Arithmetic of numbers of periodic points

Yash Paul Puri

A thesis submitted at the University of East Anglia in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

September 25, 2000

Abstract

Three problems are studied. The first is: When is a given sequence the sequence of numbers of periodic points for some map? Necessary and sufficient conditions are found for this property, and these are used to address refined versions of the question. The main results are that non-constant polynomials can never be realized in this sense, and that quadratic recurrences can only be realized under a non-trivial constraint.

The second is: When does a given sequence approximate the sequence of numbers of periodic points for some map? Some tests are obtained and, *inter alia*, we show that the sequence $(n^s \log n)$ has this property if and only if $s \geq 1$.

In the third, the growth rate of the number of points of period n is compared with the number of points of least period n. For either quantity having a finite exponential growth rate, it is shown that the other's growth is identical. However, for either quantity having a positive polynomial growth rate, it is found that the other cannot.

Generally, proofs of statements have only been included when, to my knowledge, they are original. Exceptions to this are indicated clearly in the text.

I deeply appreciate the personal support, kindness, diligence and mathematical guidance of my thesis supervisor, Thomas Ward. Thanks Tom.

Cordial thanks to Graham Everest too, for his warm wisdom, for conversations about congruences, and in particular for providing an elegant proof of Lemma 3.1.

I gratefully acknowledge the financial support of the E.P.S.R.C. for three years of this research.

Notation

Throughout, $\mathbf{C}, \mathbf{R}, \mathbf{R}^+, \mathbf{Z}, \mathbf{Z}^+$ and $\mathbf{N}$ will denote, respectively, the complex numbers, reals, non-negative reals, integers, non-negative integers and natural numbers.

Sequences will usually be denoted by lower case letters. Thus, given a sequence f and natural number n, the n-th term of f is f_n. Often, we write (f_n) for f, a subsequence of which may be written as (f_{n_r}). Respectively, (0) and (1) are the *zero* and *unit* sequences. Sometimes a sequence may be defined by listing its first few terms, as in $f = (1, 3, 1, 3, 1, 3, \ldots)$. Unless stated otherwise, it may be assumed that a sequence f takes values in $\mathbf{C}$.

For each pair of sequences f and g, the sequences $f + g$, $f - g$, fg and $\frac{f}{g}$ are defined in the usual way: $(f \pm g)_n = f_n \pm g_n$, $(fg)_n = f_n g_n$ and $(\frac{f}{g})_n = \frac{f_n}{g_n}$ for each $n \geq 1$; for $\frac{f}{g}$ it is assumed that no term of g is 0.

The divisors of each integer are assumed to be positive.

We will, now and then, use the word 'eventually' which we now explain. A statement $S(n)$ about the natural number n is said to hold eventually if it holds for all n sufficiently large. For example, $2^n > 100$ eventually. This word will also be applied to statements in which reference to $\mathbf{N}$ is implicit: for example, given two sequences f and g, in saying '$f = g$' we mean $f_n = g_n$ for each $n \in \mathbf{N}$; in saying '$f = g$ eventually' we mean $f_n = g_n$ for all n sufficiently large. It is hoped that, phrases such as 'eventually equal sequences' and 'the sequence f is eventually 0' will be clear.

All other notation, if not traditional, will be explained as needed.

Contents

Chapter 1

Introduction

This work studies the combinatorial properties of periodic orbits. The setting studied is that of arbitrary maps of countable sets, though the conclusions apply largely to homeomorphisms of compact topological spaces. In order to state the problems, we make some quick definitions here (these will be treated in greater detail in later chapters), and describe some of the results in special cases.

Let T be a map from a set X to itself. For each $n \geq 1$, define

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

to be the number of points with period n under T, viewed as a sequence $f = f(T)$. On the other hand, consider an arbitrary sequence ϕ of non-negative integers. A natural question to ask is: When is ϕ of the form $f = f(T)$? Say that $\phi \in \mathcal{ER}$ ('ϕ is exactly realizable') if there is a pair (X, T) for which $\phi = f(T)$. It is also natural to ask for a weaker form of realization: say that $\phi \in \mathcal{RR}$ ('ϕ is realizable in rate') if there is a pair (X, T) for which $\phi_n / f_n \to 1$ as $n \to \infty$.

1.1 Structure of $\mathcal{ER}$

In Chapter 2 necessary and sufficient conditions are given for membership of $\mathcal{ER}$. In order to gain further insight into the shape of $\mathcal{ER}$, the following problem has been studied. Given a natural class of non-negative integer sequences $\mathcal{S}$, can sharp statements be made about the members of $\mathcal{S} \cap \mathcal{ER}$? Some of the results proved in this thesis are the following.

Example 1.1 1. If $\mathcal{S}$ comprises the polynomials, then $\mathcal{S} \cap \mathcal{ER}$ consists of the constant polynomials.

2. If $\mathcal{S}$ comprises the geometric progressions, then $\mathcal{S} \cap \mathcal{ER}$ consists exactly of those progressions for which every prime dividing the common ratio also divides the first term.

3. If $\mathcal{S}$ comprises sequences satisfying a second order linear recurrence with integer coefficients and with a non-square discriminant, then $\mathcal{S} \cap \mathcal{ER}$ is one-dimensional (in the sense that every element of it is a rational multiple of a single sequence).

These are proved in Corollary 2.4, Lemma 2.9, and Theorem 3.1 respectively.

A great deal of the work in Chapters 2 and 3 is concerned with more general sequences. For linear recurrences that are sufficiently carefully chosen, the result above may be arrived at very quickly (cf. Section 2.6 where the Fibonacci recurrence is covered as motivation for the general case). The methods used for the second order linear recurrence are very quadratic in nature: it makes sense to ask the same question about higher-order recurrences, but different methods would be required to answer it.

1.2 Structure of $\mathcal{RR}$

The question of membership in $\mathcal{RR}$ is of course much softer than membership in $\mathcal{ER}$, but some strong conclusions can again be reached about how specific classes of sequences intersect $\mathcal{RR}$. Sequences with zeros cause some technical complications in Chapter 5, so we simply record a few here results here.

Example 1.2 1. The sequences (s^n) and (n^s) are in $\mathcal{RR}$ for each $s > 1$.

2. The sequence (n) is not in $\mathcal{RR}$.

3. The sequence $(n \log n)$ is in $\mathcal{RR}$.

1.3 Comparing growth rates

Chapter 4 is concerned with the following type of question. Given a sequence $f(T) \in \mathcal{ER}$, let g be the sequence whose n-th term is the number of points of *least* period n under T. Then what is the relationship between the growth rate of g and the growth rate of f? The following results are taken from Theorems 4.1 and 4.2.

Example 1.3 For exponential and super-exponential rates, the following hold when $g > 0$.

1. $\frac{1}{n}\log f_n \to C \in [0,\infty)$ if and only if $\frac{1}{n}\log g_n \to C \in [0,\infty)$.
2. If $\frac{1}{n}\log f_n \to \infty$, then the set $\{\frac{1}{n}\log g_n\}$ may have infinitely many limit points.

Example 1.4 Sub-exponential growth rates are more subtle.

1. For each $s \geq 1$, $\frac{f_n}{n^s} \to 0$ if and only if $\frac{g_n}{n^s} \to 0$.
2. For all $C > 0$ and $s > 1$, if $\frac{f_n}{n^s} \to C$, then the set $\{\frac{g_n}{n^s}\}$ must have infinitely many limit points, including C
3. For all $C > 0$ and $s \geq 1$, if $\frac{g_n}{n^s} \to C$, then the set $\{\frac{f_n}{n^s}\}$ must have infinitely many limit points, including C.

1.4 Background examples

At several points an argument of the following shape is used. Given a candidate sequence ϕ for membership in $\mathcal{ER}$, ϕ may be rejected by finding a congruence or an inequality that it fails. On the other hand, to accept ϕ, the realizing pair (X,T) must be exhibited or infinitely many congruences and infinitely many inequalities must be checked. It is therefore useful to have a small stock of well-known examples of pairs (X,T) for which $f = f(T)$ is known. These are standard: all the material below may be found in Lind and Marcus [8] (for the subshifts of finite type) and Chothi, Everest and Ward [4] (for the group automorphisms).

Example 1.5 Given a matrix $A \in M_k(\mathbf{Z}^+)$, there is an associated subshift of finite type (X_A, T_A), which has exactly trace(A^n) points of period n.

Two simple cases are worth mentioning:

1. If $A = (a_{ij}) \in M_k(\{0,1\})$, then

$$X_A = \{x \in \{1,\dots,k\}^{\mathbf{Z}} : a_{x_j x_{j+1}} = 1 \text{ for all } j\}$$

   and T_A is the left shift on the closed subset X_A of the compact space $\{1,\dots,k\}^{\mathbf{Z}}$.

2. If $A = (a_{ij})$ has $a_{ij} = 1$ for all i and j, then the *full shift* on k symbols is obtained, and this has k^n points of period n.

Example 1.6 Let $R = \mathbf{Z}[\frac{1}{q_1 \dots q_s}]$ be the smallest subring of the rationals in which the chosen primes $q_1, \dots, q_s$ are invertible. Then, for each $\xi \in R^\times$, the automorphism $T : X = \hat{R} \to X = \hat{R}$ dual to the automorphism $x \mapsto \xi x$ of R is a homeomorphism of a compact space with $\prod_{i=1}^{s} |\xi^n - 1|_{q_i} \times |\xi^n - 1|$ points of period n.

For example, if $s = 1$, $q_1 = 2$, and $\xi = -2$, then this construction gives a pair (X, T) for which there are $|(-2)^n - 1|_2 \times |(-2)^n - 1| = |(-2)^n - 1|$ points of period n.

Chapter 2

Exact Realization

In this chapter simple combinatorial arguments are used to give necessary and sufficient conditions for membership of $\mathcal{ER}$. These are used to describe basic properties of $\mathcal{ER}$.

2.1 Preliminaries

2.1.1 Some basic facts about the Möbius function

Definition 2.1 The *Möbius function* μ is defined on the natural numbers by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has a squared factor,} \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

Theorem 2.1 Möbius inversion formula. *Let f and g be sequences. Then $f_n = \sum_{d|n} g_d$ for each $n \geq 1$ if and only if $g_n = \sum_{d|n} \mu(n/d) f_d$ for each $n \geq 1$.*

Proof. See, for example, Hardy and Wright [6, Theorems 266 and 267]. □

Definition 2.2 A sequence ϕ is *multiplicative* if it is not identically zero and if $\phi_{mn} = \phi_m \phi_n$ for each coprime pair m, n. A multiplicative sequence is *completely multiplicative* if $\phi_{mn} = \phi_m \phi_n$ for all m, n.

The following properties of μ will be used (for their proofs see, for example, HARDY and WRIGHT [6, Section 16.3]):

$$\mu \text{ is multiplicative.} \tag{2.1}$$

$$\textstyle\sum_{d|n} \mu(d) = 1 \quad \text{if } n = 1, \qquad \sum_{d|n} \mu(d) = 0 \quad \text{if } n > 1. \tag{2.2}$$

For each natural number n, the *Euler totient* $e(n)$ is the number of natural numbers not exceeding n that are coprime to n. We have

$$e(n) = \sum_{d|n} \mu(n/d)d \quad \text{for each natural number } n. \tag{2.3}$$

If $n > 1$, and r is the number of distinct primes dividing n, then

$$\sum_{d|n} |\mu(d)| = 2^r. \tag{2.4}$$

Notation 2.1 Given a sequence f let

$$\hat{f}_n := \sum_{d|n} \mu(n/d) f_d \quad \text{for each } n \geq 1, \tag{2.5}$$

and write $\hat{f}$ for the sequence whose n-th term is $\hat{f}_n$. By the 'if' part of Theorem 2.1, a sequence f may be defined by specifying $\hat{f}_n$ for each $n \geq 1$. Then

$$f_n = \sum_{d|n} \hat{f}_d \quad \text{for each } n \geq 1\ . \tag{2.6}$$

2.1.2 Elementary properties of periodic points

Definition 2.3 Let X be a set and T be a map on X to itself. Suppose $x \in X$. If n is a natural number such that $T^n(x) = x$, then x is said to be *periodic* and to have *period* n. If x is periodic, then the *least period* of x is the least natural number n for which $T^n(x) = x$. The *orbit* O_x of x is the set $\{T^z(x) : z \in \mathbf{Z}^+\}$.

Lemma 2.1 *Let X be a set and T be a map on X to itself. For each $n \geq 1$, let*

$$F_n := \{x \in X : x \text{ has period } n\}, \quad G_n := \{x \in X : x \text{ has least period } n\}. \tag{2.7}$$

Suppose n is a natural number and $x \in X$. The following hold:

(i) *if* $x \in F_n$, *then the least period of* x *divides* n;

(ii) *if* $x \in G_n$, *then* $O_x = \{x, T(x), \ldots, T^{n-1}(x)\}$;

(iii) $F_n = \bigcup_{d|n} G_n$, *the union being disjoint;*

(iv) *if* $x \in G_n$, *then* $O_x \subseteq G_n$;

(v) *if* $x \in G_n$, *then* $\#O_x = n$;

(vi) *if* G_n *is a finite set, then* $n|\#G_n$.

Proof. (i) Let x have period n. Suppose l is the least period of x and, by the division algorithm, let $m, k \in \mathbf{Z}^+$ be such that $n = k + lm$ and $k < l$. Then

$$x = T^n(x) = T^{k+lm}(x) = T^k[(T^l)^m(x)] = T^k(x).$$

So, $x = T^k(x)$. But $k < l$ and l is the least period of x. Thus, $k = 0$. Hence, $n = lm$, proving (i).

(ii) Let x have least period n. By Definition 2.3, $\{x, T(x), \ldots, T^{n-1}(x)\}$ is a subset of O_x. To see that O_x is a subset of $\{x, T(x), \ldots, T^{n-1}(x)\}$, suppose $T^z(x) \in O_x$ for some $z \in \mathbf{Z}^+$. Let $m, k \in \mathbf{Z}^+$ be such that $z = k + nm$ and $k < n$. Thus, $T^k(x)$ is in $\{x, T(x), \ldots, T^{n-1}(x)\}$. But, $T^z(x) = T^k[(T^n)^m(x)] = T^k(x)$ since x has period n. This proves (ii).

(iii) The union is disjoint since each point in X has at most one least period. The union is a subset of F_n because if $d|n$ and $T^d(x) = x$ for some $x \in X$, then $T^n(x) = (T^d)^{n/d}(x) = x$. Also, F_n is a subset of the union because if $T^n(x) = x$ for some $x \in X$, then x has a least period which, by (i), is a divisor of n.

(iv) Let x have least period n. Take any $k \in \{0, 1, \ldots, n-1\}$. By (ii), it is enough to show that $T^k(x)$ has least period n. Now $T^n[T^k(x)] = T^k[T^n(x)] = T^k(x)$ since n is a period of x. Thus, n is a period of $T^k(x)$. Let $l \leq n$ be the least period of $T^k(x)$. So, $T^l[T^k(x)] = T^k(x)$ and, therefore, $T^{n-k}(T^l[T^k(x)]) = T^{n-k}[T^k(x)]$. Hence, $T^l[T^n(x)] = T^n(x)$ and, since n is a period of x, we have $T^l(x) = x$. But n is the least period of x. Therefore, $n \leq l$. Since $l \leq n$ as well, it follows that $l = n$. Whence, n is the least period of $T^k(x)$, which is the desired conclusion for (iv).

(v) Let x have least period n. By (ii), it is enough to show that the elements of $\{x, T(x), \ldots, T^{n-1}(x)\}$ are distinct. Suppose for a contradiction that $T^i(x) = T^j(x)$ for some i and j with

$$0 \leq i < j < n. \tag{2.8}$$

So, $T^{n-i}[T^i(x)] = T^{n-i}[T^j(x)]$, which implies $T^n(x) = T^{j-i}[T^n(x)]$. Since n is a period of x, we have $x = T^{j-i}(x)$. Here, $j - i$ is positive by (2.8) and, since n is the least period of x, we have $j - i \geq n$. Thus, $j \geq n$. But $j < n$ by (2.8). This contradiction proves (v).

(vi) Define a relation $\sim$ on G_n as follows. For each pair x and y in G_n let $x \sim y$ if and only if $x \in O_y$. To see that $\sim$ is an equivalence let w, x and y be in G_n. It is reflexive since $x \in O_x$ by Definition 2.3. It is transitive because if $z_1, z_2 \in \mathbf{Z}^+$ with $w = T^{z_1}(x)$ and $x = T^{z_2}(y)$, then $w = T^{z_1+z_2}(y)$. To show symmetry, let $x \in O_y$. By (ii), pick an r with $0 \leq r < n$ and $x = T^r(y)$. Then $T^{n-r}(x) = T^{n-r}[T^r(y)] = T^n(y) = y$ since n is a period of y. Thus, $y \in O_x$, showing that $\sim$ is symmetric. Whence, $\sim$ is an equivalence relation on G_n.

For each $x \in G_n$ the equivalence class of x is $\{y \in G_n : y \in O_x\}$. This equals O_x by (iv). Also, $\#O_x = n$ by (v). Thus, if G_n is a finite set, then $n | \#G_n$, as stated in (vi). □

2.2 The Basic Lemma

At the heart of our concern are the next definition and lemma.

Definition 2.4 A *system* is a pair (X, T) where X is a set and T is a map on X to itself.

Let f be a sequence of non-negative integers. If there is a system (X, T) such that

$$f_n = \#\{x \in X : x \text{ has period } n\} \quad \text{for each } n \geq 1,$$

then f is *exactly realizable*. When a system (X, T) has this property with respect to f, phrases such as 'f is exactly realized by (X, T)' will be used.

Denote the set of exactly realizable sequences by $\mathcal{ER}$.

Lemma 2.2 The Basic Lemma. *Let f be a sequence of non-negative integers. Then f is exactly realizable if and only if*

$$\hat{f}_n \text{ is a non-negative integer for each } n \geq 1, \tag{2.9}$$

$$n \text{ divides } \hat{f}_n \text{ for each } n \geq 1. \tag{2.10}$$

Proof. For the 'only if' part let f be exactly realizable. By Definition 2.4, choose a system (X, T) such that, with the notation of (2.7), $f_n = \#F_n$ for each $n \geq 1$. Since f is a sequence in $\mathbf{Z}^+$, the same holds for the sequence $(\#G_n)$ because $G_n \subseteq F_n$ for each $n \geq 1$. Therefore, by Lemma 2.1(iii), $f_n = \sum_{d|n} \#G_d$ for each $n \geq 1$. Hence,

$$\begin{aligned} \#G_n &= \sum_{d|n} \mu(n/d) f_d \quad \text{(by the 'only if' part of Theorem 2.1)} \\ &= \hat{f}_n \quad \text{(by the notation of (2.5))}. \end{aligned}$$

This proves (2.9) since $(\#G_n)$ is a sequence in $\mathbf{Z}^+$. By Lemma 2.1(vi), condition (2.10) follows, and proves the 'only if ' part.

For the converse, we will in fact prove a stronger statement by exhibiting a realizing system in which the map T is a homeomorphism of a compact space. This relates the later work to dynamical systems, but raises a potential subtlety (see Remark 2.1(2)).

Definition 2.5 A *dynamical system* is a triple (X, τ, T) where (X, τ) is a compact topological space and $T: X \to X$ is a homeomorphism of (X, τ).

Given a sequence f, in saying 'f is exactly realized by a dynamical system' the following is meant: there is a dynamical system (X, τ, T) such that the system (X, T) exactly realizes f.

The stronger statement to be proved is the following lemma.

Lemma 2.3 *If f is a sequence with $\hat{f}_n \in \mathbf{Z}^+$ and $n|\hat{f}_n$ for each $n \geq 1$, then f is exactly realized by a dynamical system.*

In the proof of this lemma, use will be made of the notion of 'compactification', which is now defined with an example.

Definition 2.6 Let (X_*, τ_*) and (X, τ) be topological spaces. Then (X_*, τ_*) is a *compactification* of (X, τ) if (X_*, τ_*) is compact and contains a dense subspace homeomorphic to (X, τ).

Example 2.1 In illustration, let (X, τ) be a non-compact space. An example of this, and one we will work with later, is $(\mathbf{N}, 2^{\mathbf{N}})$, the space of the natural numbers with the discrete topology. Let I be a non-empty set which does not intersect X, and adjoin it to X forming the set $X_* = X \cup I$. Define τ_* to be all sets of the following types:

(I) U, where U is in τ;

(II) $U \cup I$, where U is in τ and $X - U$ is compact in (X, τ).

Straightforward arguments show that τ_* is a topology for X_*, that (X_*, τ_*) is compact and that (X, τ) is a dense subspace of (X_*, τ_*). For the case when I is a singleton, details of these arguments may be found in, for example, in the proofs of Propositions 5.21 and 5.22 of Cain [3]. These proofs, with very few and slight changes, will also do for the general case. Thus, (X_*, τ_*) is a compactification of (X, τ). When I is a singleton it is usual to write $I = \{\infty\}$ and the compactification is called *Alexandroff* or *one-point*. It will be called *k-point* when $I = \{\infty_1, \dots, \infty_k\}$ has k elements.

Proof of Lemma 2.3. Let f be a sequence with $\hat{f}_n \in \mathbf{Z}^+$ and $n | \hat{f}_n$ for each $n \geq 1$. For each $n \geq 1$, write $s_n := \sum_{i=1}^{n} \hat{f}_i$. There are four cases:

(i) $\hat{f}$ has a positive term and is eventually 0;

(ii) $\hat{f}_1$ is positive and $\hat{f}$ is not eventually 0;

(iii) $\hat{f}_1$ is 0 and $\hat{f}$ is not eventually 0;

(iv) $\hat{f}$ is the zero sequence (0).

For case (i), suppose $\hat{f}_l$ is the last positive term of $\hat{f}$. Let $X = \{1, 2, \dots, s_l\}$ and define $T: X \to X$ to be the product of the following cycles:

$$\hat{f}_1 \text{ cycles of length } 1 \qquad (1)(2)\dots(s_1);$$

$\hat{f}_2/2$ cycles of length 2 $\qquad (s_1+1, s_1+2)(s_1+3, s_1+4)\ldots(s_2-1, s_2)$;

$\hat{f}_3/3$ cycles of length 3 $\qquad (s_2+1, s_2+2, s_2+3)\ldots(s_3-2, s_3-1, s_3)$;

and so on, ending up with the $\hat{f}_l/l$ cycles of length l below

$$(s_{l-1}+1, s_{l-1}+2, \ldots, s_{l-1}+l)\ldots(s_l-l+1, \ldots, s_l-1, s_l).$$

T is a well-defined bijection because each element of X appears in exactly one cycle. Give X the discrete topology to obtain the space $(X, 2^X)$, of which, therefore, T is a homeomorphism. This space is compact since X is finite. Whence, $(X, 2^X, T)$ is a dynamical system by Definition 2.5.

It will now be shown that, for each $n \geq 1$, the number of points of period n equals f_n. We will then be done by Definition 2.4. Recall the notation of (2.7). In the definition of T, for each n there are $\hat{f}_n/n$ cycles of length n. Hence, G_n is a finite set for each n, and $\#G_n = \hat{f}_n$. Therefore, using (2.6) and Lemma 2.1(iii), for each $n \geq 1$,

$$f_n = \sum_{d|n} \hat{f}_d = \sum_{d|n} \#G_d = \#F_n,$$

as desired. Thus, f is exactly realizable in case (i).

For (ii), let $(\mathbf{N}_*, 2^{\mathbf{N}}_*)$ be the one-point compactification of $(\mathbf{N}, 2^{\mathbf{N}})$, as explained in Example 2.1. Here, $\mathbf{N}_* = \mathbf{N} \cup \{\infty\}$. Define a map $T\colon \mathbf{N}_* \to \mathbf{N}_*$ by the product of the cycles below:

$$\underbrace{(\infty)(1)(2)\ldots(s_1-1)}_{\hat{f}_1 \text{ cycles of length } 1} \qquad \underbrace{(s_1, s_1+1)\ldots(s_2-2, s_2-1)}_{\hat{f}_2/2 \text{ cycles of length } 2}$$

$$\underbrace{(s_2, s_2+1, s_2+2)\ldots(s_3-3, s_3-2, s_3-1)}_{\hat{f}_3/3 \text{ cycles of length } 3}\ldots$$

and so on. In this definition of T, if $s_1 = 1$, then it is assumed that the cycle of length 1 is (∞). Now, $(\mathbf{N}_*, 2^{\mathbf{N}}_*)$ is compact by Example 2.1. For the same reasons as given in case (i), T is a bijection and $f_n = \#F_n$ for each $n \geq 1$. Hence, by Definitions 2.5 and 2.4, it will suffice to show that each of T and T^{-1} sends elements of $2^{\mathbf{N}}_*$ to elements of $2^{\mathbf{N}}_*$.

Recall the open sets of types (I) and (II) in Example 2.1. Let $U \in 2^{\mathbf{N}}_*$ be of type (I). Thus, U is a subset of $\mathbf{N}$. By the definition of T, the same goes for $T(U)$. Hence, $T(U)$ is in $2^{\mathbf{N}}$ and is, therefore, of type (I). So, $T(U) \in 2^{\mathbf{N}}_*$.

For open sets of type (II), note that, as in any discrete space, the compact sets in $(\mathbf{N}, 2^{\mathbf{N}})$ are the finite subsets of $\mathbf{N}$. Now let $U \cup I$ be of type (II), so that U is a subset of $\mathbf{N}$ and $\mathbf{N} - U$ is finite. We have

$$T(U \cup I) = T(U) \cup T(I) = T(U) \cup I,$$

which must be shown to be in $2^{\mathbf{N}}_*$. In fact, $T(U) \cup I$ is a set of type (II) for the following reasons: $T(U)$ is a subset of $\mathbf{N}$ and, hence, in $2^{\mathbf{N}}$; also, $\mathbf{N} - T(U)$ is finite since $\mathbf{N} - U$ is finite and $T(\mathbf{N} - U) = T(\mathbf{N}) - T(U) = \mathbf{N} - T(U)$; thus, $\mathbf{N} - T(U)$ is compact in $(\mathbf{N}, 2^{\mathbf{N}})$. So, $T(U) \cup I$ is in $2^{\mathbf{N}}_*$. We have shown that T sends open sets to open sets. For the same reasons, the same holds for T^{-1}. Hence, $(\mathbf{N}_*, 2^{\mathbf{N}}_*, T)$ is a dynamical system exactly realizing f, which settles case (ii).

For (iii), let $k > 1$ be such that $\hat{f}_1 = \cdots = \hat{f}_{k-1} = 0$ and $\hat{f}_k \neq 0$. Let $(\mathbf{N}_*, 2^{\mathbf{N}}_*)$ be the $\hat{f}_k$-point compactification of $(\mathbf{N}, 2^{\mathbf{N}})$. Here, $\mathbf{N}_* = \mathbf{N} \cup \{\infty_1, \ldots, \infty_{\hat{f}_k}\}$. Define a map $T\colon \mathbf{N}_* \to \mathbf{N}_*$ by the product of the cycles below:

$$\underbrace{(\infty_1, \ldots, \infty_k) \ldots (\infty_{\hat{f}_k - k+1}, \ldots, \infty_{\hat{f}_k})}_{\hat{f}_k/k \text{ cycles of length } k}$$

$$\underbrace{(1, 2, \ldots, k+1) \ldots (\hat{f}_{k+1} - k, \ldots, \hat{f}_{k+1})}_{\hat{f}_{k+1}/(k+1) \text{ cycles of length } k+1},$$

followed by $\hat{f}_{k+2}/(k+2)$ disjoint cycles each of length $k+2$ using the numbers $\hat{f}_{k+1} + 1, \ldots, \hat{f}_{k+1} + \hat{f}_{k+2}$, and so on. By exactly the argument used for case (ii), f is exactly realized by $(\mathbf{N}_*, 2^{\mathbf{N}}_*, T)$.

Finally, for case (iv) let $\hat{f} = 0$. So, $f = 0$ by (2.6). By Definition 2.4 and Lemma 2.1(iii), a dynamical system must be given for which $\#G_n = 0$ for each $n \geq 1$. By Lemma 2.1(v), this will be achieved if a dynamical system is exhibited in which no orbit is finite: let α be irrational; consider the compact metric space (S^1, ρ), where $S^1 = \{\omega \in \mathbf{C}\colon |\omega| = 1\}$ and ρ is the usual metric on $\mathbf{C}$; define a homeomorphism T

of (S^1, ρ) by $T(\omega) = \omega e^{2\pi i \alpha}$ for each $\omega \in S^1$; Jacobi's Theorem states that the orbit of each point of S^1 is dense in (S^1, ρ). So, (S^1, ρ, T) is a dynamical system exactly realizing f. Hence, Lemma 2.3 is proved and, therefore, so is the Basic Lemma. $\square$

Remark 2.1 1. Let

$$\widehat{\mathcal{ER}} := \{g : g \text{ is a sequence in } \mathbf{Z}^+ \text{ and } n | g_n \text{ for each } n \geq 1\}. \tag{2.11}$$

The Basic Lemma is equivalent to saying

$$\mathcal{ER} = \{f : \hat{f} \in \widehat{\mathcal{ER}}\}. \tag{2.12}$$

By the Basic lemma and Theorem 2.1, there is the following natural bijection between $\mathcal{ER}$ and $\widehat{\mathcal{ER}}$. Let $\hat{\ }: \mathcal{ER} \to \widehat{\mathcal{ER}}$ map each $f \in \mathcal{ER}$ to $\hat{f}$. This map is well defined by the 'only if' part of the lemma, and injective by the 'if' part of the theorem. Surjectivity follows from the 'only if' part of the theorem and 'if' part of the lemma, the inverse image of $g \in \widehat{\mathcal{ER}}$ being that f for which $f_n = \sum_{d|n} g_d$ for each $n \geq 1$. This surjectivity is equivalent to saying $\widehat{\mathcal{ER}} = \{\hat{f} : f \in \mathcal{ER}\}$.

2. A *metric dynamical system* is a triple (X, ρ, T) where (X, ρ) is a compact metric space and $T: X \to X$ is a homeomorphism of (X, ρ). In Lemma 2.3, it would be nice to make the stronger claim that the dynamical system exactly realizing f is metric. To see that our proof is insufficient for this claim, consider the system displayed for each of the cases (i) to (iv) into which $\hat{f}$ may fall. For case (iv) the space involved is metric. For (i) the space is finite with the discrete topology which, therefore, is metrizable. For (ii), the one-point compactification is homeomorphic to $\{0, 1, 1/2, 1/3, 1/4, \ldots\}$ with the usual metric on the reals. However, the topology in case (iii) is not metrizable because, on considering elements of I, it is seen that the topology is not Hausdorff.

   Nonetheless, there *is* a case (iii) sequence h which *is* exactly realized by a metric dynamical system. To see this, define a case (i) sequence f by $\hat{f} = (0, 2, 0, 0, 0, 0, \ldots)$ and a case (ii) sequence g by $\hat{g} = (1, 2, 3, 4, 5, 6, \ldots)$. Thus, by (2.6), $f = (0, 2, 0, 2, 0, 2, \ldots)$ and $g = (1, 3, 4, 7, 6, 12, \ldots)$. Let $h := fg =$

$(0,6,0,14,0,24,\ldots)$. So, $\hat{h}_1 = 0$. Also, h is unbounded. Hence, by (2.6), $\hat{h}$ is not eventually 0. Therefore, h is a case (iii) sequence.

Let f and g be exactly realized by metric dynamical systems (X_1, ρ_1, T_1) and (X_2, ρ_2, T_2), respectively. Let $X := X_1 \times X_2$. Define a metric ρ on X by

$$\rho((x_1,x_2),(y_1,y_2)) = \rho_1(x_1,y_1) + \rho_2(x_2,y_2) \quad \text{for all } (x_1,x_2),(y_1,y_2) \in X.$$

Define $T: X \to X$ by

$$T(x_1,x_2) = (T_1(x_1), T_2(x_2)) \quad \text{for each } (x_1,x_2) \in X.$$

It is a standard fact that (X, ρ, T) is a metric dynamical system. It is easy to show that the system (X, T) exactly realizes h, as may be confirmed on reading the second proof of Lemma 2.10(iii). Thus, h is exactly realized by a metric dynamical system.

A natural question to ask is: Is each case (iii) sequence exactly realized by a metric dynamical system? This query is appealing , but unimportant to the rest of this work. After this remark our main concern will be with the arithmetic and combinatorial properties of $\mathcal{ER}$, and not with those of dynamical systems. There are two ways of showing that a given sequence f is in $\mathcal{ER}$: we can exhibit a system which realizes f exactly or we can show that $\hat{f}_n \in \mathbf{Z}^+$ and $n|\hat{f}_n$ for each $n \geq 1$. From now on, dynamical systems will be used in the first of these ways but they will not be mentioned otherwise.

2.3 Some easy corollaries of the Basic Lemma

Corollary 2.1 *If $f, g \in \mathcal{ER}$ and $fg = 0$, then $f = 0$ or $g = 0$.*

Proof. The following more general fact will be proved: if f, g are sequences in $\mathbf{R}$ with $\hat{f}, \hat{g} \geq 0$ and $fg = 0$, then $f = 0$ or $g = 0$. The corollary will then immediately follow from the Basic Lemma.

Let f, g be in $\mathbf{R}$ with $\hat{f}, \hat{g} \geq 0$ and $fg = 0$. So, $f, g \geq 0$ by (2.6). Suppose, for a contradiction, that neither $f = 0$ nor $g = 0$. Let k, l be such that $f_k, g_l > 0$. Since

$\hat{f} \geq 0$, it follows from (2.6) that

$$f_{kl} = \sum_{d|kl} \hat{f}_d \geq \sum_{d|k} \hat{f}_d = f_k.$$

Similarly, $g_{kl} \geq g_l$. Hence, $f_{kl} g_{kl} \geq f_k g_l > 0$. This contradicts $fg = 0$ and we are done. □

Corollary 2.2 *A constant sequence in* $\mathbf{Z}^+$ *is exactly realizable.*

Proof. Suppose $z \in \mathbf{Z}^+$ and let f be the constant sequence (z). Two simple proofs are given. The first uses the Basic Lemma, and the second uses Definition 2.4.

(I) Using (2.5), for each $n \geq 1$

$$\hat{f}_n := \sum_{d|n} \mu(n/d) f_d = \sum_{d|n} \mu(n/d) z = z \sum_{d|n} \mu(n/d),$$

which, by (2.2), equals z when $n = 1$, and 0 otherwise. So, (2.9) and (2.10) hold. Thus, f is exactly realizable by the Basic Lemma.

(II) As required by Definition 2.4, it is easy to give a system which exactly realizes f. For $z = 0$, use the irrational circle rotation described at the end of the proof to the Basic Lemma. For $z > 0$, let $X = \{1, 2, \ldots, z\}$ and T be the identity map on X. Since, for each $n \geq 1$,

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

we are done. □

Corollary 2.3 *If* f *is exactly realizable, then so is* zf *for each* $z \in \mathbf{Z}^+$.

This is deduced easily using Corollary 2.2 with a later Lemma 2.10(iii). For positive z, with a simple induction, it also follows from Lemma 2.10(ii). However, it is quickly proved here using the Basic Lemma because it will help a little in the next result, which is interesting enough not to postpone.

Proof. Suppose $f \in \mathcal{ER}$ and $z \in \mathbf{Z}^+$. Write $\left(\widehat{zf}\right)_n$ for the n-th term of $\widehat{zf}$. For each $n \geq 1$, we use (2.5) and obtain

$$\left(\widehat{zf}\right)_n = \sum_{d|n} z f_d \mu(n/d) = z \sum_{d|n} f_d \mu(n/d) = z \hat{f}_n.$$

Thus, since f satisfies (2.9) and (2.10), the same goes for zf. Whence, $zf \in \mathcal{ER}$ by the Basic Lemma. □

2.3.1 Polynomials and $\mathcal{ER}$

Corollary 2.4 *No non-constant polynomial is exactly realizable.*

Proof. Suppose k is a natural number and $c_0, c_1, \ldots, c_k$ are rational numbers (cf. Remark 2.2 below) with $c_k \neq 0$. Define a polynomial ϕ by

$$\phi_n = c_0 + c_1 n + \cdots + c_k n^k \quad \text{for each } n \geq 1. \tag{2.13}$$

Assume, for a contradiction, that ϕ is exactly realizable. Let $c > 0$ be a common multiple of the denominators of the c_i's. Then $c\phi$ is a polynomial with integer coefficients, which is exactly realizable by Corollary 2.3. So, it may be assumed that the coefficients in (2.13) are all integers.

Using (2.10), it will be shown in turn that c_1 and c_k must be 0. Let p be a prime. By (2.5) and (2.13),

$$\hat{\phi}_{p^2} = \phi_{p^2} - \phi_p = c_1 p^2 + c_2 p^4 + \cdots + c_k p^{2k} - (c_1 p + c_2 p^2 + \cdots + c_k p^k),$$

which, by (2.10), is divisible by p^2. Hence, p divides c_1. Since this holds for each p, we have $c_1 = 0$. Whence, $k \geq 2$ because it is given that $k \geq 1$ and $c_k \neq 0$. Rewrite (2.13) as

$$\phi_n = c_0 + n^2(c_2 + c_3 n + \cdots + c_k n^{k-2}) \quad \text{for each } n \geq 1. \tag{2.14}$$

Let q be a prime distinct from p. By (2.5),

$$\hat{\phi}_{p^2 q} = \phi_{p^2 q} - \phi_{pq} - \phi_{p^2} + \phi_p,$$

which, by (2.10), is divisible by $p^2 q$. Now, it is apparent from (2.14) that $p^2 q$ divides $\phi_{p^2 q} - \phi_{pq}$. Thus, $p^2 q$ divides $\phi_{p^2} - \phi_p$, which, by (2.14), equals

$$c_0(1-1) + c_2(p^4 - p^2) + c_3(p^6 - p^3) + \cdots + c_k(p^{2k} - p^k). \tag{2.15}$$

Fixing p and letting $q \to \infty$, it follows that $\phi_{p^2} - \phi_p = 0$. Dividing the expression in (2.15) by p^{2k} and now letting $p \to \infty$, it is seen that $c_k = 0$. However, it is given that $c_k \neq 0$. This contradiction gives the result. □

Remark 2.2 1. In (2.13), letting n take the values $1, 2, \ldots, k+1$ in turn we obtain $k+1$ equations which may be written in matrix form as

$$\begin{bmatrix} \phi_1 \\ \phi_2 \\ \phi_3 \\ \vdots \\ \phi_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1^2 & \ldots & 1^k \\ 1 & 2 & 2^2 & \ldots & 2^k \\ 1 & 3 & 3^2 & \ldots & 3^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & k+1 & (k+1)^2 & \ldots & (k+1)^k \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}.$$

Here, the square matrix is a Vandermonde and it is straightforward to show (see, for example, Nicholson [10, page 135]) that its determinant is a non-zero integer. So, it has an inverse with rational entries. Since ϕ takes values in $\mathbf{Z}^+$, it follows that we could not have chosen the c_i's to be other than rational in the proof of Corollary 2.4.

2. Can a non-constant polynomial and an exactly realizable sequence be *eventually* equal? A basic fact helps answer this:

$$\text{if } (f_n) \text{ is exactly realizable, then so is } (f_{nK}) \text{ for each } K \geq 1. \tag{2.16}$$

To see this, let (X, T) be a system exactly realizing f. Suppose $K \geq 1$ and let $k_n := f_{nK}$ for each $n \geq 1$. Therefore, (X, T^K) is a system and, for each $n \geq 1$,

$$\begin{aligned} k_n = f_{nK} &= \{x \in X : T^{nK}(x) = x\} \quad \text{(by Definition 2.4)} \\ &= \{x \in X : (T^K)^n(x) = x\}. \end{aligned}$$

Hence, (X, T^K) exactly realizes k by Definition 2.4. This explains (2.16).

'No' is the answer to the above question: otherwise, suppose there is a polynomial ϕ as in (2.13) and an exactly realizable sequence f such that $\phi = f$ eventually; choose a natural number K such that $f_n = \phi_n$ for each $n \geq K$; then, the sequences (f_{nK}) and (ϕ_{nK}) are equal; since (f_{nK}) is exactly realizable by (2.16) and (ϕ_{nK}) is a non-constant polynomial we have a contradiction of Corollary 2.4.

2.3.2 Multiplicative sequences and $\mathcal{ER}$.

Recall Definition 2.2. By Hardy and Wright [6, Theorem 265], if $\hat{f}$ is multiplicative, then so is f. Thus, $\mathcal{ER}$ contains many multiplicative elements: choose any multiplicative sequence ϕ in $\mathbf{Z}^+$; let $\hat{f}_n := n\phi_n$ for each $n \geq 1$, so that $\hat{f}$ is multiplicative; the same goes for f, which, by the Basic Lemma, is in $\mathcal{ER}$.

Corollary 2.5 *The unit is the only completely multiplicative element of $\mathcal{ER}$.*

Proof. Let $f \in \mathcal{ER}$ be completely multiplicative. Condition (2.10) will be seen to force the result. Recall the elementary fact that the first term of a multiplicative sequence is 1. So, $f_1 = 1$. Fix a prime p and a natural number r. By (2.10) and (2.5),

$$p | \hat{f}_p = f_p - f_1 = f_p - 1, \tag{2.17}$$

$$p^r | \hat{f}_{p^r} = f_{p^r} - f_{p^{r-1}} = (f_p)^r - (f_p)^{r-1} = (f_p)^{r-1}(f_p - 1). \tag{2.18}$$

By (2.17), $p \not| f_p$. Hence, by (2.18), $p^r | f_p - 1$. This holds for each r and each p. Thus, fixing p and considering large r, we see that $f_p = 1$. Since this holds for each p and f is completely multiplicative, it follows that $f_n = 1$ for each $n \geq 1$. Since the unit sequence (1) is in $\mathcal{ER}$ by Corollary 2.2, we are done. □

2.3.3 The Euler-Fermat Theorem

The Euler-Fermat Theorem says

$$z^{e(n)} \equiv 1 \bmod n \quad \text{for all } z \in \mathbf{Z} \text{ and } n \in \mathbf{N}, \text{ where } e \text{ is the Euler totient.}$$

In a standard proof of this (see, for example, Hardy and Wright [6, Section 6.3]) it is first shown that

$$z^{p^r} \equiv z^{p^{r-1}} \bmod p^r \quad \text{for all } z \in \mathbf{Z},\ r \in \mathbf{N} \text{ and primes } p. \tag{2.19}$$

The theorem then quickly follows from some basic properties of congruences and the fact that e is multiplicative. The next corollary gives a quick route to (2.19), using only the full shift of Example 1.5 and condition (2.10) of the Basic Lemma.

Corollary 2.6 *The Euler-Fermat Theorem.*

Proof. By the comments above, we need just show (2.19). This is trivial if $z = 0$ or -1. For $z < -1$ the result easily follows from that for $z > 1$. So, let $z \in \mathbf{N}$. By Example 1.5, the sequence (z^n) is exactly realizable. By (2.5), the p^r-th term of $\widehat{(z^n)}$ is $z^{p^r} - z^{p^{r-1}}$, which, by (2.10), is divisible by p^r. □

2.4 Positivity and divisibility

Notation 2.2 A sequence ϕ has *positivity* if $\hat{\phi} \geq 0$. A sequence ϕ of integers has *divisibility* if $n|\hat{\phi}_n$ for each $n \geq 1$.

In this section we discuss the conditions under which sequences have positivity or divisibility, so that we can make better use of the Basic Lemma. By that lemma, a sequence of integers is exactly realizable if and only if it has positivity and divisibility.

Two elementary facts are:

$$\text{if two sequences have positivity, then so does their sum;} \tag{2.20}$$

$$\text{if two sequences have divisibility, then so do their sum and difference.} \tag{2.21}$$

These are clear on noting that, for arbitrary sequences f and g, we have the equality

$$\widehat{f \pm g} = \hat{f} \pm \hat{g}, \tag{2.22}$$

which is easily explained: for each $n \geq 1$, writing $(\widehat{f \pm g})_n$ for the n-th term of $\widehat{f \pm g}$, we have

$$\begin{aligned} (\widehat{f \pm g})_n &= \sum_{d|n} \mu(n/d)(f \pm g)_d \quad \text{(by (2.5))} \\ &= \sum_{d|n} \mu(n/d) f_d \pm \sum_{d|n} \mu(n/d) g_d = \hat{f}_n \pm \hat{g}_n \quad \text{(by (2.5))}, \end{aligned}$$

which verifies (2.22). For products of sequences, there are statements similar to (2.20) and (2.21) as will be seen in Corollary 2.7. However, for products, there is no equality similar to (2.22). To illustrate this, here is an example using sequences in $\mathcal{ER}$: let $\hat{f} = (1, 0, 0, 0, \ldots)$ and $\hat{g} = (1, 2, 3, 4, \ldots)$; so $f, g \in \mathcal{ER}$ by the Basic Lemma; also, $f = (1, 1, 1, 1, \ldots)$ by (2.6); since $fg = g$ we have $\widehat{fg} = \hat{g}$; but $\hat{f}\hat{g} = \hat{f}$; thus, $\widehat{fg} \neq \hat{f}\hat{g}$.

Lemma 2.4 *Let f and g be sequences. For natural numbers i and j write $[i,j]$ for their least common multiple. Then*

$$\left(\widehat{fg}\right)_n = \sum_{[i,j]=n} \hat{f}_i \hat{g}_j \quad \textit{for each } n \geq 1. \tag{2.23}$$

Here, $\left(\widehat{fg}\right)_n$ is the n-th term of the sequence $\widehat{fg}$.

Proof. For each $n \geq 1$,

$$\begin{aligned}
\left(\widehat{fg}\right)_n &= \sum_{d|n} \mu(n/d) f_d g_d \quad \text{(by (2.5))} \\
&= \sum_{d|n} \mu(n/d) \sum_{i|d} \hat{f}_i \sum_{j|d} \hat{g}_j \quad \text{(by (2.6))} \\
&= \sum_{d|n} \mu(n/d) \sum_{i,j|d} \hat{f}_i \hat{g}_j \\
&= \sum_{i,j|n} \hat{f}_i \hat{g}_j \sum_{d|n; i,j|d} \mu(n/d) \\
&= \sum_{i,j|n} \hat{f}_i \hat{g}_j \sum_{d|n; i,j|\frac{n}{d}} \mu(d) \\
&= \sum_{i,j|n} \hat{f}_i \hat{g}_j \sum_{d|\frac{n}{[i,j]}} \mu(d),
\end{aligned} \tag{2.24}$$

where the last equality is justified by the following:

$$\begin{aligned}
d|n \text{ and } \tfrac{n}{d} \text{ is a multiple of } i,j \quad &\Leftrightarrow \quad d|n \text{ and } \tfrac{n}{d} \text{ is a multiple of } [i,j] \\
&\Leftrightarrow \quad \tfrac{n}{[i,j]} \text{ is a multiple of } d.
\end{aligned}$$

By (2.2), $\sum_{d|\frac{n}{[i,j]}} \mu(d)$ is 0 when $[i,j]$ is a proper divisor of n, and is 1 when $[i,j]=n$. Whence, the lemma follows by (2.24). □

Corollary 2.7 (i) *If two sequences have positivity, then so does their product.*

(ii) *If two sequences have divisibility, then so does their product.*

Proof. Let f and g be sequences.

(i) Suppose f and g have positivity. By Notation 2.2, $\hat{f}_n, \hat{g}_n \geq 0$ for each $n \geq 1$. After a glance at (2.23), the result is clear.

(ii) Let f and g have divisibility. Look at (2.23) and fix n, i and j with $[i,j]=n$. By Notation 2.2, $i|\hat{f}_i$ and $j|\hat{g}_j$. Whence, $\hat{f}_i\hat{g}_j$ is a multiple of ij and, thus, a multiple of $[i,j]=n$. Hence, each term under the $\sum$ is divisible by n. So, $n|\left(\widehat{fg}\right)_n$, showing that fg has divisibility. (There is a different proof of this in Corollary 2.11.) □

Later, two proofs will be given showing that $\mathcal{ER}$ is closed under multiplication. One of these proofs follows very simply from the above corollary.

2.4.1 Positivity

We give simple sufficient conditions for a sequence to have positivity. For each non-negative integer r it is shown that the sequence $(n!/r!(n-r)!)$ has this property, from which, the same is deduced of the sequence (x^n) for each $x \geq 1$.

Lemma 2.5 *Let ϕ be an increasing sequence with $\phi \geq 0$. If n is a natural number with $\phi_{2n} \geq n\phi_n$, then $\hat{\phi}_{2n}, \hat{\phi}_{2n+1} \geq 0$.*

Proof. Let ϕ be an increasing sequence with $\phi \geq 0$. Suppose $\phi_{2n} \geq n\phi_n$ for some $n \in \mathbf{N}$. Then

$$\begin{aligned}
\hat{\phi}_{2n} &= \sum_{d|2n} \mu(2n/d)\phi_d \quad \text{(by (2.5))} \\
&= \phi_{2n} + \sum_{d|2n;d\neq 2n} \mu(2n/d)\phi_d \\
&\geq \phi_{2n} - \sum_{d|2n;d\neq 2n} \phi_d \quad \text{(since } \mu \geq -1 \text{ and } \phi \geq 0) \\
&\geq \phi_{2n} - \sum_{k=1}^{n} \phi_k \quad \text{(since no proper divisor of } 2n \text{ exceeds } n) \\
&\geq \phi_{2n} - n\phi_n \quad \text{(since } \phi \text{ is increasing)} \\
&\geq 0 \quad \text{(since } \phi_{2n} \geq n\phi_n).
\end{aligned}$$

Similarly, reasoning much as above,

$$\begin{aligned}
\hat{\phi}_{2n+1} &= \phi_{2n+1} + \sum_{d|2n+1;d\neq 2n+1} \mu([2n+1]/d)\phi_d \quad \geq \quad \phi_{2n+1} - \sum_{k=1}^{n} \phi_k \\
&\geq \phi_{2n} - n\phi_n \quad \geq \quad 0,
\end{aligned}$$

which proves the lemma. □

Lemma 2.6 *Let ϕ be a sequence with $\phi \geq 0$. Suppose $n > 1$ is a natural number and r is the number of distinct primes dividing n. If*

$$\phi_n \geq (2^r - 1)\max\{\phi_d : d|n, d \neq n\}, \tag{2.25}$$

then $\hat{\phi}_n \geq 0$.

Proof. Let ϕ, n and r be as given and suppose that (2.25) holds. Then

$$\begin{aligned}
\hat{\phi}_n &= \phi_n + \sum_{d|n; d\neq n} \mu(n/d)\phi_d \quad \text{(by (2.5))} \\
&\geq \phi_n - \sum_{d|n; d\neq n} |\mu(n/d)|\phi_d \quad (\text{since } \phi \geq 0) \\
&\geq \phi_n - \max\{\phi_d : d|n, d\neq n\} \sum_{d|n; d\neq 1} |\mu(d)|.
\end{aligned}$$

Now, $\sum_{d|n;d\neq 1} |\mu(d)| = 2^r - 1$ by (2.4). Whence, the lemma follows by (2.25). □

No use is made of the above lemma in this work. One can use it to show that if $x \geq 15^{1/105}$, then $\sum_{d|n} \mu(n/d)x^d \geq 0$ for each $n \geq 1$. (The details seem immaterial and are omitted.) This suggests Corollary 2.8, which we will deduce from the next lemma.

Lemma 2.7 *Let $d \in \mathbf{N}$ and $r \in \mathbf{Z}^+$. Define $\binom{d}{r}$ by*

$$\binom{d}{r} = \begin{cases} d!/r!(d-r)! & \textit{if } r \leq d, \\ 0 & \textit{otherwise.} \end{cases}$$

Then $\sum_{d|n} \binom{d}{r}\mu(n/d) \geq 0$, for all $r \geq 0$ and $n \geq 1$.

Proof. For each given $r \in \mathbf{Z}^+$, define sequences $f^{(r)}, g^{(r)}$ as follows:

$$f_n^{(r)} = \binom{n}{r} \quad \text{and} \quad g_n^{(r)} = n - r \quad \text{for each } n \geq 1.$$

Then, for all n and r, we see from (2.5) that the n-th term of $\widehat{f^{(r)}}$ is given by

$$\widehat{f_n^{(r)}} = \sum_{d|n} f_d^{(r)}\mu(n/d) = \sum_{d|n} \binom{d}{r}\mu(n/d). \tag{2.26}$$

So, we need show that $\widehat{f^{(r)}} \geq 0$ for each $r \in \mathbf{Z}^+$. Let us proceed by induction on r. Consider $\widehat{f^{(0)}}$ first. For each $n \geq 1$,

$$\begin{aligned}
\widehat{f_n^{(0)}} &= \sum_{d|n} \binom{d}{0} \mu(n/d) \quad \text{(by (2.26))} \\
&= \sum_{d|n} \mu(n/d) \quad \geq \quad 0 \quad \text{(by (2.2))},
\end{aligned}$$

showing that $\widehat{f^{(0)}} \geq 0$. As hypothesis of the induction assume that $\widehat{f^{(r)}} \geq 0$ for a fixed $r \in \mathbf{Z}^+$. Then, for each $n \geq 1$,

$$\begin{aligned}
(r+1)\widehat{f_n^{(r+1)}} &= (r+1) \sum_{d|n} \binom{d}{r+1} \mu(n/d) \quad \text{(by (2.26))} \\
&= \sum_{d|n} \binom{d}{r} (d-r)\mu(n/d) \quad \left(\text{since } (r+1)\tbinom{d}{r+1} = \tbinom{d}{r}(d-r)\right) \\
&= \text{the } n\text{-th term of } \widehat{f^{(r)} g^{(r)}} \quad \text{(by (2.5))} \\
&= \sum_{[i,j]=n} \widehat{f_i^{(r)}} \widehat{g_j^{(r)}} \quad \text{(by (2.23))} \\
&= \widehat{f_n^{(r)}} \sum_{d|n} \widehat{g_d^{(r)}} + \sum_{[i,j]=n; i \neq n} \widehat{f_i^{(r)}} \widehat{g_j^{(r)}}, \qquad (2.27)
\end{aligned}$$

where the second summand is read as 0 when $n = 1$. It is easily seen that this summand is non-negative: by the induction hypothesis $\widehat{f_i^{(r)}} \geq 0$ for each $i \geq 1$; $\widehat{g_1^{(r)}}$ does not appear in the summand; and, for each $j \geq 2$,

$$\begin{aligned}
\widehat{g_j^{(r)}} &= \sum_{d|j} (d-r)\mu(j/d) \quad \text{(by (2.5))} \\
&= \sum_{d|j} d\mu(j/d) - r \sum_{d|j} \mu(j/d) \\
&= e(j) - r.0 \quad \text{(by (2.3) and (2.2))} \\
&\geq 1.
\end{aligned}$$

Hence, by (2.27),

$$\begin{aligned}
(r+1)\widehat{f_n^{(r+1)}} &\geq \widehat{f_n^{(r)}} \sum_{d|n} \widehat{g_d^{(r)}} \quad = \quad \widehat{f_n^{(r)}} g_n^{(r)} \quad \text{(by (2.6))} \\
&= \widehat{f_n^{(r)}} (n-r),
\end{aligned}$$

which is also easily seen to be non-negative: for $n \geq r$ this is clear by the induction hypothesis; for $n < r$ we have $\widehat{f_n^{(r)}} = 0$ by (2.26). Thus, $\widehat{f_n^{(r+1)}} \geq 0$ for each $n \geq 1$. In other words, $\widehat{f^{(r+1)}} \geq 0$. This completes the induction step and proves the lemma. □

Corollary 2.8 $\sum_{d|n} x^d \mu(n/d) \geq 0$ *for all* $x \geq 1$ *and* $n \in \mathbf{N}$.

Proof. For $x = 1$ this is immediate by (2.2). Fix $x > 1$ and $n \in \mathbf{N}$. Write $x = 1 + c$ where $c > 0$. Then, for each r with $0 \leq r \leq n$, the coefficient of c^r in $\sum_{d|n} x^d \mu(n/d)$ is $\sum_{d|n} \binom{d}{r} \mu(n/d)$. Since, for each r, the latter sum is non-negative by Lemma (2.7), we are done. □

Remark 2.3 Lemma 2.7 probably has a simple combinatorial proof, in which the sum counts something and is therefore non-negative.

2.4.2 Divisibility

Necessary and sufficient conditions are given for a sequence to have divisibility. Some simple consequences of these conditions are: only the zero sequence is common $\mathcal{ER}$ and $\widehat{\mathcal{ER}}$; two different elements of $\mathcal{ER}$ cannot be eventually equal; Corollary 2.7(ii) has another proof; with the help of Corollary 2.8, geometric progressions in $\mathcal{ER}$ are completely described.

Lemma 2.8 *Let* f *be a sequence of integers. Then the next two statements are equivalent.*

(i) $n | \hat{f}_n$ *for each* $n \geq 1$.

(ii) *For all natural numbers* r, K *and primes* p *with* $p \nmid K$

$$p^r | f_{p^r K} - f_{p^{r-1} K}.$$

In (ii) *the phrase 'with* $p \nmid K$*' can be dropped.*

Proof. A proof will be given which hinges on the following:

$$f_{p^r K} - f_{p^{r-1} K} = \sum_{d|K} \hat{f}_{p^r d} \quad \text{for all } r, K \in \mathbf{N} \text{ and primes } p \text{ with } p \nmid K. \tag{2.28}$$

(We will also give a second proof that (ii) implies (i), but without using (2.28).) To see (2.28), let r, K and p be as given. By (2.6),

$$f_{p^r K} - f_{p^{r-1} K} = \sum_{d|p^r K} \hat{f}_d - \sum_{d|p^{r-1} K} \hat{f}_d,$$

which equals the right hand side of (2.28) for the following reason: p and K are coprime; hence, the set of divisors of $p^r K$ is the disjoint union of the sets

$$\{d\colon d|p^{r-1}K\} \quad \text{and} \quad \{p^r d\colon d|K\}.$$

This explains (2.28). To see that (i) implies (ii), suppose $n|\hat{f}_n$ for each $n \geq 1$. Let r, K and p be given as in (ii). Thus, for each divisor d of K we have $\hat{f}_{p^r d}$ divisible by $p^r d$ and, therefore, by p^r. Hence, p^r divides $\sum_{d|K} \hat{f}_{p^r d}$. A glance at (2.28) shows that (ii) follows.

For the converse let (ii) hold. Two arguments will be given for (i): (a) one by induction on n and using (2.28); (b) one assuming a few basic facts about the function μ.

(a) As basis of the induction note that $1|\hat{f}_1$. Suppose, as the induction hypothesis, that $n \geq 2$ and that $m|\hat{f}_m$ for each m with $n-1 \geq m \geq 1$. Fix a prime p that divides n. Write $n = p^r K$ where r, K are natural numbers and $p \nmid K$. Now, either $K = 1$ or $K \geq 2$.

Suppose $K = 1$. By (ii), p^r divides $f_{p^r} - f_{p^{r-1}}$. By (2.28), $f_{p^r} - f_{p^{r-1}} = \hat{f}_{p^r}$. Therefore, p^r divides $\hat{f}_{p^r}$. Since $n = p^r$, we have proved (i) when $K = 1$.

Now let $K \geq 2$. Write (2.28) as

$$f_{p^r K} - f_{p^{r-1} K} = \hat{f}_{p^r K} + \sum_{d<K; d|K} \hat{f}_{p^r d},$$

from which we easily deduce that $p^r|\hat{f}_{p^r K}$: the left hand side is divisible by p^r because of (ii); for each proper divisor d of K we have $n = p^r K > p^r d \geq 1$; for such d we know that $p^r d$ divides $\hat{f}_{p^r d}$ by the induction hypothesis; so, the sigma sum is divisible by p^r; it follows that $p^r|\hat{f}_{p^r K}$.

For an arbitrary prime p with $\mathrm{ord}_p(n) = r$, we have shown that $p^r|\hat{f}_{p^r K} = \hat{f}_n$. Whence, $n|\hat{f}_n$, proving that (ii) implies (i).

(b) The case $n = 1$ being trivial, fix an $n \geq 2$. Let n have canonical form $p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$, where for each $i = 1, 2, \dots, m$, each r_i is a natural number and each p_i is a prime, the primes being distinct. Write D for the set

$$\{p_1^{l_1} p_2^{l_2} \dots p_m^{l_m} \colon\ l_i = r_i \text{ or } r_i - 1 \text{ for each } i\},$$

which is a subset of the divisors of n. By (2.5),

$$\hat{f}_n := \sum_{d|n} \mu(n/d) f_d = \sum_{d \in D} \mu(n/d) f_d, \tag{2.29}$$

because if δ is a divisor of n and δ is not in D, then n/δ has a squared factor, in which case $\mu(n/\delta) = 0$ by the definition of μ.

Since m distinct primes divide n, the set D contains 2^m elements. Half of these are of the form $p_1^{r_1} K$ where K is a natural number coprime to p_1. For each K, each element of this form can be paired off with $p_1^{r_1 - 1} K$ which is also in D. Hence, by (2.29), $\hat{f}_n$ can be written as the sum of 2^{m-1} terms of the form

$$\mu\left(n/p_1^{r_1} K\right) f_{p_1^{r_1} K} - \mu\left(n/p_1^{r_1 - 1} K\right) f_{p_1^{r_1 - 1} K}. \tag{2.30}$$

Here,

$$\begin{aligned} \mu\left(n/p_1^{r_1-1} K\right) &= \mu\left(p_1 n/p_1^{r_1} K\right) \\ &= \mu(p_1)\mu\left(n/p_1^{r_1} K\right) \quad \text{(since } \mu \text{ is multiplicative by (2.1))} \\ &= (-1)\mu\left(n/p_1^{r_1} K\right) \quad \text{(by the definition of } \mu\text{)}, \end{aligned}$$

which, with (2.30), shows that $\hat{f}_n$ is the sum of terms of the form

$$\pm(f_{p_1^{r_1} K} - f_{p_1^{r_1 - 1} K}).$$

By (ii), each of these terms is divisible by $p_1^{r_1}$. So, $p_1^{r_1}$ divides $\hat{f}_n$. This argument can be repeated for each p_i with $i \geq 2$. Therefore, $n | \hat{f}_n$. This completes the second proof that (ii) implies (i).

To justify the lemma's last statement, let r, K be natural numbers and p be a prime which *may* divide K. We show that (ii) implies the divisibility of $f_{p^r K} - f_{p^{r-1} K}$ by p^r. Let (ii) hold. Write $K = p^s L$ where $s \in \mathbf{Z}^+, L \in \mathbf{N}$ and $p \nmid L$. So,

$$f_{p^r K} - f_{p^{r-1} K} = f_{p^{r+s} L} - f_{p^{r+s-1} L}.$$

By (ii), the right hand side is divisible by p^{r+s} and, hence, by p^r. Thus, p^r divides $f_{p^r K} - f_{p^{r-1}K}$. This establishes the lemma. □

Remark 2.4 In Lemma 2.8 let us restrict f so that $\hat{f} \geq 0$. Then, simpler and prettier reasoning shows that (i) implies (ii): let (i) hold with this restriction, so that f is exactly realizable by the Basic Lemma; suppose r, K and p are given as in (ii); define a sequence k by $k_n = f_{nK}$ for each $n \geq 1$; by (2.16), k is exactly realizable; by (2.10), $p^r | \hat{k}_{p^r}$; but

$$\begin{aligned} \hat{k}_{p^r} &= k_{p^r} - k_{p^{r-1}} \quad \text{(by (2.5))} \\ &= f_{p^r K} - f_{p^{r-1}K} \quad \text{(by the definition of } k\text{)}, \end{aligned}$$

showing that (ii) is necessary. It was after this easy argument was noticed that Lemma 2.8 was suggested. This lemma will often help us, as illustrated by the next four corollaries.

Corollary 2.9 *Only the zero sequence is common to $\mathcal{ER}$ and $\widehat{\mathcal{ER}}$.*

Proof. The zero sequence is in $\mathcal{ER}$ by Corollary 2.2, and in $\widehat{\mathcal{ER}}$ by (2.11). Suppose f is in each of $\mathcal{ER}$ and $\widehat{\mathcal{ER}}$. Let $K \in \mathbf{N}$ and p be a prime. Since $f \in \mathcal{ER}$ we know from (2.10) and Lemma 2.8 that $p | f_{pK} - f_K$. But $p | f_{pK}$ by (2.11). So, $p | f_K$. Fixing K and letting $p \to \infty$ it follows that that $f_K = 0$. This holds for each K. Whence, f is the zero sequence. □

The next result shows that a new exactly realizable sequence cannot be obtained from an old one by altering only finitely many terms.

Corollary 2.10 (i) *An eventually constant sequence with divisibility is constant.*

(ii) *Two eventually equal sequences with divisibility are equal.*

Proof. (i) Suppose that the sequence f has divisibility and that $f = (z)$ eventually for some integer z. Let K be a natural number and p be a prime. By the divisibility of f and Lemma 2.8, $p | f_{pK} - f_K$. Since $f_{pK} = z$ for all large p, we see that $p | z - f_K$ for all large p. Hence, $f_K = z$. This holds for each K. So, f is constant.

(ii) Suppose g and h are eventually equal sequences with divisibility. Thus, $g-h$ equals the zero sequence eventually and, by (2.21), $g-h$ has divisibility. Hence, $g-h$ is the zero sequence by (i). So, $g=h$. □

Notation 2.3 For each prime p and natural numbers r, K let

$$f_{[p,r,K]} := f_{p^r K} - f_{p^{r-1}K}.$$

Corollary 2.11 *Corollary 2.7(ii) has another proof.*

Proof. Suppose f, g are sequences having divisibility, so that $n|\hat{f}_n, \hat{g}_n$ for each $n \geq 1$. Let p be a prime and r, K be natural numbers. Then,

$$\begin{aligned}
(fg)_{[p,r,K]} &:= (fg)_{p^r K} - (fg)_{p^{r-1}K} \quad \text{(by notation 2.3)} \\
&= f_{p^r K} g_{p^r K} - f_{p^{r-1}K} g_{p^{r-1}K} \quad \text{(by definition of } fg) \\
&= (f_{p^r K} - f_{p^{r-1}K}) g_{p^r K} + (g_{p^r K} - g_{p^{r-1}K}) f_{p^{r-1}K} \\
&= f_{[p,r,K]} g_{p^r K} + g_{[p,r,K]} f_{p^{r-1}K} \quad \text{(by notation 2.3).}
\end{aligned}$$

Since we are given that $n|\hat{f}_n, \hat{g}_n$ for each $n \geq 1$, it follows from Lemma 2.8 that p^r divides both $f_{[p,r,K]}$ and $g_{[p,r,K]}$. Hence, p^r divides $(fg)_{[p,r,K]}$ by the last equality above. So, by the same lemma, $n|\left(\widehat{fg}\right)_n$ for each $n \geq 1$. Hence, fg has divisibility, giving a second proof of Corollary 2.7(ii). □

Corollary 2.12 *Let f_1 and z be integers and define the sequence f by*

$$f_n = z^{n-1} f_1 \quad \textit{for each } n \geq 1. \tag{2.31}$$

Then f has divisibility if and only if f_1 is divisible by each prime dividing z.

Proof. For the 'only if' part, let f have divisibility. So, by Notation 2.2, $n|\hat{f}_n$ for each $n \geq 1$. Suppose p is a prime dividing z. Thus, $p|\hat{f}_p$. Now, by (2.5) and (2.31),

$$\hat{f}_p = f_p - f_1 = (z^{p-1} - 1) f_1.$$

Hence, $p|(z^{p-1}-1)f_1$. But $p|z$. Whence, $p|f_1$, which proves the 'only if' part.

For the 'if' part, let f_1 be divisible by each prime dividing z. Lemma 2.8 will be used. Let p be a prime and r, K be natural numbers. Then, recalling Notation 2.3 and using (2.31),

$$\begin{aligned} f_{[p,r,K]} &= f_1\left[z^{p^r K-1} - z^{p^{r-1}K-1}\right] &\quad (2.32)\\ &= \frac{f_1}{z}\left[(z^K)^{p^r} - (z^K)^{p^{r-1}}\right]. &\quad (2.33)\end{aligned}$$

Now, either $p \not| z$ or $p|z$. If $p \not| z$, then we see from (2.19) and (2.33) that $p^r | f_{[p,r,K]}$. If $p|z$, then $p|f_1$ by our assumption. Therefore, by (2.32),

$$\operatorname{ord}_p(f_{[p,r,K]}) = \operatorname{ord}_p(z^{p^{r-1}K-1}f_1) \geq p^{r-1}K - 1 + 1 = p^{r-1}K \geq r.$$

So, again, $p^r | f_{[p,r,K]}$. Thus, by Lemma 2.8, $n|\hat{f}_n$ for each $n \geq 1$. In other words, f has divisibility, as required.

□

Second order recurrences in $\mathcal{ER}$ are the concern of Chapter 3. In some cases these will reduce to the first order. Using Corollaries 2.12 and 2.8, first order recurrences in $\mathcal{ER}$ can now be precisely and swiftly described.

Lemma 2.9 *Let c be a positive rational and $f_1 \in \mathbf{N}$. Define f by $f_n = cf_{n-1}$ for each $n \geq 2$. Then f is exactly realizable if and only if* (i) *$c \in \mathbf{N}$ and* (ii) *f_1 is divisible by each prime dividing c.*

Proof. For the 'only if' part, let f be exactly realizable. Suppose $c = c_1/c_2$ where c_1 and c_2 are coprime natural numbers. By the recurrence defining f, we have $f_n = c^{n-1}f_1$ for each $n \geq 1$. Also, by Definition 2.4, f is a sequence in $\mathbf{Z}^+$. Hence, $c_2^{n-1}|f_1$ for each $n \geq 1$. Since $f_1 \neq 0$, we have $c_2 = 1$ and so (i) holds.

Since f is exactly realizable, f has divisibility. On writing c for z in Corollary 2.12, we have (ii).

For the 'if' part let (i) and (ii) hold. By Corollary 2.12, f has divisibility. Thus, by the Basic Lemma, we need just show that f has positivity. For each $n \geq 1$, using (2.5) and $f_n = c^{n-1}f_1$,

$$\hat{f}_n = \sum_{d|n} \mu(n/d) f_d = \sum_{d|n} \mu(n/d) c^{d-1} f_1 = (f_1/c) \sum_{d|n} \mu(n/d) c^d,$$

which is non-negative by Corollary 2.8. □

2.5 Algebra in $\mathcal{ER}$

We now consider whether $\widehat{\mathcal{ER}}$ and $\mathcal{ER}$ are closed under the usual operations on sequences. For $\widehat{\mathcal{ER}}$, the following facts are easily deduced from (2.11) and are merely stated:

$$\text{if } \hat{f}, \hat{g} \in \widehat{\mathcal{ER}} \text{ with } \hat{g} > 0, \text{ then } \frac{\hat{f}}{\hat{g}} \text{ is not in general in } \widehat{\mathcal{ER}}; \tag{2.34}$$

$$\text{if } \hat{f}, \hat{g} \in \widehat{\mathcal{ER}}, \text{ then } \hat{f} - \hat{g} \in \widehat{\mathcal{ER}} \text{ if and only if } \hat{f} \geq \hat{g}; \tag{2.35}$$

$$\text{if } \hat{f}, \hat{g} \in \widehat{\mathcal{ER}}, \text{ then } \hat{f} + \hat{g} \in \widehat{\mathcal{ER}}; \tag{2.36}$$

$$\text{if } \psi \text{ is a sequence in } \mathbf{Z}^+ \text{ and } \hat{g} \in \widehat{\mathcal{ER}}, \text{ then } \psi\hat{g} \in \widehat{\mathcal{ER}}.$$

For $\mathcal{ER}$, here is the fact corresponding to (2.34): if $f, g \in \mathcal{ER}$ with $g > 0$, then $\frac{f}{g}$ is not in general in $\mathcal{ER}$. Let us give examples of $f, g \in \mathcal{ER}$ showing the different ways $\frac{f}{g}$ can fail to be in $\mathcal{ER}$, even though $\frac{f}{g}$ is a sequence in $\mathbf{Z}^+$. Let $\hat{g}$ be the sequence $(2, 6, 0, 0, 0, 0, \ldots)$, so that $g \in \mathcal{ER}$ by the Basic Lemma. By (2.6), $g = (2, 8, 2, 8, 2, 8, \ldots)$. In turn let $\hat{f}$ equal each of the following sequences:

(i) $(2, 14, 0, 0, 0, 0, \ldots)$; (ii) $(20, 4, 0, 0, 0, 0, \ldots)$; (iii) $(12, 4, 0, 0, 0, 0, \ldots)$.

Arguing as for g we see that $f \in \mathcal{ER}$. Write h for $\frac{f}{g}$.

For (i), $f = (2, 16, 2, 16, 2, 16, \ldots)$ by (2.6). Hence, $h = (1, 2, 1, 2, 1, 2, \ldots)$. By (2.5), $\hat{h} = (1, 1, 0, 0, 0, 0, \ldots)$. So, (2.9) holds for $\hat{h}$, but not (2.10) because $2 \nmid \hat{h}_2$.

For (ii), $f = (20, 24, 20, 24, 20, 24, \ldots)$, so that $h = (10, 3, 10, 3, 10, 3, \ldots)$ and $\hat{h} = (10, -7, 0, 0, 0, 0, \ldots)$. Hence, $\hat{h}$ fails both (2.9) and (2.10).

Finally for (iii), $f = (12, 16, 12, 16, 12, 16, \ldots), h = (6, 2, 6, 2, 6, 2, \ldots)$ and $\hat{h} = (6, -4, 0, 0, 0, 0, \ldots)$. Here, $\hat{h}$ fails (2.9) but satisfies (2.10).

Lemma 2.10 (i) *Let $f, g \in \mathcal{ER}$. Then $f - g \in \mathcal{ER}$ if and only if $\hat{f} \geq \hat{g}$.*

(ii) *$\mathcal{ER}$ is closed under addition.*

(iii) *$\mathcal{ER}$ is closed under multiplication.*

Each of these will be quickly proved using the work in Section 2.4. Then, (ii) and (iii) are given second proofs which are better because they argue in a simple way from the core ideas in Definition 2.4.

Proof. (i) Let $f, g \in \mathcal{ER}$. Then,

$$\begin{aligned} f - g \in \mathcal{ER} &\Leftrightarrow \widehat{f-g} \in \widehat{\mathcal{ER}} \quad \text{(by (2.12))} \\ &\Leftrightarrow \hat{f} - \hat{g} \in \widehat{\mathcal{ER}} \quad \text{(by (2.22))} \\ &\Leftrightarrow \hat{f} \geq \hat{g} \quad \text{(by (2.35))}, \end{aligned}$$

which proves (i).

For (ii) and (iii), let f and g be exactly realizable. So, by the Basic Lemma, each of f and g has positivity and divisibility. By (2.20) and (2.21), $f+g$ also has these properties. The same goes for fg, by Corollary 2.7. Thus, by the Basic Lemma, $f+g$ and fg are exactly realizable.

Second proofs of (ii) and (iii). Let f and g be exactly realizable. By Definition 2.4, choose systems (X_1, T_1) and (X_2, T_2) such that, for each $n \geq 1$,

$$f_n = \#\{x \in X_1 \colon T_1^n(x) = x\} \qquad \text{and} \qquad g_n = \#\{x \in X_2 \colon T_2^n(x) = x\}. \tag{2.37}$$

For (ii), let $X := X_1 \cup X_2$. Since the elements of X_1 or X_2 can be relabelled, assume that X_1 and X_2 are disjoint. Define $T \colon X \to X$ by

$$T(x) = \begin{cases} T_1(x) & \text{if } x \in X_1, \\ T_2(x) & \text{if } x \in X_2. \end{cases}$$

So, for each $n \geq 1$,

$$\{x \in X \colon T^n(x) = x\} = \{x \in X_1 \colon T_1^n(x) = x\} \cup \{x \in X_2 \colon T_2^n(x) = x\}.$$

The union here is disjoint since X_1 and X_2 are disjoint. Hence, by (2.37),

$$\#\{x \in X \colon T^n(x) = x\} = f_n + g_n = (f+g)_n \quad \text{for each } n \geq 1.$$

Therefore, by Definition 2.4, the system (X, T) exactly realizes $f+g$. Whence, $f + g \in \mathcal{ER}$.

For (iii), let $X := X_1 \times X_2$ and define a map $T \colon X \to X$ by

$$T(x_1, x_2) = (T_1(x_1), T_2(x_2)) \quad \text{for each } (x_1, x_2) \in X.$$

So, for each $n \geq 1$,

$$\begin{aligned} \{x \in X : T^n(x) = x\} &= \{(x_1, x_2) \in X : (T_1^n(x_1), T_2^n(x_2)) = (x_1, x_2)\} \\ &= \{(x_1, x_2) \in X : T_1^n(x_1) = x_1, T_2^n(x_2) = (x_2)\} \\ &= \{x \in X_1 : T_1^n(x) = x\} \times \{x \in X_2 : T_2^n(x) = x\}. \end{aligned}$$

Hence, by (2.37),

$$\#\{x \in X : T^n(x) = x\} = f_n g_n = (fg)_n \quad \text{for each } n \geq 1.$$

So, (X, T) exactly realizes fg by Definition 2.4. Thus, $fg \in \mathcal{ER}$. □

2.6 Fibonacci Sequences

Definition 2.7 A sequence f is *Fibonacci* if

$$f_{n+2} = f_{n+1} + f_n \quad \text{for each } n \geq 1. \tag{2.38}$$

The Fibonacci sequence F satisfies (2.38) with $F_1 = 0$ and $F_2 = 1$. *The Lucas sequence* L satisfies (2.38) with $L_1 = 1$ and $L_2 = 3$. Thus,

$$F = (0, 1, 1, 2, 3, 5, \ldots) \quad \text{and} \quad L = (1, 3, 4, 7, 11, 18, \ldots).$$

A basic induction shows the following:

$$\text{if } f \text{ is Fibonacci, then } f_n = f_1 F_{n-1} + f_2 F_n \text{ for each } n \geq 2. \tag{2.39}$$

The next theorem shows that, up to scalar multiples, the Lucas sequence L is unique amidst Fibonacci sequences: it is the only one in $\mathcal{ER}$.

Theorem 2.2 *Let f be Fibonacci with $f_1 \in \mathbf{Z}^+$. Then $f \in \mathcal{ER}$ if and only if $f_2 = 3f_1$.*

Proof. For the 'if' part let $f_2 = 3f_1$. By (2.38),

$$f = f_1(1, 3, 4, 7, \ldots) = f_1 L.$$

By Corollary 2.3, it is enough to show that $L \in \mathcal{ER}$. Example 1.5 will be used. Let

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and } t_n = \text{ trace}(A^n) \text{ for each } n \geq 1.$$

The characteristic equation of A is $x^2 = x+1$. So, $A^2 = A+I$. Thus, $A^{n+2} = A^{n+1}+A^n$ and, hence, $t_{n+2} = t_{n+1} + t_n$ for each $n \geq 1$. So, t and L both satisfy the recurrence in (2.38). Also, $t_1 = 1 + 0 = 1 = L_1$ and

$$t_2 = \text{ trace}(A^2) = \text{ trace}(A+I) = \text{ trace}(A) + \text{ trace}(I) = 1 + 2 = 3 = L_2.$$

Thus, $t = L$. Therefore, by Example 1.5, $L \in \mathcal{ER}$, proving the 'if' part.

Conversely, suppose f is in $\mathcal{ER}$. Let p be a prime. By (2.10), $p|\hat{f}_p = f_p - f_1$. Whence, by (2.39),

$$f_1(F_{p-1} - 1) + f_2 F_p \equiv 0 \bmod p. \tag{2.40}$$

This congruence holds with $f_1 = 1$ and $f_2 = 3$ because, in the 'if' part, the Lucas sequence has been shown to be in $\mathcal{ER}$. So,

$$F_{p-1} - 1 + 3F_p \equiv 0 \bmod p. \tag{2.41}$$

Now, if we can show that

$$F_p \equiv 1 \bmod p \quad \text{ for each } p \equiv 2 \bmod 5, \tag{2.42}$$

then we will be done: for $p \equiv 2 \bmod 5$, we will have $F_{p-1} \equiv -2 \bmod p$ by (2.41); which with (2.42) and (2.40) will lead to $f_2 \equiv 3f_1 \bmod p$; the result will then follow because 2 and 5 are coprime, so that, by Dirichlet's Theorem there are infinitely many p with $p \equiv 2 \bmod 5$.

To see (2.42), let $p \equiv 2 \bmod 5$. By Hardy and Wright [6, Theorem 180], $F_{p+2} \equiv 0 \bmod p$. By (2.38), $F_{p+2} = 2F_p + F_{p-1}$. So, $2F_p + F_{p-1} \equiv 0 \bmod p$, which we subtract from (2.41) to obtain (2.42). □

Remark 2.5 1. The congruence in (2.41) involving the Fibonacci sequence is just one of many that can be swiftly obtained. Since $L \in \mathcal{ER}$, condition (2.10) gives

$$\sum_{d|n} \mu(n/d) L_d \equiv 0 \bmod n \quad \text{ for each } n \geq 1.$$

Here, write $n = p^r$ where p is a prime and $r \geq 1$ to obtain

$$L_{p^r} \equiv L_{p^{r-1}} \bmod p^r,$$

or write $n = pq$ where p and q are distinct primes to obtain

$$L_{pq} + 1 \equiv L_p + L_q \bmod pq,$$

and so on. It is likely that such congruences are known. They are not commonplace, however.

2. It is fortunate that we have at hand a system which exactly realizes the Lucas sequence L. Otherwise, to show that $L \in \mathcal{ER}$, we would have to verify directly that $\hat{L} \geq 0$, that $n|\hat{L}_n$ for each $n \geq 1$, and then use the Basic Lemma. By Lemma 2.5, it is easy to show that $\hat{L} \geq 0$, as will be seen in the proof of the converse to Theorem 3.1. (That theorem deals with the exact realizability of quadratic recurrences which are more general than those in Theorem 2.2.) However, it is difficult to see how one can directly show that $n|\hat{L}_n$ for each $n \geq 1$. The Lucas sequence is one of a class of sequences giving such difficulty. For this reason, in the proof of the converse to Theorem 3.1, we will again be thankful that some systems are at hand.

3. The exact realization of second order linear recurrences with integer coefficients is fully discussed in Theorem 3.1. For third and higher order recurrences the matter is unclear, but a basic and natural query in the Fibonacci vein is as follows. Let $r \in \mathbf{N}$. Define a sequence f to be *r-Fibonacci* if

$$f_{n+r} = f_{n+r-1} + f_{n+r-2} + \cdots + f_n \quad \text{for each } n \geq 1. \tag{2.43}$$

Define *the r-Lucas sequence* $L^{(r)}$ to be the one satisfying this recurrence and $L_n^{(r)} = 2^n - 1$ for each $1 \leq n \leq r$. So, $L^{(1)}$ is the unit sequence (1) and $L^{(2)}$ is the Lucas sequence L. Write

$$A_r := \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ & & \ddots & & & \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{bmatrix},$$

which is an $r \times r$ matrix whose entries are 0 or 1. Arguing as in the proof of the 'if' part of Theorem 2.2, it can be shown that $\text{trace}((A_r)^n) = L_n^{(r)}$ for each $n \geq 1$. Thus, by Example 1.5, $L^{(r)} \in \mathcal{ER}$. Here is the basic query: Must each exactly realizable r-Fibonacci sequence be a multiple of $L^{(r)}$? This is trivial for $r = 1$, and for $r = 2$ we have Theorem 2.2. For $r \geq 3$ this question is of interest.

For each $r \in \mathbf{N}$, define *the r-Fibonacci sequence* $F^{(r)}$ to be the one for which (2.43) holds, with $F_r^{(r)} = 1$ and $F_n^{(r)} = 0$ for $1 \leq n \leq r-1$. So, $F^{(2)}$ is the Fibonacci sequence F of Definition 2.7. The divisibility properties of F have been extensively studied. This explains why, in (2.39), we chose to express each 2-Fibonacci sequence in terms of F. Similarly, for $r \geq 3$, one can express each r-Fibonacci sequence in terms of $F^{(r)}$. However, we are unaware of similar studies on $F^{(r)}$ for $r \geq 3$.

Chapter 3

When is a Quadratic Recurrence Exactly Realizable?

A complete description is given of those members of $\mathcal{ER}$ that satisfy second order linear recurrences with integer coefficients.

Theorem 3.1 *Let f_1, f_2, a and b be integers with $f_2 \geq f_1 \geq 0$ and $f_2 \geq 1$. Suppose f_1, f_2 are the first and second terms, respectively, of the sequence f for which*

$$f_{n+2} = af_{n+1} + bf_n \quad \textit{for each } n \geq 1. \tag{3.1}$$

Write

$$H := 2bf_1 - af_2 + a^2 f_1, \tag{3.2}$$

$$\Delta := a^2 + 4b, \tag{3.3}$$

$$\lambda := (a + \sqrt{\Delta})/2, \tag{3.4}$$

$$\mu := (a - \sqrt{\Delta})/2. \tag{3.5}$$

Then f is exactly realizable if and only if the following conditions hold:

$$\Delta \geq 0; \tag{3.6}$$

$$2 | f_2 - f_1; \tag{3.7}$$

$$\textit{if } 2|a, b, \textit{ then } 4|f_2; \tag{3.8}$$

$$\textit{if } \mathrm{ord}_2(a) = 1 \textit{ and } f_1 \textit{ is odd, then } 4|b+1; \tag{3.9}$$

$$\textit{for each odd prime } p, \textit{ if } p|a,b, \textit{ then } p|f_1; \tag{3.10}$$

$$\textit{if } a \leq 0, \textit{ then } b > 0; \tag{3.11}$$

$$\textit{if } a < 0, \textit{ then } f_2 = \lambda f_1; \tag{3.12}$$

$$\textit{for each odd prime } p, \textit{ if } p|b, \textit{ then } p|f_2 - af_1; \tag{3.13}$$

$$\textit{for each odd prime } p, \textit{ if } p|\Delta, \textit{ then } p|2f_2 - af_1; \tag{3.14}$$

$$f_2 \geq \mu f_1; \tag{3.15}$$

$$\Delta \textit{ is a square or } H = 0. \tag{3.16}$$

The proof of the 'only if' part of this theorem is in Section 3.1, and of the 'if' part is in Section 3.2.

Example 3.1 To get used to conditions (3.6) to (3.16), it will help a little if we deduce Theorem 2.2 from Theorem 3.1. Let f be a Fibonacci sequence with $f_1 \in \mathbf{Z}^+$. If $f_2 < f_1$ or $f_2 < 1$ or $f_2 \notin \mathbf{Z}$, then Theorem 2.2 follows trivially. So, let us suppose that $f_2 \in \mathbf{Z}$ with $f_2 \geq f_1 \geq 0$ and $f_2 \geq 1$. Thus, by Definition 2.7, the hypotheses of Theorem 3.1 hold with $a = b = 1, \Delta = 5$ and $\mu < 0$.

For the 'only if' part of Theorem 2.2, let $f \in \mathcal{ER}$. Since Δ is not a square, $2bf_1 - af_2 + a^2 f_1 = 0$ by (3.16). Therefore, $2 \cdot 1 \cdot f_1 - 1 \cdot f_2 + (1)^2 f_1 = 0$. Thus, $f_2 = 3f_1$.

For the converse of Theorem 2.2, let $f_2 = 3f_1$. Then (3.6) holds since $\Delta = 5$. Since $f_2 - f_1 = 2f_1$, the same goes for (3.7). For (3.8) to (3.13) the 'if' part fails. Condition (3.14) holds since $\Delta = 5$ and $2f_2 - af_1 = 5f_1$. The same goes for (3.15) since μ is negative. Finally, for (3.16), $H{:}= 2bf_1 - af_2 + a^2 f_1 = 2 \cdot 1 \cdot f_1 - 1 \cdot 3f_1 + (1)^2 f_1 = 0$. So, $f \in \mathcal{ER}$ by Theorem 3.1.

Example 3.2 In Theorem 3.1, suppose $a^2 + 4b$ is not a square. Then, for f to be exactly realizable, we must have $2bf_1 - af_2 + a^2 f_1 = 0$ by (3.16). In other words the ratio $\frac{f_1}{f_2}$ equals $\frac{a}{a^2+2b}$. (Note that $a^2 + 2b \neq 0$ because it is given that $f_2 \geq 1$.) In particular, for $a = b = 1$, it has been shown in Theorem 2.2 that f is exactly realizable if and only if this ratio is $1/3$.

If a^2+4b *is* a square, then the same sharp conclusion of the last paragraph cannot be made. To explain this, consider two sequences: (i) with $f_1 = 1$ and $f_2 = 5$; (ii) with $f_1 = f_2 = 3$; each of which satisfies the recurrence

$$f_{n+2} = f_{n+1} + 2f_n \quad \text{for each } n \geq 1. \tag{3.17}$$

Here, $a = 1, b = 2$ so that $\Delta = 9$. Note that $H = 0$ and $\frac{f_1}{f_2} = \frac{1}{5}$ for (i), while $H \neq 0$ and $\frac{f_1}{f_2} = 1$ for (ii). As soon as we exhibit systems exactly realizing the sequences in (i) and (ii), our point will be made.

For (i), we use the subshifts of Example 1.5 and work much as we did for the 'if' part of Theorem 2.2. Let

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix} \quad \text{and } t_n = \text{ trace}(A^n) \text{ for each } n \geq 1.$$

The characteristic equation of A is $x^2 = x + 2$. Hence, t and f both satisfy the recurrence in (3.17). Also, it is easily checked that $t_1 = 1 = f_1$ and $t_2 = 5 = f_2$. Thus, $t = f$. Therefore, by Example 1.5, $f \in \mathcal{ER}$.

For (ii), it is straightforward to check that the sequence $(|(-2)^n - 1|)$ satisfies (3.17) and that each of its first two terms is 3. Hence, $f = (|(-2)^n - 1|)$. Also, by Example 1.6, the algebraic dynamical system S dual to $x \mapsto -2x$ on the discrete group $\mathbf{Z}[\frac{1}{2}]$ has $|(-2)^n - 1|$ points of period n. It follows that f is exactly realizable.

Before leaving this example, it is worth noting that there are infinitely many possible values of the ratio $\frac{f_1}{f_2}$ for sequences in $\mathcal{ER}$ satisfying (3.17): for the above sequences in (i) and (ii), write $f^{(i)}$ and $f^{(ii)}$, respectively; for all $n_1, n_2 \in \mathbf{N}$ the sequence $(n_1 f^{(i)} + n_2 f^{(ii)})$ satisfies (3.17) and, by Lemma 2.10, is in $\mathcal{ER}$; it follows that the set of possible ratios $\frac{f_1}{f_2}$ contains the infinite set $\{\frac{n_1+3n_2}{5n_1+3n_2} : n_1, n_2 \in \mathbf{N}\}$.

Remark 3.1 Before proving necessity in Theorem 3.1, we give some notation, offer a few comments on the hypotheses of the theorem and assemble useful facts.

1. It is assumed that the values of f_1, f_2, a and b are fixed. If these values are at issue we write $f(f_1, f_2, a, b)$ for f. The sequences $f(1, a, a, b)$ and $f(a, a^2 + 2b, a, b)$ are known as *Lucas sequences*. Respectively, these will be denoted by

$u(a,b)$ and $v(a,b)$, or more simply by u and v when the values of a and b are not at issue.

So, by definition, for each $n \geq 1$,

$$u_{n+2} = au_{n+1} + bu_n, \tag{3.18}$$

$$v_{n+2} = av_{n+1} + bv_n. \tag{3.19}$$

2. We comment on the values taken by f_1, f_2, a and b in the statement of the theorem. The most general related problem would be a discussion of the exact realizability of $f(f_1, f_2, a, b)$, where f_1, f_2, a and b are allowed arbitrary values in $\mathbf{C}$. However, there would still be the following simple reasons for continuing with the given restrictions on f_1 and f_2:

   (a) By Definition 2.4, f_1 and f_2 must be non-negative integers and, by (2.5) and (2.9), $\hat{f}_2 = f_2 - f_1 \geq 0$. This explains the inequality $f_2 \geq f_1 \geq 0$ in the theorem.

   (b) We omit $f_2 = 0$ to reduce the clutter that would result from amending claims such as (3.6), (3.11) and numerous others made in the proof. The case $f_2 = 0$ is easily put aside: if f is exactly realizable, then $f_1 = 0$ because $\hat{f}_2 = f_2 - f_1 \geq 0$. Conversely, if $f_1 = 0$, then f, by definition, is the (exactly realizable) zero sequence.

   We will not discuss the general problem referred to above. Some details have been worked out and it appears that matters are little more interesting than we are offering here.

3. The following congruences for the Lucas sequence v will be used:

$$v_n \equiv \begin{cases} nab^{(n-1)/2} \bmod a^2 & \text{if } n \text{ is odd,} \\ 2b^{n/2} \bmod a^2 & \text{if } n \text{ is even .} \end{cases} \tag{3.20}$$

Let us prove these by induction. Since $v_1 = a$ and $v_2 = a^2 + 2b$, it is easily checked that (3.20) holds for $n = 1$ and 2. For the induction step pick a natural number k and assume that (3.20) holds for $1, 2, \ldots, k, k+1$. Arguing mod a^2, we will be done if we show that

$$v_{k+2} \equiv (k+2)ab^{(k+1)/2} \text{ for odd } k, \qquad v_{k+2} \equiv 2b^{(k+2)/2} \text{ for even } k.$$

Now, for each odd k,

$$\begin{aligned} v_{k+2} &= av_{k+1} + bv_k \quad \text{(by (3.19))} \\ &\equiv a[2b^{(k+1)/2}] + b[kab^{(k-1)/2}] \quad \text{(by the induction hypothesis)} \\ &= (k+2)ab^{(k+1)/2}, \end{aligned}$$

as desired. Similarly, for each even k,

$$\begin{aligned} v_{k+2} &\equiv a[(k+1)ab^{k/2}] + b[2b^{k/2}] \quad \text{(by the induction hypothesis)} \\ &= a^2[(k+1)b^{k/2}] + 2b^{(k+2)/2} \quad \equiv \quad 2b^{(k+2)/2}, \end{aligned}$$

and (3.20) is proved.

4. It is immediate from (3.3), (3.4) and (3.5) that

$$a = \lambda + \mu, \tag{3.21}$$

$$b = -\lambda\mu, \tag{3.22}$$

$$\sqrt{\Delta} = \lambda - \mu, \tag{3.23}$$

$$\lambda^2 - a\lambda - b = 0 = \mu^2 - a\mu - b. \tag{3.24}$$

By (3.3), Δ and a are both odd or are both even. So, by (3.4) and (3.5), if Δ is a square, then λ and μ are integers. Conversely, by (3.23), if λ and μ are integers, then Δ is a square. In summary,

$$\Delta \text{ is a square if and only if } \lambda, \mu \text{ are integers.} \tag{3.25}$$

5. An easy induction argument proves each of the next three equalities involving f. By (3.1) and (3.18),

$$f_n = (f_2 - af_1)u_{n-1} + f_1 u_n \quad \text{for each } n \geq 2. \tag{3.26}$$

If $b \neq 0$, then, by (3.1), (3.18) and (3.19),

$$f_n = (Hu_n + [f_2 - af_1]v_n)/2b \quad \text{for each } n \geq 1. \tag{3.27}$$

Suppose $b, \Delta \neq 0$ and let

$$\alpha := \frac{f_2 - \mu f_1}{\lambda\sqrt{\Delta}} \quad \text{and} \quad \beta := \frac{\lambda f_1 - f_2}{\mu\sqrt{\Delta}}. \tag{3.28}$$

Then, by (3.1) and (3.24), the following holds:

$$\text{if } b, \Delta \neq 0, \text{ then } f_n = \alpha\lambda^n + \beta\mu^n \text{ for each } n \geq 1. \tag{3.29}$$

6. The first important work in the rich study of Lucas sequences was given in LUCAS [9]. A systematic survey is available in RIBENBOIM [11]. We need a few basic facts about these sequences.

$$2^{n-1}u_n = \sum_{1\leq k\leq n;\ \text{odd } k} \binom{n}{k} a^{n-k}\Delta^{(k-1)/2} \quad \text{for each } n \geq 1. \tag{3.30}$$

$$v_{2n} = v_n^2 - 2(-b)^n \quad \text{for each } n \geq 1. \tag{3.31}$$

$$v_p \equiv a \bmod p \quad \text{for each prime } p. \tag{3.32}$$

$$u_p \equiv \left(\frac{\Delta}{p}\right) \bmod p \quad \text{for each odd prime } p, \tag{3.33}$$

where $\left(\frac{*}{*}\right)$ is the *Legendre symbol*, which is defined as follows: for each odd prime p and each integer z

$$\left(\frac{z}{p}\right) = \begin{cases} +1 & \text{if } p\not| z \text{ and } y^2 \equiv z \bmod p \text{ for some integer } y, \\ -1 & \text{if } p\not| z \text{ and } y^2 \not\equiv z \bmod p \text{ for each integer } y, \\ 0 & \text{if } p|z. \end{cases} \tag{3.34}$$

It is fortunate that we have the next lemma because it will be instrumental in the proof of (3.16), which is the most interesting of the conditions in Theorem 3.1.

Lemma 3.1 *If Δ is a non-square integer, then there are infinitely many primes p with $\left(\frac{\Delta}{p}\right) = -1$.*

Proof. The proof, for which we thank Graham Everest, uses some well-known facts: the Chinese Remainder Theorem, Dirichlet's Theorem, and a few identities involving the Jacobi symbol. The details of these may, respectively, be found in Sections 5.7, 7.3 and 9.7 of Apostol [1].

Dirichlet's Theorem states that for coprime natural numbers s and t there exist infinitely many primes p satisfying $p \equiv s \bmod t$.

Let P and Q be integers with $Q = q_1 q_2 ... q_k$ where the q_i are odd primes, not necessarily distinct. The *Jacobi symbol* is defined by

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{k} \left(\frac{P}{q_i}\right),$$

where $\left(\frac{p}{q_i}\right)$ is the Legendre symbol defined in (3.34). The following will be used:

(i) $\left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right) = \left(\frac{P_1 P_2}{Q}\right)$;

(ii) $\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$;

(iii) If $(P, Q) = 1$, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{[(P-1)/2][(Q-1)/2]}$;

(iv) If $P_1 \equiv P_2 \bmod Q$, then $\left(\frac{P_1}{Q}\right) = \left(\frac{P_2}{Q}\right)$;

(v) $\left(\frac{P}{Q_1}\right)\left(\frac{P}{Q_2}\right) = \left(\frac{P}{Q_1 Q_2}\right)$;

(vi) $\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2}$.

For the lemma, let Δ be a non-square integer. Write $\Delta = 2^r d$ where $r \in \mathbf{Z}^+$ and d is odd. Throughout p will denote a large prime. Suppose for now that $\Delta > 0$. The case $\Delta < 0$ is dealt with at the end. For each p

$$\begin{aligned} \left(\frac{\Delta}{p}\right) = \left(\frac{2^r d}{p}\right) &= \left(\frac{2}{p}\right)^r \left(\frac{d}{p}\right) \quad \text{(by (i))} \\ &= (-1)^{r(p^2-1)/8} \left(\frac{d}{p}\right) \quad \text{(by (ii))}. \end{aligned} \tag{3.35}$$

Now, either (I) d is a square or (II) d is not a square. For (I), r is odd since Δ is a non-square. Also, $\left(\frac{d}{p}\right) = 1$ by (3.34). Thus, by (3.35), $\left(\frac{\Delta}{p}\right) = (-1)^{r(p^2-1)/8}$, which equals -1 for those p with $p \equiv 5 \bmod 8$. Since 5 and 8 are coprime, there are infinitely many such primes by Dirichlet's Theorem. So, the lemma is proved when $\Delta > 0$ and d is a square.

Now suppose (II). Let $k, \tilde{d}$ be odd numbers and q be an odd prime such that $d = q^k \tilde{d}$ with q and $\tilde{d}$ coprime. Choose a c with

$$\left(\frac{c}{q}\right) = -1. \tag{3.36}$$

(It is a basic fact that such a c can be chosen, as argued in, for example, APOSTOL [1, Th. 9.1].) Since q and $\tilde{d}$ are coprime, use the Chinese Remainder Theorem to choose an S with

$$S \equiv c \bmod q, \tag{3.37}$$

$$S \equiv 1 \bmod \tilde{d}. \tag{3.38}$$

Similarly, since 16 and d are coprime, choose an s with

$$s \equiv 1 \bmod 16, \tag{3.39}$$

$$s \equiv S \bmod d. \tag{3.40}$$

It is easy to see that s and $16d$ are coprime: by (3.36) and (3.34), c is prime to q; so, S is prime to q by (3.37); since 1 is prime to $\tilde{d}$, it follows from (3.38) that S is prime to $\tilde{d}$; thus, S is prime to $q\tilde{d}$ and, hence, to $q^k\tilde{d} = d$; this last fact and similar reasoning with (3.39) and (3.40), quickly shows that s and $16d$ are coprime. Hence, by Dirichlet's Theorem, there are infinitely many p for which

$$p \equiv s \bmod 16d. \tag{3.41}$$

For (II), it will suffice show that $\left(\frac{\Delta}{p}\right) = -1$ for each p satisfying (3.41). Recall that we are always working with large p. Using (3.35) and (iii), and working with p as in (3.41),

$$\begin{aligned} \left(\frac{\Delta}{p}\right) &= (-1)^{r(p^2-1)/8} \left(\frac{p}{d}\right) (-1)^{[(p-1)/2][(d-1)/2]} \\ &= \left(\frac{p}{d}\right) \quad \text{(since } p \equiv 1 \bmod 16 \text{ by (3.41) and (3.39))} \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{S}{d}\right) \quad \text{(by (iv); since } p \equiv S \bmod d \text{ by (3.41) and (3.40))} \\
&= \left(\frac{S}{q^k \tilde{d}}\right) = \left(\frac{S}{q}\right)^k \left(\frac{S}{\tilde{d}}\right) \quad \text{(by (v))} \\
&= \left(\frac{c}{q}\right)^k \left(\frac{1}{\tilde{d}}\right) \quad \text{(by (3.37), (3.38) and (iv))} \\
&= (-1)^k \cdot 1 \quad \text{(by (3.36))} \\
&= -1 \quad \text{(since } k \text{ is odd)},
\end{aligned}
$$

establishing the lemma for $\Delta > 0$.

Finally, let $\Delta < 0$. (For the purposes of Theorem 3.1, this part of the proof will not be needed since $\Delta \geq 0$ by (3.6).) With r and d as above, write $-\Delta = 2^r d$. Then

$$
\begin{aligned}
\left(\frac{\Delta}{p}\right) &= \left(\frac{-\Delta}{p}\right)\left(\frac{-1}{p}\right) \quad \text{(by (i))} \\
&= \left(\frac{-\Delta}{p}\right)(-1)^{(p-1)/2} \quad \text{(by (vi))} \qquad (3.42) \\
&= (-1)^{r(p^2-1)/8}\left(\frac{d}{p}\right)(-1)^{(p-1)/2} \quad \text{(by (3.35))}. \qquad (3.43)
\end{aligned}
$$

Suppose first that $-\Delta$ is a square. Then $\left(\frac{-\Delta}{p}\right) = 1$ by (3.34). The desired result follows from (3.42) on taking $p \equiv 3 \bmod 4$ and using Dirichlet's Theorem.

Suppose now that $-\Delta$ is not a square. For d non-square, we know from case (II) that $\left(\frac{-\Delta}{p}\right) = -1$ for $p \equiv s \bmod 16d$. By (3.39), these p also satisfy $p \equiv 1 \bmod 16$. Thus, for d non-square, we are done by (3.42). Lastly, when d is a square, argue much as in (I) by allowing $p \equiv 5 \bmod 8$ in (3.43). This completes the proof of the lemma. □

3.1 Proof of Theorem 3.1: necessity

Assume that f is exactly realizable.

Proof of (3.6). For a contradiction, suppose $\Delta < 0$. Since $\Delta := a^2 + 4b$, we have $b \neq 0$. By (3.4) and (3.5), λ and μ are complex conjugates. Hence, so are α and β by

(3.28). Therefore, for each $n \geq 1$, we see from (3.29) that f_n is the real part of

$$2\left(\frac{f_2 - \mu f_1}{\sqrt{\Delta}}\right)\lambda^{n-1}.$$

In this expression, we know that λ is not real. Thus, if $f_2 - \mu f_1 \neq 0$, then f_n takes negative values which are disallowed by Definition 2.4. So, $f_2 - \mu f_1 = 0$. Here, f_2 and f_1 are real but μ is not. Whence, $f_2 = 0$, which contradicts $f_2 > 0$ in the definition of f. Thus $\Delta \geq 0$, proving (3.6).

Proof of (3.7). By (2.10), 2 divides $\hat{f}_2$. By, (2.5) $\hat{f}_2 = f_2 - f_1$.

Proof of (3.8). Let $2|a, b$. Arguing mod 4,

$$\begin{aligned}
0 \equiv \hat{f}_4 &= f_4 - f_2 \quad \text{(by (2.10) and (2.5))} \\
&= a^2 f_2 + abf_1 + bf_2 - f_2 \quad \text{(by the recurrence in (3.1))} \\
&\equiv (b-1)f_2 \quad (4|a^2, ab \text{ since } 2|a, b) \\
&\equiv f_2 \quad (b-1 \text{ is odd since } 2|b),
\end{aligned}$$

establishing (3.8).

Proof of (3.9). Let $\mathrm{ord}_2(a) = 1$ and f_1 be odd. By (3.7), f_2 is odd. Therefore, by (3.8), b is odd. So, $b \equiv \pm 1 \bmod 4$. In anticipation of a contradiction let us assume that $b \equiv 1 \bmod 4$. Arguing mod 4,

$$\begin{aligned}
0 \equiv \hat{f}_4 &= f_4 - f_2 \quad \text{(by (2.10) and (2.5))} \\
&= a^2 f_2 + abf_1 + bf_2 - f_2 \quad \text{(by (3.1))} \\
&\equiv abf_1 + bf_2 - f_2 \quad (\text{since } 2|a) \\
&\equiv 2bf_1 + bf_2 - f_2 \quad (a \equiv 2 \text{ since } \mathrm{ord}_2(a) = 1) \\
&\equiv 2f_1 + f_2 - f_2 \quad (\text{we are assuming } b \equiv 1 \bmod 4) \\
&= 2f_1.
\end{aligned}$$

Hence, $4|2f_1$. So, f_1 is even. This contradicts the fact that f_1 is odd. Thus, $b \equiv -1 \bmod 4$, as claimed in (3.9).

Proof of (3.10). Let p be an odd prime dividing a and b. By (3.1), $p|f_{n+2}$ for each $n \geq 1$. In particular $p|f_p$. Also, by (2.10), $p|\hat{f}_p = f_p - f_1$. Whence, $p|f_1$, which settles (3.10).

Proof of (3.11). Let $a \leq 0$. Therefore,

$$\begin{aligned} 0 \leq \hat{f}_4 &= f_4 - f_2 \quad \text{(by (2.9) and (2.5))} \\ &= af_3 + bf_2 - f_2 \quad \text{(by (3.1))} \\ &\leq (b-1)f_2 \quad (f_3 \geq 0 \text{ by Definition 2.4, } a \leq 0 \text{ by hypothesis}). \end{aligned}$$

Now $f_2 > 0$ by definition. So, $b > 0$, as desired.

Proof of (3.12). Let $a < 0$. By (3.11), $b > 0$ and so $\Delta := a^2 + 4b > 0$. So, (3.29) holds.

Also, by (3.21), (3.22) and (3.23), $\lambda + \mu$, $\lambda\mu$ and $\mu - \lambda < 0$, from which $\mu < 0$ and $-1 < \lambda/\mu < 0$.

Thus, we may divide (3.29) by μ^n to obtain $f_n/\mu^n = \alpha(\lambda/\mu)^n + \beta$ for each $n \geq 1$. Since $-1 < \lambda/\mu < 0$, it follows that $f_n/\mu^n \to \beta$ as $n \to \infty$. Since $\mu < 0$ and Definition 2.4 requires $f \geq 0$, we have $\beta = 0$. Hence, by the definition of β in (3.28), $f_2 = \lambda f_1$ as asserted in (3.12).

Proof of (3.13). Let p be an odd prime dividing b. So, by (3.1), $f_{n+2} \equiv af_{n+1} \bmod p$ for each $n \geq 1$. An easy induction shows that, for each $n \geq 2$,

$$f_n \equiv a^{n-2} f_2 \bmod p. \tag{3.44}$$

In particular, $p|a^{p-2}f_2 - f_p$. Also, by (2.10) and (2.5), $p|\hat{f}_p = f_p - f_1$. So, $p|a^{p-2}f_2 - f_1$. Now, if $p\not|a$, then Fermat's Little Theorem immediately establishes (3.13).

Suppose now that p divides a. We need show just that p divides f_2. By (3.44), $p|f_p, f_{2p}$ and by (3.10) we have $p|f_1$. Also, $p|\hat{f}_{2p} = f_1 - f_p - f_2 + f_{2p}$ by (2.10) and (2.5). Hence, $p|f_2$ proving (3.13).

Proof of (3.14). Let p be an odd prime dividing $\Delta := a^2 + 4b$. Consider separately the cases $p|a$ and $p\not|a$. Suppose $p|a$. Then $p|\Delta - a^2 = 4b$. So, $p|b$. Hence, by (3.13), $p|f_2$ and the result follows.

Now suppose $p\not|a$. Recall the equality in (3.30) involving the Lucas sequence u. We show the following: (i) $au_{p-1} \equiv -2 \bmod p$; (ii) $u_p \equiv 0 \bmod p$; (iii) by (2.10), the condition $p|\hat{f}_p$ gives the result.

Since $p|\Delta$, we can write $p-1$ for n in (3.30) to obtain

$$2^{p-2}u_{p-1} \equiv \binom{p-1}{1} a^{p-2} \equiv -a^{p-2} \bmod p.$$

Multiplication through by $2a$ gives $a2^{p-1}u_{p-1} \equiv -2a^{p-1} \bmod p$ and, since $p \not| a, 2$, we use Fermat's Little Theorem to obtain (i).

As for (ii), $\left(\frac{\Delta}{p}\right) = 0$ because $p|\Delta$. Therefore, $p|u_p$ by (3.33).

Lastly, arguing mod p for (iii),

$$\begin{aligned} a\hat{f}_p &= af_p - af_1 \quad \text{(by (2.5))} \\ &= a(f_2 - af_1)u_{p-1} + af_1u_p - af_1 \quad \text{(by (3.26))} \\ &\equiv (f_2 - af_1)(-2) + af_1(0) - af_1 \quad \text{(by (i) and (ii))} \\ &= af_1 - 2f_2, \end{aligned}$$

which settles (iii) because $p|\hat{f}_p$.

Proof of (3.15). By (3.6), $\Delta \geq 0$. Consider in turn the cases (i) $\Delta = 0$ and (ii) $\Delta > 0$.

For (i), we see from (3.14) that $2f_2 - af_1$ is divisible by each odd prime. So, $2f_2 - af_1 = 0$. Also, $a = 2\mu$ by (3.5). Hence, $f_2 - \mu f_1 = 0$, agreeing with (3.15).

As regards (ii), the case is trivial when $0 \geq \mu$ because f_2 is positive and f_1 is non-negative by definition. So, let $\mu > 0$. Since $\Delta > 0$, we have $\lambda > \mu$ from (3.23). Hence,

$$1 > \mu/\lambda > 0. \tag{3.45}$$

Also, by (3.22), $b \neq 0$ because $\lambda, \mu \neq 0$. So, we can use (3.29) which, on division through by λ^n, gives

$$f_n/\lambda^n = \alpha + \beta(\mu/\lambda)^n \quad \text{for each } n \geq 1.$$

This equality with (3.45) shows that f_n/λ^n tends to α as n tends to ∞. We must have $\alpha \geq 0$, otherwise, f will take negative values and conflict with Definition 2.4. Whence, $f_2 \geq \mu f_1$ by (3.28) and we are done.

Proof of (3.16). Lemma 3.1, will be crucial to our proof. Let p be an odd prime. Suppose Δ is not a square. Since $\Delta := a^2 + 4b$, we have $b \neq 0$ and (3.27) holds. Thus,

$$f_p - f_1 = (Hu_p + [f_2 - af_1]v_P - 2bf_1)/2b.$$

By (2.10) and (2.5), $p|\hat{f}_p = f_p - f_1$. So,

$$Hu_p + [f_2 - af_1]v_P - 2bf_1 \equiv 0 \bmod p.$$

On using (3.33) and (3.32),

$$H\left(\frac{\Delta}{p}\right) + [f_2 - af_1]a - 2bf_1 \equiv 0 \bmod p.$$

On recalling that $H{:}= 2bf_1 - [f_2 - af_1]a$, we have

$$H\left[\left(\frac{\Delta}{p}\right) - 1\right] \equiv 0 \bmod p. \tag{3.46}$$

It is at this point that Lemma 3.1 is brought to bear: by supposition, Δ is not a square; by that lemma, $\left(\frac{\Delta}{p}\right) = -1$ for infinitely many p; hence, (3.46) holds only if $H = 0$. We have shown that if Δ is not a square, then $H = 0$, which proves (3.16).

3.2 Proof of Theorem 3.1: sufficiency

Before arguing the converse we pause to make a comment and do some preparatory work.

Remark 3.2 A perusal of the proof, so far, will reveal that in showing necessity we have applied the conditions of the Basic Lemma, but not to their full strength: we have, merely, asked that $f, \hat{f}_4 \geq 0, 4|\hat{f}_4$ and that for each prime p we have $p|\hat{f}_p, \hat{f}_{2p}$. One may suspect that, with conditions obtained so weakly, an argument for their sufficiency may rely on a simple analysis of how the terms of f grow through its recurrence in (3.1). In this sense our argument for the converse has been only partly successful.

3.2.1 Preliminaries

Three lemmas are given. When Δ is a square or when $H{:}= 2bf_1 - af_2 + a^2f_1 = 0$, the divisibility conditions in the theorem have some basic consequences which will be needed in the proof of the converse. These consequences are proved here in the next two lemmas, away from the main arguments in the hope that the latter do not get lost amongst elementary details. The third lemma provides a congruence which will be used to show that f has divisibility when $a > 0, b \neq 0$ and Δ is a positive square.

Lemma 3.2 *Let Δ be a square, so that λ and μ are integers by* (3.25). *Let p be a prime. Then the following hold:*

$$\text{if } p|\lambda, \text{ then } p|f_2 - \mu f_1; \tag{3.47}$$

$$\text{if } p|\mu, \text{ then } p|\lambda f_1 - f_2; \tag{3.48}$$

$$\text{if } p|\lambda - \mu, \text{ then } p|f_2 - \mu f_1; \tag{3.49}$$

$$\text{if } p|\lambda, \mu, \text{ then } p|f_1; \tag{3.50}$$

$$\text{if } 2|\lambda, \mu, \text{ then } 4|f_2 - \mu f_1. \tag{3.51}$$

Proof. To see (3.47), let $p|\lambda$. Consider odd p first. Then, working mod p,

$$\begin{aligned} 0 \equiv \lambda &\equiv b \quad (\text{since } b = -\lambda\mu \text{ by } (3.22)) \\ &\equiv f_2 - af_1 \quad (\text{by } (3.13)) \\ &\equiv f_2 - \mu f_1 - \lambda f_1 \quad (\text{since } a = \lambda + \mu \text{ by } (3.21)) \\ &\equiv f_2 - \mu f_1 \quad (\text{since } p|\lambda), \end{aligned}$$

showing that (3.47) holds when p is odd. Now let $p = 2$. Then either $2|\mu$ or $2\not|\mu$. If $2|\mu$, then $2|a, b$ by (3.21) and (3.22). So, $4|f_2$ by (3.8). Hence, $2|f_2 - \mu f_1$. Lastly, if $2\not|\mu$, then $2|f_2 - \mu f_1$ by (3.7). So, (3.47) is proved.

To see (3.48), simply write λ for μ, and μ for λ in the proof of (3.47).

For (3.49), let $p|\lambda - \mu$. If $p = 2$, then we just repeat the argument used for $p = 2$ in the proof of (3.47). Now consider odd p. Since $\lambda - \mu := \sqrt{\Delta}$, we know that $p|\Delta$. So, $p|2f_2 - af_1$ by (3.6). Thus, p divides $[2f_2 - af_1 + (\lambda - \mu)f_1]$, which is exactly $2(f_2 - \mu f_1)$ because $a := \lambda + \mu$. So, $p|f_2 - \mu f_1$, as stated in (3.49).

For (3.50), suppose $p|\lambda, \mu$. Then $p|a, b$ by (3.21) and (3.22). Therefore, by (3.10), for odd p we see that $p|f_1$. For $p = 2$, we have $4|f_2$ by (3.8), so that $2|f_1$ by (3.7). This proves (3.50) and, in fact, the last sentence proves (3.51) and, therefore, the lemma. □

Lemma 3.3 *Suppose that*

$$2bf_1 - af_2 + a^2 f_1 = 0. \tag{3.52}$$

Then the following hold for each prime p:

$$\textit{if } 4|a, \textit{ then } 2|f_1; \tag{3.53}$$

$$\textit{if } p \textit{ is odd and } p|a, \textit{ then } p|f_1; \tag{3.54}$$

$$\begin{aligned} &\textit{if } \operatorname{ord}_p(a) \geq 2 \textit{ and } \operatorname{ord}_p(a) - \operatorname{ord}_p(f_1) \geq 1, \\ &\textit{then } \operatorname{ord}_p(bf_1) \geq \operatorname{ord}_p(a) + 1. \end{aligned} \tag{3.55}$$

Proof. To see (3.53), let $4|a$. By (3.52), $4|2bf_1$. So, if $2 \nmid b$, then $2|f_1$. If $2|b$, then $2|f_1$ by (3.8) and (3.7).

For (3.54), let p be an odd prime dividing a. Then $p|2bf_1$ by (3.52). So, if $p \nmid b$, then $p|f_1$. If $p|b$, then again $p|f_1$ by (3.10).

For (3.55), suppose p is a prime with $\operatorname{ord}_p(a) \geq 2$ and $\operatorname{ord}_p(a) - \operatorname{ord}_p(f_1) \geq 1$. Consider odd p first. By (3.52), $a|2bf_1$. Hence, $\operatorname{ord}_p(b) + \operatorname{ord}_p(f_1) \geq \operatorname{ord}_p(a)$. So, $\operatorname{ord}_p(b) \geq \operatorname{ord}_p(a) - \operatorname{ord}_p(f_1) \geq 1$. Thus, p divides both a and b. By (3.13), $p|f_2$. Whence,

$$\begin{aligned} \operatorname{ord}_p(bf_1) &= \operatorname{ord}_p(af_2 - a^2 f_1) \quad \text{(by (3.52))} \\ &\geq \min[\operatorname{ord}_p(af_2), \operatorname{ord}_p(a^2 f_1)] \\ &\geq \min[\operatorname{ord}_p(a) + 1, 2\operatorname{ord}_p(a)] \quad (\text{since } p|f_1, f_2, a) \\ &= \operatorname{ord}_p(a) + 1 \quad (\text{since } p|a), \end{aligned}$$

proving (3.55) when p is odd. Now let $p = 2$. By (3.53), $2|f_1$. Hence, $2|f_2$ by (3.7). So,

$$\begin{aligned} 1 + \operatorname{ord}_2(b) + \operatorname{ord}_2(f_1) &= \operatorname{ord}_2(2bf_1) \\ &= \operatorname{ord}_2(af_2 - a^2 f_1) \quad \text{(by (3.52))} \\ &\geq \min[\operatorname{ord}_2(a) + 1, 2\operatorname{ord}_2(a) + 1] \quad (\text{since } 2|f_2, a) \\ &= \operatorname{ord}_2(a) + 1, \end{aligned} \tag{3.56}$$

which shows that $\operatorname{ord}_2(b) \geq \operatorname{ord}_2(a) - \operatorname{ord}_2(f_1)$. Thus, $\operatorname{ord}_2(b) \geq 1$ by the second of the hypotheses in (3.55). Hence, 2 divides both a and b. By (3.8), $4|f_2$. Repeating the argument used in reaching (3.56),

$$\begin{aligned} 1 + \mathrm{ord}_2(bf_1) &= \mathrm{ord}_2(af_2 - a^2 f_1) \\ &\geq \min[\mathrm{ord}_2(a) + 2,\ 2\mathrm{ord}_2(a){+}1] \quad = \quad \mathrm{ord}_2(a) + 2, \end{aligned}$$

so that $\mathrm{ord}_2(bf_1) \geq \mathrm{ord}_2(a) + 1$, which completes the proof of (3.55) and the lemma. □

Lemma 3.4 *Let K, m and r be natural numbers with $1 \leq m \leq r - 1$. Then, for each prime p,*

$$\binom{p^r K - 1}{m} \equiv \binom{p^{r-1} K - 1}{m} \bmod p^{r-m}.$$

Proof. Suppose K, m, p and r are given as in the lemma. We must prove that p^{r-m} divides

$$\frac{1}{m!}\Big[(p^r K - 1)(p^r K - 2)\ldots(p^r K - m) \\ -(p^{r-1}K - 1)(p^{r-1}K - 2)\ldots(p^{r-1}K - m)\Big].$$

This is equivalent to proving that $p^{r-m+\mathrm{ord}_p(m!)}$ divides

$$(p^r K - 1)(p^r K - 2)\ldots(p^r K - m) \\ -(p^{r-1}K - 1)(p^{r-1}K - 2)\ldots(p^{r-1}K - m).$$

Now, if $\mathrm{ord}_p(m!) \leq m - 1$, then we will be done: it will then follow that $r - m + \mathrm{ord}_p\,(m!) \leq r - 1$ and, arguing mod $p^{r-m+\mathrm{ord}_p(m!)}$, we will have

$$\prod_{j=1}^{m}(p^r K - j) - \prod_{j=1}^{m}(p^{r-1}K - j) \equiv \prod_{j=1}^{m}(-j) - \prod_{j=1}^{m}(-j) \equiv 0.$$

In fact, $\mathrm{ord}_p(m!) \leq m - 1$: this is immediate from the equation

$$\mathrm{ord}_p(m!) = (m - s_m)/(p - 1),$$

where s_m is the sum of digits in m to base p. For a proof of this equation see, for example, Bachman [2, Lemma 3.1]. □

With this preparatory work out of the way, we now prove the converse of Theorem 3.1.

3.2.2 The cases in which the recurrence reduces to the first order: $\mathbf{a < 0; b = 0; \Delta = 0}$

Sufficiency is proved in each of three cases: when a is negative; when b is zero; when Δ is zero. In each case the recurrence defining f reduces to one of first order and Lemma 2.9 is used.

The case $\mathbf{a < 0}$

Let $a < 0$. Hence, by (3.12),

$$f_2 = \lambda f_1. \tag{3.57}$$

Note that (3.29) is valid here because $b > 0$ by (3.11) and the same, therefore, holds for $\Delta =: a^2 + 4b$. Our aim is to use Lemma 2.9. In turn it will be shown that:

(i) $f_n = \lambda f_{n-1}$ for each $n \geq 2$;

(ii) f_1 and λ are natural numbers;

(iii) f_1 is divisible by each prime that divides λ.

A simple way to see (i) is to use (3.57) and write $f_2 = \lambda f_1$ in (3.29) to obtain $f_n = \lambda^{n-1} f_1$ for each $n \geq 1$, and then use an easy induction.

By definition, $f_1 \geq 0$. By (3.57), $f_1 \neq 0$ because $f_2 > 0$ by definition. So, f_1 is a natural number. As for λ, note first that, since $a < 0$, we have $b > 0$ by (3.11). Thus, each of $b, -a, f_1$, and f_2 is positive. Hence, $2bf_1 - af_2 + a^2 f_1$ is positive. So, Δ is a square by (3.16), and λ is an integer by (3.25). Since $f_2 \geq f_1 > 0$, it is apparent from (3.57) that $\lambda > 0$. Whence, λ is a natural number, proving (ii).

Lastly, for (iii), let p be a prime dividing λ. Hence, $p|b$ by (3.22) and $p|f_2$ by (3.57). If $p = 2$, then $p|f_1$ by (3.7). For odd p we use (3.13) to obtain $p|af_1$, so that the result holds if $p \nmid a$. In the case $p|a$ we see from (3.10) that, again, $p|f_1$.

So, $f \in \mathcal{ER}$ by Lemma 2.9.

The case $\mathbf{b = 0}$

Assume that $b = 0$. The following will be shown: (i) $f_n = af_{n-1}$ for each $n \geq 2$; (ii) a and f_1 are natural numbers; (iii) for each prime p if $p|a$, then $p|f_1$.

Since $b = 0$, it is seen by (3.13) that each odd prime divides $f_2 - af_1$. Hence,

$$f_2 \quad = \quad af_1. \tag{3.58}$$

Thus, (i) holds by (3.1). Since, by definition, $f_2 > 0$ and $f_1 \geq 0$ we see from (3.58) that (ii) holds. If p is an odd prime and $p|a$, then $p|f_1$ by (3.10). If $2|a$, then $2|f_2$ by (3.58). Hence, $2|f_1$ by (3.7). So, (iii) holds and, by Lemma 2.9, $f \in \mathcal{ER}$.

The case $\mathbf{\Delta = 0}$

Suppose $\Delta = 0$. So, by the definition of Δ in (3.3),

$$a^2 + 4b = 0. \tag{3.59}$$

Also, by (3.14), each odd prime divides $2f_2 - af_1$. Whence, $2f_2 - af_1 = 0$, which we rewrite as

$$f_2 = (a/2)f_1. \tag{3.60}$$

A straightforward induction using (3.1), (3.59), and (3.60), shows that $f_n = (a/2)f_{n-1}$ for each $n \geq 2$.

We now show (i) $a/2$ and f_1 are natural numbers, (ii) f_1 is divisible by each prime that divides $a/2$.

By (3.59), $2|a$. By (3.60), $f_1, a > 0$ because, by definition, $f_2 > 0$ and $f_1 \geq 0$. Hence, $a/2$ and f_1 are natural numbers, proving (i).

For (ii), let $2|(a/2)$. Then, by (3.60), $2|f_2$. So, by (3.7), $2|f_1$. Also, if an odd prime p divides $a/2$, then $p|b$ by (3.59). Therefore, $p|f_1$ by (3.10).

By Lemma 2.9, $f \in \mathcal{ER}$, disposing of the case $\Delta = 0$.

3.2.3 The case $\mathbf{a = 0}$

Let $a = 0$. Thus, by (3.11), b is a natural number. The following will be shown: $f(f_1, f_2, 0, 1)$ is exactly realizable; using Lemma 2.5, Corollary 2.7(i) and the positivity of $f(f_1, f_2, 0, 1)$, the positivity of $f(f_1, f_2, 0, b)$ will be deduced for each $b \geq 2$; finally, $f(f_1, f_2, 0, b)$ will be shown to have divisibility by Lemma 2.8. The result will then follow by the Basic Lemma.

Suppose $b = 1$. Then, $f = (f_1, f_2, f_1, f_2, \ldots)$ by the recurrence defining f in (3.1). Therefore, by (2.5), $\hat{f} = (f_1, f_2 - f_1, 0, 0, \ldots)$. Now, by definition, $f_2 \geq f_1 \geq 0$. So, $\hat{f} \geq 0$. Also, by (3.7), $2 | f_2 - f_1$. Hence, $n | \hat{f}_n$ for each $n \geq 1$. By the Basic Lemma, it follows that f is exactly realizable when $b = 1$.

Now consider $b \geq 2$. By (3.1),

$$f = (f_1, f_2, bf_1, bf_2, b^2 f_1, b^2 f_2, b^3 f_1, b^3 f_2, \ldots),$$

so that f is the product of the sequences

$$g := (f_1, f_2, f_1, f_2, \ldots) \qquad \text{and} \qquad h := (1, 1, b, b, b^2, b^2, b^3, b^3, \ldots).$$

It has been shown above that $\hat{g} \geq 0$. If we can show that $\hat{h} \geq 0$, then we will be done by Corollary 2.7(i). Lemma (2.5) will be used to show that $\hat{h} \geq 0$. Note first that h is increasing and $h \geq 0$ since $b \geq 2$. If n is odd with $n \neq 3, 5$, then

$$\begin{aligned} h_{2n} - nh_n &= b^{n-1} - nb^{(n-1)/2} \quad \text{(by definition of } h) \\ &= b^{(n-1)/2}[b^{(n-1)/2} - n] \\ &\geq 2^{(n-1)/2} - n \quad \text{(since } b \geq 2) \\ &\geq 0 \quad \text{(since } n \text{ is odd, } n \neq 3, 5). \end{aligned}$$

Similarly for each even n,

$$h_{2n} - nh_n = b^{n-1} - nb^{(n-2)/2} = b^{(n-2)/2}[b^{n/2} - n] \geq 2^{n/2} - n \geq 0.$$

So, $h_{2n} - nh_n \geq 0$ for all $n \neq 3, 5$. Thus, by Lemma 2.5, $\hat{h}_n \geq 0$ for each $n \neq 6, 7, 10, 11$ and these few values of n are no exception to $\hat{h} \geq 0$, as can be checked directly with ease. For example, $\hat{h}_{10} = h_{10} - h_5 - h_2 + h_1 = b^4 - b^2 - 1 + 1 \geq 0$ since $b \geq 2$. Hence, $\hat{f} \geq 0$.

For the case $b \geq 2$, we now prove that $n | \hat{f}_n$ for each $n \geq 1$. Lemma 2.8 will be used. Let p be a prime and r, K be natural numbers. It is sufficient to prove each of the following:

(I) if p is odd and K is even, then $p^r | f_2[b^{(p^r K-2)/2} - b^{(p^{r-1}K-2)/2}]$;

(II) if p and K are odd, then $p^r | f_1[b^{(p^r K-1)/2} - b^{(p^{r-1}K-1)/2}]$;

(III) if $r \geq 2$ and k is odd, then $2^r | f_{[2,r,K]} := f_2[b^{(2^r K-2)/2} - b^{(2^{r-1}K-2)/2}]$;

(IV) if K is odd, then $2 | f_2 b^{K-1} - f_1 b^{(K-1)/2}$.

For (I), let p be odd and K be even. If $p \nmid b$, then we are done by (2.19) because

$$f_2[b^{(p^r K-2)/2} - b^{(p^{r-1}K-2)/2}] = \frac{f_2}{b}[(b^{K/2})^{p^r} - (b^{K/2})^{p^{r-1}}].$$

Now let $p|b$. By hypothesis $a = 0$. So, by (3.13), $p|f_2$. Hence,

$$\begin{aligned} \mathrm{ord}_p(f_2[b^{(p^r K-2)/2} - b^{(p^{r-1}K-2)/2}]) &\geq \mathrm{ord}_p(f_2[b^{(p^{r-1}K-2)/2}]) \\ &\geq 1 + (p^{r-1}K - 2)/2 \\ &= p^{r-1}K/2 \quad \geq \quad p^{r-1} \quad \geq \quad r, \end{aligned}$$

proving (I).

For (II), assume that p and K are odd. The matter is trivial if $f_1 = 0$. Suppose $f_1 > 0$. Then, since $a = 0$ and $b > 0$, we have $2bf_1 - af_2 + a^2 f_1 > 0$. Thus, Δ is a square by (3.16). But $\Delta := a^2 + 4b = 4b$. So, b is a square. If $p \nmid b$, then we are done by (2.19) because

$$f_1[b^{(p^r K-1)/2} - b^{(p^{r-1}K-1)/2}] = \frac{f_1}{b^{1/2}}[(b^{K/2})^{p^r} - (b^{K/2})^{p^{r-1}}].$$

If $p|b$, then $p|f_1$ by (3.10), so that

$$\begin{aligned} \mathrm{ord}_p(f_1[b^{(p^r K-1)/2} - b^{(p^{r-1}K-1)/2}]) &\geq \mathrm{ord}_p(f_1[b^{(p^{r-1}K-1)/2}]) \\ &\geq 1 + 2[(p^{r-1}K - 1)/2] \quad (b \text{ is a square}) \\ &= p^{r-1}K \quad \geq \quad r, \end{aligned}$$

proving (II).

For (III), suppose $r \geq 2$ and K is odd. There are three cases: (i) $2 \nmid b$ and $f_1 > 0$; (ii) $2 \nmid b$ and $f_1 = 0$; (iii) $2|b$.

For case (i), b is a square for the same reasons as given in (II). Note that

$$f_{[2,r,K]} = \frac{f_2}{b}[(b^{K/2})^{2^r} - (b^{K/2})^{2^{r-1}}].$$

Here, by (2.19), 2^r divides the square bracketed expression on the right hand side. So, $2^r | f_{[2,r,K]}$.

For (ii), note that

$$f_{[2,r,K]} = \frac{f_2}{b}[(b^K)^{2^{r-1}} - (b^K)^{2^{r-2}}].$$

Here, by (2.19), 2^{r-1} divides the square bracketed expression on the right hand side. Also, $2|f_2$ by (3.7). Thus, $2^r | f_{2,r,K]}$.

For (iii), $4|f_2$ by (3.8). Therefore,

$$\begin{aligned} \text{ord}_2(f_2[b^{(2^r K-2)/2} - b^{(2^{r-1}K-2)/2}]) &\geq \text{ord}_2(f_2[b^{(2^{r-1}K-2)/2}]) \\ &\geq 2 + (2^{r-1}K - 2)/2 = 1 + 2^{r-2}K \geq r, \end{aligned}$$

which settles (III).

Finally, for (IV), suppose K is odd. This is easy since $f_2 \equiv f_1 \bmod 2$ by (3.7), and $b^{K-1} \equiv b^{(K-1)/2} \bmod 2$. Hence, f has divisibility and the converse of Theorem 3.1 holds when $a = 0$.

3.2.4 The case $\mathbf{a}, \boldsymbol{\Delta} > 0, \mathbf{b} \neq 0$: proof of positivity

Suppose $a, \Delta > 0$ and $b \neq 0$. The sequence f will be shown to have positivity in each of the following three cases: $a, b \geq 1$; $a \geq 1, -1 \geq b$ and $1 > \mu$; $a \geq 1, -1 \geq b$ and $\mu \geq 1$. Lemma 2.5 will be used in all cases and Corollary 2.8 will also help in the last.

Positivity when $\mathbf{a}, \mathbf{b} \geq 1$

Let $a, b \geq 1$. Lemma 2.5 will be used. By definition, $f_2 \geq f_1 \geq 0$. So, by (3.1), f is increasing and non-negative. Now, for each $n \geq 3$,

$$\begin{aligned} f_n &:= af_{n-1} + bf_{n-2} \quad \text{(by (3.1))} \\ &\geq f_{n-1} + f_{n-2} \quad \text{(since } a, b \geq 1 \text{ and } f \geq 0) \qquad (3.61) \\ &\geq 2f_{n-2} \quad \text{(since } f \text{ is increasing).} \qquad (3.62) \end{aligned}$$

Using (3.62) repeatedly, for each even n we obtain

$$f_{2n} \geq 2f_{2n-2} \geq 2^2 f_{2n-4} \geq 2^3 f_{2n-6} \geq \ldots \geq 2^{n/2} f_n \geq n f_n. \tag{3.63}$$

Also, for each odd $n \geq 3$,

$$\begin{aligned}
f_{2n} &\geq 2^{(n-3)/2} f_{n+3} \quad \text{(by repeated use of (3.62))} \\
&\geq 2^{(n-3)/2}(f_{n+2} + f_{n+1}) \quad \text{(reasoning as for (3.61))} \\
&\geq 2^{(n-3)/2}(2f_n + f_{n+1}) \quad \text{(by (3.62))} \\
&\geq 2^{(n-3)/2}(3f_n) \quad \text{(since } f \text{ is increasing)} \\
&\geq n f_n. \qquad (3.64)
\end{aligned}$$

Since $f_2 \geq f_1 \geq 0$, it follows by (3.63) and (3.64) that $f_{2n} \geq f_n$ for each $n \geq 1$. Therefore, $\hat{f} \geq 0$ by Lemma 2.5.

Positivity when $\mathbf{a \geq 1, -1 \geq b, 1 > \mu}$

Suppose $a \geq 1, -1 \geq b$ and $1 > \mu$. Lemma 2.5 will be used after it is shown that (i) $a \geq 2 - b$ and (ii) $f_n \geq 2f_{n-1}$ for each $n \geq 3$.

Since $\Delta := a^2 + 4b \geq 1$ and $-1 \geq b$, it follows that $a^2 \geq 5$. Also, $\mu := \left[a - \sqrt{a^2 + 4b}\right]/2 < 1$ implies $a - 2 < \sqrt{a^2 + 4b}$, and the last inequality can be squared since $a^2 \geq 5$. Consequently, $a > 1 - b$ and, since a is a natural number, we have $a \geq 2 - b$. This proves (i).

A basic induction will now be used to show (ii). For $n = 3$,

$$\begin{aligned}
f_3 &:= af_2 + bf_1 \geq (2-b)f_2 + bf_1 \quad \text{(since } a \geq 2 - b\text{)} \\
&= 2f_2 + b(f_1 - f_2) \geq 2f_2 \quad \text{(since } 0 > b \text{ and, by definition, } f_2 \geq f_1\text{)}.
\end{aligned}$$

Suppose that $f_r \geq 2f_{r-1}$ for some $r \geq 3$. Then

$$\begin{aligned}
f_{r+1} &:= af_r + bf_{r-1} \geq (2-b)f_r + bf_{r-1} = 2f_r + b(f_{r-1} - f_r) \\
&\geq 2f_r \quad \text{(since } 0 > b \text{ and, by the induction hypothesis, } f_r \geq 2f_{r-1}\text{)},
\end{aligned}$$

so that (ii) holds. By definition, $f_2 \geq f_1 \geq 0$. Thus, by (ii), f is non-negative and increasing. By Lemma 2.5, we will be done as soon as it is noted that $f_{2n} \geq nf_n$ for each $n \geq 2$. For each $n \geq 2$, repeated use of (ii) gives

$$f_{2n} \geq 2f_{2n-1} \geq 2^2 f_{2n-2} \geq \cdots \geq 2^n f_n \geq n f_n.$$

Hence, $\hat{f} \geq 0$.

Positivity when $\mathbf{a} \geq \mathbf{1}, -\mathbf{1} \geq \mathbf{b}, \mu \geq \mathbf{1}$

Assume that $a \geq 1, -1 \geq b$ and $\mu \geq 1$. By (3.23), $\lambda = \mu + \Delta \geq 1 + 1 = 2$. Also, $f_2 \geq \mu f_1$ by (3.15). Now either $f_2 \leq \lambda f_1$ or $f_2 > \lambda f_1$.

For $f_2 \leq \lambda f_1$, the use of (3.29) and (2.5) gives

$$\hat{f}_n = \alpha \sum_{d|n} \mu(n/d)\lambda^d + \beta \sum_{d|n} \mu(n/d)\mu^d \quad \text{for each } n \geq 1.$$

It is easy to see that this expression is non-negative for each $n \geq 1$: $\sqrt{\Delta}, \lambda$, and μ are positive while $\lambda f_1 - f_2$ and $f_2 - \mu f_1$ are non-negative; hence, by their definitions in (3.28), α and β are non-negative; by Corollary 2.8, each of $\sum_{d|n} \mu(n/d)\lambda^d$ and $\sum_{d|n} \mu(n/d)\mu^d$ is non-negative because $\lambda, \mu \geq 1$. Whence, $\hat{f} \geq 0$ when $f_2 \leq \lambda f_1$.

For $f_2 > \lambda f_1$, an easy induction shows that $f_n > \lambda f_{n-1}$ for each $n \geq 2$: let $f_r > \lambda f_{r-1}$ for some $r \geq 2$. Then

$$\begin{aligned} f_{r+1} &:= af_r + bf_{r-1} = (\lambda + \mu)f_r - \lambda\mu f_{r-1} \quad \text{(by (3.21) and (3.22))} \\ &= \lambda f_r + \mu f_r - \lambda\mu f_{r-1} \\ &> \lambda f_r + \lambda\mu f_{r-1} - \lambda\mu f_{r-1} \quad (f_r > \lambda f_{r-1} \text{ by the induction hypothesis}), \end{aligned}$$

which equals λf_r. Consequently, since $f_1 \geq 0$ by definition, and $\lambda \geq 2$ the sequence f is non-negative and increasing. Also, for each $n \geq 1$,

$$f_{2n} > \lambda f_{2n-1} > \lambda^2 f_{2n-2} > \cdots > \lambda^n f_n > n f_n.$$

So, by Lemma 2.5, $\hat{f} \geq 0$ when $f_2 > \lambda f_1$. This completes our task in showing that f has positivity when $a > 0$ and $\Delta > 0$.

Remark 3.3 For the special case $a \geq 1, -1 \geq b$ and $1 = \mu$, there is an argument which is simpler than the one given just above. By (3.29) and (3.28),

$$\hat{f}_n := \sum_{d|n} \mu(n/d) f_d = \frac{f_2 - f_1}{\lambda\sqrt{\Delta}} \sum_{d|n} \mu(n/d)\lambda^d + \beta \sum_{d|n} \mu(n/d). \tag{3.65}$$

We need show $\hat{f}_n \geq 0$ for each $n \geq 1$. This is trivial for $n = 1$. For each $n \geq 2$ note the following: by (2.2), the second summand in (3.65) is 0; $f_2 \geq f_1$ by definition; we are given $\Delta > 0$; by (3.22), $\lambda = -b \geq 1$ and, hence, $\sum_{d|n} \mu(n/d)\lambda^d \geq 0$ by Corollary 2.8. Thus, $\hat{f} \geq 0$.

3.2.5 The case $\mathbf{a}, \boldsymbol{\Delta} > 0, \mathbf{b} \neq 0$: proof of divisibility

Let $a, \Delta > 0$ and $b \neq 0$. We show that f has divisibility by exploiting (3.16). Our task is divided into two: the case when Δ is a square and the case when $H = 0$. For the former case, the proof is self-contained in the sense that there is no appeal to a system exactly realizing f. This is untrue of our argument for the case $H = 0$. When $H = 0$ it is easily seen that $f = (f_1/a)v$ where v the Lucas sequence. Using Example 1.5, we exhibit a dynamical system exactly realizing v, from which the divisibility of f is deduced. This is immediate when a divides f_1, and less so otherwise.

Divisibility when $\boldsymbol{\Delta}$ is a square

Suppose Δ is a square. Lemma 2.8 will be used. Let p be a prime and r, K be natural numbers. It will be shown that $p^r | f_{[p,r,K]} := f_{p^r K} - f_{p^{r-1}K}$. By (3.29), (3.28) and (3.23)

$$f_n = \frac{1}{\lambda - \mu}\left[(f_2 - \mu f_1)\lambda^{n-1} + (\lambda f_1 - f_2)\mu^{n-1}\right] \quad \text{for each } n \geq 1. \tag{3.66}$$

Write g and h, respectively, for the sequences for which

$$g_n = (f_2 - \mu f_1)\lambda^{n-1} \quad \text{and} \quad h_n = (\lambda f_1 - f_2)\mu^{n-1} \quad \text{for each } n \geq 1. \tag{3.67}$$

By (3.47), if $p|\lambda$, then $p|f_2 - \mu f_1$. Thus, by Corollary 2.12, we know that g has divisibility. The same holds for h by (3.48). Using (3.66) and (3.67),

$$f_{[p,r,K]} = \frac{1}{\lambda - \mu}\begin{bmatrix} (f_2 - \mu f_1)\lambda^{p^r K - 1} + (\lambda f_1 - f_2)\mu^{p^r K - 1} \\ -(f_2 - \mu f_1)\lambda^{p^{r-1}K-1} - (\lambda f_1 - f_2)\mu^{p^{r-1}K-1} \end{bmatrix} \tag{3.68}$$

$$= \frac{1}{\lambda - \mu}\left[g_{[p,r,K]} + h_{[p,r,K]}\right]. \tag{3.69}$$

Since g and h have divisibility, $p^r|g_{[p,r,K]}+h_{[p,r,K]}$ by Lemma 2.8. Hence, by (3.69), $p^r|f_{[p,r,K]}$ when $p\not|\lambda-\mu$. So, we can suppose from now that $p|\lambda-\mu$. By the binomial theorem,

$$\begin{aligned} \lambda^{p^rK-1} &= [\mu+(\lambda-\mu)]^{p^rK-1} \\ &= \mu^{p^rK-1}+\sum_{i=1}^{p^rK-1}(\lambda-\mu)^i\binom{p^rK-1}{i}\mu^{p^rK-1-i}. \end{aligned} \tag{3.70}$$

There is a similar expression for $\lambda^{p^{r-1}K-1}$ which, along with (3.70), we substitute into (3.68). Then, some basic manipulation shows that $f_{[p,r,K]}$ is the sum of two terms, namely

$$F_{(p,r,K)} := (\mu^{p^rK-1}-\mu^{p^{r-1}K-1})f_1,$$

and

$$S_{(p,r,K)} := (f_2-\mu f_1)\begin{bmatrix} \sum_{i=1}^{p^rK-1}(\lambda-\mu)^{i-1}\binom{p^rK-1}{i}\mu^{p^rK-1-i} \\ -\sum_{i=1}^{p^{r-1}K-1}(\lambda-\mu)^{i-1}\binom{p^{r-1}K-1}{i}\mu^{p^{r-1}K-1-i} \end{bmatrix}.$$

Here, for brevity, write $\varsigma_{(p,r,K)}$ and $\sigma_{(p,r,K)}$ for the sums involving $\sum_{i=1}^{p^rK-1}$ and $\sum_{i=1}^{p^{r-1}K-1}$, respectively. Define $\sigma_{(p,1,1)}$ to be 0 for each p. Thus,

$$S_{(p,r,K)} = (f_2-\mu f_1)[\varsigma_{(p,r,K)}-\sigma_{(p,r,K)}] \quad \text{for all } p, r \text{ and } K. \tag{3.71}$$

It will now be shown that p^r divides each of $F_{(p,r,K)}$ and $S_{(p,r,K)}$. Consider $F_{(p,r,K)}$ first. Recall that we are working with those p that divide $\lambda-\mu$. If $p\not|\mu$, then $p^r|F_{(p,r,K)}$ by (2.19). If $p|\mu$, then $p|\lambda$ as well. So, $p|f_1$ by (3.50). Hence,

$$\mathrm{ord}_p(F_{(p,r,K)}) \geq \mathrm{ord}_p(\mu^{p^{r-1}K-1}f_1) \geq p^{r-1}K-1+1 = p^{r-1}K \geq r.$$

Now consider $S_{(p,r,K)}$. By (3.49), $p|f_2-\mu f_1$. Either (I) $p|\mu$ or (II) $p\not|\mu$. For (I), let $p|\mu$. Then, for each term ς in $\varsigma_{(p,r,K)}$ we have $\mathrm{ord}_p(\varsigma)\geq i-1+p^rK-1-i = p^rK-2$. Hence,

$$\mathrm{ord}_p((f_2-\mu f_1)\varsigma_{(p,r,K)}) \geq 1+p^rK-2 = p^rK-1 \geq r.$$

Thus, by (3.71), it remains to show that $p^r|(f_2-\mu f_1)\sigma_{(p,r,K)}$. This is trivial for $1=r=K$ and each prime p since $\sigma_{(p,1,1)}:=0$. If $r=2, K=1$ and $p=2$, then we are done since $4|f_2 - \mu f_1$ by (3.51). For all other triples (p, r, K) and for each term σ in $\sigma_{(p,r,K)}$ we have $\mathrm{ord}_p(\sigma) \geq p^{r-1}K - 2$, which implies

$$\mathrm{ord}_p((f_2 - \mu f_1)\sigma_{(p,r,K)}) \geq 1 + p^{r-1}K - 2 = p^{r-1}K - 1 \geq r,$$

completing the argument that $p|f_{[p,r,K]}$ when $p|\mu$.

For (II), let $p\not|\mu$. Since $p|f_2 - \mu f_1$, the result holds for $r = 1$ and all K, p. So, let $r > 1$. Again, since $p|f_2 - \mu f_1$, it is enough to show that $p^{r-1}|\varsigma_{(p,r,K)} - \sigma_{(p,r,K)}$. Note that, since $p|\lambda - \mu$, we know that p^{r-1} divides each term of $\sigma_{(p,r,K)}$ for $i \geq r$. The same holds for $\varsigma_{(p,r,K)}$. Hence, mod p^{r-1}, we have $\varsigma_{(p,r,K)} - \sigma_{(p,r,K)}$ congruent to

$$\sum_{i=1}^{r-1}(\lambda - \mu)^{i-1}\left[\binom{p^rK - 1}{i}\mu^{p^rK-1-i} - \binom{p^{r-1}K - 1}{i}\mu^{p^{r-1}K-1-i}\right].$$

Our task will be done when we show that, for each i, the square bracketed expression in the i-th term of this sum is divisible by p^{r-i}: by (2.19), for each i with $1 \leq i \leq r-1$,

$$\mu^{p^rK-1-i} \equiv \mu^{p^{r-1}K-1-i} \bmod p^r;$$

and for all such i, by Lemma 3.4,

$$\binom{p^rK - 1}{i} \equiv \binom{p^{r-1}K - 1}{i} \bmod p^{r-i};$$

on multiplying these congruences mod p^{r-i}, the desired result follows. Thus, $p^r|S_{[p,r,K]}$ when $p\not|\mu$. Therefore, f has divisibility when Δ is a square.

Divisibility when $\mathbf{H = 0}$ and $\mathbf{a}$ divides $\mathbf{f_1}$

Suppose $H := 2bf_1 - af_2 + a^2f_1 = 0$ and $a|f_1$. Then, since neither a nor b is zero, $f_1/a = (f_2 - af_1)/2b$. Hence, by (3.27),

$$f_n = \frac{f_1}{a}v_n \quad \text{for each } n \geq 1. \tag{3.72}$$

More will be shown than required. Using Example 1.5, it will be shown that the Lucas sequence v is in $\mathcal{ER}$. Since $a|f_1$, the same will hold for f by (3.72) and Corollary 2.3.

Recall the definition of v in Remark 3.1(1): $v = f(a, a^2 + 2b, a, b)$; so, v satisfies the recurrence in (3.1) with $v_1 = a$ and $v_2 = a^2 + 2b$. Suppose a is odd. (The case of even a is mentioned at the end.) Let

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} (a-1)/2 & 1 \\ b + (a^2-1)/4 & (a+1)/2 \end{bmatrix}.$$

Define a sequence t by $t_n = \text{trace}(A^n)$ for each $n \geq 1$. Since $a, \Delta > 1$, the entries in A are non-negative integers. It is easily checked that the characteristic equation of A is $x^2 = ax + b$. So, $A^2 = aA + bI$. Thus, $A^{n+2} = aA^{n+1} + bA^n$ and, hence, $t_{n+2} = at_{n+1} + bt_n$ for each $n \geq 1$. Thus, t and v both satisfy the recurrence in (3.1). Also, $t_1 = (a-1)/2 + (a+1)/2 = a = v_1$ and

$$t_2 = \text{trace}(A^2) = \text{trace}(aA + bI) = a\ \text{trace}(A) + b\ \text{trace}(I) = a^2 + 2b = v_2.$$

Thus, $t = v$. Therefore, by Example 1.5, $v \in \mathcal{ER}$ when a is odd. Working as above with the matrix $\begin{bmatrix} a/2 & 1 \\ b + a^2/4 & a/2 \end{bmatrix}$, it will be seen that the same holds when a is even. Whence, f has divisibility when $H = 0$ and $a | f_1$.

Divisibility when H = 0 and a does not divide f$_1$

Suppose $H = 0$ and a does not divide f_1. Lemma 2.8 will be used. Let p be a prime and r, K be natural numbers. By (3.72),

$$f_{[p,r,K]} := f_{p^r K} - f_{p^{r-1} K} = \frac{f_1}{a} v_{[p,r,K]} \quad \text{for all } p, r \text{ and } K. \tag{3.73}$$

Since it has just been shown that v has divisibility, we know, by Lemma 2.8, that $p^r | v_{[p,r,K]}$. Therefore, by (3.73), in showing that $p^r | f_{[p,r,K]}$, we need think only of those p for which $\text{ord}_p(a) > \text{ord}_p(f_1)$. (Since $a \nmid f_1$, there are such p.) By (3.54), if p is odd and $\text{ord}_p(a) = 1$, then $\text{ord}_p(f_1) \geq \text{ord}_p(a)$. Hence, it is enough, by Lemma 2.8 and (3.73), to prove the following:

(i) If $\text{ord}_2(a) = 1$ and f_1 is odd, then for all r and K with K odd

$$2^{r+1} | v_{2^r K} - v_{2^{r-1} K}. \tag{3.74}$$

(ii) If p is a prime with $\mathrm{ord}_p(a) \geq 2$ and $\mathrm{ord}_p(a) > \mathrm{ord}_p(f_1)$, then for all r and K

$$p^{r+\mathrm{ord}_p(a)-\mathrm{ord}_p(f_1)} | v_{p^r K} - v_{p^{r-1}K}. \tag{3.75}$$

Proof of (i). Suppose $\mathrm{ord}_2(a) = 1$ and f_1 is odd. Fix an odd K. Note that $4|b+1$ by (3.9) and, therefore, $8|(b-1)(b+1) = b^2 - 1$. On writing $b^{2^r} - 1$ as $(b^{2^{r-1}} - 1)(b^{2^{r-1}} + 1)$ for each $r \geq 1$, an easy induction shows that

$$2^{r+1} | b^{2^{r-1}} - 1 \quad (\text{for each } r \geq 2). \tag{3.76}$$

Induction on r will be used to prove (i). For $r = 1$ we must show that $4|v_{2K} - v_K$. By (3.20),

$$v_{2K} - v_K \equiv 2b^K - Kab^{(K-1)/2} \bmod 4.$$

Here, $b \equiv -1 \bmod 4$ by (3.9). Since K is odd, $K \equiv \pm 1 \bmod 4$. Also, $a \equiv 2 \bmod 4$ because $\mathrm{ord}_2(a) = 1$. Consequently,

$$v_{2K} - v_K \equiv 2(-1) - (\pm 1)(2)(\pm 1) \equiv 0 \bmod 4,$$

proving that (3.74) holds for $r = 1$. As hypothesis of the induction, suppose that (3.74) holds for a given r. To show that this supposition implies $2^{r+2}|v_{2^{r+1}K} - v_{2^r K}$, use (3.31) twice to obtain

$$\begin{aligned} v_{2^{r+1}K} - v_{2^r K} &= v_{2^r K}^2 - 2(-b)^{2^r K} - [v_{2^{r-1}K}^2 - 2(-b)^{2^{r-1}K}] \\ &= (v_{2^r K} - v_{2^{r-1}K})(v_{2^r K} + v_{2^{r-1}K}) \\ &\quad -2(-b)^{2^{r-1}K}[(-b)^{2^{r-1}K} - 1]. \end{aligned}$$

Here, 2^{r+2} divides the first summand by the induction hypothesis. For $r = 1$, the second summand equals $-2b^K(b^K + 1)$, which is divisible by 2^{1+2} because $b \equiv -1 \bmod 4$. For $r \geq 2$ the second summand equals $-2b^{2^{r-1}K}(b^{2^{r-1}K} - 1)$ which, by (3.76), is divisible by 2^{r+2}. Hence, $2^{r+2}|v_{2^{r+1}K} - v_{2^r K}$, which completes the induction step and proves (i).

Proof of (ii). Let p be a prime with $\mathrm{ord}_p(a) \geq 2$ and $\mathrm{ord}_p(a) > \mathrm{ord}_p(f_1)$. For brevity, write w, x and y, respectively, for the orders of p in a, b and f_1. Thus, by our premises, $w \geq 2$ and $w-1 \geq y$. By (3.53) and (3.54), $y \geq 1$. Also, $x \geq w-y+1$ by (3.55). These simple facts are now displayed for ease of reference.

$$x \geq w-y+1 \tag{3.77}$$

$$w-1 \geq y \geq 1 \tag{3.78}$$

Let r and K be natural numbers. Recall that v satisfies the recurrence in (3.1) with $v_1 = a$ and $v_2 = a^2+2b$. So, for each triple (p,r,K), we can write $v_{p^{r-1}K}$ as a linear combination of products of powers of a and b. For each $(p,r,K) \neq (2,2,1)$, it will be shown that each such product in $v_{p^{r-1}K}$ is divisible by p^{r+w-y}. (It is a simple exercise to verify that $2^{2+w-y}|v_2$. It will then follow that $p^{r+w-y}|v_{p^{r-1}K}$ for each (p,r,K); and on writing $r+1$ for r, we will have $p^{r+1+w-y}|v_{p^rK}$ and so $p^{r+w-y}|v_{p^rK}$, proving (ii).)

From now assume that $(p,r,K) \neq (2,2,1)$. On writing out the first few terms of the sequence v, some of which are:

$$\begin{aligned}
v_1 &= a; \\
v_2 &= a^2+2b; \\
v_3 &= a^3+3ab; \\
v_4 &= a^4+4a^2b+2b^2; \\
v_7 &= a^7+7a^5b+14a^3b^2+7ab^3; \\
v_8 &= a^8+8a^6b+20a^4b^2+16a^2b^3+2b^4;
\end{aligned}$$

we quickly notice and, using (3.19), readily prove by induction that for odd n the products involving a and b in the summands of v_n are

$$a^n, \quad a^{n-2}b, \quad a^{n-4}b^2, \quad \ldots \quad , \quad ab^{(n-1)/2}. \tag{3.79}$$

Similarly, for even n the corresponding products are

$$a^n, \quad a^{n-2}b, \quad a^{n-4}b^2, \quad \ldots \quad , \quad b^{n/2}. \tag{3.80}$$

For odd n, the orders with respect to p of the entries in (3.79) are

$$nw, \quad (n-2)w+x, \quad (n-4)w+2x, \quad \ldots \quad , \quad w+(n-1)x/2. \tag{3.81}$$

Similar use of (3.80) for even n gives

$$nw, \quad (n-2)w+x, \quad (n-4)w+2x, \quad \dots \quad , \quad nx/2. \tag{3.82}$$

For n odd, as well as even, we see from (3.81) and (3.82), that the orders increase left to right when $x \geq 2w$, and decrease when $x < 2w$. Thus, for odd $p^{r-1}K$,

$$\text{ord}_p(v_{p^{r-1}K}) \geq \ \min\ [p^{r-1}Kw, w+(p^{r-1}K-1)x/2], \tag{3.83}$$

and for even $p^{r-1}K$,

$$\text{ord}_p(v_{p^{r-1}K}) \geq \ \min\ (p^{r-1}Kw, p^{r-1}Kx/2). \tag{3.84}$$

We now establish three inequalities, (excluding the case $p=2, r=2$ and $K=1$):

(a) $p^{r-1}Kw \geq r+w-y$;

(b) $w+(p^{r-1}K-1)x/2 \geq r+w-y$ when $p^{r-1}K$ is odd;

(c) $p^{r-1}Kx/2 \geq r+w-y$ when $p^{r-1}K$ is even;

so that by (a), (b) and (3.83), we will have $p^{r+w-y}|v_{p^{r-1}K}$ for odd $p^{r-1}K$; the same will hold for even $p^{r-1}K$ by (a), (c) and (3.84); and (ii) will then be proved.

For (a),

$$\begin{aligned} p^{r-1}Kw &\geq rw \quad (\text{since } K \geq 1 \text{ and } p^{r-1} \geq r) \\ &= (r-1)(w-1)+r+w-1 \\ &\geq r+w-1 \quad (\text{since } w \geq 2 \text{ by (3.78) and } r \geq 1) \\ &\geq r+w-y \quad (\text{because } y \geq 1 \text{ by (3.78)}). \end{aligned}$$

As regards (b),

$$\begin{aligned} w+(p^{r-1}K-1)x/2 &\geq w+p^{r-1}K-1 \quad (\text{as } x \geq 2 \text{ by (3.77) and (3.78)}) \\ &\geq w+r-1 \quad (\text{since } K \geq 1 \text{ and } p^{r-1} \geq r) \\ &\geq w+r-y \quad (\text{we have } y \geq 1 \text{ by (3.78)}). \end{aligned}$$

Finally, for (c) let $p^{r-1}K$ be even. We first show that

$$p^{r-1}K - r - 1 \geq 0. \tag{3.85}$$

If $r = 1$, then K is even because $p^{r-1}K$ is even. In this case $p^{r-1}K - r - 1 = K - 2 \geq 2 - 2 = 0$.

Let $r = 2$. Here, we cannot have $K = 1$ because $K = 1$ would require $p = 2$ to ensure that $p^{r-1}K$ is even, but the case $r = 2, p = 2$ and $K = 1$ is excluded from the present discussion. Hence, when $r = 2$ we have $K \geq 2$ and so $p^{r-1}K - r - 1 = pK - 3 \geq 2 \times 2 - 3 \geq 0$.

For $r \geq 3$, we have $p^{r-1} \geq r + 1$ and so $p^{r-1}K - r - 1 \geq p^{r-1} - r - 1 \geq 0$, proving (3.85).

We can now see to (c):

$$\begin{aligned}
p^{r-1}Kx/2 &\geq (r+1)x/2 \quad (\text{by}(3.85)) \\
&= (r-1)x/2 + x \\
&\geq r - 1 + x \quad (\text{since } x \geq 2 \text{ by } (3.77) \text{ and } (3.78)) \\
&\geq r - 1 + w - y + 1 \quad (\text{by } (3.77)) \\
&= r + w - y,
\end{aligned}$$

as desired. This proves (ii) and completes the argument that f has divisibility when $H = 0$ and a does not divide f_1.

By the arguments in this subsection and Subsection 3.2.4, f is exactly realizable in the case $a, \Delta > 0$ and $b \neq 0$. It has been shown that the same holds of f in the following four cases: $a < 0$; $b = 0$; $\Delta = 0$; $a = 0$. Since these five cases are exhaustive, the converse of Theorem 3.1 is established.

Chapter 4

Growth Rate of orbits

In this chapter the growth in the number of points of period n is compared with the growth in the number of points of least period n. As expected, these behave very similarly for exponential growth rates, which is the case that arises most naturally in dynamics (cf. [7, Sect. 4], where Lind points out that if f_n is the number of points of period n under the automorphism of the 2-torus corresponding to the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, then $\hat{f}_{20}$ is only 0.006% smaller than f_{20}). On the other hand, we show below that for other growth rates (polynomial and super-exponential in particular) the two quantities may be forced to grow very differently.

4.1 Exponential growth rates

Theorem 4.1 *Let f be exactly realizable with $\hat{f} > 0$. Write $\hat{F}$ and F, respectively, for the sets $\{\frac{1}{n}\log\hat{f}_n \colon n \in \mathbf{N}\}$ and $\{\frac{1}{n}\log f_n \colon n \in \mathbf{N}\}$.*

(i) *Let C be a non-negative real. Then, $\frac{1}{n}\log\hat{f}_n \to C$ if and only if $\frac{1}{n}\log f_n \to C$.*

(ii) *$\hat{F}$ is bounded if and only if F is bounded.*

(iii) *If $\frac{1}{n}\log f_n \to \infty$, then $\hat{F}$ may have infinitely many limit points.*

Proof. (i) For the 'only if' part, let C be a non-negative real and suppose that $\frac{1}{n}\log \hat{f}_n \to C$. The proof relies on us being able to 'sandwich' the sequence $(\frac{1}{n}\log f_n)$ between the sequence $(\frac{1}{n}\log \hat{f}_n)$ and another in $\hat{F}$.

For each $n \geq 1$, write $L_n := \{d\colon d|n;\ \text{if } d'|n, \text{ then } \hat{f}_d \geq \hat{f}_{d'}\}$ and choose an $\tilde{n}$ in L_n. To see that $\tilde{n} \to \infty$ as $n \to \infty$, let a natural number N be given. Write M for $\max\{\hat{f}_m\colon 1 \leq m \leq N\}$. Then, for each $n > M$ and each m with $1 \leq m \leq N$,

$$\begin{aligned} \hat{f}_{\tilde{n}} &\geq \hat{f}_n \quad (\text{since } \tilde{n} \in \mathrm{L}_n \text{ and } n|n) \\ &\geq n \quad (\text{since } \hat{f} > 0 \text{ and, by (2.10), } n|\hat{f}_n) \\ &> M \quad (\text{by our choice of } n) \\ &\geq \hat{f}_m \quad (\text{by the definition of } M); \end{aligned}$$

so, $\hat{f}_{\tilde{n}} > \hat{f}_m$ and, hence, there is no m equal to $\tilde{n}$. Thus, $\tilde{n} > N$ whenever $n > M$, which proves that $\tilde{n} \to \infty$ as $n \to \infty$. Therefore, since $(\frac{1}{n}\log \hat{f}_n)$ converges to C, the same holds for $(\frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}})$. (There is no *a priori* reason to assume that $(\frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}})$ is a subsequence of $(\frac{1}{n}\log \hat{f}_n)$.) Now, for each $n \geq 1$,

$$\begin{aligned} \frac{1}{n}\log \hat{f}_n &\leq \frac{1}{n}\log f_n \quad (f \geq \hat{f} \text{ by (2.6)}) \\ &= \frac{1}{n}\log\left(\sum_{d|n} \hat{f}_d\right) \quad (\text{by (2.6)}) \\ &\leq \frac{1}{n}\log\left(n \max\{\hat{f}_d\colon d|n\}\right) \quad (n \text{ has no more than } n \text{ divisors}) \\ &= \frac{1}{n}\log n + \frac{1}{n}\log\left(\max\{\hat{f}_d\colon d|n\}\right) \\ &= \frac{1}{n}\log n + \frac{\tilde{n}}{n}\cdot\frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}} \quad (\text{by the definition of } \tilde{n}) \\ &\leq \frac{1}{n}\log n + \frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}} \quad (\text{since } \tilde{n} \leq n), \end{aligned}$$

so that from the first and last of these inequalities,

$$\frac{1}{n}\log \hat{f}_n \leq \frac{1}{n}\log f_n \leq \frac{1}{n}\log n + \frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}}.$$

The result now follows because $\frac{1}{n}\log n$ converges to 0 and each of $\frac{1}{n}\log \hat{f}_n$ and $\frac{1}{\tilde{n}}\log \hat{f}_{\tilde{n}}$ converges to C.

For the converse, let $\frac{1}{n}\log f_n \to C$. The argument is easy when $C = 0$: $f \geq \hat{f}$ by (2.6); it is given that $\hat{f} > 0$, so that, by (2.10), $\hat{f}_n \geq n$ for each $n \geq 1$; therefore,

$$\frac{1}{n}\log n \leq \frac{1}{n}\log \hat{f}_n \leq \frac{1}{n}\log f_n \quad \text{for each } n \geq 1;$$

here, each of $\frac{1}{n}\log n$ and $\frac{1}{n}\log f_n$ converges to 0; hence, the same holds for $\frac{1}{n}\log \hat{f}_n$.

Now suppose $C > 0$. Let $\epsilon \in (0, C/3)$ and choose N such that,

$$e^{n(C-\epsilon)} \leq f_n \leq e^{n(C+\epsilon)} \quad \text{for each } n > N. \tag{4.1}$$

For each real number x write $\lfloor x \rfloor$ for the greatest integer not exceeding x. Let B be an upper bound for F and consider large n. On using (2.6) for each of the first three steps below,

$$\begin{aligned}
f_n \;\geq\; \hat{f}_n \;&=\; f_n - \sum_{d|n;d\neq n} \hat{f}_d \;\geq\; f_n - \sum_{d|n;d\neq n} f_d \\
&\geq\; f_n - \sum_{r=1}^{\lfloor n/2 \rfloor} f_r \quad \text{(no proper divisor of } n \text{ exceeds } \lfloor n/2 \rfloor) \\
&=\; f_n - \sum_{r=1}^{N} f_r - \sum_{r=N+1}^{\lfloor n/2 \rfloor} f_r \\
&\geq\; f_n - Ne^{NB} - \sum_{r=N+1}^{\lfloor n/2 \rfloor} f_r \quad (B \text{ is an upper bound for } F) \\
&\geq\; f_n - Ne^{NB} - (\lfloor n/2 \rfloor - N)e^{\lfloor n/2 \rfloor (C+\epsilon)} \quad (f_n \leq e^{n(C+\epsilon)} \text{ by (4.1)}) \\
&\geq\; f_n - Ne^{NB} - (n/2 - N)e^{n(C+\epsilon)/2} \quad (\text{since } n/2 \geq \lfloor n/2 \rfloor) \\
&=\; f_n \left[1 - N\frac{e^{NB}}{f_n} - (n/2 - N)\frac{e^{n(C+\epsilon)/2}}{f_n} \right] \\
&\geq\; f_n \left[1 - Ne^{NB - n(C-\epsilon)} - (n/2 - N)e^{-n(C-3\epsilon)/2} \right] \quad (e^{n(C-\epsilon)} \leq f_n \text{ by (4.1)})
\end{aligned}$$

Using the first and last of the above chain of inequalities, taking logs and dividing through by n gives

$$\begin{aligned}
\frac{1}{n}\log f_n \;&\geq\; \frac{1}{n}\log \hat{f}_n \\
&\geq\; \frac{1}{n}\log f_n + \frac{1}{n}\log \left[1 - Ne^{NB-n(C-\epsilon)} - (n/2 - N)e^{-n(C-3\epsilon)/2} \right].
\end{aligned}$$

Now let $n \to \infty$. The bracketed expression converges to 1. By hypothesis $\frac{1}{n}\log f_n \to C$. Whence, $\frac{1}{n}\log \hat{f}_n \to C$, completing the proof of (i).

(ii) The 'if' part is clear since $f \geq \hat{f}$ by (2.6). For the converse let A be an upper bound for $\hat{F}$, so that $\hat{f}_n \leq e^{An}$ for each $n \geq 1$. Using (2.6),

$$f_n = \sum_{d|n} \hat{f}_d \leq \sum_{r=1}^{n} \hat{f}_r \leq \sum_{r=1}^{n} e^{Ar} \leq ne^{An} \quad \text{for each } n \geq 1.$$

Here, taking logs and dividing through by n gives

$$\frac{1}{n}\log f_n \leq \frac{1}{n}\log ne^{An} = \frac{1}{n}\log n + A < 1 + A \quad \text{for each } n \geq 1.$$

Thus, F is bounded above by $1 + A$.

(iii) For each $r \geq 1$ let $n_r = p_r p_{r+1}$ where p_r is the r-th prime. Define $\hat{f}_n = n2^{n^3}$ for each n not of the form n_r. For each n of the form n_r, define $\hat{f}_n$ as follows:

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

and so on. Since $\hat{f}_n \geq 0$ and $n|\hat{f}_n$ for each $n \geq 1$, it follows, by the Basic Lemma, that f is exactly realizable. By (2.6), for each n not of the form n_r,

$$\frac{1}{n}\log f_n \geq \frac{1}{n}\log \hat{f}_n = \frac{1}{n}\log n + n^2 \log 2.$$

Hence, $\frac{1}{n}\log f_n \to \infty$ away from the n_r's. For each n of the form n_r,

$$\frac{1}{n_r}\log f_{n_r} = \frac{1}{n_r}\log\left[\hat{f}_1 + \hat{f}_{p_r} + \hat{f}_{p_{r+1}} + \hat{f}_{n_r}\right] \quad \text{(by (2.6))}$$

$$\geq \frac{1}{n_r}\log \hat{f}_{p_{r+1}} = \frac{1}{p_r p_{r+1}}\log\left(p_{r+1}2^{p_{r+1}^3}\right) \geq \frac{1}{p_r p_{r+1}}\log\left(2^{p_{r+1}^3}\right) \geq p_{r+1}\log 2.$$

Hence, $\frac{1}{n_r}\log f_{n_r} \to \infty$ as $r \to \infty$. Therefore, $\frac{1}{n}\log f_n \to \infty$ as $n \to \infty$.

For each natural number m there is a subsequence (n_{r_k}) of (n_r) with $\hat{f}_{n_{r_k}} = n_{r_k}2^{mn_{r_k}}$ for each $k \geq 1$. Since $\frac{1}{n_{r_k}}\log n_{r_k}2^{mn_{r_k}} \to m\log 2$ as $k \to \infty$, it follows that $\hat{F}$ has infinitely many limit points. □

Remark 4.1 1. For the sequence $\hat{f}$ constructed in the proof of Theorem 4.1(iii), we have $\frac{1}{n}\log f_n$ tending to infinity independently of the definition of $\hat{f}$ along the n_r's. In that proof retaining the definition of $\hat{f}$ off the n_r's and suitably redefining $\hat{f}$ along the n_r's, it is clear that one can arrange for $\hat{F}$ to have any finite number of limit points that one wishes.

2. In Theorem 4.1, the condition $\hat{f} > 0$ ensures that the various sets and sequences are well defined. When $\hat{f}$ is allowed to take finitely many zero values, we can write

$$\hat{F} := \{\tfrac{1}{n}\log \hat{f}_n : \hat{f}_n > 0, n \in \mathbf{N}\} \quad \text{and} \quad F := \{\tfrac{1}{n}\log f_n : f_n > 0, n \in \mathbf{N}\}.$$

The theorem will then still hold because our concern is with all sufficiently large n. The proof above will require a few minor changes.

What can be said of $\lim_{n\to\infty}\frac{1}{n}\log f_n$ if $\hat{f}$ takes infinitely many zero values? Consider two elementary examples: (a) let $\hat{f}_1 = 1$ and $\hat{f}_n = 0$ for $n > 1$; (b) let $\hat{f}_p = 0$ for each prime p, and $\hat{f}_c = c2^c$ when c is not a prime. By the Basic Lemma, it is quickly seen that f is exactly realizable in each case. In (a), f is the unit sequence (1). So, $\frac{1}{n}\log f_n \to 0$. In (b), if p is a prime, then $f_p = \hat{f}_1 + \hat{f}_p = 2$. Thus, $\frac{1}{p}\log f_p \to 0$ as $p \to \infty$. However, if c is composite, then $\frac{1}{c}\log f_c \geq \frac{1}{c}\log \hat{f}_c \geq \log 2$. Therefore, $(\frac{1}{n}\log f_n)$ has no limit in case (b).

It is natural to ask whether there is an exactly realizable sequence f, with $\hat{f}$ taking infinitely many zero values and $(\frac{1}{n}\log f_n)$ having a positive limit. It is unclear whether this is a difficult question.

4.2 Polynomial growth rates

Theorem 4.2 *Let f be exactly realizable. For each real number s write $\hat{F}_s$ and F_s, respectively, for the sets $\{\frac{\hat{f}_n}{n^s} : n \in \mathbf{N}\}$ and $\{\frac{f_n}{n^s} : n \in \mathbf{N}\}$.*

(i) *For each $s > 1$, $\hat{F}_s$ is bounded if and only if F_s is bounded.*

(ii) *For each $s \geq 1$, $\frac{\hat{f}_n}{n^s} \to 0$ if and only if $\frac{f_n}{n^s} \to 0$.*

(iii) *Let $C > 0$ and $s > 1$ be given. If $\frac{f_n}{n^s} \to C$, then $\hat{F}_s$ has infinitely many limit points, including C.*

(iv) *Let $C > 0$ and $s \geq 1$ be given. If $\frac{\hat{f}_n}{n^s} \to C$, then F_s has infinitely many limit points, including C. Also, F_1 is unbounded when $\frac{\hat{f}_n}{n} \to C$.*

Proof. (i) By (2.6) and the Basic Lemma, $f \geq \hat{f} \geq 0$. So, we need just worry about upper bounds and the 'if' part is immediate. Fix $s > 1$ and let $\hat{F}$ be an upper bound for $\hat{F}_s$. Then, for each $n \geq 1$,

$$\begin{aligned}
\frac{f_n}{n^s} &= \frac{1}{n^s}\sum_{d|n} \hat{f}_d \quad \text{(by (2.6))} \\
&\leq \frac{1}{n^s}\sum_{d|n} \hat{F} d^s \quad \text{(since } \hat{F} \text{ is an upper bound for } \hat{F}_s) \\
&= \hat{F}\sum_{d|n}(d/n)^s = \hat{F}\sum_{d|n} 1/(n/d)^s \\
&= \hat{F}\sum_{d|n} 1/d^s \quad \text{(as } d \text{ ranges over the divisors of } n \text{ so does } n/d) \\
&\leq \hat{F}\sum_{r=1}^{\infty} 1/r^s,
\end{aligned}$$

which is finite since $s > 1$. So, F_s is bounded when $\hat{F}_s$ is bounded, proving (i).

Let us make a note of the simple fact just explained and used, and will use again:

$$\sum_{d|n}(d/n)^s \leq \sum_{r=1}^{\infty} 1/r^s \quad \text{for each } n \in \mathbf{N} \text{ and } s > 1. \tag{4.2}$$

(ii) The 'if' part is easy since $f \geq \hat{f} \geq 0$. For the converse, fix an $s > 1$ and suppose $\frac{\hat{f}_n}{n^s} \to 0$. (The case $s = 1$ is discussed later.) Write $t := \sum_{r=1}^{\infty} 1/r^s$. Let $\epsilon > 0$ be given and choose natural numbers n_1 and n_2 such that, for each $n \geq 1$,

$$n > n_1 \quad \Rightarrow \quad \frac{\hat{f}_n}{n^s} < \frac{\epsilon}{1+t}, \tag{4.3}$$

$$n > n_2 \quad \Rightarrow \quad \sum_{k=1}^{n_1} \frac{\hat{f}_k}{n^s} < \frac{\epsilon}{1+t}. \tag{4.4}$$

Then, for each $n \geq \max\{n_1, n_2\}$,

$$\begin{aligned}
0 &\leq \frac{f_n}{n^s} = \sum_{d|n} \frac{\hat{f}_d}{n^s} \quad \text{(by (2.6))} \\
&\leq \sum_{k=1}^{n_1} \frac{\hat{f}_k}{n^s} + \sum_{d|n; d>n_1} \frac{\hat{f}_d}{n^s} \\
&\leq \frac{\epsilon}{1+t} + \sum_{d|n; d>n_1} \frac{\hat{f}_d}{d^s} \cdot \frac{d^s}{n^s} \quad \text{(by (4.4))} \\
&\leq \frac{\epsilon}{1+t} + \frac{\epsilon}{1+t} \sum_{d|n; d>n_1} \frac{d^s}{n^s} \quad \text{(by (4.3))} \\
&\leq \frac{\epsilon}{1+t} + \frac{\epsilon}{1+t} t \quad \text{(by (4.2))} \\
&= \epsilon.
\end{aligned}$$

Since ϵ is arbitrary, by the first and last of these inequalities $\frac{f_n}{n^s} \to 0$ as $n \to \infty$. This proves (ii) when $s > 1$.

For the case $s = 1$, suppose $\frac{\hat{f}_n}{n} \to 0$. By (2.10), $n | \hat{f}_n$ for each $n \geq 1$. So, $\hat{f} = 0$ eventually. Let $N \in \mathbf{N}$ be such that $\hat{f}_n = 0$ for each $n > N$. By (2.6), $f_n = \sum_{d|n} \hat{f}_d \leq \sum_{r=1}^{N} \hat{f}_r$ for each $n \geq 1$. Hence, f is bounded. So, $\frac{f_n}{n} \to 0$.

(iii) Let $C > 0$ and $s > 1$ be given and suppose $\frac{f_n}{n^s} \to C$. For each prime p and each $r \in \mathbf{N}$ the set $\hat{F}_s$ contains $\frac{\hat{f}_{p^r}}{p^{rs}}$. Also,

$$\begin{aligned}
\frac{\hat{f}_{p^r}}{p^{rs}} &= \frac{f_{p^r} - f_{p^{r-1}}}{p^{rs}} \quad \text{(by (2.5))} \\
&= \frac{f_{p^r}}{p^{rs}} - \frac{f_{p^{r-1}}}{p^{(r-1)s} p^s}.
\end{aligned}$$

Now fix p and let $r \to \infty$. The result is that $\frac{\hat{f}_{p^r}}{p^{rs}} \to C(1 - \frac{1}{p^s})$. So, $C(1 - \frac{1}{p^s})$ is a limit point of $\hat{F}_s$ for each prime p. There are infinitely many primes. So, $\hat{F}_s$ has infinitely many limit points.

Since $C(1 - \frac{1}{p^s}) \to C$ as $p \to \infty$, we see that C is a limit point of $\hat{F}_s$. (An example of a sequence in $\hat{F}_s$ and converging to C is $\left(\frac{\hat{f}_{p_r}}{p_r^s}\right)$ where p_r is the r-th prime: using (2.5),

$$\frac{\hat{f}_{p_r}}{p_r^s} = \frac{f_{p_r}}{p_r^s} - \frac{f_1}{p_r^s}$$

which converges to C as $r \to \infty$.)

(iv) Let $C > 0$ and $s \geq 1$ be given and suppose $\frac{\hat{f}_n}{n^s} \to C$. Then, for all primes p and q, the set F_s contains $\frac{f_{pq}}{(pq)^s}$ and

$$\begin{aligned} \frac{f_{pq}}{(pq)^s} &= \frac{\hat{f}_{pq} + \hat{f}_q + \hat{f}_p + \hat{f}_1}{(pq)^s} \quad \text{(by (2.6))} \\ &= \frac{\hat{f}_{pq}}{(pq)^s} + \frac{\hat{f}_q}{q^s} \cdot \frac{1}{p^s} + \frac{\hat{f}_p + \hat{f}_1}{(pq)^s}, \end{aligned}$$

from which we see that if we fix p and let $q \to \infty$, then $\frac{f_{pq}}{(pq)^s} \to C(1 + \frac{1}{p^s})$. So, F_s has infinitely many limit points.

Arguing as we did for (iii), C is a limit point of F_s (and $\left(\frac{f_{p_r}}{p_r^s}\right)$ is a sequence in F_s converging to C).

Finally, for the last sentence of the theorem, let $\frac{\hat{f}_n}{n} \to C$ where $C > 0$. By the Basic Lemma, $\frac{\hat{f}_n}{n}$ is a non-negative integer for each $n \geq 1$. Hence, C is a natural number and $\hat{f}_n = Cn$ eventually. Choose N such that $\hat{f}_n = Cn$ for each $n > N$. Write

$$m(N, r) := (N+1)(N+2)\dots(N+r) \quad \text{for each } r \geq 1.$$

Then, for each $r \geq 1$,

$$\begin{aligned} \frac{f_{m(N,r)}}{m(N,r)} &= \frac{1}{m(N,r)} \sum_{d|m(N,r)} \hat{f}_d \quad \text{(by (2.6))} \\ &\geq \frac{1}{m(N,r)} \sum_{k=1}^{r} C \cdot \frac{m(N,r)}{N+k} \quad \left(\text{since } \tfrac{m(N,r)}{N+k} \text{ divides } m(N,r) \text{ for each } k\right) \\ &= C \sum_{k=1}^{r} \frac{1}{N+k} \quad \to \infty \quad \text{as} \quad r \to \infty, \end{aligned}$$

completing the proof of (iv) and the theorem. □

Remark 4.2 For the sake of completeness, let us deal with the statements in the last theorem when s takes values other than those mentioned.

1. If $s = 1$, then (i) is false: define f by $\hat{f}_n = n$ for each $n \geq 1$; $f \in \mathcal{ER}$ by the Basic Lemma; $\hat{F}_1$ is bounded since $\hat{F}_1 = \{1\}$; however, F_1 is unbounded by (iv).

   As for (iii), Theorem 5.1(ii) shows that there is no exactly realizable sequence f for which $\frac{f_n}{n}$ has a positive limit.

2. Now let $s < 1$. The facts are: (i) holds for $0 \leq s < 1$ but not for $s < 0$; (ii) holds for $0 < s < 1$ but not for $s \leq 0$; (iii) is false for $s = 0$, but for $0 < s < 1$ or $s < 0$ we have (iii) trivially true because $\frac{f_n}{n^s}$ cannot have a positive limit; (iv) is trivially true for $s < 1$ because $\frac{\hat{f}_n}{n^s}$ cannot have a positive limit. The arguments, being simple, are omitted.

Chapter 5

Realization in Rate

The concern of this chapter is whether, given a sequence ϕ of non-negative real numbers, there is an exactly realizable sequence f which is like ϕ in the following sense: ϕ_n and f_n are both positive or both 0 for all sufficiently large n; for ϕ not eventually 0, the ratio of the positive terms of ϕ and f tends to 1. To help discuss this, the next definition gives some notation.

5.1 Definitions and basic properties

Definition 5.1 Let χ and ϕ be an arbitrary pair of sequences in $\mathbf{R}^+$.

(i) Write $\chi \smile \phi$ when the following holds: if ϕ has infinitely many positive terms and (ϕ_{n_m}) is the subsequence of ϕ consisting of these terms, then $\frac{\chi_{n_m}}{\phi_{n_m}} \to 1$ as $m \to \infty$.

(ii) Write $\chi \frown \phi$ when there is an $N \in \mathbf{N}$ such that, for each $n > N$, $\phi_n = 0$ implies that $\chi_n = 0$.

(iii) Write $\chi \asymp \phi$ when $\chi \smile \phi$ and $\chi \frown \phi$.

Some trivial consequences of this definition are:

$$\phi \text{ is eventually 0 if and only if } \chi \smile \phi \text{ for each } \chi; \tag{5.1}$$

$$\phi \text{ is eventually 0 if and only if } \phi \frown \chi \text{ for each } \chi; \tag{5.2}$$

$$\text{if } \phi \text{ is eventually 0 and } \phi \smile \chi, \text{ then } \chi \text{ is eventually 0.} \tag{5.3}$$

For a flavour of how easy the arguments are for these, consider (5.1): for the 'only if' part, note that if ϕ is eventually 0, then ϕ fails the 'if' part in the condition defining $\smile$; for the 'if' part, choose χ to be the zero sequence; we must have ϕ eventually 0, otherwise $\frac{\chi_{n_m}}{\phi_{n_m}}$ would be 0 for each m and the limit condition in Definition 5.1(i) would fail. By (5.1), in discussing whether '$\chi \smile \phi$' holds for χ and ϕ, it will from now be assumed that ϕ is not eventually 0.

Notation 5.1 For each sequence ϕ of non-negative real numbers, which is not eventually 0, write ϕ^+ for the subsequence of ϕ consisting of the positive terms of ϕ. So, ϕ_n^+ is the n-th positive term of ϕ.

Although trivial, the next lemma will be useful. It shows that just the one symbol $\smile$ could have been used to define $\asymp$. However, two symbols have been preferred in Definition 5.1(iii) because $\frown$ is a simpler relation than $\smile$.

Lemma 5.1 (i) *If $\chi \smile \phi$, then $\phi \frown \chi$.*

(ii) *If $\chi \smile \phi$ and $\chi \frown \phi$, then $\phi \smile \chi$.*

(iii) *$\chi \asymp \phi$ if and only if $\chi \smile \phi$ and $\phi \smile \chi$.*

Proof. (i) Let $\chi \smile \phi$. If ϕ is eventually 0, then we are done by (5.2). Suppose ϕ is not eventually 0 and let $\phi^+ = (\phi_{n_m})$. Since $\chi \smile \phi$, we see from Definition 5.1(i) that $\frac{\chi_{n_m}}{\phi_{n_m}} \to 1$ as $m \to \infty$. Since this limit is positive, χ_{n_m} is positive for all m sufficiently large. Choose $M \in \mathbf{N}$ such that

$$\chi_{n_m} > 0 \text{ for each } m > M. \tag{5.4}$$

Now, suppose $\phi_n > 0$ for some $n > n_M$. Then, since $\phi^+ = (\phi_{n_m})$, there is an m with $n = n_m > n_M$. For such an m, we have $m > M$ and, hence, χ_{n_m} is positive by (5.4). Therefore, we have shown that

$$\text{for each } n > n_M, \text{ we have } \chi_n > 0 \text{ if } \phi_n > 0. \tag{5.5}$$

Whence, by Definition 5.1(ii), $\phi \frown \chi$.

(ii) Let $\chi \smile \phi$, $\chi \frown \phi$ and $\chi^+ = (\chi_{j_i})$. By Definition 5.1(ii), choose N such that for each $n > N$ we have $\chi_n = 0$ if $\phi_n = 0$. Since $\chi \smile \phi$, the discussion leading to (5.5) applies. Thus, if n is larger than each of N and n_M, then χ_n and ϕ_n are both zero or both positive. Hence, there exist $s, t \in \mathbf{N}$ such that $j_{m+t} = n_{m+s}$ for each $m \geq 1$. Therefore,

$$\lim_{i\to\infty} \frac{\phi_{j_i}}{\chi_{j_i}} = \lim_{m\to\infty} \frac{\phi_{n_m}}{\chi_{n_m}},$$

which equals 1 since $\chi \smile \phi$. So, $\phi \smile \chi$ by Definition 5.1(i), proving (ii).

(iii) By Definition 5.1(iii), $\chi \asymp \phi$ if and only if $\chi \smile \phi$ and $\chi \frown \phi$, which, by (i) and (ii), hold if and only if $\chi \smile \phi$ and $\phi \smile \chi$. □

The next fact will not be used until Lemma 5.7. It is placed here because it is basic and will help a little more in getting used to the notation.

Lemma 5.2 *Let (n_m) be a subsequence of (n). If $\chi \smile \phi$, then $(\chi_{n_m}) \smile (\phi_{n_m})$. The same holds on writing $\asymp$ for $\smile$.*

Proof. Let $\phi^+ = (\phi_{j_i})$ and $(\phi_{n_m})^+ = (\phi_{n_{m_l}})$. Suppose $\chi \smile \phi$ so that, by Definition 5.1(i), $\frac{\chi_{j_i}}{\phi_{j_i}} \to 1$ as $i \to \infty$. The same goes for $\frac{\chi_{n_{m_l}}}{\phi_{n_{m_l}}}$ as $l \to \infty$ because (n_{m_l}) is a subsequence of (j_i). Hence, $(\chi_{n_m}) \smile (\phi_{n_m})$, proving the first part.

For $\asymp$, let $\chi \asymp \phi$. So, by Lemma 5.1(iii), $\chi \smile \phi$ and $\phi \smile \chi$. Hence, by the above, $(\chi_{n_m}) \smile (\phi_{n_m})$ and $(\phi_{n_m}) \smile (\chi_{n_m})$. Thus, on using Lemma 5.1(iii) again, $(\chi_{n_m}) \asymp (\phi_{n_m})$. □

Lemma 5.3 (i) *Both $\smile$ and $\frown$ are reflexive.*

(ii) *Both $\smile$ and $\frown$ are transitive.*

(iii) *The relation $\asymp$ is an equivalence relation.*

Proof. Let ϕ, χ and ψ be sequences in $\mathbf{R}^+$.

(i) For each ϕ, choose $N = 1$ in the definition of $\frown$ to see that $\phi \frown \phi$. For each ϕ, we have $\phi \smile \phi$ because $1 = \frac{\phi_{n_m}}{\phi_{n_m}}$ in the definition of $\smile$.

(ii) Suppose $\phi \smile \chi$ and $\chi \smile \psi$. We need show $\phi \smile \psi$. Let $\psi^+ = (\psi_{n_m})$. Since $\chi \smile \psi$, we see from (5.3) that χ is not eventually 0. Let $\chi^+ = (\chi_{r_k})$. By $\phi \smile \chi$ and $\chi \smile \psi$,

$$\frac{\phi_{r_k}}{\chi_{r_k}} \to 1 \quad \text{as} \quad k \to \infty \quad \text{and} \tag{5.6}$$

$$\frac{\chi_{n_m}}{\psi_{n_m}} \to 1 \quad \text{as} \quad m \to \infty. \tag{5.7}$$

By (5.7), $\chi_{n_m} > 0$ for all m sufficiently large. This has two consequences. Firstly, since $\chi^+ = (\chi_{r_k})$, there is an $s \in \mathbf{N}$ such that (n_{m+s}) is a subsequence of (r_k); so, by (5.6),

$$\frac{\phi_{n_m}}{\chi_{n_m}} \to 1 \quad \text{as} \quad m \to \infty. \tag{5.8}$$

Secondly, for all m sufficiently large,

$$\frac{\phi_{n_m}}{\psi_{n_m}} = \frac{\phi_{n_m}}{\chi_{n_m}} \cdot \frac{\chi_{n_m}}{\psi_{n_m}}.$$

Here, let $m \to \infty$ and use (5.8) with (5.7) to see that $\frac{\phi_{n_m}}{\psi_{n_m}} \to 1$. So, $\phi \smile \psi$, showing that $\smile$ is transitive.

Now let $\phi \frown \chi$ and $\chi \frown \psi$. By the definition of $\frown$, choose N_1 and N_2 such that:

$$\text{for each } n > N_1 \quad \text{if } \chi_n = 0, \text{ then } \phi_n = 0; \tag{5.9}$$

$$\text{for each } n > N_2 \quad \text{if } \psi_n = 0, \text{ then } \chi_n = 0. \tag{5.10}$$

Let $n > \max\{N_1, N_2\}$ and suppose $\psi_n = 0$. Then, $\chi_n = 0$ from (5.10). Hence, $\phi_n = 0$ from (5.9). So, $\phi \frown \psi$, proving (ii).

(iii) The easiest way to see this is to use Lemma 5.1(iii): symmetry is immediate; since $\smile$ is reflexive by (i) and transitive by (ii), the same goes for $\asymp$. □

Definition 5.2 Let ϕ be a sequence of non-negative real numbers. Then ϕ is *realizable in rate* if there is an exactly realizable sequence f such that $f \asymp \phi$.

Phrases such as 'f realizes ϕ in rate', 'ϕ is realized in rate by f' and '$f\mathcal{R}\phi$' will mean that $f \in \mathcal{ER}$ and $f \asymp \phi$. Denote by $\mathcal{RR}$ the set of sequences which are realizable in rate. Thus,

$$\mathcal{RR} = \{\phi\colon \phi \text{ is a sequence in } \mathbf{R}^+ \text{ and } f\mathcal{R}\phi \text{ for some } f \in \mathcal{ER}\}.$$

By Lemma 5.3, the relation $\asymp$ is reflexive on sequences in $\mathbf{R}^+$. So, by Definition 5.2, $f\mathcal{R}f$ for each $f \in \mathcal{ER}$. Thus, $\mathcal{ER} \subseteq \mathcal{RR}$. Easy examples show that $\mathcal{RR}$ contains elements which $\mathcal{ER}$ does not, and that there are sequences in $\mathbf{R}^+$ which are not elements of $\mathcal{RR}$. In Section 5.4 some tests are given for membership of $\mathcal{RR}$. By Definition 5.2, $\mathcal{RR}$ contains non-integer sequences as well as integer sequences. A basic question is: Are the non-integer sequences in $\mathcal{RR}$ any more interesting than the integer sequences? The answer is 'No', and is easily arrived at by the next lemma and the corollary to it.

Notation 5.2 For each $x \in \mathbf{R}$ write $\grave{x}$ for the nearest integer to x. In other words $\grave{x}$ is the unique integer such that $x - 1/2 < \grave{x} \leq x + 1/2$. Thus,

$$\left|\frac{\grave{x}}{x} - 1\right| \leq \frac{1}{2x} \quad \text{for each } x > 0. \tag{5.11}$$

Let ϕ be a sequence in $\mathbf{R}^+$. Write $\grave{\phi}$ for the sequence whose n-th term, $\grave{\phi}_n$, is the nearest integer to ϕ_n. Since $\grave{x} = 0$ when $x = 0$, we have $\grave{\phi} \frown \phi$.

Lemma 5.4 *Let f and ϕ be sequences in $\mathbf{Z}^+$ and $\mathbf{R}^+$, respectively.*

(i) *Suppose ϕ is not eventually* 0 *and $\phi^+ = (\phi_{n_m})$. If $f \smile \phi$, then each convergent subsequence of (ϕ_{n_m}) has its limit in $\mathbf{N}$.*

(ii) *If $f \smile \phi$, then $\grave{\phi} \smile \phi$.*

(iii) *$f \asymp \phi$ if and only if* (a) *$\grave{\phi} \smile \phi$ and* (b) *$f \asymp \grave{\phi}$.*

(iv) *With ϕ as in* (i), *let $\phi_{n_m} \to \infty$ as $m \to \infty$. Then, $f \asymp \phi$ if and only if $f \asymp \grave{\phi}$.*

Proof. (i) Let $f \smile \phi$. So, by Definition 5.2(i),

$$\frac{f_{n_m}}{\phi_{n_m}} \to 1 \quad \text{as} \quad m \to \infty. \tag{5.12}$$

Suppose $(\phi_{n_{m_r}})$ is a subsequence of (ϕ_{n_m}) and that $\phi_{n_{m_r}} \to L$ as $r \to \infty$. Writing $f_{n_{m_r}} = (f_{n_{m_r}}/\phi_{n_{m_r}})\phi_{n_{m_r}}$ and, using (5.12), $f_{n_{m_r}} \to 1.L = L$ as $r \to \infty$. Since f is a sequence in $\mathbf{Z}^+$, we know $L \in \mathbf{Z}^+$. Also, by (5.12), $f_{n_m} = 0$ for at most finitely many m. Hence, $f_{n_{m_r}} \in \mathbf{N}$ for all r sufficiently large. Thus, $L \neq 0$. So, $L \in \mathbf{N}$, proving (i).

(ii) Let $f \smile \phi$ and $\phi^+ = (\phi_{n_m})$. Seeking a contradiction, suppose that $\grave{\phi} \not\smile \phi$. By the definition of $\smile$, it follows that $\left|\frac{\grave{\phi}_{n_m}}{\phi_{n_m}} - 1\right| \not\to 0$ as $m \to \infty$. Choose $\epsilon > 0$ and a subsequence $(\phi_{n_{m_l}})$ of (ϕ_{n_m}) such that

$$\left|\frac{\grave{\phi}_{n_{m_l}}}{\phi_{n_{m_l}}} - 1\right| > \epsilon \quad \text{for each} \quad l \geq 1. \tag{5.13}$$

Thus, by (5.11), $\phi_{n_{m_l}} < 1/2\epsilon$ for each $l \geq 1$. By the Bolzano-weierstrass Theorem, the bounded sequence $(\phi_{n_{m_l}})$ has a convergent subsequence $(\phi_{n_{m_{l_k}}})$ whose limit, by (i), must be a natural number N, say. In that case, $\grave{\phi}_{n_{m_{l_k}}} = N$ for all k sufficiently large. Hence, $\frac{\grave{\phi}_{n_{m_{l_k}}}}{\phi_{n_{m_{l_k}}}} \to 1$ as $k \to \infty$. This contradicts (5.13) and proves (ii).

(iii) First recall the simple fact that $\grave{\phi} \frown \phi$ for each ϕ. So, by the definition of $\asymp$, we have $\grave{\phi} \smile \phi$ if and only if $\grave{\phi} \asymp \phi$.

For the 'only if' part, let $f \asymp \phi$. So, $f \smile \phi$ by the definition of $\asymp$. Thus, (a) follows from (ii). Hence, $\grave{\phi} \asymp \phi$ and, since $\asymp$ is symmetric, $\phi \asymp \grave{\phi}$. Since both $f \asymp \phi$ and $\phi \asymp \grave{\phi}$ now hold, the transitivity of $\asymp$ gives (b).

For the converse, let (a) and (b) hold. So, $f \asymp \grave{\phi}$ and $\grave{\phi} \asymp \phi$. Transitivity of $\asymp$ implies $f \asymp \phi$, proving (iii).

(iv) We are given $\phi_{n_m} \to \infty$ as $m \to \infty$. So, by (5.11),

$$\left|\frac{\grave{\phi}_{n_m}}{\phi_{n_m}} - 1\right| \leq \frac{1}{2\phi_{n_m}} \to 0 \quad \text{as} \quad m \to \infty.$$

Thus, $\grave{\phi} \smile \phi$. So, we can delete (a) in (iii) to obtain (iv). □

So, by (iv) of this lemma, there are ϕ for which (iii) can be written more simply. Concerning (iii), let us quickly look at other cases of ϕ. For ϕ not eventually 0, three cases remain:

(I) $\phi_{n_m} < 1/2$ for infinitely many m;

(II) $\phi_{n_m} \geq 1/2$ for all m sufficiently large, and (ϕ_{n_m}) is bounded above;

(III) $\phi_{n_m} \geq 1/2$ for all m sufficiently large, and (ϕ_{n_m}) is neither bounded nor tends to infinity.

Case (I) is dull since $\grave{\phi} \not\smile \phi$ and $f \not\smile \phi$ for each f. So, (iii) holds trivially.

For (II), let u be an upper bound. So, $\frac{1}{u}\left|\grave{\phi}_{n_m} - \phi_{n_m}\right| \leq \left|\frac{\grave{\phi}_{n_m}}{\phi_{n_m}} - 1\right|$ for all m sufficiently large. Thus, in (iii), we can write '$\grave{\phi}_{n_m} - \phi_{n_m} \to 0$ as $m \to \infty$' for (a).

Finally, for (III), it is difficult to see how (a) can be replaced by a simpler condition.

Corollary 5.1 *Let $f \in \mathcal{ER}$ and ϕ be a sequence in $\mathbf{R}^+$. Then $f\mathcal{R}\phi$ if and only if $f\mathcal{R}\grave{\phi}$ and $\grave{\phi} \smile \phi$.*

Proof. We have the proof as soon as we reread Lemma 5.4(iii) and Definition 5.2. □

5.2 On being realized in rate uniquely

Given $\phi \in \mathcal{RR}$, it is of interest to ask whether there is exactly one sequence realizing ϕ in rate. When this is true of ϕ we will say 'ϕ is realized in rate uniquely'. As the next lemma shows, the question is easily answered for some sequences in $\mathcal{RR}$. However, the matter does not seem simple for unbounded sequences which do not tend to infinity. For such sequences, we have examples to give but no detailed study.

Lemma 5.5 (i) *Each bounded sequence ϕ in $\mathcal{RR}$ is realized in rate uniquely by the exactly realizable sequence which equals $\grave{\phi}$ eventually.*

(ii) *If a sequence in $\mathcal{RR}$ tends to infinity, then it is not realized in rate uniquely.*

(iii) *$\mathcal{RR}$ contains sequences which are unbounded and not tending to infinity. Some of these are not realized in rate uniquely and some are.*

Proof. (i) Let ϕ be bounded and in $\mathcal{RR}$. By Definition 5.2, choose $f \in \mathcal{ER}$ with $f \asymp \phi$. Thus, $f \frown \grave{\phi}$ and $f \smile \grave{\phi}$ by Corollary 5.1.

Consider first the easier case of $\grave{\phi}$ being eventually 0. Since $f \frown \grave{\phi}$, the same holds for f. Also, f has divisibilitty because $f \in \mathcal{ER}$. Hence, $f = 0$ by Lemma 2.10(i). This proves (i) when $\grave{\phi}$ is eventually 0.

Suppose now that $\grave{\phi}$ is not eventually 0 and let $(\grave{\phi})^+ = (\grave{\phi}_{n_m})$. Since ϕ is bounded, so is $\grave{\phi}$. Let u be an upper bound for $\grave{\phi}$. Then, for each $m \geq 1$,

$$\frac{1}{u}\left|f_{n_m} - \grave{\phi}_{n_m}\right| \leq \left|\frac{f_{n_m}}{\grave{\phi}_{n_m}} - 1\right|.$$

Here, let $m \to \infty$. The right hand side tends to 0 because $f \smile \grave{\phi}$. Thus, $f_{n_m} - \grave{\phi}_{n_m} \to 0$ as $m \to \infty$. But f and $\grave{\phi}$ are integer sequences. Hence, $f_{n_m} = \grave{\phi}_{n_m}$ for all m sufficiently large. Combining this with $f \frown \grave{\phi}$, it follows that $f = \grave{\phi}$ eventually.

It remains to show that no other sequence realizes ϕ in rate. If g is such that $g\mathcal{R}\phi$, then $g = \grave{\phi}$ eventually by exactly the argument used for f. Hence, $f = g$ eventually. Also, each of f and g has divisibility because each is in $\mathcal{ER}$. By Lemma 2.10(ii), $f = g$, proving (i).

(ii) Let $\phi \in \mathcal{RR}$ and suppose that ϕ tends to infinity. By Definition 5.2, choose $f \in \mathcal{ER}$ with $f \asymp \phi$. Thus, f tends to infinity. On defining g by $g_n = f_n + 1$ for each $n \geq 1$, it follows that $g \asymp f$. Since $f \asymp \phi$ and $\asymp$ is transitive, we have $g \asymp \phi$. Also, $g \in \mathcal{ER}$ by Corollary 2.2 and Lemma 2.10(ii). So, $g\mathcal{R}\phi$, by Definition 5.2. Hence, ϕ is not realized in rate uniquely.

(iii) Define f by $\hat{f} = (0, 2, 0, 4, 0, 6, 0, 8, \ldots)$. So, $f \in \mathcal{ER} \subseteq \mathcal{RR}$ by the Basic Lemma. By (2.6), $f_n = 0$ for odd n, and $f_n \geq \hat{f}_n \geq n$ for even n. Thus, f is a sequence in $\mathcal{RR}$ which is neither bounded nor tending to infinity. For an example of such a sequence which is not in $\mathcal{ER}$, define k by $k_n = 0$ for odd n, and $k_n = f_n + \sqrt{n}$ for even n. Since $\frac{f_{2n}}{k_{2n}} \to 1$ as $n \to \infty$, and since $f_n = k_n = 0$ for odd n, we have $f \asymp k$. By Definition 5.2, $f\mathcal{R}k$. So, $k \in \mathcal{RR}$.

To see that f is not realized in rate uniquely, define h by $\hat{h}_2 = 4$ and $\hat{h}_n = \hat{f}_n$ for $n \neq 2$. By (2.6), $h_n = f_n = 0$ for odd n. Thus, $h \frown f$. By (2.6) again, $h_n = f_n + 2$ for even n. So, for even n,

$$\frac{h_n}{f_n} = \frac{f_n + 2}{f_n} = 1 + \frac{2}{f_n} \to 1 \quad \text{as} \quad n \to \infty.$$

Hence, $h \smile f$. Also, $h \in \mathcal{ER}$ by the Basic Lemma. Therefore, $h\mathcal{R}f$ by Definition 5.2, showing that f is not realized in rate uniquely.

We now give an unbounded sequence, not tending to infinity, and realized in rate uniquely. Define $\hat{\phi}$ by $\hat{\phi}_n = n$ if n is an odd prime, and $\hat{\phi}_n = 0$ for all other n. By the Basic Lemma, $\phi \in \mathcal{ER}$. So, $\phi\mathcal{R}\phi$. Using (2.6), the following table is obtained.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\hat{\phi}_n$	0	0	3	0	5	0	7	0	0	0	11	0	13	0	0	0
ϕ_n	0	0	3	0	5	3	7	0	3	5	11	3	13	7	8	0

Let $\psi\mathcal{R}\phi$. By Definition 5.2, $\psi \in \mathcal{ER}$, $\psi \frown \phi$ and $\psi \smile \phi$. The following will be proved:

(a) $\phi_{2^k r} = \phi_r$ for all $k \geq 0$ and $r \geq 1$;

(b) for each fixed $r \geq 1$ we have $\psi_{2^k r} = \phi_r$ for all k sufficiently large;

(c) $\hat{\psi}_1 = \hat{\phi}_1$ and $\hat{\psi}_p = \hat{\phi}_p$ for each prime p;

(d) $\hat{\psi}_c = \hat{\phi}_c$ for each composite c.

By (c) and (d), we will have $\hat{\psi} = \hat{\phi}$ which, by (2.6), will prove that $\psi = \phi$.

(a) By (2.6), for each $r \geq 1$,

$$\phi_{2r} = \sum_{d|2r} \hat{\phi}_d = \sum_{d|2r;d\not| r} \hat{\phi}_d + \sum_{d|r} \hat{\phi}_d = \sum_{d|2r;d\not| r} \hat{\phi}_d + \phi_r. \tag{5.14}$$

If $d|2r$ and $d\not| r$, then d is even. By definition, $\hat{\phi}_d = 0$ for such d. So, the last sigma sum in (5.14) is 0. Hence, $\phi_{2r} = \phi_r$ for each $r \geq 1$, and a trivial induction leads to (a).

(b) Let $r \geq 1$ be given. Suppose first that $\phi_r = 0$. Thus, by (a), $\phi_{2^k r} = 0$ for each $k \geq 0$. So, by $\psi \frown \phi$, we have $\psi_{2^k r} = 0$ for all k sufficiently large. This proves (b) when $\phi_r = 0$. Now suppose that $\phi_r > 0$. Using (a) and $\psi \smile \phi$,

$$\frac{\psi_{2^k r}}{\phi_r} = \frac{\psi_{2^k r}}{\phi_{2^k r}} \to 1 \quad \text{as} \quad k \to \infty.$$

So, $\psi_{2^k r} \to \phi_r$ as $k \to \infty$. Here, note that ϕ is a sequence in $\mathbf{Z}^+$ and the same goes for ψ since $\psi \in \mathcal{ER}$. Hence, (b) holds.

(c) By definition, $\phi_1 = 0$. Thus, by (b), $\psi_{2^k} = 0$ for all k sufficiently large. Also, by (2.6), $\psi_{2^k} = \sum_{0 \leq i \leq k} \hat{\psi}_{2^i}$ for each $k \geq 0$. Therefore, by the positivity of ψ,

$$\hat{\psi}_{2^i} = 0 \quad \text{for each} \quad i \geq 0. \tag{5.15}$$

In particular, $0 = \hat{\psi}_1 = \hat{\psi}_2$. So, $\hat{\psi}_1 = \hat{\phi}_1$ and $\hat{\psi}_2 = \hat{\phi}_2$. Suppose now that p is an odd prime. By (b), choose $\kappa \geq 1$ with

$$\begin{aligned} \phi_p = \psi_{2^\kappa p} &= \sum_{d|2^\kappa p} \hat{\psi}_d \quad \text{(by (2.6))} \\ &= \sum_{i=0}^{\kappa} \left(\hat{\psi}_{2^i} + \hat{\psi}_{2^i p}\right) \\ &= \sum_{i=0}^{\kappa} \hat{\psi}_{2^i p} \quad \text{(by (5.15))}. \end{aligned} \tag{5.16}$$

Now, by the definition of ϕ and (2.6), $\phi_p = \hat{\phi}_1 + \hat{\phi}_p = p$. So, by (5.16),

$$p = \hat{\psi}_p + \sum_{i=1}^{\kappa} \hat{\psi}_{2^i p}, \tag{5.17}$$

from which it is easily deduced that $\sum_{i=1}^{\kappa} \hat{\psi}_{2^i p} = 0$: by the Basic Lemma, $\hat{\psi} \geq 0$ and $\hat{\psi}_{2^i p} = 0$ or $\hat{\psi}_{2^i p} \geq 2^i p$ for each $i \geq 1$; in (5.17), since $\hat{\psi}_p \geq 0$, equality fails if $\hat{\psi}_{2^i p} \geq 2^i p > p$ for some i with $1 \leq i \leq \kappa$; so, $\hat{\psi}_{2^i p} = 0$ for these i, with the result that $\sum_{i=1}^{\kappa} \hat{\psi}_{2^i p} = 0$. Hence, $p = \hat{\psi}_p$ by (5.17). Also, $\hat{\phi}_p = p$ by definition. Thus, $\hat{\phi}_p = \hat{\psi}_p$, proving (c).

(d) For a quick contradiction, suppose (d) is false. Let c be the least composite number with $\hat{\psi}_c \neq \hat{\phi}_c$. Since $\hat{\phi}_c = 0$ by definition, and $\psi \geq 0$, we have $\hat{\psi}_c > 0$. So,

$$\begin{aligned} \psi_c &= \hat{\psi}_c + \sum_{d|c;d\neq c} \hat{\psi}_d \quad \text{(by (2.6))} \\ &= \hat{\psi}_c + \sum_{d|c;d\neq c} \hat{\phi}_d \quad \text{(by (c) and the definition of } c) \\ &= \hat{\psi}_c + \phi_c \quad \text{(using } \hat{\phi}_c = 0 \text{ and (2.6))} \\ &> \phi_c \quad \text{(since } \hat{\psi}_c > 0) \\ &= \psi_{2^k c} \text{ for some } k \geq 1 \quad \text{(by (b))} \\ &\geq \psi_c \quad \text{(by (2.6))}, \end{aligned}$$

giving the falsehood that $\psi_c > \psi_c$. This proves (d). Thus, no sequence except ϕ can realize ϕ in rate. □

5.3 Algebra in $\mathcal{RR}$

In this section we show how elements of $\mathcal{RR}$ may be combined.

Lemma 5.6 *Let θ, ϑ, ϕ and φ be sequences in $\mathbf{R}^+$.*

(i) *If $\theta \smile \vartheta$ and $\phi \smile \varphi$, then $\theta\phi \smile \vartheta\varphi$.*

(ii) *If $\theta \asymp \vartheta$ and $\phi \asymp \varphi$, then $\theta\phi \asymp \vartheta\varphi$.*

(iii) *$\mathcal{RR}$ is closed under multiplication.*

(iv) *$\theta \asymp \vartheta$ if and only if $\theta + \phi \smile \vartheta + \phi$ for each sequence ϕ in $\mathbf{R}^+$.*

(v) *If $\theta \asymp \vartheta$ and $\phi \asymp \varphi$, then $\theta + \phi \asymp \vartheta + \varphi$.*

(vi) *$\mathcal{RR}$ is closed under addition.*

Proof. (i) Suppose $\theta \smile \vartheta$ and $\phi \smile \varphi$. Let $(\vartheta\varphi)^+ = (\vartheta_{n_m}\varphi_{n_m})$. Hence, ϑ_{n_m} is positive for each m. Thus, (ϑ_{n_m}) is a subsequence of ϑ^+. Since $\theta \smile \vartheta$, we have $\frac{\theta_{n_m}}{\vartheta_{n_m}} \to 1$ as $m \to \infty$. By similar reasoning, the same goes for $\frac{\phi_{n_m}}{\varphi_{n_m}}$. So,

$$\frac{\theta_{n_m}\phi_{n_m}}{\vartheta_{n_m}\varphi_{n_m}} = \frac{\theta_{n_m}}{\vartheta_{n_m}} \cdot \frac{\phi_{n_m}}{\varphi_{n_m}} \to 1 \cdot 1 = 1 \quad \text{as} \quad m \to \infty,$$

showing that $\theta\phi \smile \vartheta\varphi$.

(ii) Let $\theta \asymp \vartheta$ and $\phi \asymp \varphi$. By Lemma 5.1(iii), the following hold:

$$\theta \smile \vartheta; \quad \vartheta \smile \theta; \qquad \phi \smile \varphi; \quad \varphi \smile \phi.$$

Pairing the first of these with the third, the second with the fourth, and using (i), leads to $\theta\phi \smile \vartheta\varphi$ and $\vartheta\varphi \smile \theta\phi$. By Lemma 5.1(iii) again, the result follows.

(iii) Let $\vartheta, \varphi \in \mathcal{RR}$. By Definition 5.2, choose $f, g \in \mathcal{ER}$ with $f \asymp \vartheta$ and $g \asymp \varphi$. By (ii), $fg \asymp \vartheta\varphi$. Also, $fg \in \mathcal{ER}$ by Lemma 2.10(iii). Thus, by Definition 5.2, fg realizes $\vartheta\varphi$ in rate. So, $\vartheta\varphi \in \mathcal{RR}$.

(iv) For the 'only if' part suppose $\theta \asymp \vartheta$ and ϕ is a sequence in $\mathbf{R}^+$. By Definition 5.1(iii), $\theta \smile \vartheta$ and $\theta \frown \vartheta$. Let $(\vartheta + \phi)^+ = (\vartheta_{n_m} + \phi_{n_m})$ and write

$$\psi_m := \left| \frac{\theta_{n_m} + \phi_{n_m}}{\vartheta_{n_m} + \phi_{n_m}} - 1 \right| = \left| \frac{\theta_{n_m} - \vartheta_{n_m}}{\vartheta_{n_m} + \phi_{n_m}} \right| \quad \text{for each } m \geq 1. \tag{5.18}$$

By Definition 5.1(i), we need show $\psi_m \to 0$ as $m \to \infty$. Consider large m. First, let m run through the zeros of (ϑ_{n_m}). Then, $\theta_{n_m} = 0$ because $\theta \frown \vartheta$. Also, $\phi_{n_m} > 0$ because $\vartheta_{n_m} + \phi_{n_m} > 0$. Hence, by (5.18), $\psi_m = 0$ for these m. Now let m run through the positive values of (ϑ_{n_m}). By (5.18), for each $m \geq 1$,

$$\psi_m \leq \left| \frac{\theta_{n_m} - \vartheta_{n_m}}{\vartheta_{n_m}} \right| = \left| \frac{\theta_{n_m}}{\vartheta_{n_m}} - 1 \right|,$$

which tends to 0 as $m \to \infty$ because $\theta \smile \vartheta$. Thus, $\psi_m \to 0$ as $m \to \infty$, proving the 'only if' part.

For the converse, let $\theta + \phi \smile \vartheta + \phi$ for each sequence ϕ in $\mathbf{R}^+$. With $\phi = 0$ we have $\theta \smile \vartheta$. Therefore, by the definition of $\asymp$, we need just show that $\theta \frown \vartheta$. This is trivial for ϑ eventually positive. Otherwise, let (ϑ_{n_k}) be the subsequence of (ϑ_n) consisting of the zero terms of (ϑ_n). Suppose for a contradiction that $\theta \not\frown \vartheta$. Choose a subsequence $(\theta_{n_{k_r}})$ of (θ_{n_k}) such that $\theta_{n_{k_r}} > 0$ for each $r \geq 1$. Choose any sequence ϕ in $\mathbf{R}^+$ with $\phi_{n_{k_r}} = \theta_{n_{k_r}}$ for each $r \geq 1$. Write

$$\chi_r := \left| \frac{\theta_{n_{k_r}} + \phi_{n_{k_r}}}{\vartheta_{n_{k_r}} + \phi_{n_{k_r}}} - 1 \right| \qquad \text{for each } r \geq 1.$$

Note that $(\vartheta_{n_{k_r}} + \phi_{n_{k_r}})$ is a subsequence of $(\vartheta + \phi)^+$ because

$$\vartheta_{n_{k_r}} + \phi_{n_{k_r}} = \phi_{n_{k_r}} = \theta_{n_{k_r}} > 0 \quad \text{for each } r \geq 1.$$

Therefore, since $\theta + \phi \smile \vartheta + \phi$, we require $\chi_r \to 0$ as $r \to \infty$. However, by the choice of ϕ, we have $\chi_r = \left| \frac{\phi_{n_{k_r}} + \phi_{n_{k_r}}}{0 + \phi_{n_{k_r}}} - 1 \right| = 1$ for each $r \geq 1$. This contradiction proves $\theta \frown \vartheta$ and establishes (iv).

(v) Let $\theta \asymp \vartheta$ and $\phi \asymp \varphi$. So, $\vartheta \asymp \theta$ and $\varphi \asymp \phi$ because $\asymp$ is symmetric. Using (iv), on each of these relationshps in turn, results in:

$$\theta + \phi \smile \vartheta + \phi; \quad \vartheta + \phi \smile \vartheta + \varphi; \qquad \vartheta + \varphi \smile \theta + \varphi; \quad \theta + \varphi \smile \theta + \phi.$$

Since $\smile$ is transitive, the first and second of these imply $\theta + \phi \smile \vartheta + \varphi$. Similarly, the third and fourth imply $\vartheta + \varphi \smile \theta + \phi$. By Lemma 5.1(iii), the result follows.

(vi) Let f, g, ϑ and φ be as in (iii). By (v), $f + g \asymp \vartheta + \varphi$. By Lemma (2.10)(ii), $f + g \in \mathcal{ER}$. Thus, $f + g$ realizes $\vartheta + \varphi$ in rate. So, $\vartheta + \varphi \in \mathcal{RR}$. $\square$

Two simple facts involving $\frown$, and similar to (i) of the above lemma, are: (a) If $\theta \frown \vartheta$ and $\phi \frown \varphi$, then $\theta\phi \frown \vartheta\varphi$; (b) If $\theta \frown \vartheta$ and $\phi \frown \varphi$, then $\theta + \phi \frown \vartheta + \varphi$. It is easy to see that (ii) of the lemma follows from (i) and (a), and (v) follows from (iv) and (b).

Simple examples show that $\mathcal{RR}$ is neither closed under division nor under subtraction. Two not so simple ones are as follows: respectively, let θ, ϕ, χ and ψ be the sequences $(2^n), (n+2^n), (n^2)$ and (n^3); $\theta \in \mathcal{RR}$ because $\theta \in \mathcal{ER}$ by Lemma 2.9; $\phi \in \mathcal{RR}$ because $\theta \mathcal{R} \phi$; Corollary 5.2(ii) will show that $\chi, \psi \in \mathcal{RR}$; however, Corollary 5.2(i) will show that $\phi - \theta = \psi/\chi = (n) \notin \mathcal{RR}$.

5.4 Criteria for $\mathcal{RR}$

The next lemma shows that each sequence in $\mathcal{RR}$ has many subsequences which are also in $\mathcal{RR}$. This unsurprising lemma will help in the proof of Theorem 5.1(ii).

Lemma 5.7 *For each $K \in \mathbf{N}$ and each sequence ϕ in $\mathbf{R}^+$ write $\phi^{[K]}$ for the sequence $(\phi_K, \phi_{2K}, \phi_{3K}, \phi_{4K}, \ldots)$. Suppose $\phi \in \mathcal{RR}$ and f realizes ϕ in rate. Then $f^{[K]}$ realizes $\phi^{[K]}$ in rate for each $K \geq 1$.*

Proof. Suppose $f \mathcal{R} \phi$ and $K \in \mathbf{N}$. By Definition 5.2, $f \in \mathcal{ER}$ and $f \asymp \phi$. By (2.16), $f^{[K]} \in \mathcal{ER}$. Also, $f^{[K]} \asymp \phi^{[K]}$ by Lemma 5.2. Hence, $f^{[K]} \mathcal{R} \phi^{[K]}$ by Definition 5.2. □

Theorem 5.1 *Let ϕ be a sequence in $\mathbf{R}^+$, not eventually 0 with $\phi^+ = (\phi_{n_m})$.*

(i) *If for each natural number N there are $d, n > N$ such that $d | n, \phi_d > 0$ and $\phi_n = 0$, then ϕ is not realizable in rate.*

(ii) *Let $c > 0$ and suppose that $\phi_{n_m} = cn_m$ for each $m \geq 1$. Then ϕ is not realizable in rate.*

(iii) *If ϕ is unbounded and there is an $l > 1$ such that $\frac{n_m}{\phi_{n_m}} > l$ for all m sufficiently large, then ϕ is not realizable in rate.*

(iv) *For each* $n \geq 1$ *write* σ_n *for the sum of the divisors of* n. *Define a sequence* f *by* $\hat{f}_n = n\left(\frac{\hat{\phi}_n}{n}\right)^{\grave{}}$ *for each* $n \geq 1$. *If* (a) $\hat{\phi} \geq 0$ *and* (b) $\frac{\sigma_{n_m}}{\phi_{n_m}} \to 0$ *as* $m \to \infty$, *then* (c) f *realizes* ϕ *in rate.*

(v) *For each* $n \in \mathbf{N}$, *let*

$$\dot{\phi}_n := \begin{cases} -\sum_{d|n;\hat{\phi}_d<0} \hat{\phi}_d & \textit{if } \hat{\phi}_d < 0 \textit{ for some } d \textit{ dividing } n, \\ 0 & \textit{otherwise.} \end{cases}$$

Define a sequence f *by*

$$\hat{f}_n = \begin{cases} n\left(\frac{\hat{\phi}_n}{n}\right)^{\grave{}} & \textit{if } \hat{\phi}_n \geq 0, \\ 0 & \textit{otherwise.} \end{cases}$$

Suppose ϕ *is eventually positive. If* $\dot{\phi}_n = O(\sigma_n)$ *and* $\sigma_n = o(\phi_n)$, *then* f *realizes* ϕ *in rate.*

Proof. (i) The contrapositive will be proved. Let $\phi \in \mathcal{RR}$. It will be shown that there is an $N \in \mathbf{N}$ such that for all $d, n > N$ we have $\phi_d = 0$ if $d|n$ and $\phi_n = 0$. The argument is forced by the elementary fact that

$$f \in \mathcal{ER}, f_n = 0 \text{ for some } n \in \mathbf{N} \quad \Rightarrow \quad f_d = 0 \text{ for each } d \text{ dividing } n, \tag{5.19}$$

which is easy to see: let $f \in \mathcal{ER}$, $f_n = 0$ for some n and $d|n$; so, $\sum_{\delta|n} \hat{f}_\delta = 0$ by (2.6); by (2.9), $\hat{f}_\delta = 0$ for each δ dividing n; hence, $\sum_{\delta|d} \hat{f}_\delta = 0$ since each divisor of d is a divisor of n; and since $f_d = \sum_{\delta|d} \hat{f}_\delta$ by (2.6), we have proved (5.19).

Turning to $\phi \in \mathcal{RR}$, choose $f \in \mathcal{ER}$ with $f \asymp \phi$. Choose N such that,

$$\text{for each } n > N, \text{ we have } f_n \text{ and } \phi_n \text{ both 0 or both positive.} \tag{5.20}$$

Suppose now that $d, n > N$ with $d|n$ and $\phi_n = 0$. Thus, $f_n = 0$ by (5.20). Hence, $f_d = 0$ by (5.19) and, since $d > N$, we see from (5.20) that $\phi_d = 0$. This proves (i).

(ii) Suppose $c > 0$ and that $\phi_{n_m} = cn_m$ for each $m \geq 1$. For a contradiction, assume $\phi \in \mathcal{RR}$. By Definition 5.2, choose an $f \in \mathcal{ER}$ such that $f \smile \phi$ and $f \frown \phi$. There are two cases: (I) $\phi = (cn)$ eventually; (II) ϕ has infinitely many zero terms.

Consider case (I) first. It will be seen that the conditions $f \smile \phi$ and (2.10) are the source of a contradiction. Using (2.5), for each prime p and $r \geq 1$,

$$\frac{\hat{f}_{p^r}}{p^r} = \frac{f_{p^r}}{p^r} - \frac{f_{p^{r-1}}}{p^{r-1}p}.$$

Since $f \smile \phi$, we know $\frac{f_n}{cn} \to 1$ as $n \to \infty$. So, fixing p and letting $r \to \infty$, we have $\frac{\hat{f}_{p^r}}{p^r} \to c - c/p$. Now, by (2.10), $\frac{\hat{f}_{p^r}}{p^r}$ is an integer for each $r \geq 1$. Thus, the same goes for $c - c/p$, and on allowing p to go to infinity, we see that c is an integer which is divisible by each p. So, $c = 0$, contradicting the premise that $c > 0$. Whence, for case (I), ϕ is not realizable in rate.

For (II), let $K \in \mathbf{N}$ and note first that

$$\begin{aligned} \phi^{[K]} \quad &:= \quad (\phi_K, \phi_{2K}, \phi_{3K}, \phi_{4K}, \ldots) \quad \text{(as in Lemma 5.7)} \\ &= \quad cK(0 \text{ or } 1,\ 0 \text{ or } 2,\ 0 \text{ or } 3,\ 0 \text{ or } 4, \ldots). \end{aligned} \tag{5.21}$$

This sequence cannot equal (cKn) eventually, for the following reasons: by our assumption, f realizes ϕ in rate; therefore, by Lemma 5.7, $f^{[K]}$ realizes $\phi^{[K]}$ in rate; on noting that cK is positive and using the verdict on (I), we cannot have $\phi^{[K]} = (cKn)$ eventually.

Thus, by (5.21), $\phi^{[K]}$ has infinitely many zero terms. But, $f^{[K]} \frown \phi^{[K]}$ since $f^{[K]}$ realizes $\phi^{[K]}$ in rate. So, $f^{[K]}$ has has infinitely many zero terms. Therefore, using (2.6) and (2.9) on the exactly realizable sequence $f^{[K]}$, we see that $f_1^{[K]} (= f_K) = 0$. This holds for each K. So, $f = 0$. Since $f \smile \phi$ by assumption, it follows that ϕ is eventually 0. However, by hypothesis, ϕ is not eventually 0. This contradiction shows that ϕ is not realizable in rate in case (II), and establishes (ii).

(iii) With ϕ and l as given, suppose for a contradiction that $\phi \in \mathcal{RR}$. By Definition 5.2, choose $f \in \mathcal{ER}$ with $f \smile \phi$ and $f \frown \phi$. Since, by (2.6) and (2.9),

$$\frac{f_{n_m}}{\phi_{n_m}} = \frac{f_{n_m}}{n_m} \cdot \frac{n_m}{\phi_{n_m}} \geq \frac{\hat{f}_{n_m}}{n_m} \cdot \frac{n_m}{\phi_{n_m}} \quad \text{for each } m \geq 1, \tag{5.22}$$

it will suffice to show, as we shall below, that $\frac{\hat{f}_{n_m}}{n_m} \geq 1$ for infinitely many m: it will then follow, by (5.22), that $\frac{f_{n_m}}{\phi_{n_m}} > 1 \cdot l = l > 1$ for infinitely many m; hence, it will be false that $\frac{f_{n_m}}{\phi_{n_m}} \to 1$ as $m \to \infty$, contradicting $f \smile \phi$ and proving (iii).

Since $f \smile \phi$ and ϕ is unbounded, the same holds for f. Hence, $\hat{f}$ has infinitely many positive terms by (2.6) and (2.9). Again by (2.6) and (2.9), $\hat{f} \frown f$. Also, since $f \frown \phi$ and $\frown$ is transitive, it follows that $\hat{f} \frown \phi$. Thus, off the n_m's we can have $\hat{f}$ positive only finitely many times. Whence, $\hat{f}_{n_m}$ is positive for infinitely many m, and for these m we see from (2.10) that $\frac{\hat{f}_{n_m}}{n_m} \geq 1$.

(iv) Let f and σ be as given and suppose that (a) and (b) hold. In order, let us verify that $f \in \mathcal{ER}$, $f \frown \phi$ and $f \smile \phi$. The result will then follow by Definition 5.2. For each $n \geq 1$, we have $\frac{\hat{f}_n}{n} = \left(\frac{\hat{\phi}_n}{n}\right)^{\backprime}$, which is a non-negative integer by (a). Hence, by the Basic Lemma, $f \in \mathcal{ER}$.

Let $\phi_n = 0$ for some $n \geq 1$. By (2.6), $\phi_n = \sum_{d|n} \hat{\phi}_d = 0$. Therefore, by (a) and the definition of $\hat{f}$, we have $\hat{\phi}_d = 0 = \hat{f}_d$ for each d dividing n. Using (2.6) again, $f_n = \sum_{d|n} \hat{f}_d = 0$. Thus, $f \frown \phi$.

For each $n \geq 1$,

$$\begin{aligned} |f_n - \phi_n| &= \left| \sum_{d|n} d \left(\frac{\hat{\phi}_d}{d}\right)^{\backprime} - \hat{\phi}_d \right| \quad \text{(by (2.6) and the definition of } \hat{f}\text{)} \\ &\leq \sum_{d|n} d \left| \left(\frac{\hat{\phi}_d}{d}\right)^{\backprime} - \frac{\hat{\phi}_d}{d} \right| \leq \sum_{d|n} d \cdot \frac{1}{2} = \frac{\sigma_n}{2}. \end{aligned}$$

Hence, $\left|\frac{f_{n_m} - \phi_{n_m}}{\phi_{n_m}}\right| \leq \frac{\sigma_{n_m}}{2\phi_{n_m}}$, which, by (b), tends to 0 as m tends to infinity. So, $f \smile \phi$, proving (iv).

(v) Let $\dot{\phi}$ and f be as given. Suppose that ϕ is eventually positive, $\dot{\phi}_n = O(\sigma_n)$ and $\sigma_n = o(\phi_n)$. Define ψ by

$$\hat{\psi}_n = \begin{cases} \hat{\phi}_n & \text{if } \hat{\phi}_n \text{ is non-negative,} \\ 0 & \text{if } \hat{\phi}_n \text{ is negative.} \end{cases}$$

It will first be shown that $\psi \asymp \phi$ and then, using (iv), that ψ is realized in rate by f. Since $\asymp$ is transitive, the result will then follow. By (2.6) and the definitions of ψ and ϕ,

$$\psi_n = \sum_{d|n} \hat{\psi}_d = \sum_{d|n} \hat{\phi}_d + \dot{\phi}_n = \phi_n + \dot{\phi}_n \quad \text{for each } n \geq 1.$$

Therefore, since ϕ is eventually positive,

$$\frac{\psi_n}{\phi_n} - 1 = \frac{\dot{\phi}_n}{\phi_n} = \frac{\dot{\phi}_n}{\sigma_n} \cdot \frac{\sigma_n}{\phi_n} \quad \text{for all } n \text{ sufficiently large.}$$

Here, since $\dot{\phi}_n = O(\sigma_n)$ and $\sigma_n = o(\phi_n)$, it follows that $\frac{\psi_n}{\phi_n} - 1$ tends to zero as n tends to infinity. Thus, $\psi \asymp \phi$ as claimed.

By the definition of ψ, we have $\hat{\psi} \geq 0$ and $\hat{\psi} \geq \hat{\phi}$. Hence, (iv)(a) holds for ψ. Also, by (2.6), $\psi \geq \phi$. So, ψ must be eventually positive because it is given that ϕ is. Thus, $\sigma_n = o(\psi_n)$ because $\sigma_n = o(\phi_n)$. Hence, (iv)(b) holds for ψ. It is easy to check that $\hat{f}_n = n\grave{\left(\frac{\hat{\psi}_n}{n}\right)}$ for each $n \geq 1$. So, by (iv), f realizes ψ in rate. □

We are now quite well placed to discuss whether some familiar sequences are in $\mathcal{RR}$.

Corollary 5.2 *Let c and s be positive real numbers.*

(i) $(cn^s) \notin \mathcal{RR}$ *for* $0 < s \leq 1$; $\quad (cn^s) \in \mathcal{RR}$ *for* $s > 1$.

(ii) $(cs^n) \in \mathcal{RR}$ *for* $s > 1$.

Before the proof, we should mention that it is because of dullness and not difficulty that some values of s are not referred to in this lemma. Two elementary facts are:

$$\text{given } c \geq 0, \text{ then } (c) \in \mathcal{RR} \text{ if and only if } c \in \mathbf{Z}^+; \tag{5.23}$$

$$\text{if } \phi \in \mathcal{RR} \text{ and } \phi_n \to 0, \text{ then } \phi \text{ is eventually } 0. \tag{5.24}$$

In (5.23), the 'if' part holds because $\mathcal{ER}$ contains all constant sequences in $\mathbf{Z}^+$, and $\mathcal{ER} \subseteq \mathcal{RR}$. For the 'only if' part, Corollary 5.1 requires $(\grave{c}) \smile (c)$. This holds only if $\grave{c} = c$. Hence, $c \in \mathbf{Z}^+$.

For (5.24), let $\phi \in \mathcal{RR}$ and $\phi_n \to 0$. So, $\grave{\phi}$ is eventually 0, and Corollary 5.1 requires $\grave{\phi} \smile \phi$. By, (5.3), ϕ is eventually 0.

Thus, by (5.23), the case $s = 0$ is dull for (i) of this lemma; the same goes for (ii) with $s = 0$ or 1. By (5.24), we know what happens when $s < 0$ in (i); the same goes for (ii) with $0 < s < 1$.

Proof. For (i), let $\phi = (cn^s)$. So, $(n_m) = (m)$ in the notation of Theorem 5.1. With $s = 1$, ϕ is a special case of Theorem 5.1(ii). For $0 < s < 1$, Theorem 5.1(iii) can be used because ϕ is unbounded and $\frac{n}{cn^s} \to \infty$ as $n \to \infty$. This proves the first part of (i).

Let $s > 1$. It will be shown that (a) and (b) of Theorem 5.1(iv) hold. (The argument given here for (a), also works for $s \geq 0$.) Since ϕ is multiplicative, the same goes for $\hat{\phi}$ by (2.1). Thus, on checking that $\hat{\phi}_1 = c > 0$, it will suffice to show that $\hat{\phi}_{p^r} \geq 0$ for each prime p and $r \geq 1$. Now

$$\begin{aligned}\hat{\phi}_{p^r} &= \phi_{p^r} - \phi_{p^{r-1}} \quad \text{(by (2.5))} \\ &= cp^{rs} - cp^{(r-1)s} = cp^{(r-1)s}(p^s - 1) \geq 0 \quad \text{(since } c > 0 \text{ and } s \geq 0).\end{aligned}$$

So, $\hat{\phi} \geq 0$, showing that (a) holds. For reference we record the fact just proved:

$$\widehat{(n^s)} \geq 0 \quad \text{for each } s \geq 0. \tag{5.25}$$

To see that (b) of Theorem 5.1(iv) holds, write

$$\frac{\sigma_n}{cn^s} = \frac{\sigma_n}{n^{1+(s-1)/2}} \cdot \frac{1}{cn^{(s-1)/2}}. \tag{5.26}$$

By HARDY and WRIGHT [6, Theorem 322],

$$\sigma_n = O\left(n^{1+\delta}\right) \text{ for every positive } \delta. \tag{5.27}$$

Writing δ for $(s-1)/2$ and recalling that $s > 1$, we see from (5.26) and (5.27) that $\frac{\sigma_n}{cn^s} \to 0$. Hence, by Theorem 5.1(iv), ϕ is in $\mathcal{RR}$.

(ii) Let $s > 1$. Then, $\frac{\sigma_n}{cs^n} \leq \frac{n^2}{cs^n} \to 0$ as $n \to \infty$. Also, $\widehat{(cs^n)} = c\widehat{(s^n)} \geq 0$ by Corollary 2.8. Hence, by Theorem 5.1(iv), (cs^n) is in $\mathcal{RR}$. □

Corollary 5.3 *Let $r \in \mathbf{N}, c > 0$ and $s \geq 1$. Then $(cn^s[\log n]^r)$ is realizable in rate.*

Note that one cannot expect a proof through some simple use of Lemma 5.6(iii): for each r the sequence $([\log n]^r)$ is unbounded and $\frac{n}{[\log n]^r} \to \infty$ as $n \to \infty$; so, $([\log n]^r)$ is not realizable in rate by Theorem 5.1(iii). The proof of this corollary uses a basic fact about the Mangoldt function Λ, which is defined on the natural numbers by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and some } m \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

So, $\Lambda \geq 0$. Basic reasoning shows (see Apostol [1, Theorem 2.10], for example) that

$$\log n = \sum_{d|n} \Lambda(d) \quad \text{for each } n \geq 1. \tag{5.28}$$

Proof. Theorem 5.1(iv) will be used. Let $\phi = (cn^s[\log n]^r)$ and $\psi = (\log n)$. By (5.25), $\widehat{(cn^s)} = c\widehat{(n^s)} \geq 0$. By (5.28) and the Möbius inversion formula of Theorem 2.1, $\hat{\psi} = \Lambda \geq 0$. We may view ϕ as a product of $r+1$ sequences, r of which are $(\log n)$. Then, using Corollary 2.7(i), a simple induction shows that $\hat{\phi} \geq 0$. Thus, (a) of Theorem 5.1(iv) holds.

For (b) of Theorem 5.1(iv),

$$\frac{\sigma_n}{cn^s[\log n]^r} = \frac{\sigma_n}{n \log\log n} \cdot \frac{n \log\log n}{cn^s[\log n]^r} \quad \text{for each } n \geq 2.$$

Here, the end fraction tends to 0 as $n \to \infty$. Hence, the desired result will follow if we can be sure that the middle fraction is bounded. This is indeed the case: by Hardy and Wright [6, Theorem 323], a more precise fact is that

$$\limsup_{n\to\infty} \frac{\sigma_n}{n \log\log n} = e^{\gamma},$$

where γ is Euler's constant. Thus, by Theorem 5.1(iv), $(cn^s[\log n]^r)$ is in $\mathcal{RR}$. □

Remark 5.1 In Lemma 5.3, consider the general case when r and s are allowed to be real numbers. Since the sequence (cn^s) has been fully discussed, let us assume that r is not 0. For ϕ to continue to be well defined, suppose that for each $r < 0$ we have chosen an $r_1 \in \mathbf{R}^+$ and defined $[\log 1]^r$ to be r_1. The following are easily deduced:

(I) if $s > 1$, then for each r we have $\frac{\sigma_n}{\phi_n} \to 0$ as $n \to \infty$;

(II) if $s = 1$, then for each $r > 0$ we have $\frac{\sigma_n}{\phi_n} \to 0$ as $n \to \infty$;

(III) for all other values of r and s, the sequence ϕ fails to be realizable in rate by Theorem 5.1(iii) or by (5.24).

Thus, for the values of r and s referred to in (I) and (II), it is of interest to know whether $\dot{\phi}_n = O(\sigma_n)$. If so, then Theorem 5.1(iv) will be of use. By the argument in Lemma 5.3, the stronger fact is that $\hat{\phi} \geq 0$ when $r \in \mathbf{N}$ and $s \geq 1$. For other r and s, the interest remains.

Example 5.1 So far, part (v) of Theorem 5.1 has not been used. Whenever it could have been used, we have had $\hat{\phi} \geq 0$ and part (iv) of the theorem has done the job. It would be nice to illustrate Theorem 5.1(v) with an example of a familiar sequence ϕ for which $\hat{\phi}_n$ is negative for *infinitely* many n. This seems difficult. However, as will now be shown, pertinent examples are easily contrived using familiar sequences. Let ψ be any sequence which is eventually positive, with $\hat{\psi} \geq 0$ and $\sigma_n = o(\psi_n)$. As Corollary 5.3 shows, an example of such a ψ is $(n \log n)$. Using ψ, a sequence ϕ will now be constructed, which obeys the conditions of Theorem 5.1(v) and for which $\hat{\phi}_n$ is negative for infinitely many n. Define ϕ by

$$\hat{\phi}_n = \begin{cases} -n & \text{for } n \in \{2^2, 2^4, 2^6, \ldots\}, \\ \hat{\psi}_n + \hat{\psi}_{2n} + 2n & \text{for } n \in \{2^1, 2^3, 2^5, \ldots\}, \\ \hat{\psi}_n & \text{otherwise.} \end{cases} \tag{5.29}$$

After some basic work, it is found that

$$\sum_{i=1}^{r} \hat{\phi}_{2^i} = \begin{cases} \sum_{i=1}^{r} \hat{\psi}_{2^i} & \text{if } r \text{ is even,} \\ \hat{\psi}_{2^{r+1}} + 2^{r+1} + \sum_{i=1}^{r} \hat{\psi}_{2^i} & \text{if } r \text{ is odd.} \end{cases} \tag{5.30}$$

Using (2.6), let us show that $\phi \geq \psi$. Write $\tilde{n}$ for the order of 2 in n, and T for the set $\{2, 2^2, 2^3, \ldots\}$. If n is odd, then $\phi_n = \psi_n$ because $\hat{\phi}_n = \hat{\psi}_n$ for such n. If $\tilde{n} \geq 1$, then

$$\begin{aligned} \phi_n = \sum_{d|n} \hat{\phi}_d &= \sum_{d|n; d \notin T} \hat{\phi}_d + \sum_{i=1}^{\tilde{n}} \hat{\phi}_{2^i} \\ &\geq \sum_{d|n; d \notin T} \hat{\psi}_d + \sum_{i=1}^{\tilde{n}} \hat{\psi}_{2^i} \quad \text{(by (5.29) and (5.30))} \\ &= \psi_n. \end{aligned}$$

So, $\phi \geq \psi$. Thus, ϕ is eventually positive since ψ is, and $\sigma_n = o(\phi_n)$ since $\sigma_n = o(\psi_n)$. The next task is to show that $\dot{\phi}_n = O(\sigma_n)$. By (5.29),

$$\dot{\phi}_n = \begin{cases} 0 & \text{for } \tilde{n} \in \{0, 1\}, \\ 2^2 + 2^4 + \cdots + 2^{\tilde{n}} & \text{for } \tilde{n} \in \{2, 4, 6, \ldots\}, \\ +2^2 + 2^4 + \cdots + 2^{\tilde{n}-1} & \text{for } \tilde{n} \in \{3, 5, 7, \ldots\}. \end{cases}$$

But $1 + 2 + 2^2 + \cdots + 2^{\tilde{n}} \leq \sigma_n$. Thus, $\dot{\phi}_n \leq \sigma_n$. Whence, by Theorem 5.1(v), ϕ is realizable in rate.

5.5 Remarks

This miscellany of comments is mainly about Theorem 5.1. Here, (i), (ii), (iii), (iv) and (v) refer to the various parts of that theorem.

(1) With the reasoning of Example 5.1 still fresh in our minds, we can quickly answer the following about (v): Given that ϕ is eventually positive, does not the O condition follow from the o condition? With ψ as in that example, define a new ϕ by

$$\hat{\phi}_n = \begin{cases} -n^2 & \text{for } n \in \{2^2, 2^4, 2^6, \ldots\}, \\ \hat{\psi}_n + \hat{\psi}_{2n} + 4n^2 & \text{for } n \in \{2^1, 2^3, 2^5, \ldots\}, \\ \hat{\psi}_n & \text{otherwise.} \end{cases}$$

Working much as in Example 5.1, it is found that ϕ is eventually positive and that $\sigma_n = o(\phi_n)$. However, it is an easy task to see that $\frac{\phi_{2^{2n}}}{\sigma_{2^{2n}}} \to \infty$ as $n \to \infty$.

(2) The variety of examples is now sufficient for us to note that, for a sequence ϕ, there is no simple connection between ϕ being in $\mathcal{RR}$ and $\hat{\phi}$ being non-negative:

for ϕ defined in (5.29), it has been shown in Example 5.1 that $\phi \in \mathcal{RR}$ and that $\hat{\phi}_n$ is negative for infinitely many n;

$\phi \in \mathcal{RR}$ and $\hat{\phi} \geq 0$ for each $\phi \in \mathcal{ER}$; by the proofs to Corollaries 5.2 and 5.3, there are similar sequences which are not in $\mathcal{ER}$;

$(n) \notin \mathcal{RR}$ by (ii), and $\widehat{(n)} \geq 0$ by (5.25);

(ii) gives easy examples of sequences ϕ for which $\phi \notin \mathcal{RR}$ and $\hat{\phi} \not\geq 0$.

(3) Simple examples show that each 'if, then' statement in the theorem fails to have a converse.

For (i): define ϕ by $\phi_n = 0$ if n is a prime or 1, and $\phi_n = n$ otherwise. By (ii), $\phi \notin \mathcal{RR}$. However, the 'if' part fails in (i).

For (iii): define ϕ by $\phi_n = 1$ if n is a prime, and $\phi_n = 0$ otherwise. For each $N \in \mathbf{N}$ there is a prime $p > N$ with $\phi_p > 0$ and $\phi_{p^2} = 0$. So, by (i), $\phi \notin \mathcal{RR}$. But, the 'if' part in (iii) fails since ϕ is bounded. A second example is the sequence $(2n)$ which, by (ii), is not in $\mathcal{RR}$. For $(2n)$, the condition involving l fails.

For (iv): there are sequences in $\mathcal{ER}$ for which (c) and (a) hold without (b). For each $\phi \in \mathcal{ER}$, both (c) and (a) hold: (a) holds by (2.9); by (2.10), $\hat{f}_n := n(\frac{\hat{\phi}_n}{n}) = n(\frac{\hat{\phi}_n}{n}) = \hat{\phi}_n$ for each $n \geq 1$; hence, $f = \phi$; and since each exactly realizable sequence realizes itself in rate, we have (c). However, the limit in (b) is infinite for each bounded ϕ in $\mathcal{ER}$. Less dull is σ itself: $\hat{\sigma} = (n)$; so that $\sigma \in \mathcal{ER}$ by the Basic Lemma; but the limit in (b) is 1. Also, there are ϕ in $\mathcal{ER}$ for which the sequence $(\frac{\sigma_{n_m}}{\phi_{n_m}})$ is oscillating: for example, define $\hat{\phi}_n$ to be n when n is not a prime, and 0 when n is a prime; thus, $\phi \in \mathcal{ER}$ by the Basic Lemma; using (2.6), for each prime p,

$$\frac{\sigma_p}{\phi_p} = \frac{1+p}{1} \quad \text{and} \quad \frac{\sigma_{p^2}}{\phi_{p^2}} = \frac{1+p+p^2}{1+p^2};$$

which, respectively, tend to infinity and 1 as p tends to infinity, showing that (b) does not hold. Incidentally, this example shows that sequences in $\mathcal{RR}$ cannot simply be thought of as fast or slow compared to σ.

For (v): for the sequence ϕ just mentioned, $\hat{\phi}_1 > 0$. So, ϕ is eventually positive. The O condition holds for ϕ but, as just explained, the o condition does not. The sequence σ fails the converse for the same reasons, as will each sequence in $\mathcal{ER}$ which is bounded and eventually positive.

The converses to (iv) and (v) may fail in other ways but these have not been been studied.

(4) By the comments to (iv) and (v) in part (3) of this remark, there are sequences in $\mathcal{RR}$ but the theorem cannot tell us that they are. The theorem is similarly inadequate for sequences not in $\mathcal{RR}$. Consider, for example, the Euler totient e. For e, it is easy to see that (i) and (ii) are of no use. Although e is unbounded, note that for each prime p we have $\frac{p}{e_p} = \frac{p}{p-1}$ which tends to 1 as p tends to infinity. Thus, (iii) is of no use.

To see that $e \notin \mathcal{RR}$, let $f \in \mathcal{ER}$. Then, for each $r \geq 1$,

$$\frac{f_{2^r}}{e_{2^r}} = \frac{f_{2^r}}{2^r - 2^{r-1}} = \frac{f_{2^r}}{2^r} \cdot 2.$$

Here, $\frac{f_{2^r}}{2^r}$ is a non-negative integer by the Basic Lemma. Hence, $\frac{f_{2^r}}{e_{2^r}}$ cannot tend to 1 as r tends to infinity. So, $f \not\sim e$. Since this holds for each $f \in \mathcal{ER}$, we see, by Definition 5.2, that $e \notin \mathcal{RR}$.

(5) In (iii), the condition '$l > 1$' cannot be weakened. There is an unbounded ϕ with $\frac{n_m}{\phi_{n_m}} > 1$ for all m sufficiently large, but with ϕ realizable in rate. To see this, define f and ϕ as follows:

$$\hat{f}_n = n \text{ when } n \text{ is a prime, and 0 otherwise;} \tag{5.31}$$

$$\phi_n = f_n - 1 \text{ when } n \text{ is a prime, and } \phi_n = f_n \text{ otherwise.} \tag{5.32}$$

By the Basic Lemma, f is exactly realizable. From now let $n > 1$. By (2.6) and (5.31),

$$f_n = \text{the sum of the distinct primes dividing } n. \tag{5.33}$$

So, f is unbounded and, by (5.32), the same goes for ϕ. Now consider the fraction $\frac{n}{\phi_n}$. Using (5.32) and (5.33),

$$\text{for prime } n, \qquad \frac{n}{\phi_n} = \frac{n}{f_n - 1} = \frac{n}{n-1} > 1. \tag{5.34}$$

For composite n, suppose $k > 1$ and that $p_1 < p_2 < \cdots < p_k$ are the distinct primes dividing n. Then,

$$\begin{aligned}
\frac{n}{\phi_n} &= \frac{n}{f_n} \quad (\text{by (5.32)}) \\
&\geq \frac{\Pi_{i=1}^k p_i}{\sum_{i=1}^k p_i} \quad (n \geq \Pi_{i=1}^k p_i \text{ and, by (5.33), } f_n = \textstyle\sum_{i=1}^k p_i) \\
&> \frac{p_1^{k-1} p_k}{k p_k} \quad (\Pi_{i=1}^k p_i \geq p_1^{k-1} p_k \text{ and } \textstyle\sum_{i=1}^k p_i < k p_k) \\
&= \frac{p_1^{k-1}}{k} \geq \frac{2^{k-1}}{k} \geq 1.
\end{aligned}$$

So, $\frac{n}{\phi_n} > 1$ for composite n, which, with (5.34), shows that $\frac{n}{\phi_n} > 1$ for each $n \geq 2$.

It is left to note that $\phi \in \mathcal{RR}$. In fact, by (5.32) and (5.33), it is clear that $f\mathcal{R}\phi$: $\frac{f_n}{\phi_n} = 1$ for composite n; for prime n we have $\frac{f_n}{\phi_n} = \frac{n}{n-1}$ which tends to 1 as n tends to infinity; thus, $f \asymp \phi$; since $f \in \mathcal{ER}$ we are done by Definition 5.2.

Chapter 6

Open problems

Several natural open problems are suggested by the work above.

6.1 Exact realization constraints

Can $\mathcal{ER}$ be completely described by the homeomorphisms of a single compact metric space? In other words, in the language of Chapter 2: Does a compact metric space (X, ρ) exist such that $f \in \mathcal{ER}$ only if there is a homeomorphism T of (X, ρ) for which (X, T) exactly realizes f? The natural candidate for X is a Cantor set: it is clear that too many restrictions on the space X may impose further constraints on $\mathcal{ER}$ that are outside the scope of this work (in the spirit of, for example, Sharkovskiĭ [12] and Hall [5]).

6.2 General recurrences and Exact realization

Is there a proof of Theorem 3.1 which is less exclusively quadratic in nature? Even for linear recurrences with integer coefficients, it is impossible to see how the conditions in that theorem can be generalised. For such recurrences, Remark 3.2 offers more hope. By that remark, if f satisfies (3.1), then necessary and sufficient conditions for f to be in $\mathcal{ER}$ are: $f, \hat{f}_4 \geq 0, 4|\hat{f}_4$ and $p|\hat{f}_p, \hat{f}_{2p}$ for each prime p. These conditions allow some sensible although naive conjectures for higher order linear recurrences with integer coefficients. For general recurrences, the problem apppears intractable.

6.3 Other sequences in $\mathbf{Z}^+$

There are many other natural classes of sequences in $\mathbf{Z}^+$. For example, if u is an elliptic divisibility sequence in the sense of Morgan Ward [13], it would be interesting to discover when $|u|$ can lie in $\mathcal{ER}$.

6.4 Realization in rate of slow sequences

One mystery of $\mathcal{RR}$, of course, is its lower edge. An open problem is this: Is $(n \log\log n)$ in $\mathcal{RR}$? More generally, if $\phi \in \mathcal{RR}$ with $\frac{\phi_n}{n} \to \infty$, then is $(n \log(\frac{\phi_n}{n})) \in \mathcal{RR}$?

Bibliography

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[2] George Bachman, *Introduction to p-Adic Numbers and Valuation Theory*, Academic Press, New York and London, 1964.

[3] George L. Cain, *Introduction to General Topology*, Addison-Wesley, Reading MA, 1994.

[4] V. Chothi, G. Everest and T. Ward, *S-integer dynamical systems: periodic points*, J. für die Riene Angew. Math. **489** (1997), 99-132.

[5] Toby Hall, *The creation of horseshoes*, Nonlinearity, **7** (1994), no. 3, 861-924.

[6] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., Clarendon Press, Oxford, 1979.

[7] D.A. Lind *Dynamical properties of quasihyperbolic toral automorphisms,* Ergod. Th. Dynam. Sys. **2** (1982), 49-68.

[8] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, 1995.

[9] E. Lucas, *Théorie des functions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

[10] W.K. Nicholson, *Introduction to Abstract Algebra*, John Wiley & Sons, New York, 1999.

[11] P. Ribenboim, *The Fibonacci numbers and the Arctic Ocean.* In M. Behara, R. Fritsch, and R. G. Lintz, editors, Symposia Gaussian, Conf. A (Proceedings of the Second Gaussian Symposium, München), pages 41–83, W. de Gruyter, Berlin, 1995.

[12] A.N. Sharkovskiĭ, *Coexistence of cycles of a continuous map of the line into itself*, Ukrain Mat. Zh. **16** (1964), no. 1, 61-71; Translated by J. Tolosa in Internat. J. Bifurc. Chaos Appl. Sci. Engrg, **5** (1995), no. 5, 1263-1273.

[13] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31-74.