arXiv:math.DS/9907003 v2 26 Apr 2001

ARITHMETIC AND GROWTH OF PERIODIC ORBITS

YASH PURI AND THOMAS WARD

Abstract. Two natural properties of integer sequences are introduced and studied. The first, *exact realizability*, is the property that the sequence coincides with the number of periodic points under some map. This is shown to impose a strong inner structure on the sequence. The second, *realizability in rate*, is the property that the sequence asympototically approximates the number of periodic points under some map. In both cases we discuss when a sequence can have that property. For exact realizability, this amounts to examining the range and domain among integer sequences of the paired transformations

$$\mathrm{Per}_n = \sum_{d|n} d\mathrm{Orb}_d; \qquad \mathrm{Orb}_d = \frac{1}{n}\sum_{d|n}\mu(n/d)\mathrm{Per}_d \qquad \textbf{ORBIT}$$

that move between an arbitrary sequence of non-negative integers Orb counting the orbits of a map and the sequence Per of periodic points for that map. Several examples from the Encyclopedia of Integer Sequences arise in this work, and a table of sequences from the Encyclopedia known or conjectured to be exactly realizable is given.

Contents

Date: July 10, 2004.
The first author gratefully acknowledges the support of E.P.S.R.C. grant 96001638.

1. Introduction

Let $T : X \to X$ be a map. Three measures of growth in complexity for T are given by the *number of points with period* n,

$$f_n(T) = \#\{x \in X \mid T^n x = x\},$$

the *number of points with least period* n,

$$f_n^*(T) = \#\{x \in X \mid T^n(x) = x \text{ and } \#\{T^k x\}_{k\in\mathbb{Z}} = n\},$$

and the *number of orbits of length* n,

$$f_n^o(T) = f_n^*(T)/n.$$

In this note we assume that $f_n(T)$ is finite for $n \geq 1$ and give some results on what arithmetic properties the sequence $(f_n(T))$ may have, and show when the growth in $(f_n(T))$ is related to the growth in $(f_n^*(T))$. It will be convenient to adopt the following notation: a sequence $a_1, a_2, a_3, \dots$ is denoted (a_n) or simply a.

Definition 1.1. Let $\phi = (\phi_n)$ be a sequence of non-negative integers. Then

1. $\phi \in \mathcal{ER}$ (*exactly realizable*) if there is a set X and a map $T : X \to X$ for which $f_n(T) = \phi_n$ for all $n \geq 1$;
2. $\phi \in \mathcal{RR}$ (*realizable in rate*) if there is a set X and a map $T : X \to X$ for which $f_n(T)/\phi_n \to 1$ as $n \to \infty$.

None of the results below are changed if the realizing maps are required to be homeomorphisms of a compact X, but this is not pursued here.

2. Exact realization

The set of points with period n under T is the disjoint union of the set of points with least period d under T for d dividing n, so

$$f_n(T) = \sum_{d|n} f_d^*(T). \tag{1}$$

Equation (1) may be inverted via the Möbius inversion formula to give

$$f_n^*(T) = \sum_{d|n} \mu(n/d) f_d(T), \tag{2}$$

where $\mu(\cdot)$ is the Möbius function. On the other hand, the set of points with least period n comprises exactly f_n^o orbits each of length n, so

$$0 \leq f_n^*(T) = \sum_{d|n} \mu(n/d) f_d(T) \equiv 0 \bmod n. \tag{3}$$

It is clear (since one may take $X = \mathbb{N}$ and make T to be a permutation with the appropriate number of cycles of each length) that these are the only conditions for membership in $\mathcal{ER}$.

Lemma 2.1. *Let ϕ be a sequence of non-negative integers. Then $\phi \in \mathcal{ER}$ if and only if $\sum_{d|n} \mu(n/d)\phi_d$ is non-negative and divisible by n for all $n \geq 1$.*

Everything that follows is a consequence of this lemma. Before considering properties of $\mathcal{ER}$ as a whole, some examples are considered. The sequences that arise here are therefore close in spirit to the 'eigen-sequences' for the transformation **MÖBIUS** discussed in [1] with the additional requirement that the sequence f^* be divisible by n and non-negative.

Example 2.2.

1. The Fibonacci sequence A000045 is not in $\mathcal{ER}$. Using (3) we see that $f_3 - f_1$ must always be divisible by 3, but the Fibonacci sequence begins $1, 1, 2, 3, \dots$. By contrast the golden mean shift (see [10]) shows that the closely related Lucas sequence A000204 is in $\mathcal{ER}$. This will be dealt with in greater generality in Section 2.2 below.
2. For any map T, equation (3), when n is a prime p, states that
$$f_p(T) \equiv f_1(T) \bmod p.$$
If $A \in GL_k(\mathbb{Z})$ is an invertible integer matrix with no unit root eigenvalues, then the periodic points in the corresponding automorphism of the k-torus show that
$$\det(A^p - I) \equiv \det(A - I) \bmod p$$
for all primes p.
3. Similarly, if $B \in M_k(\mathbb{N})$ is a matrix of non-negative integers, the associated subshift of finite type (see [10]) shows that
$$\operatorname{trace}(B^p) \equiv \operatorname{trace}(B) \bmod p$$
for all primes p. When $k = 1$ this is Fermat's little theorem. When $B = [2]$, so $f_n = 2^n$, f_n^o is the sequence A001037 (shifted by one) counting irreducible polynomials of degree n over $\mathbb{F}_2$.
4. The subshifts of finite type give a family of elements of $\mathcal{ER}$ of exponential type. Another family comes from Pascal's triangle: if $k > 1$, $1 \leq j < k$ and $a_n = \binom{kn}{jn}$, then $a \in \mathcal{ER}$. For $k = 2$ and $j = 1$, if $f_n = f_n(T)$ for the realizing map T, then f_n^* is the sequence A007727 counting $2n$-bead black and white strings with n black beads and fundamental period $2n$.

5. Connected S-integer dynamical systems (see [3], [13] for these and the next example): a subset $S \subset \{2, 3, 5, 7, 11, \dots\}$ and a rational $\xi \neq 0$ are given with the property that $|\xi|_p > 1 \implies p \in S$. The resulting system constructs a map $T : X \to X$ for which
$$f_n(T) = \prod_{p \leq \infty} |\xi^n - 1|_p.$$
With $\xi = 2, S = \{2, 3, 5, 7\}$ this gives the sequence
$$1, 1, 1, 1, 31, 1, 127, 17, 73, 341, 2047, 13, 8191, 5461, 4681, \dots$$
in $\mathcal{ER}$.
6. Zero-dimensional S-integer dynamical systems: a prime p is fixed, a subset S of the set of all irreducible polynomials in $\mathbb{F}_p[t]$ and a rational function $\xi \in \mathbb{F}_p(t)$ are given, with the property that $|\xi|_f > 1 \implies f \in S$. The resulting system constructs a map $T : X \to X$ for which
$$f_n(T) = |\xi^n - 1|_{t^{-1}} \times \prod_{f \in S} |\xi^n - 1|_f$$
where $|\cdot|_{t^{-1}}$ is used to denote the valuation 'at infinity' induced by $|t|_{t^{-1}} = p$. Taking $p = 2$, $S = \{t - 1\}$ and $\xi = t$ gives the formula
$$f_n(T) = 2^{n - 2^{\mathrm{ord}_2(\mathrm{n})}}$$
and the sequence A059991 in $\mathcal{ER}$.

2.1. **Algebra of exactly realizable sequences.** The set $\mathcal{ER}$ – or the ring $K_0(\mathcal{ER})$ – has a very rich structure. Say that a sequence $a \in \mathcal{ER}$ *factorizes* if there exists sequences $b, c \in \mathcal{ER}$ with $a_n = b_n c_n$ for all $n \geq 1$, and is *prime* if such a factorization requires one of b or c to be the constant sequence (1).

Lemma 2.3. *$\mathcal{ER}$ contains the constant sequences and is closed under addition and multiplication. Elements of $\mathcal{ER}$ may have infinitely many non-trivial factors. There are non-trivial primes in $\mathcal{ER}$.*

Proof. The constant sequence (1) is in $\mathcal{ER}$ since it is realized by taking X to be a singleton. The condition in Lemma 2.1 is closed under addition. On the other hand, if ϕ and ψ are exactly realized by systems (X, T) and (Y, S), then $(X \times Y, T \times S)$ exactly realizes $(\phi_n \cdot \psi_n)$. For each $k \geq 1$ define a sequence $r^{(k)}$ by $r^{(k)}_n = 0$ for $1 < n \leq k$ and $r^{(k)}_n = 1$ for $n > k$ or $n = 1$. Then $a^{(k)} \in \mathcal{ER}$, where $a^{(k)}_n = \sum_{d|n} d r^{(k)}_d$. Since for each n the sequence $a^{(1)}_n, a^{(2)}_n, a^{(3)}_n, \dots$ has only finitely many terms not equal to 1, the product $\prod_{k \geq 1} a^{(k)} = (1, 3, 16, 245, 1296, 41160, \dots)$

is an element of $\mathcal{ER}$ with infinitely many non-trivial factors. Finally, the sequence $(1,3,1,3,\dots)$ is a non-trivial prime in $\mathcal{ER}$. □

In [9, Sect. 6] a periodic point counting argument is used to show that the full p-shift, for p a prime, is not topologically conjugate to the direct product of two dynamical systems. In that argument, special properties of subshifts of finite type are needed (specifically, the fact that $f_{p^k}(T)=1$ for all $k\geq 1$ implies that $f_n(T)=1$ for all $n\geq 1$ for such systems). This result does not follow from the arithmetic of $\mathcal{ER}$ alone: for example, $(3^n)\in\mathcal{ER}$ factorizes into $(1,3,1,3,\dots)\times(3,3,3^3,3^3,\dots)$ in $\mathcal{ER}$ (neither of which can be realized using a subshift of finite type). A similar factorization is possible for (p^n) and any odd prime p (see [11] for the details).

Lemma 2.4. *There are no non-constant polynomials in $\mathcal{ER}$. There are non-trivial multiplicative sequences in $\mathcal{ER}$, but there are no completely multiplicative sequences apart from the constant sequence* (1).

Proof. Assume that

$$P(n)=c_0+c_1n+\cdots+c_kn^k$$

with $c_k\neq 0$, $k\geq 1$, and that $(P(n))\in\mathcal{ER}$. After multiplying the divisibility condition (3) by the least common multiple of the denominators of the (rational) coefficients of P, we produce a polynomial with integer coefficients satisfying (3). It is therefore enough to assume that the coefficients c_i are all integers. Let (f_n) and (f_n^*) be the periodic points and least periodic points in the corresponding system (X,T), and let p be any prime. By (2),

$$f_{p^2}^*=f_{p^2}-f_p,$$

so

$$\begin{aligned} f_{p^2}^o=\frac{f_{p^2}^*}{p^2} &= \frac{f_{p^2}-f_p}{p^2}\\ &= \frac{1}{p^2}\left(c_1p^2+c_2p^4+\cdots+c_kp^{2k}-(c_1p+c_2p^2+\cdots+c_kp^k)\right)\\ &\in -\frac{c_1}{p}+\mathbb{Z}, \end{aligned}$$

and therefore p divides c_1 for all primes p, showing that $c_1=0$.

Now let q be another prime, and recall that

$$\mu(1)=1,\mu(p)=-1,\mu(q)=-1,\mu(p^2)=0,\mu(p^2q)=0,\mu(pq)=1.$$

Since $c_1=0$,

$$f_n=c_0+n^2(c_2+c_3n+\cdots+c_kn^{k-2}), \tag{4}$$

and by (3)

$$p^2q\big|f_{p^2q}-f_{pq}-f_{p^2}+f_p=f^*_{p^2q},$$

so

$$\frac{f_{p^2}-f_p}{p^2q}\in\mathbb{Z}$$

by (4). It follows that

$$c_0(1-1)+c_2(p^4-p^2)+c_3(p^6-p^3)+\cdots+c_k(p^{2k}-p^k)\in q\mathbb{Z}$$

for all primes q and p (since $f_{p^2}-f_p$ is certainly divisible by p^2). So

$$c_0(1-1)+c_2(p^4-p^2)+c_3(p^6-p^3)+\cdots+c_k(p^{2k}-p^k)=0;$$

taking the limit as $p\to\infty$ of $\frac{1}{p^{2k}}(f_{p^2}-f_p)$ shows that $c_k=0$. This contradiction proves the first statement.

There are many multiplicative sequences in $\mathcal{ER}$: if f^* is any multiplicative sequence, then so is the corresponding sequence f (see [7, Theorem 265]). A multiplicative sequence ϕ is *completely multiplicative* if $\phi_{nm}=\phi_n\phi_m$ for all $n,m\geq 1$. Assume that $\phi\in\mathcal{ER}$ is completely multiplicative, with f the realising sequence. For p a prime and any $r\geq 1$,

$$f^*_{p^r}=f_{p^r}-f_{p^{r-1}}=f_p^r-f_p^{r-1}$$

by (2). It follows that

$$p^r\big|f_p^{r-1}(f_p-1).$$

With $r=1$ this implies that $f_p=1+pk_p$ for all p, $k_p\in\mathbb{N}_0$. Now

$$p^r\big|(1+pk_p)^{r-1}pk_p$$

for all p and $r\geq 1$. It follows that $k_p\equiv 0 \bmod p^r$ for all $r\geq 1$, so $k_p=0$ for all p. It follows that $f_p=1$ for all primes p, so $f_n=1$ for all $n\geq 1$. □

Examples show that the additive convolution $(\sum_{i+j=n+1,1\leq i,j\leq n}\phi_i\psi_j)$ of sequences $\phi,\psi\in\mathcal{ER}$ is not in general in $\mathcal{ER}$. Similarly, the multiplicative convolution $(\sum_{d|n}\phi_d\psi_{n/d})$ is not in general in $\mathcal{ER}$. There is also no closure under quotients: $(2^n)\in\mathcal{ER}$ is term-by-term divisible by the constant sequence $(2)\in\mathcal{ER}$, but $(2^{n-1})\notin\mathcal{ER}$.

2.2. **Binary recurrence sequences.** In this section we expand on the observation made in Example 2.2.1 by showing that $\mathcal{ER}$ only contains special binary recurrences.

Theorem 2.5. *If $\Delta=a^2+4b$ is not a square, and $(a,a^2+2b)=1$, then a sequence u with $u_1,u_2\geq 1$ satisfying the recurrence*

$$u_{n+2}=au_{n+1}+bu_n \text{ for } n\geq 1 \tag{5}$$

is in $\mathcal{ER}$ if and only if $\frac{u_2}{u_1} = \frac{a^2+2b}{a}$.

As an application, Example 2.2.1 becomes the sharper result that the Lucasian sequence $a, b, a+b, a+2b, 2a+3b, \dots$ lies in $\mathcal{ER}$ if and only if $b = 3a$. Moreover, if $f_1 = 1, f_2 = 1, f_3 = 2, \dots$ is the Fibonacci sequence, then an easy consequence of Theorem 2.5 is that for any $k \geq 1$ the sequence $f_k, f_{k+1}, f_{k+2}, \dots$ is not in $\mathcal{ER}$. The more general case with square discriminant, a and a^2+2b having a common factor and arbitrary u_1, u_2 is dealt with in [11].

Proof. First assume that $\frac{u_2}{u_1} = \frac{a^2+2b}{a}$. Then, by the assumption, the sequence u is a multiple of the sequence $a, a^2+2b, a^3+3ab, \dots$ which is in $\mathcal{ER}$ because the subshift of finite type corresponding to the matrix $\begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix}$ realizes it (and therefore any multiple of it).

Conversely, assume that u is a sequence in $\mathcal{ER}$ satisfying (5). Write x for the sequence

$$x : 2b, 2ab, 2(a^2b + b^2), \dots$$

and y for the sequence

$$y : 2ab, 2(a^2b + 2b^2), \dots,$$

both satisfying the recurrence (5). Notice that

$$2bu_n = Ax_n + By_n,$$

for integers A and B. By (3), for any prime p

$$Ax_p + By_p \equiv Ax_1 + By_1 \bmod p. \tag{6}$$

On the other hand, it is well-known that $x_p \equiv 2b(\frac{\Delta}{p}) \bmod p$ (where $(\frac{\Delta}{p})$ is the Legendre symbol), and $y_p \equiv 2ab \bmod p$ (by the previous paragraph: y is in $\mathcal{ER}$). So (6) implies that

$$2bA\left(\left(\frac{\Delta}{p}\right) - 1\right) \equiv 0 \bmod p \tag{7}$$

for all primes p.

We now claim that the Legendre symbol $(\frac{\Delta}{p})$ is -1 for infinitely many values of the prime p. This completes the proof of Theorem 2.5, since (7) forces $A = 0$ and hence u is a multiple of $\frac{1}{2b}y$, namely $a, a^2+2b, \dots$.

To see the claim, choose c such that $(c, \Delta) = 1$ and the Jacobi symbol $(\frac{c}{\Delta}) = -1$. Then by Dirichlet, there are infinitely many primes p with $p \equiv c \bmod \Delta$ and $p \equiv 1 \bmod 4$. For such primes, $(\frac{p}{\Delta}) = (\frac{\Delta}{p}) = -1$, which completes the proof. ☐

The case of square discriminant is much more involved. A full treatment is in [11]; here we simply show by examples that the result as stated no longer holds in general.

Example 2.6. 1. There are infinitely many possible values of the ratio $\frac{u_2}{u_1}$ for binary recurrent sequences in $\mathcal{ER}$ satisfying

$$u_{n+2} = u_{n+1} + 2u_n. \tag{8}$$

To see this we construct two different realizing examples and then take linear integral combinations of them. The first is the subshift of finite type T corresponding to the matrix $A = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$. This system has (by [10, Proposition 2.2.12]) $f_n(T) = \mathrm{trace}(A^n)$, which is the sequence of Jacobsthal–Lucas numbers A014551:$1, 5, 7, 17, \dots$ (shifted by one) and has initial ratio 5. On the other hand, the algebraic dynamical system S dual to $x \mapsto -2x$ on the discrete group $\mathbb{Z}[\frac{1}{2}]$ has (see, for example, [3, Lemma 5.2]) $f_n(S) = |(-2)^n - 1|$, which begins $3, 3, 9, 15, \dots$ and has ratio 1. Now we may apply Lemma 2.3 as follows. If $s, t \in \mathbb{N}$ then $(tf_n(T) + sf_n(S))$ in $\mathcal{ER}$ is a sequence satisfying (8). It follows that the set of possible ratios $\frac{u_2}{u_1}$ contains the infinite set $\{\frac{5t+3s}{t+3s} \mid s, t \in \mathbb{N}\}$.

2. A simpler example is given by the Mersenne recurrence. Since (2^n) and (1) are both in $\mathcal{ER}$, for any $t, s \geq 0$ the sequence $(t2^n + s)$ satisfying the recurrence

$$u_{n+2} = 3u_{n+1} - 2u_n \tag{9}$$

is in $\mathcal{ER}$. Thus the set of possible ratios $\frac{u_2}{u_1}$ for exactly realizable solutions of (9) contains the infinite set $\left\{\frac{4t+s}{2t+s} \mid s, t \in \mathbb{N}\right\}$.

For higher order recurrences with companion polynomials irreducible over the rationals, it is clear that some analogue of Theorem 2.5 holds. The rational solutions of a kth order reccurence form a rational k-space; the smallest subspace contained in $\mathcal{ER}$ has dimension strictly smaller than k. Is this dimension always 1?

3. Realization in rate

Write $\lfloor x \rfloor$ for the greatest integer less than or equal to x and $\lceil x \rceil$ for the smallest integer greater than or equal to x. In this section we assume that sequences are never zero. Different complications arise from zeros of sequences and these are discussed in detail in [11].

Theorem 3.1. *Let α, β be positive constants.*

1. *If $\phi_n \to \infty$ with $\frac{\phi_n}{n} \to 0$, then $\phi \notin \mathcal{RR}$.*

2. *The sequence* $(\lfloor n^\alpha \rfloor) \in \mathcal{RR}$ *if and only if* $\alpha > 1$.
3. *The sequence* $(\lfloor \beta^n \rfloor) \in \mathcal{RR}$ *if and only if* $\beta \geq 1$.

Proof. 1. Assume that $\phi \in \mathcal{RR}$ and let f be the corresponding sequence of periodic points. Then $\frac{f_n}{\phi_n} \to 1$, so $\{\frac{f_n}{\phi_n}\}$ is bounded. It follows that $\{\frac{f_n^*}{\phi_n} = \frac{n}{\phi_n} f_n^o\}$ is bounded, and hence $f_n^* = n f_n^o = 0$ for all large n. This implies that f_n is bounded, and so $\frac{f_n}{\phi_n} \to 0$, which contradicts the assumption.
2. For $\alpha \in (0,1)$ this follows from part 1. Suppose therefore that $(n) \in \mathcal{RR}$. Then there is a sequence $f \in \mathcal{ER}$ with $f_n/n \to 1$, so for p a prime, $pf_p^o = f_p^* = f_p - f_1^*$, and therefore $f_p^o \to 1$ as $p \to \infty$. Since f_p^o is an integer, it follows that $f_p^o = 1$ for all large p. Now let q be another large prime. Then

$$\frac{f_{pq}}{pq} = \frac{f_{pq}^* + f_p^* + f_q^* + f_1^*}{pq} = \frac{f_{pq}^*}{pq} + \frac{1}{p} + \frac{1}{q} + \frac{f_1^*}{pq},$$

so

$$\frac{1}{p} + \frac{1}{q} + \frac{f_1^*}{pq} - \frac{f_{pq}}{pq} \in \mathbb{Z}.$$

Fix p large and let q tend to infinity to see that

$$\frac{1}{p} \in \mathbb{Z},$$

which is impossible. The same argument shows that f_n/n cannot have any positive limit as $n \to \infty$.

For $\alpha > 1$, let $f_n^o = \lceil n^{\alpha-1} \prod_{p|d}(1 - p^{-\alpha}) \rceil$, where the product runs over prime divisors only. Then

$$\sum_{d|n} d^\alpha \prod_{p|d}(1 - p^{-\alpha}) = n^\alpha \leq \sum_{d|n} d f_d^o = f_n \leq n^\alpha + \sum_{d|n} d,$$

so $0 \leq f_n - \phi_n \leq o(n^\alpha)$.
3. This is clear: for $\beta < 1$ the sequence is eventually 0; for $\beta > 1$ the construction used in part 2. works. ☐

There are sequences growing more slowly than n^α in $\mathcal{RR}$: in [11, Chap. 5] it is shown that $(\lfloor Cn^s (\log n)^r \rfloor) \in \mathcal{RR}$ for any $r \geq 1, C > 0, s \geq 1$.

4. Comparing orbits with periodic points

As is well-known, if f^* grows fast enough, then f grows very much like f^* (though not conversely in the case of super-exponential growth: cf. Theorem 4.2 below). Throughout this section $f_n = f_n(T)$ and $f_n^* = f_n^*(T)$ for some map T.

Remark 4.1. That f_n^* is close to f_n when f_n is growing exponentially has been commented on by Lind in [8, Sect. 4]. He points out, using (2), that if T is the automorphism of the 2-torus corresponding to the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ then $f_{20}^*(T)$ is only 0.006% smaller than $f_{20}(T)$. The sequence f of periodic points for this map is A004146.

Theorem 4.2. 1. *If* $\frac{1}{n}\log f_n^* \to C \in [0,\infty]$ *then* $\frac{1}{n}\log f_n \to C$ *also.*
2. $\frac{1}{n}\log f_n^* \to C \in (0,\infty)$ *if and only if* $\frac{1}{n}\log f_n \to C$*.*
3. *If* $\frac{1}{n}\log f_n \to \infty$ *then* $\left\{\frac{1}{n}\log f_n^*\right\}$ *may be unbounded with infinitely many limit points.*

Proof. 1. If $\frac{1}{n}\log f_n^* \to \infty$ then $\frac{1}{n}\log f_n \to \infty$ also, since $f_n \geq f_n^*$ for all n. If $\frac{1}{n}\log f_n^* \to C \in [0,\infty)$, then (for n large enough to have $f_n^* \neq 0$)

$$\begin{aligned} \frac{1}{n}\log f_n^* \leq \frac{1}{n}\log f_n &= \frac{1}{n}\log\left(\sum_{d|n} f_d^*\right) \\ &\leq \frac{1}{n}\log n + \frac{1}{n}\log \max_{d|n}\{f_d^*\}. \end{aligned}$$

For each such n, choose $\tilde{n} \in \{d \mid d|n, f_d^* \geq f_{d'}^* \ \forall\ d'|n\}$ so that $f_{\tilde{n}}^* = \max_{d|n}\{f_d^*\}$ and $\frac{\tilde{n}}{n} \leq 1$. Then

$$\begin{aligned} \frac{1}{n}\log f_n &\leq \frac{1}{n}\log n + \frac{\tilde{n}}{n}\cdot\frac{1}{\tilde{n}}\log f_{\tilde{n}}^* \\ &\leq \frac{1}{n}\log n + \frac{1}{\tilde{n}}\log f_{\tilde{n}}^* \to C. \end{aligned}$$

2. It is enough to show that if $\frac{1}{n}\log f_n \to C \in (0,\infty)$ then $\frac{1}{n}\log f_n^* \to C$ also. For $r \geq 1$,

$$f_r \geq f_r^* = -\sum_{d|r, d\neq r} f_d^* + f_r \geq f_r - \sum_{d|r, d\neq r} f_d.$$

Let R be an upper bound for $\{\frac{1}{n}\log f_n \mid f_n \neq 0\}$ and pick $\epsilon \in (0, 3C)$. Choose N so that

$$r > N \implies e^{r(C-\epsilon)} \leq f_r \leq e^{r(C+\epsilon)}.$$

Then for $r > 2N$ (so that $r^*, N \leq \lfloor \frac{r}{2} \rfloor$),

$$\begin{aligned} f_r \geq f_r^* &\geq f_r - \sum_{n=1}^{N} f_n - \sum_{n=N+1}^{\lfloor r/2 \rfloor} f_n \\ &\geq f_r - \left(Ne^{NR} + (r/2 - N)e^{r(C+\epsilon)/2}\right) \\ &\geq f_r\left(1 - Ne^{NR - r(C-\epsilon)} - (r/2 - N)e^{-r(C-3\epsilon)/2}\right), \end{aligned}$$

and the bracketed expression converges to 1 as $r \to \infty$. Taking logs and dividing by r gives the result.

3. Write $p_1, p_2, \dots$ for the sequence of primes. Let $n_r = p_r p_{r+1}$, and define a sequence (f_k^*) as follows. For k not of the form n_r, define $f_k^* = k \cdot 2^{k^3}$. For k of the form n_r define f_k^* according to the following scheme:

$$\begin{aligned}
f_{n_1}^* &= n_1 2^{n_1} \\
f_{n_2}^* &= n_2 2^{n_2}, f_{n_3}^* = n_3 2^{2n_3} \\
f_{n_4}^* &= n_4 2^{n_4}, f_{n_5}^* = n_5 2^{2n_5}, f_{n_6}^* = n_6 2^{3n_6} \\
f_{n_7}^* &= n_7 2^{n_7}, f_{n_8}^* = n_8 2^{2n_8}, f_{n_9}^* = n_9 2^{3n_9}, f_{n_{10}}^* = n_{10} 2^{4n_{10}}
\end{aligned}$$

and so on. Then $\frac{1}{n} \log f_n \to \infty$ off the n_r's clearly. Along the sequence (n_r),

$$f_{n_r} = f_{n_r}^* + f_{p_r}^* + f_{p_{r+1}}^* + f_1^* \geq f_{p_{r+1}}^*,$$

so

$$\frac{1}{n_r} \log f_{n_r} \geq \frac{1}{p_r p_{r+1}} \log \left(p_{r+1} \cdot 2^{p_{r+1}^3} \right) \to \infty.$$

On the other hand, along a subsequence of n_r's chosen to have $f_{n_r}^* = n_r 2^{\ell n_r}$ for a fixed $\ell \in \mathbb{N}$ (which will exist by construction), we realize $\ell \log 2$ as a limit point of the sequence $\frac{1}{n} \log f_n^*$. □

Finally, we turn to comparing these growth rates in a sub-exponential setting. For polynomial growth, the next result shows that f and f^* are forced to behave very differently.

Theorem 4.3. *Let C and α be positive constants.*

1. *For $\alpha > 1$, the set $\{\frac{f_n^*}{n^\alpha}\}$ is bounded if and only if $\{\frac{f_n}{n^\alpha}\}$ is bounded.*
2. *For $\alpha > 1$, $\frac{f_n}{n^\alpha} \to 0$ if and only if $\frac{f_n^*}{n^\alpha} \to 0$.*
3. *If $\frac{f_n}{n^\alpha} \to C$ for some $\alpha > 1$, then $\{\frac{f_n^*}{n^\alpha}\}$ has infinitely many limit points.*
4. *If $\frac{f_n^*}{n^\alpha} \to C$ for some $\alpha \geq 1$, then $\{\frac{f_n}{n^\alpha}\}$ has infinitely many limit points.*

Proof. 1. Let R be an upper bound for $\{\frac{f_n^*}{n^\alpha}\}$. Then

$$\frac{f_n}{n^\alpha} \leq \frac{1}{n^\alpha} \sum_{d|n} R d^\alpha = R \sum_{d|n} \left(\frac{d}{n}\right)^\alpha \leq R \sum_{d=1}^{\infty} \frac{1}{d^\alpha} < \infty.$$

The converse is obvious.

2. One direction is clear. Assume that $\frac{f^*_n}{n^\alpha} \to 0$. Fix $\epsilon > 0$; choose $M_1 \in \mathbb{N}$ so that

$$n > M_1 \implies \frac{f^*_n}{n^\alpha} < \frac{\epsilon}{1+\beta}$$

where $\beta = \sum_{k=1}^{\infty} \frac{1}{k^\alpha}$. Choose M_2 so that

$$n > M_2 \implies \sum_{r=1}^{M_1} \frac{f^*_r}{n^\alpha} < \frac{\epsilon}{1+\beta}.$$

Then for $n \geq \max\{M_1, M_2\}$,

$$\begin{aligned} 0 \leq \frac{f_n}{n^\alpha} = \sum_{d|n} \frac{f^*_d}{n^\alpha} \quad &\leq \quad \sum_{r=1}^{M_1} \frac{f^*_r}{n^\alpha} + \sum_{d|n, d>M_1} \frac{f^*_r}{n^\alpha} \\ &= \quad \sum_{r=1}^{M_1} \frac{f^*_r}{n^\alpha} + \sum_{d|n, d>M_1} + \frac{d^\alpha}{n^\alpha} \cdot \frac{f^*_d}{d^\alpha} \\ &\leq \quad \frac{\epsilon}{1+\beta} + \frac{\epsilon}{1+\beta} \sum_{d|n, d>M_1} \frac{d^\alpha}{n^\alpha} \\ &\leq \quad \frac{\epsilon}{1+\beta} + \beta \frac{\epsilon}{1+\beta} \leq \epsilon. \end{aligned}$$

3. Assume that $\frac{f_n}{n^\alpha} \to C > 0$. Then $\frac{f^*_p}{p^\alpha} \to C$ along primes. For a fixed prime p,

$$\frac{f^*_{p^r}}{p^{r\alpha}} = \frac{f_{p^r}}{p^{r\alpha}} - \frac{f_{p^{r-1}}}{p^{(r-1)\alpha}} \cdot \frac{1}{p^\alpha} \to \left(1 - \frac{1}{p^\alpha}\right) C$$

as $r \to \infty$.

4. Assume that $\frac{f^*_n}{n^\alpha} \to C > 0$. Then $\frac{f_p}{p^\alpha} \to C$ along primes. For fixed prime p and q prime,

$$\frac{f_{pq}}{(pq)^\alpha} = \frac{f^*_{pq} + f^*_q + f^*_p + f^*_1}{(pq)^\alpha} \to \left(1 + \frac{1}{p^\alpha}\right) C$$

as $q \to \infty$. □

Remark 4.4. For the case $\frac{f^*_n}{n} \to C > 0$ in Theorem 4.3, $\frac{f_n}{n}$ is unbounded: similar arguments show that

$$\frac{f_{p_1 p_2 \dots p_m}}{p_1 p_2 \dots p_m} \geq \sum_{i=1}^{m} \frac{1}{p_i} \to \infty$$

as $m \to \infty$.

5. Examples

Few of the standard sequences turn out to be in $\mathcal{E}R$. Here we list a few that are, and one that nearly is. In some cases the proof proceeds by exhibiting a realizing map, in others by proving the congruence. Section 6 contains a table with many sequences from the Encyclopedia in $\mathcal{ER}$; in particular all sequences realized by oligomorphic permutation groups from [2] that fall in $\mathcal{ER}$ are listed.

Example 5.1. 1. Many trivial sequences are in $\mathcal{ER}$, among them A00004, A00012, A00079 (shifted by one), A00203.

2. A023890, the sum of non-prime divisors, is in $\mathcal{ER}$ since it corresponds to having one orbit of each composite length.
3. A000984 (shifted by one). As pointed out in Example 2.2.4, the sequence of central binomial coefficients $\binom{2n}{n}$ is in $\mathcal{ER}$ for a combinatorial reason. Similarly the sequences of the form $\binom{kn}{jn}$ are all in $\mathcal{ER}$: these include A005809 ($k = 3, j = 1$).
4. A001035 (shifted by one) counts the number of distinct posets on n labeled elements. The first 16 terms of this sequence are known, and so the congruence (3) can be verified for $n \le 16$. However, the sequence is not in $\mathcal{ER}$. We are grateful to Greg Kuperberg for suggesting the following explanation. Write $\mathcal{P}(n)$ for the set of poset structures on $\mathbb{Z}/n\mathbb{Z}$. Then for $d|n$, there is an injection $\phi_{d,n} : \mathcal{P}(d) \to \mathcal{P}(n)$ obtained by pulling back a poset structure using the canonical homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. For certain values of n, including all prime values, we claim that those posets that do not appear in the image of one of these injections come in families of size a multiple of n, which gives the congruence (3). by Möbius inversion. Translation gives an action of $\mathbb{Z}/n\mathbb{Z}$ on $\mathcal{P}(n)$; if a given poset lies on a free orbit then that orbit is the family. In general, suppose that the stabilizer of an orbit is $\mathbb{Z}/(n/d)\mathbb{Z}$, but it is not in the image of $\phi_{d,n}$. Then there is a natural action of the wreath product $\mathbb{Z}/d\mathbb{Z}\mathrm{wr}S_{n/d}$ defined by permuting the points in each coset of $\mathbb{Z}/(n/d)\mathbb{Z}$ and adding a multiple of n/d. If n is the product of two primes (and for many other n) then the size of the orbits of this action are divisible by n. However, at $n = 18$ there are orbits of size $\pm 6 \bmod 18$, so here we expect the congruence (3) to fail.
5. A001945: $1, 1, 1, 5, 1, 7, 8, 5, 19, \dots$ is in $\mathcal{E}R$ since it counts the periodic points in the automorphism of the 3-torus given by the

matrix $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. This sequence has been studied computationally for prime appearances (see [4]) and it comes from the cubic polynomial with smallest Mahler measure (see [6]).

6. The large class of elliptic divisibility sequences (see [5]) and Somos sequences seem never to fall in $\mathcal{ER}$.
7. Three interesting sequences that seem to be in $\mathcal{ER}$ are the Euler sequence A000364 and the sequences A006953, A006954 connected with the Bernoulli numbers.

Example 5.2. Sequences in $\mathcal{ER}$ arise from the combinatorics of an iterated map. It is a natural question to ask what an orbit of **ORBIT** looks like, and whether there are any asymptotic properties associated to it. The simplest orbit starts with the unit sequence A000007. Applying **ORBIT** iteratively to this gives the following sequence of sequences (in each case, the sequence counts the number of periodic points in a map which has the number of orbits of length n given by the nth entry in the previous sequence).

$1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$ (A000007)

$1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$(A000012)

$1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, 39, 20$(A000203)

$1, 7, 13, 35, 31, 91, 57, 155, 130, 217, 133, 455, 183, 399, 403$(A001001)

$1, 15, 40, 155, 156, 600, 400, 1395, 1210, 2340, 1464, 6200, 2380, 6000$

$1, 31, 121, 651, 781, 3751, 2801, 11811, 11011, 24211, 16105, 78771, 30941$

$1, 63, 364, 2667, 3906, 22932, 19608, 97155, 99463, 246078, 177156$

$1, 127, 1093, 10795, 19531, 138811, 137257, 788035, 896260, 2480437$

$1, 255, 3280, 43435, 97656, 836400, 960800, 6347715, 8069620, 24902280$

$1, 511, 9841, 174251, 488281, 5028751, 6725601, 50955971, 72636421$

$1, 1023, 29524, 698027, 2441406, 30203052, 47079208, 408345795$

$1, 2047, 88573, 2794155, 12207031, 181308931, 329554457, 3269560515$

$1, 4095, 265720, 11180715, 61035156, 1088123400, 2306881200$

$1, 8191, 797161, 44731051, 305175781, 6529545751, 16148168401$

$1, 16383, 2391484, 178940587, 1525878906, 39179682372, 113037178808$

$1, 32767, 7174453, 715795115, 7629394531, 235085301451$

$1, 65535, 21523360, 2863245995, 38146972656, 1410533397600$

The arithmetic and growth properties of these sequences will be explored elsewhere. The sequence of first, second and third terms comprise A000012, A000225, and A003462 respectively.

6. Summary

Being exactly realizable is a strong symmetry property of an integer sequence. In this table we summarize the sequences from the Encyclopedia found to be exactly realizable, together with the corresponding sequence counting the orbits, and any other information. All the sequences are expected to have realizing maps – the inclusion of a map means that we know of a map that is natural in some sense (for example, has a finite description or is algebraic). Direct proofs of the congruence are cited in some brief fashion – a question mark indicates that we do not know a proof and seek one, e means it is easy, and a combinatorial counting problem suggests why the number of orbits is a non-negative integer. The combinatorial counting problems and maps are labelled as follows.

- POLY: the orbits count the number of irreducible polynomials over a finite field.
- NECK(k): the orbits count the number of aperiodic necklaces with n beads in k colours.
- NECK: the orbits count a family of necklaces with constraint – see the encyclopedia entry for details.
- KUMMER: follows from the Kummer and von Staudt congruences.
- COMB: follows from standard combinatorics arguments.
- CHK: the orbit sequence is a 'CHK' transform.
- S(1):S-integer map with $\xi = 2, S = \{2, 3\}, k = \mathbb{Q}$.
- S(2):S-integer map with $\xi = t, S = \{t + 1\}, k = \mathbb{F}_2(t)$.
- R: irrational circle rotation.

Of course there are often many ways to fill in the last column. If there is a natural realizing map, then that fact in itself is usually the best proof of the congruence. Sequences marked with a question mark in the first column are not known to be in $\mathcal{ER}$ at all: they just seem to satisfy the congruence for the first twenty or so terms. A star indicates that the initial term of the sequence is shifted by one. Of course any non-negative integer sequence at all can appear in the second column, so the selection here is based on the following arbitrary criterion: either the periodic point sequence or the orbit counting sequence is 'interesting'.

$f_n(T)$	$f_n^o(T)$	T	Proof of (3)
A00004	A00004	R	e
A00012	A00007	singleton	e
A000079*	A001037	full 2-shift	POLY

A000203	A00012	-	e
A000204	A006206	golden mean shift	NECK
A000244*	A027376*	full 3-shift	POLY
A000302*	A027377*	full 4-shift	POLY
A000351*	A001692*	full 5-shift	POLY
A000364*?	A060164	-	-
A000400*	A032164	full 6-shift	NECK(6)
A000420*	A001693	full 7-shift	POLY
A000593	A000035*	-	e
A000670*	A060223	e	
A000984*	A060165	-	COMB
A001001	A000203	-	e
A001018*	A027380*	full 8-shift	POLY
A001019*	A027381*	full 9-shift	POLY
A001020*	A032166	full 11-shift	NECK(11)
A001021*	A032167	full 12-shift	NECK(12)
A001022*	A060216	full 13-shift	NECK(13)
A001023*	A060217	full 14-shift	NECK(14)
A001024*	A060218	full 15-shift	NECK(15)
A001025*	A060219	full 16-shift	NECK(16)
A001026*	A060220	full 17-shift	NECK(17)
A001027*	A060221	full 18-shift	NECK(18)
A001029*	A060222	full 19-shift	NECK(19)
A001157	A000027	-	e
A001158	A000290*	-	e
A001641?	A060166	-	-
A001642?	A060167	-	-
A001643?	A060168	-	-
A001700	A022553	-	-
A001945	A060169	auto of $\mathbb{T}^3$	-
A004146*	A032170	auto of $\mathbb{T}^2$	CHK
A005809*	A060170	-	COMB
A006953?	A060171	-	KUMMER?
A006954?	A060479	-	KUMMER?
A011557*	A032165*	full 10-shift	NECK(10)
A023890	A005171	-	e
A027306*	A060172	-	COMB
A035316	A010052*	-	e
A047863*	A060224	-	-
A048578	A060477	4-shift $\cup$ singleton	-
A056045	A060173	-	COMB
0,2,0,6,0,8,0,14,...	A000035	-	e

A059928	A060478	auto of $\mathbb{T}^{10}$	e
A059990	A060480	S(1)	-
A059991	A060481	S(2)	-

Table 1: Exactly realizable sequences.

References

[1] M. Bernstein and N.J.A. Sloane. Some canonical sequences of integers, *Linear Algebra Appl.* , **226/228**:57–72, 1995.

[2] Peter J. Cameron. Sequences realized by oligomorphic permutation groups, *J. Integer Seq.* , **3**:Article 00.1.5, html document (electronic), 2000.

[3] Vijay Chothi, Graham Everest, and Thomas Ward. S-integer dynamical systems: periodic points. *J. Reine Angew. Math.* , **489**:99–132, 1997.

[4] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in sequences associated to polynomials (after Lehmer). *LMS J. Comput. Math.* , **3**:125–139 (electronic), 2000.

[5] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.* , **4**:1–13 (electronic), 2001.

[6] Graham Everest and Thomas Ward, *Heights of polynomials and entropy in algebraic dynamics* , Springer-Verlag, London, 1999.

[7] G.H. Hardy and E.M. Wright. *An introduction to the Theory of Numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[8] D.A. Lind. Dynamical properties of quasihyperbolic toral automorphisms. *Ergodic Theory Dynamical Systems* , **2**(1):49–68, 1982.

[9] D.A. Lind. The entropies of topological Markov shifts and a related class of algebraic integers. *Ergodic Theory Dynamical Systems* , **4**(2):283–300, 1984.

[10] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding* . Cambridge University Press, Cambridge, 1995.

[11] Y. Puri. *Arithmetic Properties of Periodic Orbits* . PhD thesis, The University of East Anglia, 2000.

[12] N.J.A. Sloane. *Online Encyclopedia of Integer Sequences* .

[13] Thomas Ward. Almost all S-integer dynamical systems have many periodic points. *Ergodic Theory Dynamical Systems* , **18**:471–486 (1998).

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.

E-mail address: t.ward@uea.ac.uk