$ for all invariant measures μ on $\mathbb{K}^c$, $\{s \in \mathbb{K}^c :$ the left and right endpoints of the principal n-subwords of s go to minus and plus infinity is of μ-measure one.

5. Given an arbitrary β we can intersect S_β with S_q for all rational q and get another set of measure one. Hence in a slight abuse of notation we assume that S_β is invariant under conjugation by rational rotations.

6. For $s \in \mathcal{K}_\alpha$, if $r_n(s) = i$ and x is the corresponding element of $[0, 1)$ then x is in the i^{th} level of the tower corresponding to the n^{th} approximation to $\mathcal{R}_\alpha$. This tower is given by $\mathcal{R}_{\alpha_n}$.

In the geometric picture, at stage n, we have a tower of intervals of the form $[i\alpha_n, i\alpha_n + 1/q_n)$ ordered in the dynamical ordering–where the successor of the interval $[i\alpha_n, i\alpha_n + 1/q_n)$ is $[(i+1)\alpha_n, (i+1)\alpha_n + 1/q_n)$. Thus level I_{i+1} is $I_i + \alpha_n$.

Passing from stage n to stage $n+1$ involves subdividing the old levels into new levels, which are of the form $[i\alpha_{n+1}, i\alpha_{n+1} + 1/q_{n+1})$. These subintervals move diagonally up and to the right through the n-levels. The diagonal movement corresponds to addition of α_{n+1}. The key formula is 15:

$$\alpha_{n+1} = \alpha_n + 1/q_{n+1}.$$

As illustrated in diagrams 9 and 10 of [13] and Figure 3, the $n+1$ tower proceeds diagonally up through the n-tower. This is evident from the form of equation 15 and the fact that $q_{n+1} = k_n l_n q_n^2$.

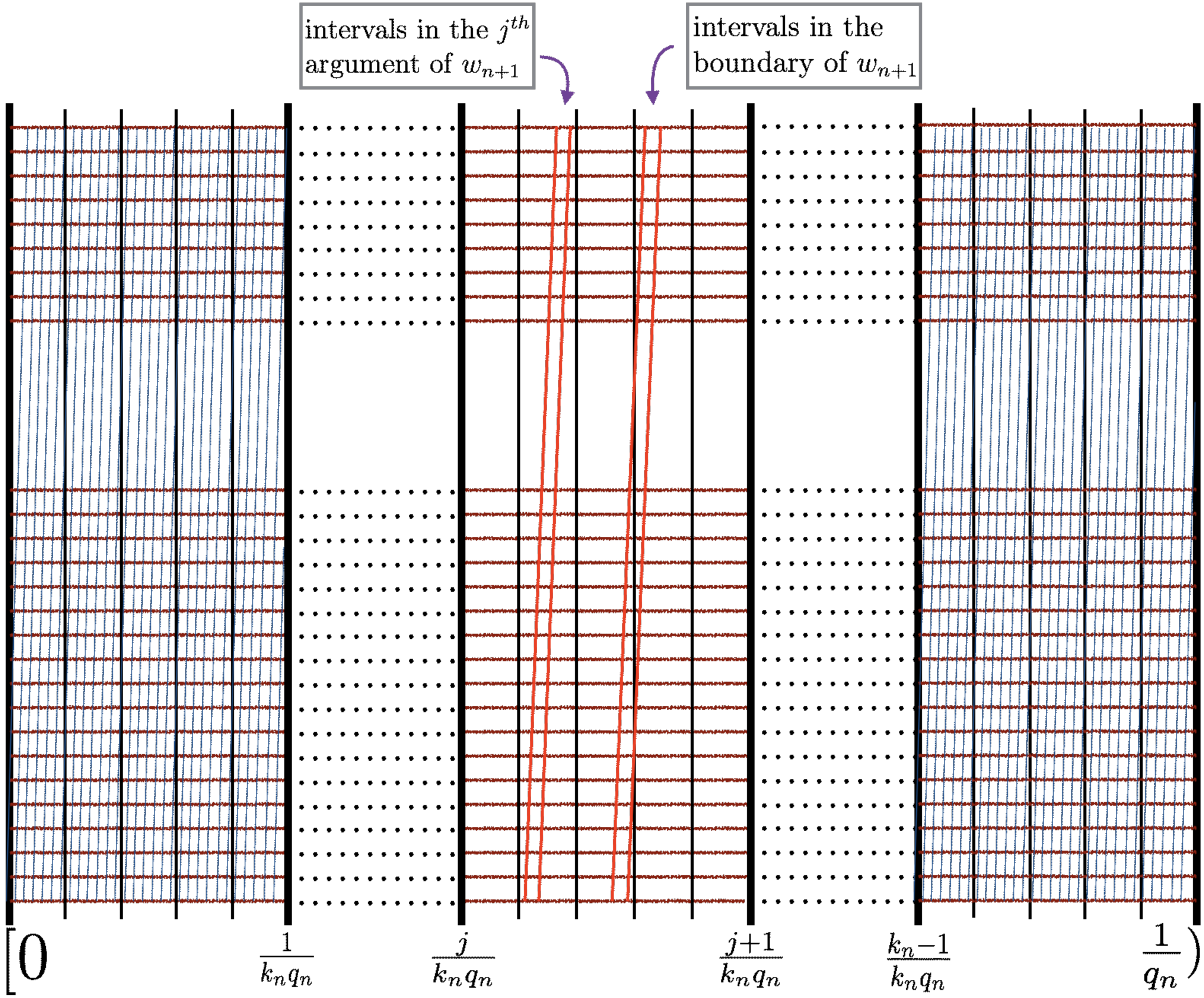

Figure 3: The n-tower, showing the diagonal progression of the $n+1$-tower. The heavy horizontal lines are the levels $(i\alpha_n, i\alpha_n + 1/q_n)$, starting with $[0, 1/q_n)$ on the bottom. The levels the $n+1$-tower are the horizontal segments between the diagonal lines.

Again, following [13], the geometric picture in Figure 3 corresponds to the symbolic representation as a circular system in the following way. Some of the diagonal paths hit the left or right vertical strips bounding the $[j/k_nq_n, (j+1)/k_nq_n)$ subdivisions of the levels. Those diagonals correspond to the boundary portion of the $n+1$-words (the b's and the e's). The diagonal paths that start in the region $[j/k_nq_n, (j+1)/k_nq_n)$ and traverse from the bottom to the top level while staying in that region correspond to the j^{th} argument of the $\mathcal{C}$ operator at stage n.

Restating this in terms of the isomorphism φ_0 between $\mathcal{K}_\alpha$ and $([0,1), \mathcal{R}_\alpha)$, if s_1 and s_2 are mature elements of $\mathcal{K}_\alpha$ corresponding to $x_1, x_2 \in S^1$, then:

- x_1, x_2 belong to two diagonal strips that do not touch a vertical strip and with base in the same interval $[j/k_nq_n, (j+1)/k_nq_n)$

  iff

- Inside their principal $n+1$-subwords, $s_1(0)$ and $s_2(0)$ are in n-words coming from the same argument w_j^α of $\mathcal{C}(w_0^\alpha, w_1^\alpha, \dots w_{k_n-1}^\alpha)$.

We now continue the enumeration of basic notions in [14] we use here.

7. In a very slight variation of the notation of [14], when we are comparing s with t we define $d^n(s,t) = r_n(t) - r_n(s) \pmod{q_n}$. In this argument frequently $t = \mathcal{S}_\beta(s)$ and if β is clear from the context we simply write $d^n(s)$. If x and y correspond to s and t, the number $d^n(s,t)$ can be viewed either as the number of levels in the n-tower between x and y or as the difference between the locations of 0 in the principal n-subwords of s and t.

8. For mature s and t, the result of shifting t by $-d^n(s,t)$ units is that the location of 0 is in the same position in its principal n-subword as is the position of $s(0)$ in its principal n-subword.

9. Applying the shift map $d^{n+1}(s,t)$ times to s moves its zero to the same point as t's is relative to its $n+1$ subword. Subsequently moving it back $-d^n(s,t)$ steps moves the zero of result back to the same position in its n-subword as zero is in s's n-subword. In other words, if s' is the result of applying the shift map to s $d^{n+1}(s,t) - d^n(s,t)$ times, then 0 is in the same position relative to the n-block of s' as it is in s.

10. The $n+1$-word in the construction sequence for $\mathcal{K}_\alpha$ is of the form

    $$\mathcal{C}(w_0^\alpha, w_1^\alpha \dots w_{k_n-1}^\alpha)$$

    and hence if s is mature at stage n then $s(0)$ occurs in an n-block corresponding to the position of $w_{j_0}^\alpha$ for some j_0. We can ask whether the j_0 corresponding to the principal n-subword of the $(d^{n+1}(s,t) - d^n(s,t))$-shift of s is the same as the j_0 corresponding to the principal n-subword of s.

    If it does, then s and t are *well-matched* at stage n and if not the s and t are *ill-matched* at stage n.

11. If s' is the result of shifting s $d^{n+1}(s,t) - d^n(s,t)$ times then the 0 of s' is in the same w_j^α as is the zero of t. So for the purposes of determining whether s is well-β-matched at stage n, we can compare which argument of $\mathcal{C}$ $s(0)$ and $t(0)$ belong to. As a result we can speak of s and t well or ill-matched at stage n. If x and y are the corresponding members of $[0,1)$ we can say say that x and y are well or ill-matched at stage n.

We are now ready to construct the non-central β. We do this by induction. At stage 1, $a_1 = 0$. At stage n, we let $\beta_n = \sum_{p=1}^{n-1} \frac{a_p}{k_p q_p}$. For $i = 0, \dots 6^n - 1$, in the terminology of item 11 consider

$$M_i = \{x : x \text{ and } x + \beta_n + i/k_n q_n \text{ are well-matched}\}.$$

Since the M_i's are disjoint, for some i, $\lambda(M_i) \leq \frac{1}{6^n}$. Let a_n be such an i and let $\beta_{n+1} = \beta_n + a_n/k_n q_n$. Finally we let $\beta = \sum_1^\infty \frac{a_p}{k_p q_p}$, so $\beta = \lim_{n\to\infty} \beta_n$.

To see this works, we first show that:

> For almost all x, for large enough m, if s_m corresponds to $x + \beta_m$ then for all mature $n \leq m, r_n(s_m) = r_n(\mathcal{S}_\beta(s))$.

This is a Borel-Cantelli argument. Note that if $r_m(s_m) = r_m(\mathcal{S}_\beta(s))$ then for all mature $n \leq m, r_n(s_m) = r_n(\mathcal{S}_\beta(s))$. Hence it suffices to show that for almost all s, all sufficiently large m, $r_m(s_m) = r_m(\mathcal{S}_\beta(s))$.

If x corresponds to s then the only way that $r_m(s_m) \neq r_m(\mathcal{S}_\beta(s))$ is if $x + \beta_m$ is in a different level of the m-tower than $x + \beta_m + \sum_{p=m}^\infty \frac{a_p}{k_p q_p}$. In turn, the only way that this can happen is if for some i,

$$x + \beta_m \in [i\alpha_m + 1/q_m - \sum_{p=m}^\infty \frac{a_p}{k_p q_p}, i\alpha_m + 1/q_m).$$

The latter interval is the right hand portion of a level in the m-tower, i.e. of an interval of the form $[i\alpha_m, i\alpha_m + 1/q_m)$.

The collection of x that have this property for a given level i has measure $\sum_{p=m}^\infty \frac{a_p}{k_p q_p}$. Since there are q_m many levels i, the measure of all of the x with this property at stage m is $q_m * \left(\sum_{p=m}^\infty \frac{a_p}{k_p q_p}\right)$. Computing:

$$\begin{aligned} q_m * \left(\sum_{p=m}^\infty \frac{a_p}{k_p q_p} \right) &= \frac{a_m}{k_m} + q_m * \sum_{m+1}^\infty \frac{a_p}{k_p q_p} \\ &< \frac{a_m}{k_m} + \frac{q_m}{q_{m+1}} \sum_{m+1}^\infty \frac{a_p}{k_p} \\ &\leq \frac{a_m}{k_m} + \frac{1}{k_m l_m q_m} C, \end{aligned}$$

where $C = \sum_1^\infty \frac{a_p}{k_p}$. Since we assume that $\sum \frac{6^n}{k_n} < \infty$ and $a_p < 6^{n-1}$, C is finite. We see immediately that the measures of the collections of x such that at some stage m the level of $x + \beta_m$ in the m-tower is different from the level of $x + \beta$ in the m-tower is summable. By Borel-Cantelli, it follows that for almost all s there is an N for all $m \geq N$, $r_m(s_m) = r_m(\mathcal{S}_\beta(s))$.

From the choice of a_n for all but a set of measure at most $1/6^n$, the s are ill-matched with s_{n+1}. Again by the Borel-Cantelli lemma, for almost all s there is an N_1 for all $n \geq N_1$ s and s_{n+1} are ill-matched. Since for almost all s and all large enough n the level of s_{n+1} is equal to the level $\mathcal{S}_\beta(s)$ it follows that for almost all s and all large enough n s is ill-matched with $\mathcal{S}_\beta(s)$. If ν is the unique invariant measure on $\mathcal{K}_\alpha$ then equation 33 of [14] defines

$$\Delta_n(\beta) = \nu(\{s : s \text{ is ill-}\beta\text{-matched at stage } n\}).$$

We have shown that $\Delta_n(\beta) \to_n 1$. Hence

$$\Delta(\beta) = \sum_n \Delta_n(\beta)$$

is infinite. Hence we have shown that β is not central. $\dashv$

We now prove Lemma 38

$\vdash$ [Lemma 38] First note that the analysis in section 6.3, on page 50 of [14], says that for any non-central β we can choose hd_1 and hd_2 and a spaced out set G such that, as in equation 35 on page 50, letting

$$\not\Downarrow_n = \{s : s \text{ is ill-}\beta\text{-matched at stage } n \text{ and in configuration } P_{hd_1,hd_2}\}$$

we get equation 36 on page 50 of [14]:

$$\sum_{n \in G} \nu(\not\Downarrow_n) = \infty. \tag{18}$$

We now observe that for $n < m \in G$, $\not\Downarrow_n$ and $\not\Downarrow_m$ are probabilistically independent. This follows from Lemma 75 on page 47 of [14]: belonging to $\not\Downarrow_n$ is an issue of the value of $d^{n+1} - d^n$. The differences $d^{m+1} - d^m$ are independent of the differences $d^{n+1} - d^n$, hence the sets $\not\Downarrow_n$ and $\not\Downarrow_m$ are pairwise independent. Which level x is on in the n-tower is independent of whether or not x is misaligned at the next stage.

Let M_m be the collection of s that are mature at stage m. Then applying the "hard" Borel-Cantelli lemma, for almost all $s \in M_m$, there are infinitely many $n \in G, s \in \not\Downarrow_n$. Since $\bigcup_m M_m$ has measure one, for almost all $s \in \mathbb{K}^c$ there are infinitely many $n, s \in \not\Downarrow_n$.

We now argue that if $\mathcal{J}_1$ and $\mathcal{J}_2$ are two joinings of $\mathbb{K}^c \times \mathbb{K}^c$ over $\mathcal{S}_\beta$, then they are identical. Thus they are both the relatively independent joining. The result follows from the following claim which is an analogue of the claim in Proposition 32 of [10]:

Claim Let $\mathcal{J}$ be a joining of $\mathbb{K}^c$ with itself that projects to the graph joining of $\mathcal{K}_\alpha$ with itself given by $\mathcal{S}_\beta$. Then for all cylinder sets $\langle a \rangle \times \langle b \rangle$ in $\mathbb{K}^c \times \mathbb{K}^c$, the density of occurrences of (a, b) in a generic pair (x, y) for $\mathcal{J}$ does not depend on the choice of (x, y).

$\vdash$ Since β is non-central, and x, y are generic and $\mathcal{J}$ extends $\mathcal{S}_\beta$, we know that for infinitely many $n \in G$ the n-words of x and y are misaligned. Let G^* be this set.

It suffices to show that:

- There is a sequence of subblocks of the principal $n+1$-subwords of x and y of total length B_n,
- as $n \in G^*$ goes to infinity, B_n/q_{n+1} goes to 0,
- after removing the subwords in B_n the number of occurrences of $\langle a \rangle \times \langle b \rangle$ is independent of the choice of (x, y).

Fix a large $n \in G^*$. We count occurrences of (a,b) in (x,y) over the portion of the principal $n+1$-subwords of x that overlap with the $n+1$-blocks of y. As in Proposition 32 of [10], we show that, up to a negligible portion, this is independent of (x,y). From the definition of $\not\Downarrow_n$ for $n \in G$, there are fixed values of hd_1 and hd_2. The number hd_2 determines the overlap of the $n+1$-block of x containing $x(0)$ is the left or right overlap. For convenience, assume that $hd_1 = L$ and $hd_2 = R$.

First: discard n-subwords that are not mature. This is a negligible portion.

Next, shift y back by $d^n(x)$, so that the mature n-subwords of x in the principal $n+1$-subword are aligned along the overlap of the principal $n+1$ subword of y with the corresponding n-subword of y.[11]

Then by specification J.10.1 and the fact that x and y are misaligned, any pair of n–words (u,v) occurs almost exactly $1/s_n^2$ times. So, after discarding a negligible portion of the occurrences all pairs occur the same number of times. Shifting them all back by $d^n(x)$, an amount determined by β and thus independent of x and y, gives a collection of counts of occurrences of (a,b) in all pairs $(u, sh^{d^n}(v))$ with all pairs occurring essentially the same number of times. The result is independent of the choice of x and y. The errors from the negligible portions and they go to zero in proportion to $n+1$. This proves the claim. ⊣

3.3 Diffeomorphisms of the Torus

The map $\mathcal{F} \circ F_{\mathcal{O}}$ maps codes for Π^0_1 sentences to construction sequence for circular systems. We now indicate how to realize circular systems as diffeomorphisms and why these diffeomorphisms are computable. The realization map is described completely in [13]. We review it here to verify its effectiveness.

The construction is in two stages. In both parts a sequence of periodic transformations is constructed and the limits are isomorphic to the given uniform circular system. In both constructions, the torus, viewed as $[0,1]\times[0,1]$ with appropriate edges identified, is divided into rectangles. These are then permuted by the periodic transformations according to the action of the shift operator on the circular system. In the first stage, this permutation is built without regard to continuity. The result is an abstract measure preserving transformation. In the second part, using smooth approximations to these permutations, the limit is a C^∞ diffeomorphism.

The main tool for moving from the discontinuous, symbolic transformations to the smooth geometric transformations is the Anosov-Katok method of Approximation by Conjugacy [1]. To allow for this smoothing the parameter sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$ must have the sequence of l_n's grow sufficiently fast.

The lower bounds $l_n^*(\langle k_m : m \le n\rangle, \langle l_m : m < n\rangle)$ will be determined inductively, the complete list of requirements on l_n^* appears in Appendix A.

For the moment we assume we are given the circular sequence $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ with prescribed coefficient sequences $\langle k_n, l_n : n \in \mathbb{N}\rangle$ where the l_n grow sufficiently fast.

The periodic approximations to the first stage transformation are of the form

$$T_n = Z_n \circ \overline{\mathcal{R}}_{\alpha_n} \circ Z_n^{-1} \tag{19}$$

which result from conjugating horizontal rotations $(x,y) \mapsto_{\overline{\mathcal{R}}_{\alpha_n}} (x+\alpha_n, y)$, with the more complicated transformations $h_n : \mathbb{T}^2 \to \mathbb{T}^2$ that permute rectangular subsets of $\mathbb{T}^2$. The α_n are the rationals constructed from the coefficient sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$ described in section 3.1.1. The maps Z_n are of the form

$$Z_n = h_1 \circ h_2 \circ \ldots \circ h_n$$

[11] Sections 4.3-4.6 of [14] discuss how the spacings of left and right overlaps correspond.

where h_i codes the combinatorial behavior of the i^{th} application of the $\mathcal{C}$-operation. The initial, discontinuous transformation T will then be the almost-everywhere pointwise limit of the sequence $\langle T_n : n \in \mathbb{N}\rangle$.

In the second part of the construction the h_n's will be replaced by smooth transformations h_n^s that are close measure theoretic approximations to the h_n's. This results in a new sequence

$$H_n = h_1^s \circ h_2^s \circ \cdots \circ h_n^s. \tag{20}$$

The analogue of equation 19 for the final smooth transformation is:

$$S_n = H_n \, \overline{\mathcal{R}}_{\alpha_n} \, H_n^{-1} \tag{21}$$

The sequence of S_n's converge in the C^∞-topology to a C^∞ measure preserving transformation $S : \mathbb{T}^2 \to \mathbb{T}^2$.

Why do we do this? In [13] it is shown that T is measure isomorphic to $\mathbb{K}^c$. Hence if $\mathbb{K}^c = \mathcal{F} \circ F(N)$ we have φ_N is true if and only $T \cong T^{-1}$. Since $S \cong T$, φ_N is true if and only $S \cong S^{-1}$. Thus if we define the realization function R by setting $R(\mathbb{K}^c) = S$, we see that $R \circ \mathcal{F} \circ F_{\mathcal{O}}$ is a reduction of the collection of codes for true Π_1^0-sentences to the set of recursive diffeomorphisms isomorphic to their inverses. This is the content of figure 1.

In addition to these results in [13], we will show that the sequence of S_n's can be taken to be effective, converge in the C^∞ topology and that if $S(N)$ comes from N and $S(M)$ comes from M, then $S(N) \ncong S(M)$. This will complete the proof of Theorem 1.

3.3.1 Painting the circular system on the torus

We encode the symbolic system $\mathbb{K}^c$ on the torus by inductively constructing the sequence of h_n's. The map h_0 is the identity map corresponding to $\mathcal{W}_0^c = \Sigma$. To build h_{n+1}, $\mathbb{T}^2$ is subdivided into rectangles which are then permuted.

Definition 39 (Rectangular subdivisions)**.** *Let $n, m \in \mathbb{N}$.*

- *For an arbitrary natural number q, $\mathcal{I}_q$ represent the collection of intervals* $[0, \frac{1}{q}),\ [\frac{1}{q}, \frac{2}{q}),\ \ldots, [\frac{q-1}{q}, 1)$.
- *Given $\mathcal{I}_q$ and $\mathcal{I}_s$, let $\mathcal{I}_q \otimes \mathcal{I}_s$ be the collection of all rectangles $R = I_0 \times I_1$, where $I_0 \in \mathcal{I}_q$ and $I_1 \in \mathcal{I}_s$.*
- *Let $D \subseteq \mathbb{T}^2$. Then, for a collection of rectangles ξ, the restriction of ξ to D is given by*
$$\xi \upharpoonright D = \{R \cap D : R \in \xi\}.$$
- *Recall the parameter sequences $\langle q_n : n \in \mathbb{N}\rangle$ and $\langle s_n : n \in \mathbb{N}\rangle$. Further recall that $s_n = |\mathcal{W}_n^c|$ and $q_n = |u|$ for $u \in \mathcal{W}_n^c$. Define*
$$\xi_n = \mathcal{I}_{q_n} \otimes \mathcal{I}_{s_n}.$$
- *Lastly, for $0 \le i < q_n$ and $0 \le j < s_n$, let $R_{i,j}^n$ be the element of ξ_n given by $[\frac{i}{q_n}, \frac{i+1}{q_n}) \times [\frac{j}{s_n}, \frac{j+1}{s_n})$.*

Note that there is a straightforward description of the action of $\overline{\mathcal{R}}_{\alpha_n}$ on ξ_n:

$$\overline{\mathcal{R}}_{\alpha_n} : R_{i,j}^n \mapsto R_{i+p_n,j}^n$$

where addition in the subscript is performed modulo q_n.

The map h_{n+1} will be defined as a permutation of $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}}$ and thus induces a permutation of ξ_{n+1}. It is important to make h_{n+1} commute with $\overline{\mathcal{R}}_{\alpha_n}$. To do this h_{n+1} is first defined on $(\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}}) \upharpoonright ([0, 1/q_n) \times [0, 1))$ and then copied over equivariantly to $\mathbb{T}^2$.

Constructing the h_n's: The paper [13] is concerned with realizing circular systems, and so builds the h_n's in terms of the *prewords* used to construct the sequence $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$. In the case that $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ is in the range of $\mathcal{F}$, the prewords are determined by the underlying odometer based sequence $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$. We describe h_{n+1} directly in terms of the odometer sequence $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle = F_{\mathcal{O}}(N)$.

Fix enumerations $\langle w_s^n : 0 \leq s < s_n\rangle$ of each $\mathcal{W}_n$. The words in $\mathcal{W}_{n+1}$ are concatenations of words in $\mathcal{W}_n$:

$$w_s^{n+1} = w_0 w_1 \dots w_{k_n-1}$$

where each $w_i = w_{s'}^n$ for some s'.

To each w_s^{n+1} associate the horizontal strip $[0,1) \times [s/s_{n+1}, (s+1)/s_{n+1})$ and each $w_{s'}^n$ with $[0,1) \times [s'/s_n, (s'+1)/s_n)$.

Proposition 40. *There is a permutation of $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}} \upharpoonright [0, 1/q_n) \times [0,1)$ such that for all $0 \leq s < s_{n+1}$,*

if $w_i = w_{s'}^n$ then

$$\begin{aligned} h_{n+1}([i/k_n q_n, (i+1)/k_n q_n) \times [s/s_{n+1}, (s+1)/s_{n+1})) \\ \subseteq [0, 1/q_n) \times [s'/s_n, (s'+1)/s_n). \end{aligned} \tag{22}$$

$\vdash$ Equation 22 gives regions that each atom of $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}} \upharpoonright [0,1/q_n) \times [0,1)$ must be sent to by h_{n+1}. To prove there is such a permutation we see that each region has exactly the same number of subrectangles as the cardinality of the collection of atoms that must map into it.

We count occurrences of n-words in $(n+1)$-words. Fix a word

$$w_s^{n+1} = w_0 w_1 \dots w_{k_n-1} \in \mathcal{W}_{n+1}.$$

Then, by strong uniformity each n-word $w_{s'}^n$ occurs k_n/s_n times as a w_i. So each word w_s^{n+1} puts k_n/s_n rectangles in a target region. Since there are s_{n+1} many words of the form w_s^{n+1} the target regions must contain $s_{n+1}(k_n/s_n)$ rectangles.

Each horizontal strip of $[0,1) \otimes \mathcal{I}_{s_n}$ is divided into s_{n+1}/s_n many horizontal strips by $[0,1) \otimes \mathcal{I}_{s_{n+1}}$ and each vertical strip of $\mathcal{I}_{q_n} \otimes [0,1)$ is divided into k_n many vertical strips by $\mathcal{I}_{k_n q_n} \otimes [0,1)$. Thus each atom of the partition $\xi_n \upharpoonright [0,1/q_n) \times \mathcal{I}_s$ is divided into $k_n(s_{n+1}/s_n)$ rectangles by $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}}$. In particular $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}} \upharpoonright [0,1/q_n) \times [s'/s_n, (s'+1)/s_n)$ has $k_n(s_{n+1}/s_n)$ many atoms.

Hence each target region contains the same number of rectangles as atoms sent to it and there is a map h_{n+1} satisfying equation 22. $\dashv$

Since h_{n+1} is a permutation of $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}} \upharpoonright [0,1/q_n) \times [0,1)$ for each $1 \leq i < q_n$, it can be copied onto each $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}} \upharpoonright [ip/q_n, (ip+1)/q_n)$. The result of this is a permutation of $\mathcal{I}_{k_n q_n} \otimes \mathcal{I}_{s_{n+1}}$ (and hence ξ_{n+1}) that commutes with the rotation $\overline{\mathcal{R}}_{\alpha_n}$.

Remark 41. *It is a clear that h_{n+1} can be defined in a primitive recursive way using the data $\mathcal{W}_{n+1}$.*

Remark It is shown in [13] that having defined the sequence of h_n's in this manner, for sufficiently fast growing l_n the transformations T_n converge in measure to a measure preserving transformation $T : (\mathbb{T}^2, \lambda) \to (\mathbb{T}^2, \lambda)$ that is isomorphic to the original circular system defined by $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$. The map taking $\langle \mathcal{W}_m^c : m \leq n\rangle$ to T_n is primitive recursive.

3.3.2 Smoothing the T_n

We now must smooth the T_n's to produce S_n's that have measure-theoretic limit S which is isomorphic to T. Secondly, we show that S is a recursive diffeomorphism.

For our discussion of smoothing we need an effective complete metric on the C^∞-diffeomorphisms. Note that the C^∞ topology is the coarsest common refinement of the C^k topologies for each $k \in \mathbb{N}$. There are many choices for effective/recursive metrics generating the C^k topology for each k. These metrics can be defined explicitly in terms of the partial derivatives $\frac{\partial^j}{\partial^{j_0} x_0 \partial^{j_1} x_1 \dots \partial^{j_l} x_l}$, for $j \leq k$. Given an effective sequence of complete metrics $\langle d^k : k \in \mathbb{N} \rangle$ generating the C^k topologies, with distances bounded by 1, then

$$d^\infty = \sum_{k=0}^{\infty} 2^{-(k+1)} d^k$$

generates the C^∞ topology.

Fix such a complete effective metric giving rise to the C^∞ topology on $\mathbb{T}^2$. Without loss of generality we can assume that

$$d^\infty(S,T) \leq \max_{x \in \mathbb{T}^2} d_{\mathbb{T}^2}(S(x), T(x)), \tag{23}$$

where $d_{\mathbb{T}^2}$ is the ordinary metric on $\mathbb{T}^2$.

To pass from the discontinuous Z_n's to diffeomorphisms, the h_i's are replaced by smooth h_i^s which are very close approximations and give the H_n's in equation 20. Then the H_n's will also be diffeomorphisms. While there is no control over the C^∞-norms of the H_n, the key observation at the heart of the Anosov-Katok method is the following: if h_{n+1}^s commutes with $\overline{\mathcal{R}}_{\alpha_n}$ then

$$\begin{aligned} S_n &= H_n \circ \overline{\mathcal{R}}_{\alpha_n} \circ H_n^{-1} \\ &= H_n \circ h_{n+1}^s \circ (h_{n+1}^s)^{-1} \circ \overline{\mathcal{R}}_{\alpha_n} \circ H_n^{-1} \\ &= H_n \circ h_{n+1}^s \circ \overline{\mathcal{R}}_{\alpha_n} \circ (h_{n+1}^s)^{-1} \circ H_n^{-1} \\ &= H_{n+1} \circ \overline{\mathcal{R}}_{\alpha_n} \circ H_{n+1}^{-1}. \end{aligned} \tag{24}$$

Hence by taking α_{n+1} sufficiently close to α_n, S_{n+1} can be taken as close as necessary to S_n in the C^∞-norm.

To carry out this plan we begin by describing how we smooth the h_n's. This is done explicitly in Theorem 35 of [13], which says:

Theorem 42 (Smooth permutations)**.** *Let $\mathbb{T}^2$ be divided into the collection of rectangles $\mathcal{I}_n \otimes \mathcal{I}_m$ and choose $\epsilon > 0$. Let σ be a permutation of the rectangles. Then there is an area preserving C^∞-diffeomorphism $\varphi : \mathbb{T}^2 \to \mathbb{T}^2$ such that φ is the identity on a neighborhood of the boundary of $[0,1] \times [0,1]$ and for all but a set of measure at most ϵ, if $x \in R$, then $\varphi(x) \in \sigma(R)$ for all $R \in \mathcal{I}_n \otimes \mathcal{I}_m$.*

In Lemma 36 of [13] it is shown that an arbitrary permutation of $\mathcal{I}_n \otimes \mathcal{I}_m$ can be built by taking a composition of transpositions of adjacent rectangles. The transformation φ is then built effectively as a composition of smooth near-transpositions that swap adjacent rectangles. We summarize the proof from [13]. The reader wanting more background details can consult Appendix D of [9], where it is shown that the construction can be carried out recursively in a code for the permutation σ.

The main technical point for building the near-transpositions of adjacent rectangles is captured by showing that for all $0 < \gamma < 1$ and arbitrarily small $\epsilon < 1 - \gamma$, there is a diffeomorphism φ_0 of the unit disk in $\mathbb{R}^2$ such that:

1. φ_0 rotates the top half of the disk of radius γ to the bottom half and vice versa.

2. φ_0 is the identity in a neighborhood of the unit circle of width less than ϵ.

The map φ_0 is constructed by considering a primitive recursive C^∞ map $f : [0, 1] \to [0, \pi]$ that is identically equal to π on $[0, \gamma]$ and is 0 in a neighborhood of 1. Then φ_0 rotates the circle of radius r by $f(r)$ radians. Taking γ very close to 1 gives a smooth near transposition.

Using Riemann mapping theorem techniques, these rotations of the disk can be copied over to measure preserving maps from $[-1, 1] \times [0, 1]$ to itself that

1. take all but $1 - \epsilon/2$ mass of $[-1, 0] \times [0, 1]$ to $[0, 1] \times [0, 1]$ and vice versa,

2. are analytic on the interior of $[-1, 1] \times [0, 1]$,

3. are the identity in a neighborhood of the boundary.

Since every permutation of $\{0, 1, \dots mn\}$ can be written as a composition of less than or equal to $(nm)^2$ transpositions of the form $(k, k+1)$, given any σ we can build φ by taking ϵ small enough and composing sufficiently good approximations between adjacent rectangles corresponding to the transpositions composed to create σ.

Building S_n. Using Theorem 42 we can effectively choose a smooth h^s_{n+1} which well-approximates h_{n+1} measure theoretically. By choosing the approximation well, we can guarantee that the S_n in equation 21 moves the partitions ξ_n very close to where the T_n's move the ξ_n's.

Since h^s_{n+1} is effective, using the continuity of composition with respect to d^∞, S_{n+1} can be made arbitrarily close to S_n by taking α_{n+1} sufficiently close to α_n. Thus if α_n converges to α sufficiently quickly, the sequence $\langle S_n : n \in \mathbb{N}\rangle$ is Cauchy with respect to the complete metric d^∞ and hence converges to a smooth measure preserving diffeomorphism S. Taking the sequence of h^s_n's to be sufficiently close to the h_n's the S_n's are sufficiently close to the T_n's to apply Lemma 30 of [13] to show that the diffeomorphism S is measure theoretically isomorphic to T. Hence $(\mathbb{T}^2, \lambda, S)$ is measure theoretically isomorphic to $(\mathbb{K}^c, \nu, \textsc{Sh})$.

The induction. The discussion above was predicated on choosing the l_n's to grow *fast enough*. We now show how to inductively choose lower bounds l^*_n on the l_n. Numerical Requirement E gives one collection of lower bounds for the l's, independently of the choices of the maps H_n and numbers α_n. Hence we choose l^*_n to dominate this sequence of lower bounds, as well as the lower bounds we add here.

Suppose we have defined H_{n+1} from h^s_{n+1} and H_n in a manner that satisfies equation 24 holds and that the H_n's can be computed effectively. Then, for any given ϵ, and small rational β,

$$d^\infty(H_{n+1}\overline{\mathcal{R}}_{\alpha_n+\beta}H^{-1}_{n+1}, H_n\overline{\mathcal{R}}_{\alpha_n}H^{-1}_n) \tag{25}$$

can be primitively recursively computed to within a given ϵ. Moreover, this is a decreasing function of β for small $\beta > 0$. Thus one one can effectively find a δ such that if $|\alpha_{n+1} - \alpha_n| < \delta$, then $d^\infty(S_{n+1}, S_n) < 2^{-(n+1)}$.

Recall the definitions of the $\alpha_n = p_n/q_n$ from equations 13, 14 and 15. Then α_n does not depend on l_n and

$$\alpha_{n+1} = \alpha_n + 1/k_n l_n q^2_n.$$

Thus to make α_{n+1} close to α_n it suffices to make l_n sufficiently large that

$$1/k_n l_n q^2_n < \delta. \tag{26}$$

Numerical Requirement G The parameter l_n is chosen sufficiently large that

$$d^\infty(S_{n+1}, S_n) < 2^{-(n+1)} \tag{27}$$

The numbers α_n, $\langle \mathcal{W}_m^c : m \leq n\rangle$ and $\langle h_m^s : m \leq n+1\rangle$ determine the δ in equation 26 and thus how large l_n must be. All of this data can be computed recursively from $\langle \mathcal{W}_m : m \leq n+1\rangle$. (We note that neither the choice of s_{n+1} nor the definition h_{n+1}^s uses l_n.)

3.3.3 The effective computation of S_n

We now show that each element of the sequence $\langle S_n : n \in \mathbb{N}\rangle$ is effectively computable (Definition 8).

Claim 43. *The functions h_n^s and $\mathcal{R}_{\alpha_n}$ are effectively computable C^∞-functions. As a consequence each S_n is effectively uniformly continuous.*

Proof of Claim 43. For simplicity of exposition, we only show how to compute the modulus of continuity and approximation for S_n itself; finding the modulus of continuity and approximations to the higher differentials is conceptually identical but notationally cumbersome.

Recall that we must produce two functions:

- A modulus of continuity, $d : \mathbb{N} \to \mathbb{N}$, and
- An approximation, $f : (\{0,1\} \times \{0,1\})^{<\mathbb{N}} \to (\{0,1\} \times \{0,1\})^{<\mathbb{N}}$.

It is routine to check that if T_0 and T_1 are effectively uniformly continuous—that is, if there exist moduli of continuity d_0 and d_1 and approximations f_0 and f_1 corresponding to each—then the composition, $T_1 \circ T_0$ is effectively uniformly continuous.

The second part of the claim follows from the first since Equations (21) and (20) show,

$$S_n = h_1^s \circ h_2^s \circ \cdots \circ h_n^s \circ \overline{\mathcal{R}}_{\alpha_n} \circ (h_n^s)^{-1} \circ \cdots \circ (h_2^s)^{-1} \circ (h_1^s)^{-1}. \tag{28}$$

The case of $\overline{\mathcal{R}}_{\alpha_n}$ is particularly simple. Since $\overline{\mathcal{R}}_{\alpha_n}$ is an isometry, it has a Lipschitz constant of 1. In particular, the modulus of continuity is simply given by $d(n) = n$, and, since $\overline{\mathcal{R}}_{\alpha_n}$ is well-defined on rational points, we can also determine the approximation by setting f to be

$$([x]_m, [y]_m) \mapsto ([x]_m + [\alpha_n]_m, [y]_m)$$

Where $[z]_m$ denotes the smallest dyadic rational $k \times 2^{1-m}$ for $0 \leq k \leq 2^m$ minimizing $|z - [z]_m|$.

In the case of h_m^s for $m \leq n$, recall from the discussion after Theorem 42 that h_m^s can be built as a composition of a sequence of smooth transpositions:

$$h_m^s = \sigma_0^s \circ \sigma_1^s \circ \cdots \circ \sigma_{t(m)}^s$$

Note that the number of transpositions necessary, $t(m) < |\xi_{m+1}|^2 = (k_m \cdot q_m \cdot s_{m+1})^2$, and is a computable function of m since it is the number of transpositions necessary to build the permutation in Proposition 40.

Since σ_j^s is a *smooth* transposition of an explicit form (see in Appendix D of [9] for background details), one can calculate a uniform Lipschitz constant L_j^s for it; hence, taking $L_m > \max_{s \leq t(m)} L_j^s$, we have that

$$|h_m^s(x) - h_m^s(y)| < (L_m)^{t(m)+1} |x - y|.$$

Consequently, a suitable modulus of continuity for h_m^s is given by

$$d(n) = n + \lceil t(m) \cdot \log_2(L_m) \rceil, \tag{29}$$

where $\lceil x \rceil$ is the smallest integer greater than x. The construction of a primitive recursive approximation to h_m^s is straightforward from the primitive recursive approximations to the σ_n^s's. As we remarked in Section 1.5, it follows that $(h_m^s)^{-1}$ is primitive recursive. $\dashv$

In summary, the modulus of continuity and approximation for S_n can be calculated using the following steps:

1. Compute the $\langle h_m : m \leq n \rangle$;
2. Build the approximations to h_m^s and $(h_m^s)^{-1}$ using h_m and the smooth transpositions σ_i^s
3. Compute the moduli of continuity of $\langle h_m^s : m \leq n \rangle$ and their inverses;
4. Compute $\langle \alpha_m : m \leq n \rangle$ (and, consequently, the approximations and moduli of continuity for $\langle \overline{\mathcal{R}}_{\alpha_m} : m \leq n \rangle$);
5. Compute the approximation and modulus of continuity of S_n by composing the approximations and moduli of continuity calculated in Steps 1 through 4 according to Equation (28).

3.4 Completing the proof

Theorem 1 claims the existence a computable function F, which on inputting a natural number N (corresponding to the Π_1^0 sentence $\varphi = \varphi_N$) outputs a code for a computable diffeomorphism $S(N)$ of $\mathbb{T}^2$. Whether or not $S(N)$ is measure theoretically conjugate to $S(N)^{-1}$ is equivalent to the truth or falsity of φ. Finally for different numerical inputs the corresponding S's will not be isomorphic. In summary, letting $S = S(N)$,

(A) If N codes φ, then φ is true if and only iff $S \cong S^{-1}$

(B) On input N, F recursively determines a code for an effectively C^∞ map of the torus to itself, i.e., F determines:

- i.) A computable function $d : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, where $d(k, -)$ computes the moduli of uniformity of the k^{th} differential of $S(N)$, and
- ii.) A computable function $f(k, -)$ where $f(k, -)$ is a map on dyadic rational points of $\mathbb{T}^2$ approximating $D^k S(N)$ (the k-th differential of $S(N)$). Given an input that is precise to $d(k, n)$ digits, $f(k, -)$ approximates the first n-partial derivatives $\{\frac{\partial^n}{\partial^i x \partial^{n-i} y} : 0 \leq i \leq n\}$ to n-digits.

(C) If $N \neq M$, then the associated diffeomorphisms $S(N)$ and $S(M)$ are not conjugate.

Because the function F maps natural numbers to natural numbers (the codes for the diffeomorphisms) we let $F^\flat$ be the associated function $R \circ \mathcal{F} \circ F_{\mathcal{O}}$ that maps into the space of actual diffeomorphisms. It produces a diffeomorphism of $\mathbb{T}^2$ from a Gödel number N for a Π_1^0 sentence. We show $F^\flat$ satisfies (A) and (C) and then argue there is a (primitively) computable routine coded by $F(N)$ that has the same values.

Item (A) Given N, $F_{\mathcal{O}}(N)$ computes an odometer-based construction sequence $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$. By Theorem 10, if $\mathbb{K}(N)$ is the uniquely ergodic symbolic shift associated with the construction sequence then $\mathbb{K}(N) \cong \mathbb{K}(N)^{-1}$ if and only if φ is true.

The sequences $\langle h^s_n : n \in \mathbb{N}\rangle$, $\langle l_n : n \in \mathbb{N}\rangle$, and $\langle \mathcal{W}^c_n : n \in \mathbb{N}\rangle$ are computed. If $\mathbb{K}^c$ is the circular system associated with $\langle \mathcal{W}^c_n : n \in \mathbb{N}\rangle$, then Proposition 36 shows that $\mathbb{K}^c \cong (\mathbb{K}^c)^{-1}$ if and only if φ is true.

Finally the realization map R preserves isomorphism. So if $S = R(\mathbb{K}^c)$, then $(\mathbb{T}^2, \lambda, S) \cong (\mathbb{T}^2, \lambda, S^{-1})$ if and only if φ is true.

Item (C) We need to see that for $M < N, S(N) \ncong S(M)$. Since the realization map R preserves isomorphism it suffices to see that $(\mathbb{K}^c)^M = \mathcal{F} \circ F_{\mathcal{O}}(M)$ is not isomorphic to $(\mathbb{K}^c)^N$.

By Corollary 35 we see that the Kronecker factor of $\mathbb{K}^M$ is $\mathcal{K}_{\alpha^M}$. Any isomorphism between $(\mathbb{K}^c)^N$ and $(\mathbb{K}^c)^M$ must take the respective Kronecker factor of one to the other, hence would imply an isomorphism between $\mathcal{K}_{\alpha^N}$ and $\mathcal{K}_{\alpha^M}$.

However this is impossible since Corollary 35 implies that $\pi > \alpha^M > \alpha^N > 0$.

Item (B) $F^\flat$ is a map from $\mathbb{N}$ to diffeomorphisms. By the result of Section 3.3.3, the diffeomorphisms are recursive. We must show that there is a recursive algorithm coding a function F that computes the moduli of continuity and approximations to each $F^\flat(N)$ and its differentials.

We use the notation $\mathbb{d}^N$ to denote the modulus of continuity returned by $F(N)$, and we use the notation $\mathbb{f}^N$ to denote the approximation. Without loss of generality, we restrict our attention to $d(0, -)$ and $f(0, -)$—that is, the C^0 modulus of continuity and approximation of S. The calculation for $d(k, -)$ and $f(k, -)$ for $k > 0$ is virtually identical conceptually. We simplify the notation of (B) above and write $\mathbb{d}^N(n)$ for $d(0, n)$ and $\mathbb{f}^N(\vec{s}, \vec{t})$ for $f(0, \vec{s}, \vec{t})$.

Let us first consider the modulus of continuity. The routine for computing $\mathbb{d}^N$ depends on choosing a large number of numerical parameters:

$$\epsilon_n, e(n), s_n, k_n, l_n, P_N.$$

These have numerical dependencies that are generally of the form $a_n \gg b_n$ or $a_n \ll b_n$. It is routine that these can be satisfied in a primitive recursive manner–provided that the dependencies are consistent. This is verified in Appendix A where it is shown that the dependencies among these constants form a directed acyclic graph.

The subroutine we describe next comes during the computation of $F(N)$, and hence we may assume that we have the coefficients $k_n(N-1), l_n(N-1)$ already computed. This computation was made during the first n steps of the computation of $F(N-1)$, but we neglect that recursion in this discussion.

For the inductive construction we note that:

For each $0 \le m \le n+1$, make the following calculations, which recursively depend on smaller m. Specifically, $\mathcal{W}_m$ is built from $\mathcal{W}_{m-1}$ using the Substitution Lemma (Proposition 21) as described in section 2.6. Then h^s_m is built from the information in the words in $\mathcal{W}_m$. This allows l_m to be chosen large enough that Numerical Requirement G holds. This in turn defines p_m and q_m and allows $\mathcal{W}^c_m$ to be built.

The algorithm is illustrated in Figure 4.

1. Using $\langle \epsilon_k : k \le m\rangle$ and $\mathcal{W}_{m-1}$, choose k_m large enough to satisfy the Numerical Requirements C and D and apply the Substitution Lemma $m+1$ times to generate $\mathcal{W}_m$;

2. Build h_m, smooth it to get h_m^s and hence H_m. Calculate H_m's modulus of continuity.

3. Choose l_m sufficiently large that Numerical Requirements E and F hold (with $n+1=m$).

4. Build $\mathcal{W}_m^c$.

5. Calculate the approximation and modulus of continuity corresponding to S_m using the methods of Section 3.3.3.

6. Continue until $m = n+1$ and $d^{S_N}(n+1)$, the $n+1^{st}$ approximation to the modulus of continuity of S_{n+1} is determined.

7. Output $d(n+1)(n+1) = d^{S_N}(n+1)$.

At the end, using the modulus of continuity d corresponding to S_{n+1}, output $\mathbb{d}^N(n) = d(0, n+1)$ where $d(n+1)$ is the modulus of continuity of S_{n+1}.

To verify that this procedure actually yields a modulus of continuity for S, recall that by Numerical Requirement G, Equation (27), it follows that

$$d^\infty(S_{n+1}, S) < 2^{-(n+1)}.$$

By inequality 23,

$$\max_{x \in \mathbb{T}^2} d_{\mathbb{T}^2}(S_{n+1}(x), S(x)) \leq d^\infty(S_{n+1}, S) < 2^{-(n+1)}.$$

Since $d(n+1)$ yields the number of digits of input necessary to approximate S_{n+1} to an accuracy of $2^{-(n+1)}$, it follows that the approximation of S_{n+1} is *itself* an approximation of S which, given $d(n+1)$ digits of binary input, is accurate to within 2^{-n}.

The approximation f for S is calculated almost identically, except for the output. Given

$$([x]_{\mathbb{d}^N(n)}, [y]_{\mathbb{d}^N(n)}) \in (\{0,1\} \times \{0,1\})^{d(n)}$$

the output is

$$\mathbb{f}^N(n+1) = \Big(f_0([x]_{\mathbb{d}^N(n)}, [y]_{\mathbb{d}^N(n)}), f_1([x]_{\mathbb{d}^N(n)}, [y]_{\mathbb{d}^N(n)})\Big)$$

where $f(n+1) = (f_0, f_1)$ is the approximation of S_{n+1} produced in Step 5, again in the notation that $[z]_m$ is a m-digit binary approximation of z.

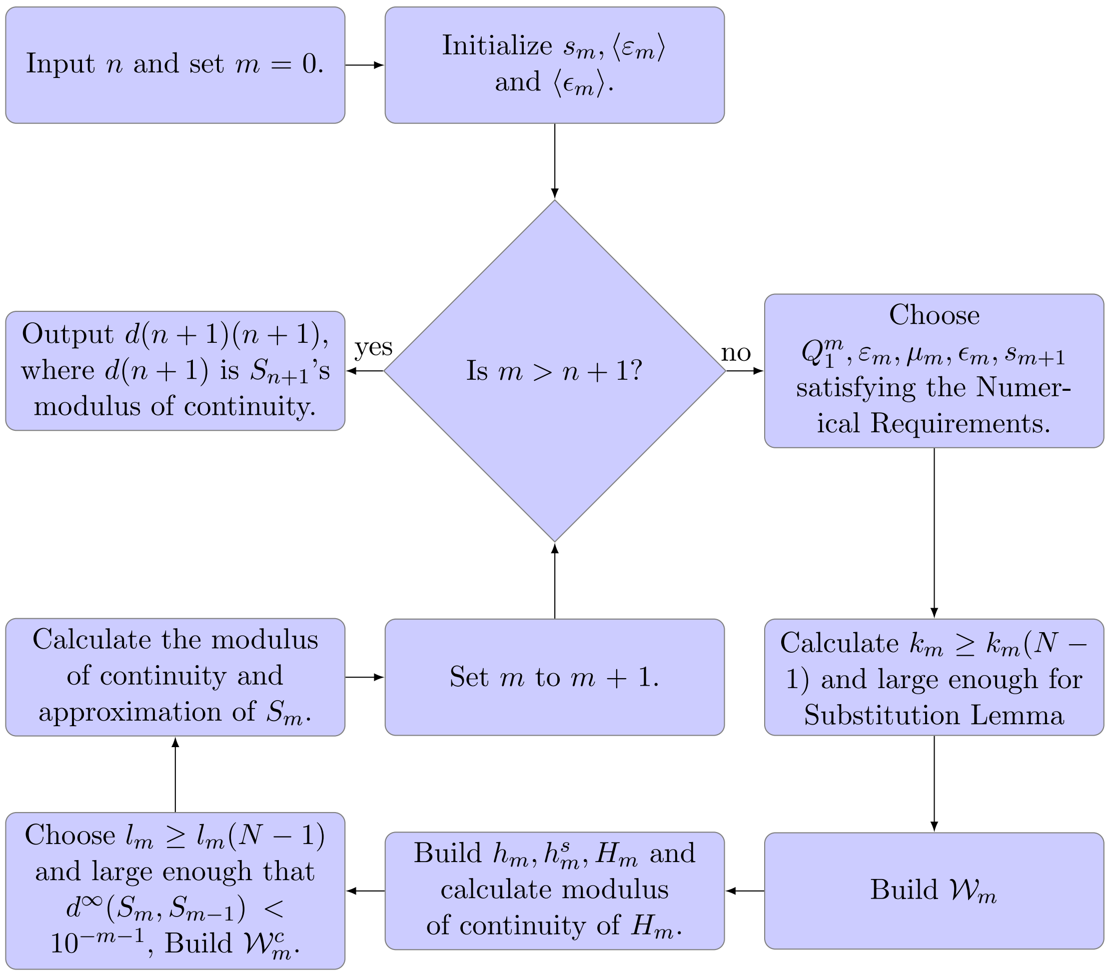

Figure 4: The algorithm for calculating the modulus of continuity d^N of S. This algorithm is easily altered to produce the approximation $\mathbb{f}^N$ of S simply by changing the output to $(f_0(\vec{x}, \vec{y}), f_1(\vec{x}, \vec{y}))$, where $f(n+1) = (f_0, f_1)$ is S_{n+1}'s approximation.

Appendix

In [9] there are three more appendices giving well-known background on topics in logic, dynamical systems and a proof of the "pasting lemma" we use in this paper. The pasting lemma there is a simplified version of an original proved by Moser ([22]).

A Numerical Parameters

A.1 The Numerical Requirements Collected.

In this appendix we review the requirements on the numerical parameters used in the construction. Specifically, in constructing the diffeomorphism $F(N)$ we build construction sequences $\langle \mathcal{W}_n : n \in \mathbb{N}\rangle$, $\langle \mathcal{W}_n^c : n \in \mathbb{N}\rangle$ that depend on N and realize the corresponding circular system $\mathbb{K}^c$ as a diffeomorphism. These steps are intertwined–for example the circular system is built as a function of the sequence $\langle k_n, l_n : n \in \mathbb{N}\rangle$. In turn the l_n are chosen as function of $\langle \mathcal{W}_m : m \leq n\rangle$ in order to facilitate the smooth construction. To rigorously complete the proof we need to review all of these parameters and see that the inductive choices can be made consistently in a primitive recursive way.

At many stages in this paper we appeal to results from [14]. Hidden in those appeals is a sequence of parameters $\langle \mu_n : n \in \mathbb{N}\rangle$ that is not explicitly mentioned in the construction presented here. For this reason in this review we include the inductive construction of $\langle \mu_n : n \in \mathbb{N}\rangle$.

A substantial difference between this paper and earlier constructions is that the domain of the reductions in [10] and [14] is the space of trees of finite sequences of natural numbers. The analogue in this paper is that the only trees considered here are the trees of sequences $\langle (0, 1, \dots n) : n < \Omega\rangle$ for Ω finite or infinite depending on the input N. We note that these trees are really "stalks" and are finite or infinite depending on Ω. Since the trees used in this paper are of this very special form, the requirements are easier to satisfy.

Another difference with this paper and [14] is that in the earlier paper it sufficed to pick the parameters *small enough* or *big enough* in the correct order to satisfy the Numerical Requirements. In this paper we are concerned with having an effective construction, so we need to be more explicit about the Numerical Requirements in certain places, or otherwise argue that they can be satisfied primitively recursively.

Closely following section 11 of [14] we begin with a review of the inductive requirements from [10]. We give them in the notation of [14]. These inductive requirements are modified and simplified in the construction in the current manuscript. We note the versions used in this paper.

Requirements that were instituted in [10] and their modifications. These requirements were dubbed *Inherited Requirements* in [14]. Requirements that were new in [14] are called simply *Numerical Requirements*, and requirements that explicitly used in the text of this paper are labelled with capital letters A-F.

Recall that the number of elements of $\mathcal{W}_m$ is denoted s_m; the numbers Q_s^m and C_s^m denote the number of classes and sizes of each class of $\mathcal{Q}_s^m$ respectively. From the construction in [10] we have sequences $\langle \epsilon_n : n \in \mathbb{N}\rangle$, $\langle s_n, k_n, e(n) : n \in \mathbb{N}\rangle$.

Inherited Requirement 1 $\langle \epsilon_n : n \in \mathbb{N}\rangle$ is summable.

Inherited Requirement 2 $2^{e(n)}$ the number of $\mathcal{Q}_{i+1}^n$ classes inside each $\mathcal{Q}_i^n$ class. The strictly monotone sequence of numbers $e(n)$ will be chosen to grow fast enough that

$$2^{(n+2)}2^{-e(n+1)} < \epsilon_n \tag{30}$$

Similarly we set $C_n^n = 2^{e(n)}$ for $m \leq n$ as well.

Modification: In this paper the construction is simplified so to build $\mathcal{W}_{n+1}$ we have exactly $n+2$-substitutions of each of size $2^{2e(n+1)}$. Hence we can replace this requirement by the simple formula $s_n = 2^{(n+1)e(n)}$. In particular s_m, Q_i^m and C_i^m are all to be powers of 2.

Inherited Requirement 3 For all n,

$$2\epsilon_n s_n^2 < \epsilon_{n-1} \tag{31}$$

Inherited Requirement 4

$$\epsilon_n k_n s_{n-1}^{-2} \to \infty \text{ as } n \to \infty \tag{32}$$

Inherited Requirement 5

$$\prod_{n \in \mathbb{N}} (1 - \epsilon_n) > 0 \tag{33}$$

Comment: Since this is equivalent to the summability of the ϵ_n-sequence, it is redundant and we will ignore in the rest of this paper

Inherited Requirement 6 (Original Version) There will be prime numbers p_i such that $K_i = p_i^2 s_{i-1} K_{i-1}$ (i.e. $k_i = p_i^2 s_{i-1}$). The p_n's grow fast enough to allow the probabilistic arguments in [10] involving k_n to go through.

Modification For all n, $k_n = P_N 2^\ell s_n$, where for each n, ℓ is large enough for the substitution argument involving k_n to go through.

Comment: In [10] K_n was a product of a sequence of prime numbers. The requirement on the sequences of prime numbers was that they were almost disjoint for different trees and that they grew sufficiently quickly. In this paper K_N is $P_N * 2^\ell$ for a large ℓ.

Since we have only one collection of very special trees the requirement simplifies to needing that the ℓ in the exponent grows sufficiently quickly for the Substitution Lemma (Proposition 21) argument to work.

Inherited Requirement 7 s_n is a power of 2.

Comment: This again is redundant as the modified Inherited Requirement 2 says directly that $s_n = 2^{(n+1)e(n)}$.

Inherited Requirement 8 For all n, $\epsilon_n < 2^{-n}$.

Numerical Requirements introduced in [14]

Numerical Requirement 1 $l_0 > 20$ and $\sum_{k=n} 1/l_k < 1/l_{n-1}$.

Numerical Requirement 2 $\langle \varepsilon_n : n \in \mathbb{N} \rangle$ is a sequence of numbers in $[0, 1)$ such that $6 \sum_{n>N} \varepsilon_n < \varepsilon_N$.

Numerical Requirement 3 k_n, l_n and q_n grow fast enough that $\varepsilon_n k_n \to \infty$, $\varepsilon_n l_n \to \infty$, $\varepsilon_n q_n \to \infty$.

Numerical Requirement 4 $\sum \frac{|G_1^n|}{Q_1^n} < \infty$.

Modification In this paper case $|G_1^n| \leq 2$ so numerical requirement 4 becomes

$$\sum_n \frac{1}{Q_1^n} < \infty.$$

Comment: Since $Q_1^n = 2^{e(n)}$ and Inherited Requirement 2 implies that $2^{n+1}2^{-e(n)} \to 0$, this requirement is redundant in this paper.

Numerical Requirement 5 μ_n is chosen sufficiently small relative to $\min(\varepsilon_n, 1/Q_1^n)$.

Explicitly: let $t_n = \min(\varepsilon_n, 1/Q_1^n)$ and take

$$0 < \mu_n < t_n \min_{k \leq n} 2^{-n-2} \left(\frac{1}{t_k}\right).$$

Then for all m

$$t_m > \sum_{n=m}^{\infty} \frac{\mu_n}{t_n}.$$

Numerical Requirement 6 l_n is big enough relative to a lower bound determined by $\langle k_m, s_m : m \leq n\rangle$, $\langle l_m : m < n\rangle$ and s_{n+1} to make the periodic approximations to the diffeomorphism $F(N)$ converge. Moreover $k_n \leq l_n$.

Numerical Requirement 7 s_n goes to infinity as n goes to infinity and s_{n+1} is a power of s_n.

Comment Since s_n is a power of $2^{e(n)}$ we know that $s_n \to \infty$ as long as $e(n) \to \infty$. Making s_{n+1} a power of s_n is simply an algebraic condition on $e(n+1)$.[12]

Numerical Requirement 8 $s_{n+1} \leq s_n^{k_n}$.

Numerical Requirement 9 The ϵ_n's are decreasing, $\epsilon_0 < 1/40$ and $\epsilon_n < \varepsilon_n$.

Numerical Requirement 10 k_n is chosen large enough relative to the lower bound determined by s_{n+1}, ϵ_n to apply the Substitution Lemma and construct the words in $\mathcal{W}_{n+1}$. Implicitly this requires that $1/k_n < \epsilon_n^3/4$.

Comment: This is essentially the same as Inherited Requirement 6.

Numerical Requirement 11 ϵ_n is small relative to μ_n.

Modification Remark 94 of [14] discusses quantities $r(x,y), r(x,\mathcal{C}), f(x)$ that are determined by counting occurrences of x, y in words in an alphabet $\mathcal{L}$ with s letters that have a given length ℓ. It says that for all $\mu > 0$ there is an $\epsilon = \epsilon(\mu, s)$ such that if for all $x, y \in \mathcal{L}$,

$$\left|\frac{r(x,y)}{\ell} - \frac{1}{s^2}\right| < \epsilon$$

then for all x:

$$\left|\frac{r(x,\mathcal{C})}{f(x)} - \frac{C}{s}\right| < \mu$$

[12] Any choice of $e(n+1)$ with $e(n+1) = (k-1)n + k - 2 + ke(n)$ makes $s_{n+1} = s_n^k$. So we choose $e(n+1)$ of this form using a large k.

From the proof of the lemma it is straightforward to find an explicit formula for $\epsilon(\mu, |C|, \ell, s)$ for an upper bound on ϵ. The *small relative clause* can be rephrased as asking that

$$\epsilon_n < \epsilon(\mu_n, C_1^n, q_n, s_n).$$

Since $C_1^n = 2^{-e(n)}s_n$, $\epsilon(\mu_n, C_1^n, q_n, s_n)$ is really a function of μ, q_n, s_n.

Numerical Requirement 12 $\epsilon_0 k_0 > 20$, the $\epsilon_n k_n$'s are increasing and $\sum 1/\epsilon_n k_n < \infty$.

Numerical Requirement 13 The numbers ϵ_n should be small enough, as a function of Q_1^n, that for all $w_0, w_1 \in \mathcal{W}_{n+1}^c \cup \text{Rev}(\mathcal{W}_{n+1}^c)$ with $[w_0]_1 \neq [w_1]_1$ the following inequality holds:

$$\left| \frac{|\{i \in I^* : [u'_i]_1 = [v'_i]_1\}|}{|I^*|} - \frac{1}{Q_1^n} \right| < \frac{1}{Q_1^n}. \tag{34}$$

Numerical Requirements introduced in this paper

In this paper we have some supplemental numerical requirements. We list only those that are not redundant given the requirements listed above.

Numerical Requirement B $k_n(N-1) \leq k_n(N)$.

Numerical Requirement D $1/k_n < \epsilon_n^3/100$.

Numerical Requirement E $l_n(N-1) \leq l_n(N)$.

Numerical Requirement F $\sum \frac{6^n}{k_n} < \infty$.

Numerical Requirement G $d^\infty(S_{n+1}, S_n) < 2^{-(n+1)}$.

A.2 Resolution

A list of parameters, their first appearances and their constraints

We classify the constraints on a given sequence according to whether they refer to other sequences or not.

Computable collections of requirements on an element x_n in a sequence $\vec{x} = \langle x_n : n \in \mathbb{N}\rangle$ that are all of the form "x_n is large enough" or all of the form "x_n is small enough" that inductively refer to $\langle x_m : m \leq n-1\rangle$ are straightforwardly consistent and can be satisfied with a primitive recursive construction. For example a requirement that a certain inductively constructed sequence involving a given variable be summable is satisfied by asking that the n^{th} sequence be less than 2^{-n}. Similarly conditions that refer to the first n steps in the computation of any parameters in $F(N-1)$ are not at risk of being circular and hence can be satisfied without affecting the conditions themselves. We call these *Absolute* conditions.

Those requirements on $\vec{x}$ that refer to other sequences $\vec{y}$ risk the possibility of being circular and thus inconsistent. We refer to these conditions as *Dependent* conditions. The Dependent conditions are those that introduce the risk of not having solution. (See [14] for more discussion of this.)

1. **The sequence $\langle k_n : n \in \mathbb{N}\rangle$.**

   Absolute conditions:

A1 The sum $\sum_n 6^n/k_n$ is finite.

A2 $k_0 = P_N$ and $k_n(N) \geq k_n(N-1)$

Dependent conditions:

D1 Numerical Requirement 10, is a lower bound for k_n depends on s_{n+1}, ϵ_n, asking that k_n be large enough for the word construction using the Substitution Lemma to work.

Why is this primitive recursive? Given s_{n+1} and ϵ_n, the discussion in the proof of Lemma 23 shows that a lower bound for k_n can be given from Hoeffding's Inequality (Theorem 22) in a primitive recursing way. So the issue is circularity rather than computability.

D2 Inherited Requirement 6. In this context it says that $K_n = P_N 2^\ell s_n$ for a large ℓ.

Why is this primitive recursive? K_n is defined inductively $K_n = k_{n-1}k_{n-2}\ldots k_0$. So D3 is easily seen since $k_0 = P_N$ and for $n > 0$, k_n is defined in equation 11 where it is s_n times 2^ℓ for some ℓ. The size of ℓ is determined by **D1**.

D3 From Inherited Requirement 4, equation 32 requires that $\epsilon_n k_n s_{n-1}^{-2}$ goes to ∞ as n goes to ∞.

Why is this primitive recursive?: This can be satisfied primitively recursively by choosing k_n to be an integer larger than $\frac{s_n^2}{\epsilon_n}$.

We note that equation 32 implies that $\epsilon_n k_n > s_n^2$ and by requirement 7 $s_n \to \infty$. Hence $\sum 1/\epsilon_n k_n$ is finite.

D4 Numerical Requirement 8 implies that k_n is large enough that $s_{n+1} \leq s_n^{k_n}$.

Comment: This is easily satisfied by taking $k_n \geq \frac{log(s_{n+1})}{log(s_n)}$.

D5 Numerical Requirement D says $1/k_n < \epsilon_n^3/100$. *Comment:* As long as ϵ_n is defined before k_n, Requirement D is immediate by taking $k_n > 4/\epsilon_n^3$.

D6 Numerical Requirement 12 says that $\epsilon_0 k_0 > 20$ and the $\epsilon_n k_n$'s are increasing and $\sum 1/\epsilon_n k_n$ is finite.

Why is this primitive recursive? As noted the summability condition follows from D3. The other part of Numerical Requirement 12 is satisfied primitive recursively by taking k_n to be an integer at least $\frac{n}{\epsilon_n}$.

From D1-D5, we see that k_n is dependent on the choices of $\langle k_m, l_m : m < n\rangle, \langle s_m : m \leq n+1\rangle$, and ϵ_n, and these dependencies can be satisfied primitively recursively.

2. **The sequence $\langle l_n : n \in \mathbb{N}\rangle$.**

Absolute conditions

A3 Numerical Requirement E: $l_n(N) \geq l_n(N-1)$.

A4 Numerical Requirement 1 says that $1/l_n > \sum_{k=n+1}^{\infty} 1/l_k$. We also require that $l_n > 20{*}2^n$, an exogenous requirement.

Dependent conditions

D7 By Numerical Requirement 6, l_n is bigger than a number determined by $\langle k_m, s_m : m \leq n\rangle, \langle l_m : m < n\rangle$ and s_{n+1}. This is superseded by the more explicit Numerical Requirement G says that $d^\infty(S_{n+1}, S_n) < 2^{-(n+1)}$.

Why is this primitive recursive? The $\| \|_\infty$-norm of $S \circ T$ can be computed effectively from the $\| \|_\infty$-norms of S and T. In particular there is a primitively recursively computable real number M such that

$$\begin{aligned} d^\infty(S_{n+1}, S_n) &< M|\alpha_{n+1} - \alpha_n| \\ &\leq \frac{M}{q_{n+1}}. \end{aligned}$$

and the latter inequality is from equation 15.

D8 By Numerical Requirement 3, $\varepsilon_n q_n \to \infty$. This can be arranged by taking l_n to be large enough relative to ε_n that $\varepsilon_n q_n > \max(\varepsilon_{n-1} q_{n-1}, n)$.
Why is this primitive recursive? Because $q_{n+1} = k_n l_n q_n^2$ there is an explicit lower bound on l_n in terms of ϵ_{n+1}.

Thus l_n depends on $\langle k_m, s_m : m \leq n\rangle$, $\langle l_n : m < n\rangle$, ε_{n+1} and s_{n+1}.

3. **The sequences $\langle s_n : n \in \mathbb{N}\rangle$ and $\langle e(n) : n \in \mathbb{N}\rangle$.** We treat these sequences as equivalent since $s_n = 2^{(n+1)e(n)}$.

<u>Absolute conditions</u>

A5 Inherited Requirement 7 says that s_n is a power of 2.

A6 The sequence s_n goes to infinity.

A7 s_{n+1} is a power of s_n.

<u>Dependent conditions</u>

D9 The function $e(n) : \mathbb{N} \to \mathbb{N}$ referred to in equation 30 gives the number of $\mathcal{Q}^n_{s+1}$ classes inside each $\mathcal{Q}^n_s$ class. It has the dependent requirement that $2^{n+1}2^{-e(n)} < \epsilon_{n-1}$. Moreover $s_n = 2^{(n+1)e(n)}$.

The result is that s_{n+1} depends on the first $n+1$ elements of $\mathcal{T}$ $\langle k_m, s_m, l_m : m < n\rangle$, s_n, and ϵ_n.[13]

Why is primitive recursive? The only requirement for choosing s_{n+1} is that

$$2^{-e(n+1)} < \epsilon_n 2^{-n}$$

and this is clearly primitively recursively satisfiable.

4. **The sequence $\langle \epsilon_n : n \in \mathbb{N}\rangle$.**

<u>Absolute conditions</u>

A8 Numerical Requirement 9 and Inherited Requirement 1 say that the $\langle \epsilon_n : n \in \mathbb{N}\rangle$ is decreasing and summable and $\epsilon_0 < 1/40$.

A9 Inherited Requirement 8 says that $\epsilon_n < 2^{-n}$

<u>Dependent conditions</u>

[13] It is important to observe that the choice of s_{n+1} does *not* depend on k_n or l_n.

D10 Numerical Requirement 9 says $\epsilon_n < \varepsilon_n$.

D11 Equation 31 of Inherited Requirement 3 says $2\epsilon_n s_n^2 < \epsilon_{n-1}$

D12 Numerical Requirement 11 says that ϵ_n must be small enough relative to μ_n.
Why is this primitive recursive? This is shown in [14] using Lemma 97, which describes how to calculate an explicit function $\epsilon(\mu_n, q_n, s_n)$ such that Numerical Requirement 11 holds if $\epsilon_n < \epsilon(\mu_n, q_n, s_n)$.

D13 Numerical Requirement 13 says that ϵ_n is small as a function of Q_1^n.
Why is this primitive recursive? This is shown in the argument in Sublemma 99 of [14], which gives appropriate effective upper bounds using Hoeffding's Inequality.

The result is that ϵ_n depends exogenously on the first n elements of $\mathcal{T}$, and on Q_1^n, s_n, ε_n, ϵ_{n-1} and μ_n.

5. **The sequence $\langle \varepsilon_n : n \in \mathbb{N} \rangle$.**

<u>Absolute conditions</u>

A10 Numerical Requirement 2 says that $6 \sum_{n>N} \varepsilon_n < \varepsilon_N$. This can be arranged by taking $\varepsilon_n < 12^{-n}\varepsilon_{n-1}$.

<u>Dependent conditions</u>

Numerical Requirement 3 imposes three potential Dependent conditions on ε_n: $\varepsilon_n k_n \to \infty$, $\varepsilon_n l_n \to \infty$, $\varepsilon_n q_n \to \infty$. We deal with these in turn.

(a) The requirement that $\langle \varepsilon_n k_n : n \in \mathbb{N} \rangle$ goes to infinity already follows from the fact that $\epsilon_n < \varepsilon_n$ and item D6.

(b) $\langle \varepsilon_n l_n : n \in \mathbb{N} \rangle$ goes to infinity. This follows from $k_n \leq l_n$, which is covered in Dependent condition D7.

(c) $\langle \varepsilon_n q_n : n \in \mathbb{N} \rangle$ goes to infinity. This follows from Dependent condition D8.

Since Numerical Requirement 3 from items D6-8, all of the requirements on $\langle \varepsilon_n : n \in \mathbb{N} \rangle$ are absolute or follow from previously resolved dependencies. Moreover they are trivial to satisfy primitively recursively.

6. **The sequence $\langle Q_1^n : n \in \mathbb{N} \rangle$.**

Recall Q_1^n is the number of equivalence classes in $\mathcal{Q}_1^n$. We require:

<u>Absolute conditions</u>

A11 The only requirement on the choice of Q_1^n not accounted for by the choices of the other coefficients is that $\sum 1/Q_1^n < \infty$.

<u>Dependent conditions</u>

None.

7. **The sequence $\langle \mu_n : n \in \mathbb{N} \rangle$.**

This sequence gives the required pseudo-randomness in the timing assumptions.

<u>Absolute conditions</u>

None.

<u>Dependent conditions</u>

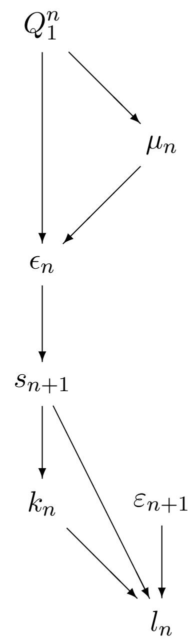

Figure 5: Order of choice of Numerical parameters dependency diagram.

D14 Numerical Requirement 5 appearing in this paper is written explicitly as follows: Set $t_n = \min(\varepsilon_n, 1/Q_1^n)$ and take

$$0 < \mu_n < t_n \min_{k \leq n} 2^{-n-2} \left(\frac{1}{t_k}\right).$$

Then for all m

$$t_m > \sum_{n=m}^{\infty} \frac{\mu_n}{t_n}.$$

Thus Numerical Requirement 5 requires that μ_n satisfy a primitive recursive dependent condition depending on ε_n and Q_1^n.

The recursive dependencies of the various coefficients are summarized in Figure 5, in which an arrow from a coefficient to another coefficient shows that the latter is dependent on the former.

Order of choices We begin by setting: $s_0 = 2, s_1 = 8, p_0 = 0, q_0 = k_0 = 1, l_0 = 21$. Q_1^0 is not defined, but Q_1^1 is determined by s_1. $\mu_0 = \epsilon_0 = k_0 = l_0 = 1$, $\varepsilon_0 = 1.1$, $\varepsilon_1 = \varepsilon_0/12$,

Assume:

The coefficient sequences $\langle k_m, l_m, Q_1^m, \mu_m, \epsilon_m : m < n\rangle$, $\langle \varepsilon_m : m \leq n\rangle$ and s_n have been chosen. It is know whether $n < \Omega$.

To do:

Choose $k_n, l_n, Q_1^n, \mu_n, \epsilon_n, \varepsilon_{n+1}$ and s_{n+1}. Each requirement is to choose the corresponding variable *large enough* or *small enough* where these adjectives are determined by the dependencies enumerated above.

Figure 5 gives an order to consistently choose the next elements on the sequences; Choose the successor coefficients in the following order:

$$Q_1^n, \varepsilon_n, \mu_n, \epsilon_n, s_{n+1}, k_n, l_n.$$

References

[1] D. V. Anosov and A. B. Katok. New examples in smooth ergodic theory. Ergodic diffeomorphisms. *Trudy Moskov. Mat. Obšč.*, 23:3–36, 1970.

[2] Hirotada Anzai. On an example of a measure preserving transformation which is not conjugate to its inverse. *Proc. Japan Acad.*, 27:517–522, 1951.

[3] S. Banerjee and P. Kunde. Real-analytic abc constructions on the torus. *Ergodic Theory and Dynamical Systems*, 39(10):2643–2688, 2019.

[4] Shilpak Banerjee. Non-standard real-analytic realizations of some rotations of the circle. *Ergodic Theory Dynam. Systems*, 37(5):1369–1386, 2017.

[5] Vasco Brattka, Peter Hertling, and Klaus Weihrauch. A tutorial on computable analysis. In *New computational paradigms*, pages 425–491. Springer, New York, 2008.

[6] Martin Davis, Yuri Matijasevič, and Julia Robinson. Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 323–378. (loose erratum). Amer. Math. Soc., Providence, R. I., 1976.

[7] Herbert B. Enderton. *A mathematical introduction to logic.* Harcourt/Academic Press, Burlington, MA, second edition, 2001.

[8] Matthew Foreman. A descriptive view of ergodic theory. In *Descriptive set theory and dynamical systems (Marseille-Luminy, 1996)*, volume 277 of *London Math. Soc. Lecture Note Ser.*, pages 87–171. Cambridge Univ. Press, Cambridge, 2000.

[9] Matthew Foreman. Godel diffeomorphisms. arXiv:2009.06735, pages 1–94, 2020.

[10] Matthew Foreman, Daniel J. Rudolph, and Benjamin Weiss. The conjugacy problem in ergodic theory. *Ann. of Math. (2)*, 173(3):1529–1586, 2011.

[11] Matthew Foreman and Benjamin Weiss. Odometers and circular systems: measures invariant under diffeomorphisms. *To Appear.*

[12] Matthew Foreman and Benjamin Weiss. From odometers to circular systems: a global structure theorem. *J. Mod. Dyn.*, 15:345–423, 2019.

[13] Matthew Foreman and Benjamin Weiss. A symbolic representation for Anosov-Katok systems. *J. Anal. Math.*, 137(2):603–661, 2019.

[14] Matthew Foreman and Benjamin Weiss. Measure preserving diffeomorphisms of the torus are unclassifiable. *arXiv:1705.04414v2*, pages 1–80, 2020.

[15] Johann Gaebler. The reverse math strength of Gödelian diffeomorphisms. *To Appear.*

[16] Eli Glasner. *Ergodic theory via joinings*, volume 101 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[17] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38(1):173–198, 1931.

[18] Paul R. Halmos. *Lectures on ergodic theory.* Chelsea Publishing Co., New York, 1960.

[19] Paul R. Halmos and John von Neumann. Operator methods in classical mechanics. II. *Ann. of Math. (2)*, 43:332–350, 1942.

[20] Jeffrey C. Lagarias. An elementary problem equivalent to the Riemann hypothesis. *Amer. Math. Monthly*, 109(6):534–543, 2002.

[21] Yuri V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts, 1993.

[22] Jürgen Moser. On the volume elements on a manifold. *Trans. Amer. Math. Soc.*, 120:286–294, 1965.

[23] Piergiorgio Odifreddi. *Classical recursion theory*, volume 125 of *Studies in Logic and the Foundations of Mathematics.* North-Holland Publishing Co., Amsterdam, 1989. The theory of functions and sets of natural numbers, With a foreword by G. E. Sacks.

[24] Karl Petersen. *Ergodic theory*, volume 2 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1989. Corrected reprint of the 1983 original.

[25] Marian B. Pour-El and J. Ian Richards. *Computability in analysis and physics.* Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1989.

[26] Daniel J. Rudolph. *Fundamentals of measurable dynamics.* Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1990. Ergodic theory on Lebesgue spaces.

[27] J. von Neumann. Zur Operatorenmethode in der klassischen Mechanik. *Ann. of Math. (2)*, 33(3):587–642, 1932.

[28] Peter Walters. *An introduction to ergodic theory*, volume 79 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1982.

[29] Benjamin Weiss. *Single orbit dynamics*, volume 95 of *CBMS Regional Conference Series in Mathematics.* American Mathematical Society, Providence, RI, 2000.