Can. J. Math., Vol. XXVI, No. 6, 1974, pp. 1356–1371

RECURSIVELY GENERATED PERIODIC SEQUENCES

R. P. KURSHAN AND B. GOPINATH

1. Introduction. A sequence (x_n) $(n = 1, 2, \ldots)$ is periodic if $x_{n+p} = x_n$ for some p and all n. Periodic sequences arise naturally in geometry and arithmetic in the study of mosaic patterns [**4**], continued fractions and frieze patterns [**3**; **5**]. Some digital oscillators and tone generators also generate periodic sequences. In these cases one computes the period p of the sequence in question. On the other hand, in pseudo random sequences and cryptography [**8**] it is required to recursively generate sequences of large periods.

We say a sequence $(\mathbf{x}_n)_{n=1}^{\infty}$ of k-dimensional vectors is *recursively generated* if there exists a (vector valued) function $\mathbf{f}$ such that $\mathbf{x}_{n+1} = \mathbf{f}(\mathbf{x}_n)$. This is a generalization of the more usual recursion

$$(1.1) \qquad y_n = g(y_{n-k}, \ldots, y_{n-1}) \quad (n > k)$$

where the y_i's are scalars. The $\mathbf{f}$ associated with (1.1) is

$$(1.2) \qquad \mathbf{f}(x_1, \ldots, x_k) = (x_2, \ldots, x_k, g(x_1, \ldots, x_k)).$$

The advantage of the representation (1.2) is that the periodicity of $(y_n)_n$ can be examined through the structure of g via periodicity of $\mathbf{f}$: if $y_{n+p} = y_n$ for all n (independent of the initial values $y_1, \ldots, y_k$), then p-fold composition of $\mathbf{f}$: $\mathbf{f}^p \equiv \mathbf{f} \circ \mathbf{f} \circ \ldots \circ \mathbf{f}$ satisfies $\mathbf{f}^p(\mathbf{x}) = \mathbf{x}$; indeed,

$$\mathbf{f}^p(y_1, \ldots, y_k) = \mathbf{f}^{p-1}(y_2, \ldots, y_k, g(y_1, \ldots, y_k)) = \ldots =$$
$$\mathbf{f}(y_p, y_{p+1}, \ldots, y_{p+k-1}) = (y_{p+1}, \ldots, y_{p+k}) = (y_1, \ldots, y_k).$$

In this paper we consider those recursions whose respective generators $\mathbf{f}$ have a power series expansion about a fixed point; in particular, it makes sense to consider the Jacobian of $\mathbf{f}$ at that point (i.e., the linear part of $\mathbf{f}$ with respect to its power series expansion). We show that one can determine the period of $\mathbf{f}$ by merely computing the period of the Jacobian at zero of $\mathbf{f}'$, a certain affine translation of $\mathbf{f}$. Using this, we provide sharp bounds for the minimum k, given the period of $\mathbf{f}$, and the maximum period of $\mathbf{f}$, given k, when the ground field is the rationals.

The theory is applied to differential equations; and some examples are discussed.

Throughout, F will denote a subfield of the complex numbers. (Actually, it suffices to assume char $F = 0$, if all power series are either taken to be polynomials or are considered as formal series ("expanded" about $\mathbf{0}$)–thus obvi-

Received May 1, 1973 and in revised form, October 26, 1973.

ating (1.7) and concern about convergence.) Vectors and vector valued functions will be distinguished by natural bold face type, e.g., $\mathbf{x}$ is a vector, x_i is the ith component of $\mathbf{x}$ and $\mathbf{x} = (x_1, \ldots, x_k)$; similarly, if $U \subset F^k$, $\mathbf{f}: U \rightarrow F^k$, then $\mathbf{f} = (f_1, \ldots, f_k)$ where $f_i : U \rightarrow F$. The dimension k of the underlying space will be called the *memory* of $\mathbf{f}$ (cf. (1.1)), and unless otherwise stated, we assume throughout that all vector valued functions are of memory k.

Let N denote the nonnegative integers and let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k) \in N^k$. Given a vector $\mathbf{x} \in F^k$, we will use the notation $\mathbf{x}^{\boldsymbol{\alpha}}$ to denote the scalar $x_1^{\alpha_1} \cdot \ldots \cdot x_k^{\alpha_k}$. We say that a scalar valued function g is *analytic* in a neighborhood U of a point $\mathbf{x}_0 \in F^k$, if there are scalars $c_{\boldsymbol{\alpha}} (\boldsymbol{\alpha} \in N^k)$ such that for each $\mathbf{x} \in U$ and each 1-1 onto map $\omega: N \rightarrow N^k$ the series

$$(1.3) \qquad \sum_{i=0}^{\infty} c_{\boldsymbol{\omega}(i)} (\mathbf{x} - \mathbf{x}_0)^{\boldsymbol{\omega}(i)}$$

converges to $g(\mathbf{x})$. In this case, instead of (1.3) we can write

$$(1.4) \qquad g(\mathbf{x}) = \sum_{\alpha \in N^k} c_{\alpha} (\mathbf{x} - \mathbf{x}_0)$$

without ambiguity. Note that this is equivalent to the condition that (1.3) converges absolutely to $g(\mathbf{x})$, and hence the power series expansion (1.4) is unique in the sense that if $\sum c'_{\boldsymbol{\alpha}} (\mathbf{x} - \mathbf{x}_0)^{\boldsymbol{\alpha}}$ also converges absolutely to $g(\mathbf{x})$ in U, then $c_{\boldsymbol{\alpha}} = c_{\boldsymbol{\alpha}}'$ for all $\boldsymbol{\alpha}$. We say g is analytic in an open set if g is analytic in a neighborhood of each point of that open set.

We say $\mathbf{f}$ is *analytic* in an open set U if each component f_i is analytic there. If $\mathbf{f}$ is analytic in an open set U and $\mathbf{g}$ is analytic in an open set containing $\mathbf{f}(U)$, then $\mathbf{g} \circ \mathbf{f}$ is analytic in U. The proofs of this and the preceding assertions can be found in [**7**, §9.1–9.3]. (All functions are single-valued.)

One can alternatively view $\mathbf{f}$ in a formal sense. Let $\mathbf{x}$ be a k-dimensional indeterminate, $\mathbf{x} = (x_1, \ldots, x_k)$ and for $c_{\boldsymbol{\alpha}} \in F$ let $\mathbf{f}$ be the formal power series

$$(1.5) \qquad \mathbf{f}(\mathbf{x}) = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}.$$

(With formal power series, operations are performed term by term, and for $\mathbf{f}'(\mathbf{x}) = \sum c_{\boldsymbol{\alpha}}' \mathbf{x}^{\boldsymbol{\alpha}}$, $\mathbf{f}' = \mathbf{f}$ if and only if each $c_{\boldsymbol{\alpha}}' = c_{\boldsymbol{\alpha}}$.) The term *analytic* will also be used to designate the formal power series (1.5); this will not lead to confusion, as assertions regarding functions analytic (in the first sense) in a neighborhood of $\mathbf{0}$ remain true when "analytic" is construed in the second (formal) sense: one must merely disregard mention of neighborhoods and domains. For $\mathbf{f}$ the formal power series (1.5), we define $\mathbf{f}(\mathbf{0})$ to be the "constant" term $c_{(0,\ldots,0)}$; the reader should construe the phrase "$\mathbf{f}$ is analytic in a neighborhood of a fixed point" as applied to (1.5), to mean merely: $\mathbf{f}(\mathbf{0}) = \mathbf{0}$.

The function $\mathbf{f}$ will be said to have a *fixed point* $\mathbf{x}_0$ if there exists some vector $\mathbf{x}_0$ such that $\mathbf{f}(\mathbf{x}_0) = \mathbf{x}_0$. We will use $\mathbf{I}(I)$ to denote the identity function (matrix) $\mathbf{I}(\mathbf{x}) = \mathbf{x} (I\mathbf{x} = \mathbf{x})$. The n-fold iteration of $\mathbf{f} : \mathbf{f} \circ \ldots \circ \mathbf{f}$ will be denoted $\mathbf{f}^n$. Whenever we write $\mathbf{f}^n$ we assume there is some open set $U \subset F^k$

such that $\mathbf{f}$ is defined on $\bigcup_{i=1}^{n-1} \mathbf{f}^i(U)$. Where there is a possibility of confusing $f^n(x)$ with the n-fold product $f(x) \cdot f(x) \cdot \ldots \cdot f(x)$, the latter will be denoted $f(x)^n$.

A sequence of vectors $(\mathbf{x}_n)_n$ is said to be periodic of period p if $\mathbf{x}_{n+p} = \mathbf{x}_n$ for all n, and p is the smallest such positive integer. If the sequence is recursively generated by $\mathbf{f}$ (so $\mathbf{x}_{n+1} = \mathbf{f}(\mathbf{x}_n)$ for all n), $\mathbf{f}$ need not be periodic in the sense that for $\mathbf{x}$ in the domain of $\mathbf{f}$, $\mathbf{f}^p(\mathbf{x}) = \mathbf{x}$ (for example, $f(x) = -x^3$ recursively generates the periodic sequence $x_n = (-1)^n$, but is not itself periodic in any open set); however, if in some set U, $\mathbf{f}^p(\mathbf{x}) = \mathbf{x}$, then for any initial vector $\mathbf{x}_1 \in U$, the sequence $(\mathbf{x}_n)_n$ recursively generated by $\mathbf{f}$ is periodic. Notice that if for some set D, $\mathbf{f}$ is defined in $U = \bigcup_{i=0}^{p-1} \mathbf{f}^i(D)$ and $\mathbf{f}^p = \mathbf{I}$ in D, then $\mathbf{f}(U) = U$ and $\mathbf{f}^p = \mathbf{I}$ in U.

We define the period of the generator $\mathbf{f}$, denoted per $\mathbf{f}$, to be the smallest positive integer p such that $\mathbf{f}^p = \mathbf{I}$ in the domain U of $\mathbf{f}$. If $(\mathbf{x}_n)_n$ is recursively generated by a periodic $\mathbf{f}$, then the period p of $(\mathbf{x}_n)_n$ divides $q = \text{per } \mathbf{f}$, as $x_{n+p} = x_n = \mathbf{f}^q(\mathbf{x}_n) = x_{n+q}$ for all n. Notice that if $\mathbf{f}$ is also continuous in U, then $\mathbf{f}$ is a homeomorphism between U and $\mathbf{f}(U)$. Furthermore, if $\mathbf{f}^p$ is analytic in a connected open set U, and $\mathbf{f}$ is periodic of period p in some nonempty open subset $U' \subset U$, then $\mathbf{f}$ is periodic of period p in all of U: this follows by the "principle of analytic continuation" [7, 9.4.2] which in this case says that since $\mathbf{f}^p = \mathbf{I}$ in U', this must hold throughout U. In fact, more can be said if $\mathbf{f}$ is a rational function (that is, each f_i is a quotient of polynomials). In this case, suppose by means of a power series expansion valid in some neighborhood U, it is determined that $\mathbf{f}$ is periodic of period p in U. Then each component $(\mathbf{f}^p)_i (i = 1, \ldots, k)$ is a rational function, say P_i/Q_i, and in U, $P_i(\mathbf{x})/Q_i(\mathbf{x}) - x_i = 0$; i.e.,

$$(1.6) \qquad P_i(\mathbf{x}) - x_i Q_i(\mathbf{x}) = 0$$

in the nonempty open set U. Hence (1.6) holds for all $\mathbf{x} \in F^k$, and thus $\mathbf{f}$ is periodic of period p in the complement of $\{\mathbf{x} | Q(\mathbf{x}) = 0\}$.

On the other hand, one may think of $(\mathbf{x}_n)_n$ as a sequence of indeterminates, defined formally by $\mathbf{x}_{n+1} = \mathbf{f}(\mathbf{x}_n)$ where $\mathbf{f}$ is now considered to be a formal power series. In this case, of course, the period of $(\mathbf{x}_n)_n$ and the period of $\mathbf{f}$ are identical.

For $\lambda \in F$ we define per λ to be the multiplicative order of λ.

The following proposition, of course, does not apply to formal power series.

(1.7) PROPOSITION. *Suppose* $\mathbf{f}$ *is periodic in a neighborhood* U *of a fixed point* $\mathbf{x}_0$. *Define* $\mathbf{f}'(\mathbf{x}) = \mathbf{f}(\mathbf{x} + \mathbf{x}_0) - \mathbf{x}_0$; *then* $\mathbf{f}'(\mathbf{0}) = \mathbf{0}$ *and* $\mathbf{f}'$ *is analytic in a neighborhood* U' *of* $\mathbf{0}$. *Furthermore,* $\mathbf{f}'$ *is periodic in* U' *and the period of* $\mathbf{f}$ *in* U *is equal to the period of* $\mathbf{f}'$ *in* U'.

Proof. Clearly $\mathbf{f}'(\mathbf{0}) = \mathbf{f}(\mathbf{x}_0) - \mathbf{x}_0 = \mathbf{0}$, and $\mathbf{f}'$ is the composition of the analytic functions $\mathbf{f}$, $\mathbf{g}(\mathbf{x}) = \mathbf{x} + \mathbf{x}_0$, and $\mathbf{g}^{-1}$ valid in the neighborhood $U' =$

$U - \mathbf{x}_0$ of $\mathbf{0}$. Furthermore, $\mathbf{f}'^n = (\mathbf{g}^{-1} \circ \mathbf{f} \circ \mathbf{g})^n = \mathbf{g}^{-1} \circ \mathbf{f}^n \circ \mathbf{g}$ for all n, and the result follows.

Hence, in order to determine the period of an analytic function $\mathbf{f}$ with a fixed point, it is sufficient to determine the period of the translated analytic function $\mathbf{f}'$ with fixed point $\mathbf{0}$. This is the crux of our analysis.

Although not all periodic analytic functions have a fixed point, the counter-examples are fairly pathological. In fact, we have the following:

(1.8) THEOREM. *Let f be a periodic analytic function with period p, memory k, and suppose that the underlying field F contains the real numbers. If p is a power of a prime, or $k = 3$ or 4, then f has a fixed point.*

The proof of (1.8), due to P. A. Smith, appears in [**12**, p. 350].

In what follows we consider analytic $\mathbf{f}$ with fixed point 0; this completely identifies the case when $\mathbf{f}$ is a function analytic in a neighborhood of 0, with the case when $\mathbf{f}$ is a formal power series.

Any analytic function (or formal power series) $\mathbf{f}$ can be expressed as the sum of its homogeneous components: for $i = 1, \ldots, k$ let h_i be the homogeneous component of f_i of degree $d \geqq 0$, if such exists, and otherwise let $h_i = 0$; then $\mathbf{h} = (h_1, \ldots, h_k)$ is the homogeneous component of $\mathbf{f}$ of degree d unless $\mathbf{h} = 0$, in which case we say that $\mathbf{f}$ has no homogeneous component of degree d. We will reserve $\mathbf{l}$ to denote the homogeneous component of degree 1; in the case of analytic functions, $\mathbf{l}$ is precisely the Jacobian of $\mathbf{f}$, evaluated at $\mathbf{0}$. In any case $\mathbf{l}$ will be called the *linear part* of $\mathbf{f}$. For a nonzero $\mathbf{f}$ with polynomial components, we define deg $\mathbf{f}$ to be the maximum of the (total) degrees of the components f_i, and we define md $\mathbf{f}$ to be the degree of the homogeneous component of $\mathbf{f}$ of minimal degree; we define the *base* of $\mathbf{f}$ to be the homogeneous component of $\mathbf{f}$ of minimal degree > 1 if such exists, and $\mathbf{0}$ otherwise. Hence, if $\mathbf{f}$ has a linear part $\mathbf{l}$ and $\mathbf{f} = \mathbf{l} + \mathbf{g}$, then either $\mathbf{g} = 0$ or md $\mathbf{g} \geqq 2$ and in that case we can write $\mathbf{g} = \mathbf{h} + \boldsymbol{\varphi}$ where $\mathbf{h}$ is the base of $\mathbf{g}$ and either $\varphi = 0$ or md $\varphi >$ md $\mathbf{h} =$ deg $\mathbf{h} =$ md $\mathbf{g}$; in other words, either $\varphi_j = 0$ or deg $\varphi_j >$ deg $\mathbf{h}$, for each j.

2. The one-dimensional case. We start by considering an example. Clearly the sequence $(x_n)_n$, generated by the recursion $x_{n+1} = 1/x_n$, is periodic of period 2. Here $k = 1$, $f(x) = 1/x$, and per $f = 2$. Obviously $f(1) = 1$ and therefore f has a fixed point; and f is analytic in a neighborhood of 1. Translating (x_n) to a neighborhood of 0, let $y_n = x_n - 1$; then y_n is periodic of period 2, and

$$y_{n+1} = 1/(y_n + 1) - 1.$$

The generator f' of the translated recursion (y_n) is

$$f'(y) = 1/(y + 1) - 1;$$

furthermore $f'(0) = 0$ and f' is analytic in a neighborhood of 0.

In a neighborhood of 0,

$$f'(y) = -y + y^2 - y^3 + \ldots.$$

Obviously the linear part l' of f' satisfies $l'(y) = -y$; and the nonlinear part $g'(y) = y^2 - y^3 + \ldots$ has base $h'(y) = y^2$; and md $g' = 2$. Notice here that $2 = \text{per } l' = \text{per } f' = \text{per } f$. Hence, in this example, to find per f, it suffices to find per l'. This behavior happily occurs in all dimensions k, as we shall see in the next section.

Although the following two results fail in higher dimensions, one might find in them a suggestion of what is to follow.

(2.1) PROPOSITION. *Suppose $f(x)$ and $g(x)$ are two polynomials. Then* $\deg f \circ g = \deg f \cdot \deg g$.

Proof. Let

$$f(x) = \sum_{i=0}^{m} a_i x^i, \qquad g(x) = \sum_{j=0}^{n} b_j x^j, a_m b_n \neq 0;$$

then $(f \circ g)(x) = a_m b_n{}^m x^{nm}$ + terms of lower degree.

(2.2) COROLLARY. *If $f(x)$ is a periodic polynomial, then $f(x)$ is linear.*

Proof. We get $(\deg f)^{\text{per} f} = \deg f^{\text{per} f} = \deg \mathbf{I} = 1$.

Notice, then, that every periodic polynomial is of the form $f(x) = ax + b$ where $a^{\text{per} f} = 1$; b can be arbitrary unless $a = 1$, in which case we must have $b = 0$. Indeed, $f^p(x) = a^p x + b(1 + a + \ldots + a^{p-1}) = a^p x + b(a^p - 1)/(a - 1)$ whenever $a \neq 1$ (where f^p is the p-fold iteration).

3. The multidimensional case. It happens that some features of the one dimensional recursion remain intact in the higher dimensional cases.

Our point of departure is the fact that the Corollary (2.2) fails in general for both memory larger than 1 (i.e., $\mathbf{f}$ a vector-vector valued polynomial) and f a scalar valued power series of infinite degree (valid somewhere). An example of the former with $k = 2$ is

$$\text{(3.1)} \qquad \mathbf{f}(\mathbf{x}) = (x_1 + x_2{}^3, -x_2),$$

as $\mathbf{f}^2(\mathbf{x}) = (x_1 + x_2{}^3 + (-x_2)^3, -(-x_2)) = \mathbf{x}$. For the latter case, $f(x) = 1/x$ clearly has period 2 (and is of infinite degree).

What remains intact in higher dimensions is first of all the ability to compute the period of $\mathbf{f}$ by computing the period of a linear function. The following theorem applies identically to formal power series or analytic functions (in a neighborhood of $\mathbf{0}$), and the term "analytic" may be inferred either way.

(3.2) THEOREM. *Let* $\mathbf{f}$ *be analytic* (in a neighborhood U of $\mathbf{0}$), *suppose* $\mathbf{f}(\mathbf{0}) = \mathbf{0}$ *and suppose* $\mathbf{f}$ *is periodic* (in U). *Then* $\mathbf{f}$ *has a periodic linear part* (Jacobian) *whose period is exactly equal to the period of* $\mathbf{f}$.

The above theorem allows the following restatement of (1.7):

(3.3) COROLLARY. *Suppose* $\mathbf{f}$ *is a periodic function analytic in a neighborhood of a fixed point* $\mathbf{x}_0$. *Then* per $\mathbf{f}$ *is exactly equal to the period of the Jacobian of* $\mathbf{f}'(\mathbf{x}) \equiv \mathbf{f}(\mathbf{x} + \mathbf{x}_0) - \mathbf{x}_0$, *evaluated at* $\mathbf{0}$.

(Of course, a periodic Jacobian does not imply a periodic $\mathbf{f}$.)
We need some further results to obtain the proof of (3.2).

(3.4) LEMMA. *If* $\mathbf{f}$ *and* $\mathbf{g}$ *are functions,* $\mathbf{g}$ *analytic in some neighborhood of a vector* $\mathbf{u}$ *and* $\mathbf{f}$ *analytic in some neighborhood of* $\mathbf{g}(\mathbf{u})$, *and if* $\mathbf{g}, \mathbf{f} \circ \mathbf{g} \neq 0$, *then* $\operatorname{md} \mathbf{f} \circ \mathbf{g} \geqq \operatorname{md} \mathbf{f} \cdot \operatorname{md} \mathbf{g}$.

Proof. For each $j = 1, \ldots, k$ we can express the jth component of $\mathbf{f} \circ \mathbf{g}$ as

$$f_j \circ \mathbf{g} = \sum_{\boldsymbol{\alpha}} c_{j\boldsymbol{\alpha}} g_1^{\alpha_1} \ldots g_k^{\alpha_k}.$$

Thus, a nonzero monomial summand m of lowest degree, of a component of $\mathbf{f} \circ \mathbf{g}$ will be of the form $m = c_{j\boldsymbol{\alpha}}(m_{11} \cdot \ldots \cdot m_{1\alpha_1}) \ldots (m_{k1} \cdot \ldots \cdot m_{k\alpha_k})$ for some j and some $\boldsymbol{\alpha}$, where m_{it} is a monomial summand of g_i. Hence

$$\begin{aligned} \deg m_{it} \geqq \operatorname{md} \mathbf{g} \text{ and } \operatorname{md} f_j \circ \mathbf{g} = \deg m = \deg m_{11} + \ldots + \deg m_{1\alpha_1} \\ + \ldots + \deg m_{k1} + \ldots + \deg m_{k\alpha_k} \geqq \alpha_1 \operatorname{md} \mathbf{g} + \ldots \\ + \alpha_k \operatorname{md} \mathbf{g} = (\alpha_1 + \ldots + \alpha_k) \cdot \operatorname{md} \mathbf{g} \geqq \operatorname{md} \mathbf{f} \cdot \operatorname{md} \mathbf{g}. \end{aligned}$$

(3.5) COROLLARY. *Suppose* $\mathbf{l}$ *and* $\mathbf{l}'$ *are respectively the linear parts of* $\mathbf{f} = \mathbf{l} + \mathbf{g}$ *and* $\mathbf{f}' = \mathbf{l}' + \mathbf{g}'$, *both* $\mathbf{f}$ *and* $\mathbf{f}'$ *are analytic in a neighborhood of* $\mathbf{0}$, *and* $\mathbf{f}(\mathbf{0}) = \mathbf{g}(\mathbf{0}) = \mathbf{0}$. *Then the linear part of* $\mathbf{f} \circ \mathbf{f}'$ *is* $\mathbf{l} \circ \mathbf{l}'$.

Proof. $\mathbf{f} \circ \mathbf{f}' = (\mathbf{l} + \mathbf{g}) \circ (\mathbf{l}' + \mathbf{g}') = \mathbf{l} \circ \mathbf{l}' + \mathbf{l} \circ \mathbf{g}' + \mathbf{g} \circ \mathbf{f}'$; by (3.4), $\mathbf{l} \circ \mathbf{g}'$ and $\mathbf{g} \circ \mathbf{f}'$ have no linear part.

(3.6) COROLLARY. *With* $\mathbf{f}$ *as in* (3.5), *the linear part of* $\mathbf{f}^n$ *is* $\mathbf{l}^n$; *if* $\mathbf{f}$ *has no linear part, then neither does* $\mathbf{f}^n$.

(3.7) PROPOSITION. *Let* $\mathbf{f}$ *be analytic* (in a neighborhood of $\mathbf{0}$), *suppose* $\mathbf{f}(\mathbf{0}) = \mathbf{0}$, *and suppose* $\mathbf{f}$ *has linear part* $\mathbf{l}$ *and base* $\mathbf{h}$. *Then for any* $n = 1, 2, \ldots$, *the base of* $\mathbf{f}^n$ *is*

$$\sum_{i=1}^{n} \mathbf{l}^{n-i} \circ \mathbf{h} \circ \mathbf{l}^{i-1}.$$

Proof. We may assume $\mathbf{h} \neq 0$. For some n let $\mathbf{H}$ be the base of $\mathbf{f}^n$. For some $\boldsymbol{\psi}, \boldsymbol{\varphi}$, we may write $\mathbf{f}^{n+1} = \mathbf{f} \circ \mathbf{f}^n = (\mathbf{l} + \mathbf{h} + \boldsymbol{\psi}) \circ (\mathbf{l}^n + \mathbf{H} + \boldsymbol{\varphi})$ where either $\boldsymbol{\psi} = \mathbf{0}$ or else $\operatorname{md} \boldsymbol{\psi} > \deg \mathbf{h}$, and either $\boldsymbol{\varphi} = \mathbf{0}$, or $\mathbf{H} = \boldsymbol{\varphi} = \mathbf{0}$ or else $\operatorname{md} \boldsymbol{\varphi} > \deg \mathbf{H} = \deg \mathbf{h}$. Expanding, we obtain $\mathbf{f}^{n+1} = \mathbf{l}^{n+1} + \mathbf{l} \circ \mathbf{H} + \mathbf{l} \circ \boldsymbol{\varphi} + \mathbf{h} \circ (\mathbf{l}^n + \mathbf{H} + \boldsymbol{\varphi}) + \boldsymbol{\psi} \circ \mathbf{f}^n$. Furthermore, $\mathbf{h} \circ (\mathbf{l}^n + \mathbf{H} + \boldsymbol{\varphi}) = \mathbf{h} \circ \mathbf{l}^n + \boldsymbol{\theta}$ where for each m, θ_m is a sum of terms of the form $T = c(s_1 t_1 u_1) \ldots (s_k t_k u_k)$; here u_j is a power of φ_j (unless $\boldsymbol{\varphi} = \mathbf{0}$ in which case, $u_j = 1$) and t_j is a power of H_j. Not both powers are zero, and if $\boldsymbol{\varphi} = \mathbf{0}$, t_j must be a nonzero power;

s_j is a power of $(\mathbf{l}^n)_j$, c is a scalar, and since deg $\mathbf{h} > 1$, the sum of the exponents of $s_1, t_1, u_1, \ldots, s_k, t_k, u_k$ must be greater than 1. Assume T is of lowest possible degree. Then either $\mathbf{H} = \mathbf{0}$ in which case (by the above) $\boldsymbol{\theta} = \mathbf{0}$, or else md $\boldsymbol{\theta} =$ md $T >$ deg $\mathbf{H} =$ deg $\mathbf{h}$. Furthermore, md $\mathbf{l} \circ \boldsymbol{\varphi}$ and md $\boldsymbol{\psi} \circ \mathbf{f}^n$ are both greater than deg $\mathbf{h}$ by (3.4), unless the respective function is zero. Thus the base of $\mathbf{f}^{n+1}$ is $\mathbf{l} \circ \mathbf{H} + \mathbf{h} \circ \mathbf{l}^n$. The proposition follows by induction on n.

Proof of (3.2). By (3.6), $\mathbf{f}$ has a linear part $\mathbf{l}$ and the linear part of $\mathbf{I} = \mathbf{f}^p$ is $\mathbf{l}^p$, i.e., $\mathbf{l}^p = \mathbf{I}$. Consequently, per $\mathbf{l}|p$. Let $q =$ per $\mathbf{l}$, $qr = p$. The linear part of $\mathbf{f}^q$ is $\mathbf{l}^q = \mathbf{I}$; suppose $p \neq q$, and let $\mathbf{f}^q = \mathbf{I} + \mathbf{g}$. Let $\mathbf{h}$ be the base of $\mathbf{g}$. By (3.7), the base of $(\mathbf{f}^q)^n(\mathbf{x})$ is $n\mathbf{h}(\mathbf{x})$ for all n. Thus $\mathbf{x} = (\mathbf{f}^q)^r(\mathbf{x}) = \mathbf{x} + r\mathbf{h}(\mathbf{x}) + \boldsymbol{\varphi}$ where $\boldsymbol{\varphi} = \mathbf{0}$ or md $\boldsymbol{\varphi} >$ deg $\mathbf{h}$. But the base of $\mathbf{x}$ is $\mathbf{0}$, so $r\mathbf{h}(\mathbf{x}) = 0$; it follows that $\boldsymbol{\varphi} = \mathbf{h} = 0$ and $p = q$.

(3.8) PROPOSITION. *Suppose the field F is algebraically closed, and let $\mathbf{f}$ be as in* (3.2), *with $\mathbf{f} = \mathbf{l} + \mathbf{g}$. Let $\mathbf{h}$ be the base of $\mathbf{g}$,*

$$h_j(\mathbf{x}) = \sum_{\boldsymbol{\alpha}} a_{j\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}} \quad (1 \leqq j \leqq k),$$

and let L be the matrix associated with $\mathbf{l}$ with respect to some basis for F^k. Then L can be diagonalized so that it has the form

$$\begin{bmatrix} \rho^{s_1} & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & \rho^{s_k} \end{bmatrix}$$

where $\rho \in F$ and $s_1, \ldots, s_k$ are positive integers. Furthermore, $s_j \not\equiv s_1\alpha_1 + \ldots + s_k\alpha_k$ (mod p) for each $\boldsymbol{\alpha}$ such that $a_{j\boldsymbol{\alpha}} \neq 0$.

Proof. Since F is algebraically closed, L is diagonalizable (see [**1**, p. 252]); the diagonal elements will all be pth roots of unity, and hence can each be written as a power of a primitive pth root of unity—ρ say. By (3.7),

$$0 = \sum_{i=1}^{p} L^{p-i}\mathbf{h}(L^{i-1}\mathbf{x})$$

and thus for each $j = 1, \ldots, k$

$$\begin{aligned} 0 &= \sum_{i=1}^{p} \rho^{s_j(p-i)} h_j(\rho^{s_1(i-1)}x_1, \ldots, \rho^{s_k(i-1)}x_k) \\ &= \sum_{i,\boldsymbol{\alpha}} a_{j\boldsymbol{\alpha}}\rho^{s_j(p-i)}\rho^{\alpha_1 s_1(i-1)} \ldots \rho^{\alpha_k s_k(i-1)} x_1^{\alpha_1} \ldots x_k^{\alpha_k}. \end{aligned}$$

Fixing $\boldsymbol{\alpha}$, set $s = s_1\alpha_1 + \ldots + s_k\alpha_k$. Then either

$$a_{j\boldsymbol{\alpha}} = 0 \quad \text{or} \quad 0 = \sum_{i=0}^{p} \rho^{s_j(p-i)}\rho^{s(i-1)} = \rho^{s_jp-s} \sum_{i=1}^{p} \rho^{(s-s_j)i}.$$

This will (always) be true unless $p|s - s_j$.

4. Minimum k for given p. In the case when the characteristic polynomial of L (a matrix representation of $\mathbf{l}$) has rational coefficients, we can determine the minimum possible memory k necessary for a function $\mathbf{f}$ to be periodic of period p. Hence we also find the maximum period attainable for a given k.

The Euler function φ has value $\varphi(n)$ equal to the number of integers less than and relatively prime to n; (m, n) denotes the greatest common divisor of m and n.

(4.1) LEMMA. *If $n, m > 2$ then $\varphi(n)\varphi(m) \geqq \varphi(n) + \varphi(m)$.*

Proof. If $n, m > 2$ then $(\varphi(n) - 1)(\varphi(m) - 1) > 0$ and $\varphi(n)\varphi(m) = (\varphi(n) - 1)(\varphi(m) - 1) + \varphi(n) + \varphi(m) - 1 > \varphi(n) + \varphi(m) - 1$.

Suppose now $\mathbf{f}$ is analytic and periodic in a neighborhood of a fixed point $\mathbf{x}_0$. Let

$$p = \prod_{i=1}^{t} p_i^{\alpha_i}$$

be the canonical prime decomposition of the integer $p = \operatorname{per} \mathbf{f}$, and (as always) let k be the memory of $\mathbf{f}$. Let L be a matrix representation of the linear part $\mathbf{l}'$ of $\mathbf{f}'(\mathbf{x}) = \mathbf{f}(\mathbf{x} + \mathbf{x}_0) - \mathbf{x}_0$ (cf. (1.7)) and suppose the coefficients of the characteristic polynomial of L are rational (this could be verified directly if $\mathbf{x}_0 = \mathbf{0}$ whence $\mathbf{f}' = \mathbf{f}$; and, in any case, this would be satisfied if F were the field of rational numbers). Under these conditions we obtain the following

(4.2) THEOREM.

(a) $$k \geqq \sum_{i=1}^{t} \varphi(p_i^{\alpha_i}) - 1$$

and if $(p, 4) \neq 2$, the inequality is strict.

(b) *There exists an integer $q(k)$* (dependent on k) *such that for any corresponding period p, $p \leqq q(k)$.*

Proof. (a) Since k and p are invariants under the translation $\mathbf{f} \to \mathbf{f}'$, we may as well assume $\mathbf{f} = \mathbf{f}'$ so $\mathbf{f}(\mathbf{0}) = \mathbf{0}$. Then L is the matrix of the linear part of $\mathbf{f}$; and per $L = p$ by (3.2). Let χ be the characteristic polynomial of L; all the eigenvalues of L, and hence all the roots of χ are pth roots of unity. Since the coefficients of χ are rational, χ is a product of cyclotomic polynomials. Let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of L and let $r_1, \ldots, r_m (m \leqq k)$ be the distinct values assumed by per $\lambda_1, \ldots,$ per λ_k; let c_i be the (unique) cyclotomic polynomial having roots of order $r_i (i = 1, \ldots, m)$. Then each $c_i | \chi$ and since $c_1, \ldots, c_m$ are distinct, $\prod_{i=1}^m c_i | \chi$. Furthermore, since L is diagonalizable (see [**1**, p. 252]) with $\lambda_1, \ldots, \lambda_k$ on the diagonal, $p =$ per $L = \text{lcm}\,\{r_1, \ldots, r_m\}$ and hence each $p_i^{\alpha_i}$ $(i = 1, \ldots, t)$ must appear as a factor of one or more of the integers $r_1, \ldots, r_m$. If $(p, 4) \neq 2$ then each $p_i^{\alpha_i} > 2$, and using the well known fact that if $(n, m) = 1$ then $\varphi(nm) = \varphi(n)\varphi(m)$, we obtain

$$\sum_{i=1}^{m} \varphi(r_i) \geqq \sum_{i=1}^{t} \varphi(p_i^{\alpha_i})$$

by repeated use of (4.1). If (p, 4) = 2 then for exactly one i, $p_i^{\alpha_i} = 2$, say $i = 1$. Then as, in the first case,

$$\sum_{i=1}^{m} \varphi(r_i) \geqq \sum_{i=2}^{t} \varphi(p_i^{\alpha_i}).$$

Set $\delta = 1$ if (p, 4) = 2 and $\delta = 0$ otherwise. Then

$$k = \deg \chi \geqq \deg \prod_{i=1}^{m} c_i = \sum_{i=1}^{m} \deg c_i = \sum_{i=1}^{m} \varphi(r_i) \geqq \sum_{i=1}^{t} \varphi(p_i^{\alpha_i}) - \delta.$$

(b) Let $q_1, \ldots, q_r$ be the primes less than or equal to $(k + 2)$ and let

$$B = \left\{ \boldsymbol{\beta} \in N^r \,\middle|\, \sum_{i=1}^{r} \varphi(q_i^{\beta_i}) \leqq k + 1 \right\}.$$

Then $|B|$ is finite; choose $\boldsymbol{\beta} \in B$ such that $q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$ is maximal. Setting $q(k)$ equal to this last number proves the theorem.

(4.3) PROPOSITION. *Given a positive integer p with prime decomposition $p = \prod_{i=1}^t p_i^{\alpha_i}$, there exists a periodic function of finite degree, with period p, integer coefficients and memory $\sum_{i=1}^t \varphi(p_i^{\alpha_i}) - \delta$ where $\delta = 1$ if $(p, 4) = 2$ and 0 otherwise.*

Proof. If $p = 1$ or $p = 2$ then $g(x) = x$ or $g(x) = -x$, respectively, does the job. Otherwise, if $(p, 4) \neq 2$ let $k = \sum_{i=1}^t \varphi(p_i^{\alpha_i})$ and let $c_i (i = 1, \ldots, t)$ be the cyclotomic polynomial with roots of order $p_i^{\alpha_i}$; if $(p, 4) = 2$ we may assume $p_1^{\alpha_1} = 2$, and we let $k = \sum_{i=2}^t \varphi(p_i^{\alpha_i})$, we define $c_1 = 1$, and let c_2 be the cyclotomic polynomial with roots of order $2p_2^{\alpha_2}$; let c_i be as above for $i > 2$. Note that $\varphi(2p_2^{\alpha_2}) = \varphi(2)\varphi(p_2^{\alpha_2}) = \varphi(p_2^{\alpha_2})$ and hence in either case, $k = \deg \prod_{i=1}^t c_i$. Write

$$\prod_{i=1}^{t} c_i = \lambda^k + a_1\lambda^{k-1} + \ldots + a_k \equiv \chi$$

(the a_j's are integers, since the coefficients of each c_i are integers), and let **1** be the (linear) periodic function having $k \times k$ matrix

$$L = \begin{bmatrix} 0 & 1 & & & & & 0 \\ & 0 & 1 & & & & \\ & & & \cdot & & & \\ & & & & \cdot & & \\ & & & \cdot & & \cdot & \\ & & & & \cdot & & \\ & & & & & \cdot & \\ & 0 & & & & 0 & 1 \\ -a_k & & \cdot & \cdot & \cdot & -a_2 & -a_1 \end{bmatrix}. \tag{4.3.1}$$

As L is similar to the diagonal matrix $D = \text{diag } (\lambda_1, \ldots, \lambda_k)$ where the λ_i's are the roots of χ (L is the rational canonical form of D), $\mathbf{l}$ has period p (and memory k).

(4.4) *Notes.* (i) Let L and χ be as in the proof of (4.3), let $\{\lambda_{ij}\}_j$ be the roots of c_i and let $D_i = \text{diag } (\lambda_{ij})_j$, for each $i = 1, \ldots, t$ (if $\{\lambda_{1j}\}_j = \emptyset$, D_1 is 0×0 matrix). Then L is similar to the diagonal matrix diag $(D_1, \ldots, D_t)$ and each D_i is similar to a matrix L_i of the form (4.3.1), *i.e.*, its rational canonical form. In this case the a_j's of (4.3.1) (considered now as the matrix L_i) are the coefficients of c_i, and if $(p, 4) \neq 2$ they are all 0 or 1 (see [**11**, p. 206]) since the roots of each c_i are of prime power order; if $(p, 4) = 2$ then the coefficients are 0 or ± 1. In fact, for large α_i (the exponent of p_i) the preponderance of the coefficients are 0: indeed, if $F_n(\lambda)$ is the cyclotomic polynomial with roots of order n, then for a prime q and integer $\alpha > 0$, $F_q(\lambda) = \lambda^{q-1} + \ldots + \lambda + 1$, $F_{q^\alpha}(\lambda) = F_q(\lambda^{q^{\alpha-1}})$ and if $q \neq 2$, $F_{2q^\alpha}(\lambda) = F_{q^\alpha}(-\lambda)$. Hence the matrix L is similar to the matrix

$$\begin{bmatrix} L_1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & L_t \end{bmatrix} \tag{4.4.1}$$

whose elements are all 0 or ± 1.

(ii) When F is a finite field, if we minimize k with respect to the class of $\mathbf{f}$'s which are periodic of period p over all finite fields, we also obtain the inequalities of (4.2).

(iii) The periodic function $\mathbf{l}$ with matrix representation (4.3.1) is of the form of $\mathbf{f}$ in (1.2), with associated $g(\mathbf{x}) = -a_k x_1 + a_{k-1} x_2 - \ldots - a_1 x_k$.

The following two propositions were communicated to the authors by N. J. A. Sloane.

https://doi.org/10.4153/CJM-1974-129-6 Published online by Cambridge University Press

(4.5) PROPOSITION. *Given an even integer* $k \geqq 2$, *there exists an integer* $p \not\equiv 2$ (*modulo* 4) *with prime decomposition* $p = \prod p_i^{\alpha_i}$, *such that* $k = \sum \varphi(p_i^{\alpha_i})$.

Proof. If $k = 2$ or 4, we may take $p = 3$ or 8 respectively. For $k \geqq 6$, we form two sequences $k_0 = k, k_1, \ldots, k_{r-1}$ and $n_0 = 1, n_1, \ldots, n_r = p$ satisfying

$$2 \leqq k_{i+1} \leqq k_{i/2} \quad \text{for} \quad 0 \leqq i < r - 1,$$
$$2 \leqq k_{r-1} \leqq 4,$$

where p has the property in the statement of the theorem. The sequences are constructed as follows. Bertrand's postulate [**9**, p. 371] implies that for $k_i \geqq 6$, there exists a prime p_i such that

$$(k_i + 1)/2 < p_i \leqq k_i.$$

We take $k_{i+1} = k_i - p_i + 1$ and $n_{i+1} = p_i n_i$. Then $2 \leqq k_{i+1} \leqq k_{i/2}$ and the p_i are distinct and greater than 3. We repeat this step until a $k_{i+1} = k_{r-1}$ is obtained which is less than 5. For $k_{r-1} = 2$ or 4, let $l = 3$ or 8 and let $p = n_r = l n_{r-1}$. Then p has the desired property.

(4.6) PROPOSITION. *Let*

$$M_k = \max \{p | k = \sum \varphi(p_i^{\alpha_i}), \textit{where } p = \pi_{p_i}{}^{d_i}\};$$

then

$$\limsup_k \frac{\log M_k}{(k \log k)^{\frac{1}{2}}} = 1.$$

The proof of (4.6) is a modification of the proof in [**10**, § 61] of Landau's theorem on the maximum order of a permutation of k letters.

Actual computations have been made of M_k for $k \leqq 201$, and of $N_p = \min \{k | k = \sum \varphi(p_i^{\alpha_i})\}$ for $p = \pi p_i^{\alpha_i} \leqq 10{,}004$.

5. Examples. First, we describe how our previous results could be used to compute the period of an analytic **f**. Then we illustrate this through explicit computations in two examples.

(5.1) Computation of the period of an **f** analytic in a neighborhood of a fixed point, in five steps:

(1st) Translate $\mathbf{f} \rightarrow \mathbf{f}'$ (see (1.7)) analytic in a neighborhood of **0**.

(2nd) Compute the Jacobian of $\mathbf{f}'$ evaluated at **0**: this is the linear part of the power series expansion about **0** of $\mathbf{f}'$, and is equal to the $k \times k$ matrix

$$L = \left(\frac{\partial f_i'(x)}{\partial x_j} \bigg|_{\mathbf{x}=0} \right).$$

(3rd) Compute the characteristic polynomial of L: $\chi(\lambda) = \det (L - \lambda I)$ (see (5.2.i) below).

(4th) Find the k roots of χ: $\lambda_1, \ldots, \lambda_k$; if the modulus of any λ_i is other than 1, $\mathbf{f}$ cannot be periodic. If $|\lambda_i| = 1$ $(i = 1, \ldots, k)$, and if χ has rational coefficients, are all the λ_i's of finite order, less than or equal to $q(k)$ (see (4.2.b))? That is, for each $i = 1, \ldots, k$ is there an integer n_i, $0 < n_i \leqq q(k)$ such that $\lambda_i^{n_i} = 1$? If not, then $\mathbf{f}$ is not periodic. In any case, let p be the least common multiple of $\{\text{per } \lambda_1, \ldots, \text{per } \lambda_k\}$; if χ has rational coefficients and $p > q(k)$, then $\mathbf{f}$ is not periodic.

(5th) Test: is $\mathbf{f}'^p = \mathbf{I}$? The original $\mathbf{f}$ is periodic if and only if the answer is yes (see (5.2.ii) below).

(5.2) *Notes.* (i) Suppose $\mathbf{f}$ has the form (1.2). Then the Jacobian of $\mathbf{f}$ has the simple form

$$L = \begin{bmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & 0 \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & \cdot & \cdot & \\ & & & & \cdot & \\ & & & & & \cdot \\ & 0 & & & 0 & 1 \\ a_1 & & \cdot\ \cdot\ \cdot & & a_{k-1} & a_k \end{bmatrix}$$

where $a_i = (\partial g(\mathbf{x})/\partial x_i)|_{\mathbf{x}=\mathbf{0}}$ $(i = 1, \ldots, k)$ (i.e., where the linear part of g: $l(\mathbf{x}) = a_1x_1 + \ldots + a_kx_k$); the characteristic polynomial of L is $\chi(\lambda) = \lambda^k - a_k\lambda^{k-1} - a_{k-1}\lambda^{k-2} - \ldots - a_1$. Furthermore, any fixed point $\mathbf{x}_0$ of $\mathbf{f}$ must have the form $\mathbf{x}_0 = (a, a, \ldots, a)$ for some $a \in F$. Hence, it is necessary and sufficient for $\mathbf{f}$ to have a fixed point, that the function of a: $G(a) \equiv g(a, a, \ldots, a) - a$ have a solution $G(a) = 0$. If g is a polynomial, this will always obtain (in the completion of F), unless $g(a, a, \ldots, a) = a + c$ for some nonzero c in F, i.e., unless $a = a_1a + \ldots + a_ka = (\sum a_i)a$. This will happen only if $\sum a_i = 1$, i.e., if $\chi(1) = 0$. Thus, when g is a polynomial, $\mathbf{f}$ has a fixed point if no eigenvalue of the linear part of $\mathbf{f}$ is 1.

(ii) To determine if $\mathbf{f}'^p = \mathbf{I}$ (or equivalently, if $\mathbf{f}^p = \mathbf{I}$), one could, of course, perform the p iterations, and see what happens. On the other hand, if $\mathbf{f}^p \neq \mathbf{I}$, then the algebraic surface defined by $\mathbf{f}^p(\mathbf{x}) - \mathbf{x} = 0$ is of measure zero, and hence by simply testing

$$\text{(5.2.1)} \quad \mathbf{f}^p(\mathbf{x}_0) - \mathbf{x}_0 = 0?$$

at a single point $\mathbf{x}_0$ selected from a nonlattice distribution one can determine with probability one whether or not $\mathbf{f}^p = \mathbf{I}$. (Certainly, if $\mathbf{f}^p(\mathbf{x}_0) \neq \mathbf{x}_0$, we know $\mathbf{f}$ cannot be periodic.)

S. P. Lloyd has kindly pointed out to us that if each component of $\mathbf{f}$ is a polynomial of degree less than or equal to d, then each component of $\mathbf{f}^p$ is a polynomial of degree less than or equal to $d' = d^p$, and there are $N = \binom{k + d'}{d'}$

terms in each component $(\mathbf{f}^p)_i$. Hence, by choosing N vectors

$$\overset{1}{\mathbf{x}}, \ldots, \overset{N}{\mathbf{x}}$$

such that

$$\det \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \overset{1}{x}_1 & \overset{2}{x}_1 & \cdots & \overset{N}{x}_1 \\ \overset{1}{x}_2 & \overset{2}{x}_2 & \cdots & \overset{N}{x}_2 \\ \vdots & & & \vdots \\ (\overset{1}{x}_1)^2 & (\overset{2}{x}_1)^2 & \cdots & (\overset{N}{x}_1)^2 \\ \vdots & & & \vdots \\ \overset{1}{x}_1\overset{1}{x}_2 & \overset{2}{x}_1\overset{2}{x}_2 & \cdots & \overset{N}{x}_1\overset{N}{x}_2 \\ \vdots & & & \vdots \end{vmatrix} \neq 0,$$

$\mathbf{f}^p - \mathbf{I}$ vanishes on $\left\{\overset{1}{\mathbf{x}}, \ldots, \overset{N}{\mathbf{x}}\right\}$ only if it is identically zero. Hence, it suffices to test (5.2.1) at N points.

Consider the recursion

$$(5.3) \qquad u_{n+2} = (1 + u_{n+1})/u_n.$$

This example arises in frieze patterns [**5**]. One of the first published accounts of the periodicity of (5.3) is due to Lyness [**13**], although the earliest reference to the pattern that gives rise to it is in 1602 by Nathaniel Torporley (see DeMorgan [**6**]).

We shall now examine (5.3) in terms of our preceding analysis. Set $g(x_1, x_2) = (1 + x_2)/x_1$, $f_1(x_1, x_2) = x_2$, $f_2(\mathbf{x}) = g(\mathbf{x})$ (here $k = 2$.) Then (5.3) is a recursion generated by g, of the type (1.1), and the corresponding function (1.2) is $\mathbf{f} = (f_1, f_2)$. We see that $\mathbf{f}$ has a fixed point $\mathbf{x}_0 = (a, a)$ (with respect to the completion of F — cf. (5.2.i)), where a is any root of

$$(5.3.1) \quad (1 + a)/a - a = 0.$$

We define $\mathbf{f}'(\mathbf{x}) = \mathbf{f}(\mathbf{x} + \mathbf{x}_0) - \mathbf{x}_0$ (cf. (1.7)), so $\mathbf{f}'(\mathbf{x}) = (x_2, g'(\mathbf{x}))$ where

$$g'(\mathbf{x}) = g(\mathbf{x} + \mathbf{x}_0) - a = g(x_1 + a, x_2 + a) - a = \left(1 + \frac{1}{a} - a - x_1 + \frac{x_2}{a}\right)\left(1 + \frac{x_1}{a}\right)^{-1},$$

where (in a neighborhood of $\mathbf{0}$) $(1 + x_1/a)^{-1} = 1 - x_1/a + \ldots$ and so the linear part l of g' is

$$l(\mathbf{x}) = -\frac{(1+a)}{a^2}x_1 + \frac{1}{a}x_2 = -x_1 + \frac{1}{a}x_2$$

by (5.3.1). By (5.2.i) we see that the characteristic polynomial of the linear part of $\mathbf{f}'$ is

(5.3.2) $\lambda^2 - \lambda/a + 1.$

We will prove that if λ is a root of (5.3.2), then λ is a primitive fifth root of unity. From (5.3.2) we get $\lambda^3 = -\lambda(1 - \lambda/a)$, $\lambda^4 = -\lambda^2(1 - \lambda/a)$, and hence

(5.3.3) $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 = \dfrac{1+a}{a^2}\lambda^2 - \dfrac{1}{a}\lambda + 1 = \lambda^2 - \dfrac{1}{a}\lambda + 1.$

Since any root of (5.3.3) is a primitive fifth root of unity, the result follows.

Hence, if $\mathbf{f}$ is periodic, its period must be 5. Iteration of $\mathbf{f}$ five times shows that indeed $\mathbf{f}^5 = \mathbf{I}$. (Note that since $\varphi(5) > 2$, the coefficients of (5.3.2) cannot be rational, by (4.2.a).)

J. H. Conway (private communication) conveyed the following example of a periodic recursion:

(5.4) $a_{n+4} = a_n a_{n+3}/(a_n a_{n+2} - a_{n+1}).$

Its period can be determined as in (5.3). The memory of this recursion is 4, i.e., $k = 4$, the generator is $g(x_1, x_2, x_3, x_4) = x_1x_4/(x_1x_3 - x_2)$, and the associated $\mathbf{f}$ (cf. (1.2)) has fixed point $\mathbf{x}_0 = (2, 2, 2, 2)$.

The translated $\mathbf{f}'(\mathbf{x}) = \mathbf{f}(\mathbf{x} + \mathbf{x}_0) - \mathbf{x}_0$ has fourth component

$$f_4'(\mathbf{x}) = \frac{\frac{1}{2}x_1x_4 - x_1x_3 + x_4 - 2x_3 + x_2 - x_1}{1 - (\frac{1}{2}x_2 - x_1 - x_3 - \frac{1}{2}x_1x_3)}$$
$$= -x_1 + x_2 - 2x_3 + x_4 + \text{(higher order terms)}$$

and thus the characteristic polynomial of the matrix representation (5.2.ii) of the linear part of $\mathbf{f}'$ is

(5.4.1) $\chi(\lambda) = \lambda^4 - \lambda^3 + 2\lambda^2 - \lambda + 1 = (\lambda^2 + 1)(\lambda^2 - \lambda + 1).$

The roots of $\lambda^2 + 1 = 0$ are clearly fourth roots of unity, and the roots of $\lambda^2 - \lambda + 1 = 0$ satisfy $\lambda^3 - \lambda^2 + \lambda = 0$, i.e., $\lambda^3 = -1$, so the roots of

$\lambda^2 - \lambda + 1$ are sixth roots of unity. Hence, given that (5.4) is periodic, its period is lcm $\{4, 6\} = 12$.

Other periodic recursions such as (5.4) can be found in [**2**].

Conway (in his private communication) suggested that for periodic recursions such as (5.4), where the associated g is a rational function, the period p may satisfy the inequality $3k \geqq p$. Notice that the characteristic polynomial has integer coefficients. We know from (4.2) that

$$k + 1 \geqq \sum_{i=1}^{r} \varphi(p_i^{\alpha_i})$$

where $\Pi p_i^{\alpha_i}$ is the canonical prime decomposition of p and in fact, for any such k and p, an $\mathbf{f}$ with memory k and period p exists. From this we can see that the conjecture $3k \geqq p$ is false (it fails for the first time for $p = 20$, with $k = 2 + 4 = 6$). However, when the associated χ (5.4.1) has rational coefficients, the inequalities of (4.2) apply.

6. Differential equations.

For R^+ the nonnegative real numbers, let

$$(6.1) \qquad \begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{f}(\mathbf{x}(t)) \quad t \in R^+ \\ \mathbf{x}(0) &= \mathbf{X} \end{aligned}$$

be a system of first order differential equations ("·" denotes differentiation with respect to t). (We assume here that the solutions for (6.1) exist and are unique, and that the solution $x(t)$ depends analytically on the initial condition x; (cf. [**7**, 10.7.5]).) As before let $\mathbf{l}$ be the linear part of $\mathbf{f}$. Assume $\mathbf{f}(\mathbf{0}) = \mathbf{0}$ and $\mathbf{f}$ analytic in a neighborhood of $\mathbf{0}$. Let $\mathbf{\Theta}(\mathbf{X}, t) = \mathbf{x}(t)$ where $\mathbf{x}(0) = \mathbf{X}$. Therefore $\mathbf{\Theta}(\mathbf{X}, t)$ represents the dependence of the solution $\mathbf{x}(t)$ on the initial condition $\mathbf{x}(0) = \mathbf{X}$; in particular

$$(6.2) \qquad \mathbf{\Theta}(\mathbf{\Theta}(\mathbf{X}, t), t') = \mathbf{\Theta}(\mathbf{X}, t + t').$$

It can be proved that if L is the matrix representation of $\mathbf{l}$ then

$$\exp [Lt] = \sum_{i=0}^{\infty} \frac{t^i L^i}{i!}$$

is the matrix representation of $\mathbf{\Lambda}(t)$, the linear part of $\mathbf{\Theta}(\mathbf{X}, t)$; and $\mathbf{\Theta}(\mathbf{0}, t) = \mathbf{0}$.

(6.3) LEMMA. *The set of points t such that $\mathbf{\Theta}(\mathbf{X}, t) = \mathbf{X}$ is discrete, provided L has at least one nonzero eigenvalue.*

Proof. Let λ be any nonzero eigenvalue of L. Then $\exp [\lambda t]$ is an eigenvalue of $\mathbf{\Lambda}(t) = \exp [Lt]$ and hence $\exp [\lambda t] = 1$ for every t such that $\mathbf{\Theta}(\mathbf{X}, t) = \mathbf{X}$. This completes the proof.

The system (6.1) is periodic if there exists a $t \neq 0$ such that $\mathbf{\Theta}(\mathbf{X}, t) = \mathbf{X}$.

The period of the system (6.1) is t^* where

$$t^* = \underset{t>0}{\text{mi}\varphi}\,\{\Theta(\mathbf{X}, t) = \mathbf{X}\}$$

which, by (6.3) always exists if (6.1) is periodic. It is clear then that if $\Theta(\mathbf{X}, t) = \mathbf{X}$, then $t = mt^*$ for some positive integer m.

(6.4) THEOREM. *If the system* (6.1) *is periodic, then its period is the period of the linear system*

(6.4.1) $\dot{\mathbf{z}}(t) = \mathbf{l}(\mathbf{z}(t))$

where $\mathbf{l}$ *is the linear part of* $\mathbf{f}$, *provided* L *has at least one nonzero eigenvalue.*

Proof. Let t^* be the period of system (6.4.1); then $\mathbf{z}(t) = \mathbf{z}(t + t^*)$, and therefore $\exp\,[Lt^*] = I$. Therefore the linear part of $\Theta(\mathbf{X}, t^*)$: $\Lambda(t^*)$ is equal to I. Hence the period of (6.1) must be an integer multiple of t^*, say rt^*. Therefore the function $\Theta(\mathbf{X}, t^*)$ has period r; that is, if

$$\mathbf{x}_n = \Theta(\mathbf{x}_{n-1}, t^*), \quad \mathbf{x}_0 = \mathbf{x}(0) = \mathbf{X}$$

then $x_r = \mathbf{x}(rt^*) = \mathbf{X}$. But from (3.2) $r = 1$. Hence the period of (6.1) is t^*.

Remarks. The period of the linear system (6.4.1) is easily computed from its eigenvalues.

Also when all the eigenvalues of L are zero, it is easily proved using Jordan canonical form that $\Theta(\mathbf{X}, t) = \mathbf{I}$ for some $t \neq 0$. Hence L is diagonalizable, and therefore L iz zero. Furthermore by (6.2), $\Theta(\mathbf{X}, t/n)$ is periodic of period n. But the linear part of $\Theta(\mathbf{X}, t/n)$ is $\mathbf{I}$ (since $L = 0$). Therefore as in the proof of (3.2), it is clear that $\Theta(\mathbf{X}, t/n) = \mathbf{X}$ for every n. Since $t/n \to 0$ as $n \to \infty$, and $\Theta(\mathbf{X}, t)$ is assumed analytic in $s\Theta(\mathbf{X}, s) = \mathbf{X}$ for all s, it follows that $\mathbf{f}(\mathbf{X}) = 0$.

REFERENCES

1. W. Burnside, *Theory of groups of finite order* (Dover, New York, 1955).
2. J. H. Conway and R. L. Graham, *On periodic sequences defined by recurrence* (unpublished).
3. C. M. Cordes and D. P. Roselle, *Generalized frieze patterns* (to appear).
4. H. S. M. Coxeter, *Regular polytopes* (Dover, New York, 1973).
5. ——— *Frieze patterns*, Acta Arith. *18* (1971), 297–310.
6. A. DeMorgan, *On the invention of circular parts*, Phil. Mag. *22* (1843), 350–353.
7. J. Dieudonné, *Foundations of modern analysis* (Academic Press, New York, 1969).
8. S. W. Golomb, *Shift register sequences* (Holden-Day, Inc., San Francisco, 1967).
9. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford University Press, Oxford, 1954).
10. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen* (Teubner, Leipzig, 1909).
11. S. Lang, *Algebra* (Addison-Wesley, New York, 1965).
12. S. Lefschetz, *Algebraic topology*, Amer. Math. Soc. Colloquium Publication VXXVII, New York, 1942.
13. R. C. Lyness, *Notes 1581 and 1847*, Math. Gaz. *26* (1942), p. 62; *29* (1945), p. 251.

Bell Laboratories,
Murray Hill, New Jersey