Article:

Jaidee, S, Moss, P and Ward, T (2019) Time-changes preserving zeta functions. Proceedings of the American Mathematical Society, 147 (10). pp. 4425-4438. ISSN: 0002-9939

https://doi.org/10.1090/proc/14574

TIME-CHANGES PRESERVING ZETA FUNCTIONS

SAWIAN JAIDEE, PATRICK MOSS, AND TOM WARD

To Graham Everest (1957–2010), in memoriam

Abstract. We associate to any dynamical system with finitely many periodic orbits of each period a collection of possible time-changes of the sequence of periodic point counts for that specific system that preserve the property of counting periodic points for some system. Intersecting over all dynamical systems gives a monoid of time-changes that have this property for all such systems. We show that the only polynomials lying in this monoid are the monomials, and that this monoid is uncountable. Examples give some insight into how the structure of the collection of maps varies for different dynamical systems.

1. Introduction

We are concerned with operations (that we will call time-changes) that act on integer sequences and preserve the following property. An integer sequence (a_n) is called *realizable* if there is a map $T\colon X \to X$ with the property that

$$a_n = \mathrm{Fix}_{(X,T)}(n) = |\{x \in X \mid T^n x = x\}|$$

for all $n \geqslant 1$. In this case we will also say that the sequence (a_n) is *realized* by the *system* (X,T). If we require X to be a compact metric space and T to be a homeomorphism, or indeed if we require T to be a C^∞ diffeomorphism of the 2-torus, then the same collection of sequences is characterized by this definition (by work of Puri and the last author [8] or Windsor [11], respectively). Notice that not all integer sequences are realizable: certainly if (a_n) is realizable then $a_n \geqslant 0$ for all $n \geqslant 1$, but there are congruence conditions as well. For example, $a_2 - a_1$ is the number of points that live on closed orbits of length precisely 2 under the map T, so $a_2 - a_1$ must be both non-negative and even.

Certain operations on integer sequences preserve the property of being realizable for trivial reasons. If (a_n) is realized by (X,T) and (b_n) by (Y,S), then the product sequence (a_nb_n) is realized by the Cartesian product $T\times S\colon X\times Y \to X\times Y$, defined by $(T\times S)(x,y) = (T(x),S(y))$ for all $(x,y) \in X\times Y$. Similarly, the sum (a_n+b_n) is realized by the disjoint union $T\sqcup S\colon X\sqcup Y \to X\sqcup Y$, where $T\sqcup S$ is defined as

$$(T\sqcup S)(z) = \begin{cases} T(z) & \text{if } z \in X; \\ S(z) & \text{if } z \in Y. \end{cases}$$

Date: February 6, 2019.
2010 *Mathematics Subject Classification.* Primary 37P35, 37C30, 11N32.
The first author thanks Khon Kaen University for funding a research visit to Leeds University, and thanks the Research Visitors' Centre at Leeds for their hospitality. The third author thanks the Lorentz Centre, Leiden, where much of the work was done.

All these statements may also be expressed in terms of the *dynamical zeta function* of (X,T), formally defined as $\zeta_{(X,T)}(z)=\exp\left(\sum_{n\geqslant 1}\mathrm{Fix}_{(X,T)}(n)\frac{z^n}{n}\right)$. Here we are interested in properties of the collection of all possible dynamical zeta functions. Thus, for example, the space of all zeta functions is closed under multiplication, because the sum of two realizable sequences is realizable, and is closed under a Hadamard-like formal multiplication because the product is. We refer to work of Carnevale and Voll [1] or Pakapongpun and the last author [6, 7] for more on the combinatorial and analytic properties of these 'functorial' operations on realizable sequences.

A different kind of operation on sequences (or on zeta functions) is a *time change*, defined as follows. Any function $h\colon\mathbb{N}\to\mathbb{N}$ defines an operation on integer sequences by sending (a_n) to $(a_{h(n)})$. If the original sequence (a_n) is realized by (X,T), then this may be thought of as replacing the sequence of iterates $T,T^2,T^3,\dots$, whose fixed point counts give the sequence (a_n), with the time-changed sequence $T^{h(1)},T^{h(2)},T^{h(3)},\dots$. The question we are interested in is this: counting the number of points fixed by those iterates $T^{h(1)},T^{h(2)},T^{h(3)},\dots$ gives an integer sequence. Is it possible that this sequence counts periodic points for some (other) system (Y,S)?

Definition 1. For a map $T\colon X\to X$ with $\mathrm{Fix}_{(X,T)}(n)<\infty$ for all $n\geqslant 1$, define

$$\mathscr{P}(X,T)=\{h\colon\mathbb{N}\to\mathbb{N}\mid\left(\mathrm{Fix}_{(X,T)}(h(n))\right)\text{ is a realizable sequence}\}$$

to be the set of *realizability-preserving time-changes for* (X,T). Also define

$$\mathscr{P}=\bigcap_{\{(X,T)\}}\mathscr{P}(X,T)$$

to be the monoid of *universally realizability-preserving time-changes*, where the intersection is taken over all systems (X,T) for which $\mathrm{Fix}_{(X,T)}(n)<\infty$ for all $n\geqslant 1$.

Some remarks are in order.

(a) Clearly the identity map defined by $h(n)=n$ for all $n\in\mathbb{N}$ lies in $\mathscr{P}(X,T)$ for any system (X,T). Thus $\mathscr{P}$ is non-empty.
(b) If functions h_1,h_2 lie in $\mathscr{P}$, then their composition $h_1\circ h_2$ also lies in $\mathscr{P}$, because by definition if (a_n) is a realizable sequence then $(a_{h_2(n)})$ is also realizable, and so $(a_{h_1(h_2(n))})$ is too. Thus $\mathscr{P}$ is a monoid inside the monoid of all maps $\mathbb{N}\to\mathbb{N}$ under composition.
(c) Notice that $\mathscr{P}(X,T)$ is a certain collection of functions defined by (X,T), but it will typically be some *other system* (Y,S) that bears witness to the statement $h\in\mathscr{P}(X,T)$, by satisfying the property

$$\mathrm{Fix}_{(Y,S)}(n)=\mathrm{Fix}_{(X,T)}(h(n))$$

for all $n\geqslant 1$.
(d) The requirement that $\mathrm{Fix}_{(X,T)}(n)<\infty$ for all $n\geqslant 1$ is natural for the type of question we are interested in, and will be assumed of all systems from now on.

It is not obvious that any non-trivial maps h could have either of the properties in Definition 1, but the following simple examples show how functions with this type of property can arise.

Example 2. If $|X| = 1$, then $\mathrm{Fix}_{(X,T)}(n) = 1$ for all $n \geqslant 1$, so the sequence of periodic point counts for (X, T) is the constant sequence $(1, 1, 1, \dots)$. Any function $h\colon \mathbb{N} \to \mathbb{N}$ time-changes this constant sequence to itself, so lies in $\mathscr{P}(X, T)$ because it is realized by the system (X, T) itself. Thus in this case $\mathscr{P}(X, T) = \mathbb{N}^{\mathbb{N}}$ is the monoid of all maps $\mathbb{N} \to \mathbb{N}$.

Example 3. If $h\colon \mathbb{N} \to \mathbb{N}$ is a constant function, with $h(n) = k$ for all $n \geqslant 1$, then for any system (X, T) the time-change produces the constant sequence whose nth term is $\mathrm{Fix}_{(X,T)}(k)$ for all $n \geqslant 1$. This sequence is realized by the system (Y, S), where $|Y| = \mathrm{Fix}_{(X,T)}(k)$ and S is the identity map. That is, $h \in \mathscr{P}$.

Example 4. For any system (X, T) we clearly have $\mathrm{Fix}_{(X,T)}(2n) = \mathrm{Fix}_{(X,T^2)}(n)$ for all $n \geqslant 1$, because the $2n$th iterate of T is the nth iterate of T^2. Thus the map h defined by $h(n) = 2n$ for all $n \geqslant 1$ is a member of $\mathscr{P}(X, T)$ for any system (X, T), and so is universally realizability-preserving. Thus $h \in \mathscr{P}$.

Our purpose is to prove two results about the structure of $\mathscr{P}$, and describe some examples that expose more subtle possibilities for the collection of functions $\mathscr{P}(X, T)$.

Theorem 5. *A polynomial lies in $\mathscr{P}$ if and only if it is a monomial.*

We illustrate what is going on in Theorem 5 with examples. Some of these involve statements about specific dynamical systems, and an adequate reference for these results is [2, Ch. 11].

Example 6. (a) Let (X, T) denote the 'golden mean' system. This is one of a family of maps called shifts of finite type. It is defined on the space

$$X = \{(x_n)_{n\in\mathbb{Z}} \in \{0, 1\}^{\mathbb{Z}} \mid x_k = 1 \implies x_{k+1} = 0 \text{ for all } k \in \mathbb{Z}\}$$

by the left shift, so T sends $(x_n)_{n\in\mathbb{Z}}$ to the sequence whose kth term is x_{k+1} for all $k \in \mathbb{Z}$. Then it may be shown that

$$\mathrm{Fix}_{(X,T)}(n) = \operatorname{trace} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \tag{1}$$

for all $n \geqslant 1$, so $\mathrm{Fix}_{(X,T)}(n)$ is the nth Lucas number, the sequence of periodic point counts begins $(1, 3, 4, 7, 11, \dots)$, and $\zeta_{(X,T)}(z) = \frac{1}{1-z-z^2}$. The Cartesian square $T \times T$ is also a shift of finite type, and a calculation shows that

$$\zeta_{(X\times X,T\times T)}(z) = \tfrac{1}{(1+z)(1-2z-2z^2+z^3)}.$$

Theorem 5 asserts in part that the map h defined by $h(n) = n^2$ for all $n \geqslant 1$ lies in $\mathscr{P}$. In particular, this means that there is *some* system (Y, S) whose sequence of periodic point counts is obtained by sampling the Lucas sequence along the squares, namely $(1, 7, 76, 2207, \dots)$. Such a system cannot be conjugate to a shift of finite type, because $\limsup_{n\to\infty} \frac{1}{n^2} \log \mathrm{Fix}_{(Y,S)}(n) = \log\left(\frac{1+\sqrt{5}}{2}\right) > 0$, while shifts of finite type have periodic point counts that only grow exponentially fast, because they can be expressed in terms of the trace of powers of an integer matrix as in (1).

(b) In the reverse direction, Theorem 5 says that the map h defined by $h(n) = n^2+1$ for all $n \geqslant 1$ is not universally realizability-preserving. This means there must be *some* system (X, T) with the property that time-changing by sampling its periodic point counts along the polynomial n^2+1 produces an integer sequence which cannot be the periodic point count of *any* map. A system that bears witness to the fact that $h \notin \mathscr{P}$ may be constructed as follows. Let $X = \mathbb{N}$, and define a map $T\colon X \to X$ as follows:

- $T(1) = 1$, so the subset $\{1\}$ consists of a single closed orbit of length 1 for T;
- $T(2) = 3$, and $T(3) = 2$, so the subset $\{2, 3\}$ consists of a single closed orbit of length 2 for T;
- $T(4) = 5, T(5) = 6$, and $T(6) = 4$, so the subset $\{4, 5, 6\}$ consists of a single closed orbit of length 3 for T;

and so on, resulting in a system (X, T) which has exactly one closed orbit of length n for every $n \geqslant 1$. We will write $\mathrm{Orb}_{(X,T)}(n) = 1$ for all $n \geqslant 1$ to express this. Now $\mathrm{Fix}_{(X,T)}(n) = \sum_{d\,|n} d\mathrm{Orb}_{(X,T)}(d) = \sigma(n)$ (the sum of divisors of n), since the points fixed by T^n are exactly the union of the d points lying on each closed orbit of length d for each divisor d of n. Thus the sequence of periodic point counts for (X, T) begins $(1, 3, 4, 7, 6, 12, \dots)$. Time-changing this along the polynomial given by $n^2 + 1$ gives the sequence $(3, 6, 18, 18, 42, \dots)$ which cannot count the periodic points of any map, as such a map would need to have $\frac{6-3}{2}$ closed orbits of length 2.
(c) A Lehmer–Pierce sequence, with nth term $|\det(A^n - I)|$ for some integer matrix A, counts periodic points for an ergodic toral endomorphism if it is non-zero for all $n \geqslant 1$. Time-changing it along the squares then gives a sequence that counts periodic points for some map, and this sequence has a characteristic quadratic-exponential growth rate, resembling a 'bilinear' or 'elliptic' divisibility sequence. However, it will have fundamentally different arithmetic properties, and cannot be an elliptic sequence by work of Luca and the last author [4].

Theorem 5 suggests that $\mathscr{P}$ is (unsurprisingly) small, but work of the second author may be used to show that there are many other maps in $\mathscr{P}$, resulting in the following result. This will be proved in Section 3.

Theorem 7. *The monoid $\mathscr{P}$ is uncountable.*

2. Proofs of Theorem 5

First we recall from [8] that an integer sequence (a_n) is realizable if and only if

$$\frac{1}{n}\sum_{d\,|n}\mu(n/d)a_d = \frac{1}{n}\sum_{d\,|n}\mu(d)a_{n/d} \in \mathbb{N}_0 \tag{2}$$

for all $n \geqslant 1$, where μ denotes the Möbius function. Equivalently, (a_n) is realizable if and only if $(\mu * a)(n)$ is non-negative and divisible by n for all $n \geqslant 1$, where $*$ denotes Dirichlet convolution.

The condition (2) characterizes realizability because we have

$$a_n = \mathrm{Fix}_{(X,T)}(n) = \sum_{d\,|n} d\mathrm{Orb}_{(X,T)}(d)$$

for all $n \geqslant 1$ if and only if

$$\mathrm{Orb}_{(X,T)}(n) = \frac{1}{n}\sum_{d\,|n}\mu(n/d)\mathrm{Fix}_{(X,T)}(d) = \frac{1}{n}(\mu * a)(n)$$

is the number of closed orbits of length n under T, for all $n \geqslant 1$.

Proof of 'if' in Theorem 5: monomials preserve realizability. We follow the method of the thesis [5] of the second author. Assume that $h(n) = cn^k$ for some $c \in \mathbb{N}$ and $k \in \mathbb{N}_0$.

If $k = 0$, then the result is clear, as the constant sequence $(a_c, a_c, a_c, \dots)$ is realized by the space comprising a_c points all fixed by a map (as mentioned in Example 3 above). If (a_n) is realized by (X, T), then (a_{cn}) is realized by (X, T^c) for any $c \in \mathbb{N}$ (as mentioned in Example 4 above for $c = 2$), so it is enough to consider the case $h(n) = n^k$ for some $k \geqslant 1$.

Assume therefore that (a_n) is realizable — which for this argument we think of as satisfying (2) rather than in terms of a system that realizes the sequence — and write $b_n = a_{n^k}$ for $n \geqslant 1$. We wish to show property (2) for the sequence (b_n). Fix $n \in \mathbb{N}$, and let $n = p_1^{n_1} \cdots p_r^{n_r}$ be its prime decomposition, with $n_j \geqslant 1$ for $j = 1, \dots, r$. Then

$$(\mu * b)(n) = a_{n^k} - \sum_{p_i} a_{n^k/p_i^k} + \sum_{p_i, p_j} a_{n^k/p_i^k p_j^k} - \cdots + (-1)^r a_{n^k/p_1^k \cdots p_r^k} \tag{3}$$

where $p_i, p_j, \dots$ are distinct members of $\{p_1, \dots, p_r\}$. Let

$$\delta = n^k / p_1^{k-1} \cdots p_r^{k-1},$$

so in particular $n \big| \delta$. Let

$$e = \sum_{\substack{m \,|n^k \\ \delta \,|m}} \sum_{d \,|m} \mu(m/d) a_d. \tag{4}$$

Since (a_n) is realizable, we have by (2) that

$$m \Big| \sum_{d \,|m} \mu(m/d) a_d \geqslant 0,$$

so in particular $e \geqslant 0$ and $n \big| e$. Thus it is enough to show that $e = (\mu * b)(n)$. Let $m \big| n^k$ with $\delta \big| m$, so that we may write

$$m = p_1^{k(n_1-1)+j_1} \cdots p_r^{k(n_r-1)+j_r} \tag{5}$$

with $1 \leqslant j_1, \dots, j_r \leqslant k$. Thus by (4) we have

$$e = \sum_{j_1=1}^{k} \cdots \sum_{j_r=1}^{k} \sum_{d \,|m} \mu(d) a_{m/d}$$

with m given by (5). Let

$$m_1 = m / p_1^{k(n_1-1)+j_1} = p_2^{k(n_2-1)+j_2} \cdots p_r^{k(n_r-1)+j_r}. \tag{6}$$

Then we have

$$\sum_{d \,|m} \mu(d) a_{m/d} = \sum_{d \,|m_1} \mu(d) \big(a_{m/d} - a_{m/p_1 d} \big).$$

Thus, because m_1 is independent of j_1,

$$\sum_{j_1=1}^{k} \sum_{d \,|m} \mu(d) a_{m/d} = \sum_{d \,|m_1} \sum_{j_1=1}^{k} \mu(d) \big(a_{m/d} - a_{m/p_1 d} \big)$$

and hence

$$\sum_{j_1=1}^{k}\sum_{d\,|m}\mu(d)a_{m/d}=\sum_{d\,|m_1}\mu(d)\big(a_{p_1^{kn_1}m_1/d}-a_{p_1^{k(n_1-1)}m_1/d}\big).$$

It follows from (4) that

$$e=\sum_{j_2=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d\,|m_1}\mu(d)\big(a_{p_1^{kn_1}m_1/d}-a_{p_1^{kn_1}m_1/p_1^k d}\big),$$

where m_1 is given by (6). The same procedure may be repeated, first setting

$$m_2=m_1/p_2^{k(n_2-1)+j_2},$$

to obtain $e=e_1-e_2$, where

$$e_1=\sum_{j_3=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d\,|m_2}\mu(d)\big(a_{p_1^{kn_1}p_2^{kn_2}m_2/d}-a_{p_1^{kn_1}p_2^{kn_2}m_2/p_2^k d}\big)$$

and

$$e_2=\sum_{j_3=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d\,|m_2}\mu(d)\big(a_{p_1^{kn_1}p_2^{kn_2}m_2/p_1^k d}-a_{p_1^{kn_1}p_2^{kn_2}m_2/p_1^k p_2^k d}\big).$$

Continuing inductively shows that each expression obtained matches up with a term in (3), as required. □

Proof of 'only if' in Theorem 5: only monomials preserve realizability. This argument proceeds rather differently, because we are free to construct dynamical systems with convenient properties to constrain what the polynomial can be. So assume that

$$h(n)=c_k+c_{k-1}n+c_{k-2}n^2+\cdots+c_0n^k$$

is a polynomial in $\mathscr{P}$ with $c_0\neq 0$, $k\geqslant 1$, and $h(\mathbb{N})\subset\mathbb{N}$. For completeness we recall the following well-known result.

Lemma 8. *The coefficients of h are rational, and the set of primes dividing some $h(n)$ with $n\in\mathbb{N}$ is infinite.*

Proof. We have

$$\begin{pmatrix}h(1)\\h(2)\\h(3)\\\vdots\\h(k+1)\end{pmatrix}=\begin{pmatrix}1&1&1&\cdots&1\\1&2&4&\cdots&2^k\\1&3&9&\cdots&3^k\\\vdots\\1&(k+1)&(k+1)^2&\cdots&(k+1)^k\end{pmatrix}\begin{pmatrix}c_k\\c_{k-1}\\c_{k-2}\\\vdots\\c_0\end{pmatrix},$$

and the determinant $\prod_{1\leqslant i<j\leqslant k+1}(j-i)$ of this matrix (a so-called 'Vandermonde' determinant, an instance of Stigler's law [12]) is non-zero, so the coefficients of h are all rational.

Turning to the prime divisors of the values of h, if $c_k=0$ the claim is clear, and if $k=1$ then c_0 and c_1 are integers so we may write c_1+c_0n as $\gcd(c_1,c_0)\big(c_1'+c_0'n\big)$ with $\gcd(c_1',c_0')=1$ to see this, so assume that $c_k\neq 0$ and $k>1$. Then we may write $h(n)=np(n)+c_k$ for some polynomial p of positive degree. We may not have $p(\mathbb{N}) \subset \mathbb{N}$ of course, but h (and hence p) certainly has rational coefficients. Then we have

$$\frac{m!c_k^2 p(m!c_k^2) + c_k}{c_k} = m!c_k p(m!c_k^2) + 1 = \frac{h(m!c_k^2)}{c_k}.$$

If m is large then $p(m!c_k^2)$ is an integer because p has rational coefficients and c_k is rational, so $h(m!c_k^2)$ must be divisible by some prime greater than m. $\square$

Using Lemma 8, we let q be a very large prime dividing some value of h, let n_0 be the smallest value of n such that $q\big|h(n)$, and let (X,T) consist of a single orbit of length q. (Looking further ahead, it is here that we are failing to solve question (e) from Section 5, in that we choose the system using information from the candidate polynomial rather than universally.) Then, by construction,

$$a_n = \mathrm{Fix}_{(X,T)}(n) = \begin{cases} 0 & \text{if } q\not|\, n; \\ q & \text{if } q\big|n. \end{cases} \tag{7}$$

Thus the assumption that $h \in \mathscr{P}$ means that $(a_{h(n)})$ is a realizable sequence, and we know from (7) that it only takes on the values 0 and q. Since q is prime, we have

$$a_{h(1)} \equiv a_{h(q)} \pmod q$$

by (2). Since $(a_{h(n)})$ only takes the values 0 and q, we deduce from (7) that n_0 is the smallest n such that $a_{h(n)} = q$. Thus the sequence $(a_{h(n)})$ starts

$$(a_{h(n)}) = (0, \dots, 0, q, \dots) \tag{8}$$

with the first q in the $h(n_0)$th place. Now $(a_{h(n)})$ is, by the assumption that $h \in \mathscr{P}$, realizable by some dynamical system (Y,S), so (8) says that S has no fixed points, no points of period 2, and so on, but it has q points of period $h(n_0)$. By (2) this is only possible if $h(n_0)\big|q$, so we deduce that

$$h(n_0) = q. \tag{9}$$

Now consider the points of period $2n_0$ in (Y,S). There are $a_{h(2n_0)}$ of these points, and of course any point fixed by S^{n_0} is also fixed by S^{2n_0}, so

$$a_{h(2n_0)} \geqslant a_{h(n_0)} = q.$$

On the other hand, the sequence $(a_{h(n)})$ only takes on the values 0 and q, so in fact

$$a_{h(2n_0)} = q.$$

The same argument shows that $a_{h(jn_0)} = q$ for all $j \geqslant 1$. By (7), it follows that $q\big|h(jn_0)$ for all $j \geqslant 1$. Thus we have

$$\begin{aligned} h(n_0) &= c_k + c_{k-1}n_0 + \cdots + c_0 n_0^k \equiv 0, \\ h(2n_0) &= c_k + c_{k-1}2n_0 + \cdots + c_0 2^k n_0^k \equiv 0, \\ &\vdots \\ h((k+1)n_0) &= c_k + c_{k-1}(k+1)n_0 + \cdots + c_0 (k+1)^k n_0^k \equiv 0 \end{aligned}$$

modulo q. That is,

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^k \\ 1 & 3 & 9 & \cdots & 3^k \\ \vdots & & & & \\ 1 & (k+1) & (k+1)^2 & \cdots & (k+1)^k \end{pmatrix} \begin{pmatrix} c_k \\ c_{k-1}n_0 \\ c_{k-2}n_0^2 \\ \vdots \\ c_0 n_0^k \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

modulo q. Since k is fixed and q is large, the determinant $\prod_{1\leqslant i<j\leqslant k+1}(j-i)$ of this matrix is non-zero modulo q, so we deduce that the matrix is invertible modulo q, and hence

$$c_{k-j}n_0^j \equiv 0 \pmod{q} \tag{10}$$

for $j = 0, \dots, k$.

Now, by definition, n_0 is the smallest n with $q\big|h(n)$, which tells us nothing about the size of n_0. However, we have seen in (9) that the realizability preserving property shows that $h(n_0) = q$. It follows that for large q we have

$$n_0 \approx \left(\frac{q}{c_0}\right)^{1/k} \ll q$$

since $c_0 \neq 0$. So (10) shows that

$$c_{k-j}n_0^j \approx c_{k-j}\left(\frac{q}{c_0}\right)^{j/k} \ll q$$

for $j \leqslant k-1$, and therefore the congruences in (10) in fact imply a list of equalities,

$$c_k = c_{k-1} = \cdots = c_1 = 0$$

because we can choose q to be as large as we please. It follows that $h(n) = c_0 n^k$, as claimed. We can of course deduce nothing about c_0, because $c_0 n_0^k \approx q$. □

3. Examples and Proof of Theorem 7

The statement that monomials are realizability-preserving in Theorem 5 may be applied in several ways to give (potentially) new results about existing sequences as follows. If (a_n) is an integer sequence known to be realized by some system (X, T), then Theorem 5 says that (a_{n^k}) is also realizable for any $k \in \mathbb{N}$. The basic relation (2) then allows us to deduce three types of result:

- *Congruences* in the spirit of Fermat's little theorem, because
$$\sum_{d\,|n} \mu(n/d) a_{d^k} \equiv 0$$
modulo n for all $n \geqslant 1$.
- *Positivity statements*, because $\sum_{d\,|n} \mu(n/d) a_{d^k} \geqslant 0$ for all $n \geqslant 1$.
- *Integrality statements*, because the collection of all closed orbits for a system (X, T) may be thought of as a disjoint union of individual orbits, showing that
$$\zeta_{(X,T)}(z) = \exp\left(\sum_{n\geqslant 1} \mathrm{Fix}_{(X,T)}(n)\tfrac{z^n}{n}\right) = \prod_{n\geqslant 1}\left(1 - z^n\right)^{-\mathrm{Orb}_{(X,T)}(n)},$$

so the Taylor expansion of $\zeta_{(X,T)}(z)$ at $z = 0$ automatically has integer coefficients, and hence the Taylor expansion of $\exp\left(\sum_{n\geqslant 1} a_{n^k}\frac{z^n}{n}\right)$ at $z = 0$ has integral coefficients.

The congruence statements may be thought of as generalizations of Fermat's little theorem because of the following simple example.

Example 9. The full shift T on $a \geqslant 2$ symbols (that is, the left shift on the sequence space $X = \{1, 2, \ldots, a\}^{\mathbb{Z}}$) has $\mathrm{Fix}_{(X,T)}(n) = a^n$ for all $n \geqslant 1$. Following the three observations above, we deduce from Theorem 5 the following statements, for any $k \in \mathbb{N}$ and for all $n \geqslant 1$:

- $\sum_{d\,|n} \mu(n/d)a^{d^k} \equiv 0$ modulo n, so in particular we have $a^{p^k} \equiv a$ modulo p for any prime p;
- $\sum_{d\,|n} \mu(n/d)a^{d^k} \geqslant 0$;
- the Taylor expansion of $\exp\left(\sum_{n\geqslant 1} a^{n^k}\frac{z^n}{n}\right)$ at $z = 0$ has integer coefficients.

These statements are all straightforward, but the same conclusions hold starting from any realizable sequence (a_n). To illustrate the type of conclusions one may reach, we list some less straightforward examples. Links to the Online Encyclopedia of Integer Sequences [10] are included for convenience. In each case a family of congruence, positivity, and integrality results of the same shape follow from Theorem 5.

- The Bernoulli numerators (τ_n) or denominators (β_n), define by $\left|\frac{B_{2n}}{2n}\right| = \frac{\tau_n}{\beta_n}$ in lowest terms for all $n \geqslant 1$, where $\frac{t}{\mathrm{e}^t-1} = \sum_{n=0}^{\infty} B_n\frac{t^n}{n!}$ (see A27641, shown to be realizable in [3]; A2445 shown to be realizable in [5], respectively).
- The Euler numbers $\left((-1)^n E_{2n}\right)$, where $\frac{2}{\mathrm{e}^t+\mathrm{e}^{-t}} = \sum_{n=0}^{\infty} E_n\frac{t^n}{n!}$ (see A364, shown to be realizable in [5]).
- The Lucas sequence $(1, 3, 4, 7, 11, \ldots)$ (see A204 and [9] for its special status as a realizable sequence).
- The divisor sequence $(\sigma(n)) = (1, 3, 4, 7, 6, 12, 8, \ldots)$.

Example 10. The following sequences of coefficients are integral, answering questions raised in the relevant Online Encyclopedia of Integer Sequences entry.

- The sequence A166168 is the sequence of Taylor coefficients of the zeta function of the dynamical system with periodic point data given by time-changing the Lucas sequence along the squares, and so is integral as conjectured in the Online Encyclopedia of Integer Sequences. More generally, the same property holds for the Lucas sequence sampled along any integer power.
- We have $\exp\left(\sum_{n\geqslant 1}\sigma(n)\frac{z^n}{n}\right) = \sum_{n\geqslant 0} p(n)z^n$, where p is the partition function A41; time-changing along the squares gives as Taylor coefficients the Euler transform of the Dedekind ψ function. The argument here shows that sampling along any power also gives integral Taylor coefficients.

Because of the diversity of integer sequences satisfying the condition (2), it is clear that the property of preserving realizability is extremely onerous. Indeed, the forward direction of Theorem 5 (stating that monomials are universally realizability-preserving) is a little surprising, and one might ask if there are any further functions with this property. In fact Moss [5] has constructed many such maps.

Lemma 11. *Let p be a prime, and define $g_p\colon \mathbb{N} \to \mathbb{N}$ by*

$$g_p(n) = \begin{cases} n & \text{if } p \nmid n; \\ pn & \text{if } p | n. \end{cases}$$

Then g_p lies in $\mathscr{P}$.

Proof. Let (a_n) be a realizable sequence and write $(b_n) = (a_{g_p(n)})$. We need to show that (b_n) satisfies (2). Fix n, and write $n = p^{\mathrm{ord}_p(n)} m$ with $\gcd(m,p) = 1$.

Assume first that $\mathrm{ord}_p(n) = 0$. Then $p \nmid n$ and so

$$\sum_{d\,|n} \mu(n/d) b_d = \sum_{d\,|n} \mu(n/d) a_d$$

and so (b_n) satisfies (2) at n.

Next assume that $\mathrm{ord}_p(n) = 1$, so that $n = pm$ and $p \nmid m$. Then

$$\begin{aligned}(\mu * b)(n) = \sum_{d\,|pm} \mu(d) b_{pm/d} &= \sum_{d\,|m} \mu(d) b_{n/d} + \mu(p) \sum_{d\,|m} \mu(d) b_{m/d} \\ &= \sum_{d\,|m} \mu(d) a_{p^2m/d} - \sum_{d\,|m} \mu(d) a_{m/d} \qquad (11)\end{aligned}$$

since μ is multiplicative. Now

$$\begin{aligned}(\mu * a)(pn) = (\mu * a)(p^2 m) &= \sum_{d\,|p^2m} \mu(d) a_{p^2m/d} \\ &= \sum_{d\,|m} \mu(d) a_{p^2m/d} - \sum_{d\,|m} \mu(d) a_{pm/d} \qquad (12)\end{aligned}$$

and

$$\begin{aligned}(\mu * a)(n) = (\mu * a)(pm) &= \sum_{d\,|pm} \mu(d) a_{pm/d} \\ &= \sum_{d\,|m} \mu(d) a_{pm/d} - \sum_{d\,|m} \mu(d) a_{m/d}. \qquad (13)\end{aligned}$$

Adding (12) and (13) gives

$$(\mu * a)(pn) + (\mu * a)(n) = \sum_{d\,|m} \mu(d) a_{p^2m/d} - \sum_{d\,|m} \mu(d) a_{m/d} = (\mu * b)(n)$$

by (11), so (b_n) satisfies (2) at n.

Finally, assume that $\mathrm{ord}_p(n) \geqslant 2$. Then

$$\sum_{d\,|n} \mu(n/d) b_d = \underbrace{\sum_{d\,|m} \mu(n/d) a_d}_{\Sigma_0} + \sum_{j=1}^{\mathrm{ord}_p(n)} \underbrace{\sum_{d\,|m} \mu(n/p^j d) a_{pd}}_{\Sigma_j}$$

Now $\mu\big(\frac{n}{d}\big) = 0$ for all d dividing m, so $\Sigma_0 = 0$.

Similarly, $\mu\big(\frac{n}{p^j d}\big) = 0$ for $j \leqslant \mathrm{ord}_p(n) - 2$, so $\Sigma_j = 0$ for $1 \leqslant j \leqslant \mathrm{ord}_p(n) - 2$.

For the two remaining terms, we have

$$\begin{aligned}\Sigma_{\mathrm{ord}_p(n)} + \Sigma_{\mathrm{ord}_p(n)-1} &= \sum_{d\,|m} \mu(m/d)a_{pd} + \sum_{d\,|m} \mu(pm/d)a_{pd} \\ &= \sum_{d\,|m} \mu(m/d)a_{pd} - \sum_{d\,|m} \mu(m/d)a_{pd} = 0,\end{aligned}$$

so (2) holds trivially for (b_n) at n.

We deduce that (b_n) satisfies (2) for all $n \geqslant 1$, as required. □

Proof of Theorem 7. Let $S = \{p_1, p_2, \dots\} \subseteq \{2, 3, 5, 7, 11, \dots\}$ be any set of primes, and define $g_S \colon \mathbb{N} \to \mathbb{N}$ formally by $g_S = g_{p_1} \circ g_{p_2} \circ \cdots$ in the notation of Lemma 11. For definiteness, we write a set of primes as $\{p_{j_1}, p_{j_2}, \dots\}$ with $p_{j_1} < p_{j_2} < \cdots$. More precisely, the map g_S then may be defined as follows. For $n \in \mathbb{N}$ the set

$$\{p_j \mid p_j \text{ divides } n\} = \{p_{j_1}, \dots, p_{j_t}\}$$

is finite, and then we define

$$g_S(n) = g_{p_{j_1}} \circ \cdots \circ g_{p_{j_t}}(n).$$

If S and T are different subsets of the primes, then there is a prime p in the symmetric difference of S and T, and clearly $g_S(p) \neq g_T(p)$. It follows that there are uncountably many different functions g_S.

Formally, we also need to slightly improve the simple observation that $\mathscr{P}$ is a monoid in Section 1 (remark (b) after Definition 1), as follows. If $(h_1, h_2, \dots)$ is a sequence of functions in $\mathscr{P}$ with the property that

$$\{j \in \mathbb{N} \mid h_j(n) \neq n\} = \{j_n^{(1)}, j_n^{(2)}, \dots, j_n^{(r_n)}\}$$

is finite for any $n \in \mathbb{N}$, then the infinite composition $h = h_1 \circ h_2 \circ \cdots$ defined by

$$h(n) = h_{j_n^{(1)}} \circ \cdots \circ h_{j_n^{(r_n)}}(n)$$

for any $n \in \mathbb{N}$ is also in $\mathscr{P}$. This is clear, because for any given n checking (2) only involves evaluating h on finitely many terms. We deduce that there are uncountably many different elements of $\mathscr{P}$ from Lemma 11. □

4. Dynamical systems with additional polynomial time-changes

As mentioned in Example 2, if X simply comprises a single fixed point for T then $\mathscr{P}(X,T) = \mathbb{N}^{\mathbb{N}}$. Less trivial systems will have fewer maps that preserve realizability, and the complex way in which properties of a map relate to the structure of its associated set of maps are illustrated here by examples of systems (X,T) with

$$\mathscr{P} \subsetneq \mathscr{P}(X,T) \subsetneq \mathbb{N}^{\mathbb{N}}. \tag{14}$$

Example 12. Let $T \colon X \to X$ be the full shift on $a \geqslant 2$ symbols, so that we have $\mathrm{Fix}_{(X,T)}(n) = a^n$ for all $n \geqslant 1$. Then we claim (this is an observation from the thesis of the second named author [5]) that if $h(n) = c_0 + c_1 n + \cdots + c_k n^k$ is any polynomial with non-negative integer coefficients, then $h \in \mathscr{P}(X,T)$. By Theorem 5, we know that the sequence (a^{n^j}) is realized by some map $T_j \colon X \to X$ for any $j = 1, \dots, k$. Certainly the constant sequence $(a, a, \dots)$ is realized by the identity map T_0 on a set with a elements. Then the Cartesian product

$$S = \underbrace{T_0 \times \cdots \times T_0}_{c_0 \text{ copies}} \times \underbrace{T_1 \times \cdots \times T_1}_{c_1 \text{ copies}} \times \cdots \times \underbrace{T_k \times \cdots \times T_k}_{c_k \text{ copies}}$$

acting on $Y = X^{c_0+c_1+\cdots+c_k}$ has

$$\mathrm{Fix}_{(Y,S)}(n) = a^{c_0}\left(a^n\right)^{c_1}\cdots\left(a^{n^k}\right)^{c_k} = a^{h(n)}$$

for $n \geqslant 1$, by construction. Thus $h \in \mathscr{P}(X,T)$, showing that $\mathscr{P}(X,T)$ is strictly larger than $\mathscr{P}$. On the other hand, if the map that exchanges 1 and 2 (and fixes all other elements of $\mathbb{N}$) lies in $\mathscr{P}(X,T)$, then we must be able to find some dynamical system $S\colon Y \to Y$ with $\mathrm{Fix}_{(Y,S)}(1) = a^2$ and $\mathrm{Fix}_{(Y,S)}(2) = a$. This forces $a^2 \leqslant a$ (because every fixed point of a map is also fixed by the second iterate of the map), so $a \leqslant 1$. It follows that $\mathscr{P}(X,T)$ is strictly smaller than $\mathbb{N}^{\mathbb{N}}$, since $a \geqslant 2$.

In general it is not at all easy to describe $\mathscr{P}(X,T)$ — indeed with the exception of the trivial case $\mathbb{N}^{\mathbb{N}}$ which arises for the identity map on a finite set, we have no examples with a complete description any more insightful than the definition. Example 12 relies on the accidental fact that $a^n a^m = a^{n+m}$, allowing us to translate Cartesian products of systems into addition in the time-change. The next example of a system satisfying (14) relies on a different arithmetic trick, as well as the result from Example 12.

Example 13. Let $T\colon X \to X$ be the map $x \mapsto -ax$ modulo 1 on the additive circle $X = \mathbb{R}/\mathbb{Z}$ for some integer $a \geqslant 2$. Then we have $\mathrm{Fix}_{(X,T)}(n) = a^n - (-1)^n$ for $n \geqslant 1$, and we claim that if $h(n) = n^2 + 1$, then $h \in \mathscr{P}(X,T)$. (In fact, the same argument shows the same property for any polynomial with non-negative coefficients, but for simplicity of notation we consider this specific example.) To prove this, we first show that

$$\eta(n) = \sum_{d\,|n}(-1)^d\mu(n/d) = 0 \tag{15}$$

for all $n > 2$. Writing $\boldsymbol{\mu}(s) = \sum_{n\geqslant 1}\frac{\mu(n)}{n^s}$, $\boldsymbol{\zeta}$ for the Riemann zeta function, and $\boldsymbol{\eta}$ for the Dirichlet η-function $\sum_{n\geqslant 1}\frac{(-1)^{n-1}}{n^s}$, it is clear that $\boldsymbol{\eta}(s) = (1-2^{-s})\boldsymbol{\zeta}(s)$ by splitting into odd and even terms, and $\boldsymbol{\zeta}\boldsymbol{\mu} = 1$, so $\boldsymbol{\mu}(s)\boldsymbol{\eta}(s) = (1-2^{1-s})$ for $\Re(s) > 1$. It follows that $\eta(1) = -1$, $\eta(2) = 2$, and $\eta(n) = 0$ for $n > 2$.

As all our other arguments are elementary, for completeness we also show (15) directly, by separating out the power of 2 dividing n, as follows.

- If $n > 2$ is odd, then
$$\eta(n) = -\sum_{d\,|n}\mu(n/d) = -\sum_{d\,|n}\mu(d) = 0.$$
- If $n = 2^k$ for some $k > 1$, then
$$\eta(n) = \sum_{d\,|2^k}(-1)^d\mu(2^k/d) = \mu(1) + \mu(2) = 0.$$
- If $n = 2m$ with $m > 2$ odd, then
$$\eta(n) = \sum_{d\,|2m}\mu(d)(-1)^{2m/d} = \sum_{d\,|m}\mu(d)\big((-1)^{2m/d} - (-1)^{m/d}\big) = 2\sum_{d\,|m}\mu(d) = 0.$$
- Finally, if $n = 2^k m$ with $k, m > 1$ and m odd, then
$$\eta(n) = \sum_{d\,|2^k m}\mu(d)(-1)^{2^k m/d} = \sum_{d\,|m}\mu(d)\big((-1)^{2^k m/d} - (-1)^{2^{k-1}m/d}\big) = 0.$$

We now show that $h \in \mathscr{P}(X,T)$ using the basic relation (2). That is, we need to show the congruence and positivity properties in (2) for the sequence (a_n) defined by $a_n = a^{n^2+1} + (-1)^n$ for $n \geqslant 1$ (since $(-1)^{n^2+1} = -(-1)^n$). Now $(a*\mu)(1) = a^2 - 1$ and $(a*\mu)(2) = a^2(a^3-1)+2$, so we see that $(a*\mu)(n)$ is non-negative and divisible by n for $n = 1, 2$ as desired. For $n > 2$, we have

$$(a*\mu)(n) = \sum_{d\,|n} \mu(n/d)a^{d^2+1} + \sum_{d\,|n} (-1)^d \mu(n/d) = \sum_{d\,|n} \mu(n/d)a^{d^2+1} \tag{16}$$

since $\eta(n) = 0$. Now a special case of Example 12 shows that the sequence (a^{n^2+1}) is realizable, so by (2) the last sum in (16) must be non-negative and divisible by n for all $n > 2$. This shows that (a_n) is a realizable sequence, and hence $h \in \mathscr{P}(X,T)$. To see that $\mathscr{P}(X,T)$ is not everything, notice that if the map exchanging 1 and 3 lies in $\mathscr{P}(X,T)$, then $a^3 \leqslant a$, which is impossible.

5. Questions

(a) The simple arguments showing that realizable sequences can be added and multiplied may be seen using disjoint unions and products of dynamical systems. Is there a similar argument showing that monomials preserve realizability? For example, from a 'natural' system (X,T) with $a_n = \mathrm{Fix}_{(X,T)}(n)$ for all $n \geqslant 1$ (a smooth map on a compact manifold, say), is there a simple construction of a system $(X^{(2)}, T^{(2)})$ with the property that

$$\mathrm{Fix}_{(X^{(2)},T^{(2)})}(n) = a_{n^2}$$

for all $n \geqslant 1$? Of course the proof above notionally 'constructs' such a system because it can be used to extract a formula for how many orbits of each length such a map must have, but in a far from natural or geometric way.

(b) There is no *a priori* reason for any given $\mathscr{P}(X,T)$ to be a monoid under composition of functions, though $\mathscr{P}$ clearly is. For cases with $\mathscr{P}(X,T) \supsetneq \mathscr{P}$, what combinatorial properties of $(\mathrm{Fix}_{(X,T)}(n))$ determine the property that $\mathscr{P}(X,T)$ is a monoid?

(c) Is there a sequence of systems $\big((X_n,T_n)\big)_{n\geqslant 1}$ with the property that

$$\mathscr{P}(X_n,T_n) \supsetneq \mathscr{P}(X_{n+1},T_{n+1})$$

for all $n \geqslant 1$?

(d) Can a non-trivial permutation of $\mathbb{N}$ lie in $\mathscr{P}$?

(e) Is there a map $T\colon X \to X$ with the property that the only polynomials in $\mathscr{P}(X,T)$ are monomials?

(f) Is there a map $T\colon X \to X$ with the property that $\mathscr{P}(X,T) = \mathscr{P}$?

References

[1] A. Carnevale and C. Voll, *Orbit Dirichlet series and multiset permutations*, Monatsh. Math. **186** (2018), no. 2, 215–233. MR 3808651

[2] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003. MR 1990179

[3] G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, *Integer sequences and periodic points*, J. Integer Seq. **5** (2002), no. 2, Article 02.2.3, 10. MR 1938222

[4] F. Luca and T. Ward, *An elliptic sequence is not a sampled linear recurrence sequence*, New York J. Math. **22** (2016), 1319–1338. MR 3576291

[5] P. Moss, *The arithmetic of realizable sequences*, Ph.D. thesis, University of East Anglia, 2003.

[6] A. Pakapongpun and T. Ward, *Functorial orbit counting*, J. Integer Seq. **12** (2009), no. 2, Article 09.2.4, 20. MR 2486259
[7] ———, *Orbits for products of maps*, Thai J. Math. **12** (2014), no. 1, 33–44. MR 3194906
[8] Y. Puri and T. Ward, *Arithmetic and growth of periodic orbits*, J. Integer Seq. **4** (2001), no. 2, Article 01.2.1, 18. MR 1873399
[9] ———, *A dynamical property unique to the Lucas sequence*, Fibonacci Quart. **39** (2001), no. 5, 398–402. MR 1866354
[10] N. J. A. Sloane (editor), *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org.
[11] A. J. Windsor, *Smoothness is not an obstruction to realizability*, Ergodic Theory Dynam. Systems **28** (2008), no. 3, 1037–1041. MR 2422026
[12] B. Ycart, *A case of mathematical eponymy: the Vandermonde determinant*, Rev. Histoire Math. **19** (2013), no. 1, 43–77. MR 3155603

Department of Mathematics, Faculty of Science, Khon Kaen University, Thailand.
E-mail address: `jsawia@kku.ac.th`

E-mail address: `pbsmoss2@btinternet.com`

Ziff Building 13.01, University of Leeds, LS2 9JT, U.K.
E-mail address: `t.b.ward@leeds.ac.uk`