ISRAEL JOURNAL OF MATHEMATICS, Vol. 72, Nos. 1-2, 1990

THE ALGEBRAIC STRUCTURE OF LINEARLY RECURSIVE SEQUENCES UNDER HADAMARD PRODUCT

BY

RICHARD G. LARSON[a,†] AND EARL J. TAFT[b]

[a]*Department of Mathematics, University of Illinois at Chicago, Chicago, IL 60680, USA; and*
[b]*Department of Mathematics, Rutgers University, New Brunswick, NJ 08903, USA*

ABSTRACT

We describe the algebraic structure of linearly recursive sequences under the Hadamard (point-wise) product. We characterize the invertible elements and the zero divisors. Our methods use the Hopf-algebraic structure of this algebra and classical results on Hopf algebras. We show that our criterion for invertibility is effective if one knows a linearly recursive relation for a sequence and certain information about finitely-generated subgroups of the multiplicitive group of the field.

1. Introduction

In this paper we describe the algebraic structure of linearly recursive sequences with respect to the Hadamard product. Specifically, in Theorem 1.1 we characterize the invertible elements of this algebra, and in Theorem 1.2 we characterize the zero divisors of this algebra. Similar work in the case that the base field has characteristic 0 was done by Benzaghou [2] using analytic methods, and more recently by Reutenauer [7] for an arbitrary characteristic using more algebraic methods. The methods used here make explicit use of the Hopf-algebraic structure of the algebra of linearly recursive sequences, and of classical results on the structure of Hopf algebras. We also prove that the criterion we give here for Hadamard invertibility is effective in the sense that, given a minimal polynomial which the linearly recursive sequence satisfies, and the ability effectively to answer questions about subgroups of the group of nonzero elements of the base field, we can determine whether a linearly recursive sequence is Hadamard invertible.

† Supported in part by NSF Grant DMS 870-1085.
Received August 17, 1989 and in revised form January 1, 1990

Linearly recursive sequences have been studied in computer science in the context of feedback shift registers. See [8] for details.

If $a,\ b \neq 0$ the sequence $(b, ab, \ldots, a^n b, \ldots)$ is a linearly recursive sequence (satisfying the relation $f_{n+1} = af_n$). Its inverse with respect to the Hadamard product $(b^{-1}, a^{-1}b^{-1}, \ldots, a^{-n}b^{-1}, \ldots)$ is also a linearly recursive sequence (satisfying the relation $f_{n+1} = a^{-1}f_n$). The sequence $(b, ab, \ldots, a^n b, \ldots)$ is called a *geometric sequence (with multiplier a)*.

An important notion for linearly recursive sequences is interlacing: if $(e_n)_{n\geq 0}, (f)_{n\geq 0}, \ldots, (g_n)_{n\geq 0}$ are linearly recursive sequences, their interlacing is the sequence

$$e_0, f_0, \ldots, g_0, e_1, f_1, \ldots, g_1, e_2, f_2, \ldots, g_2, \ldots$$

More precisely, suppose that $f_i = (f_{i,n})_{n\geq 0}$ is a linearly recursive sequence satisfying the polynomial $p_i(X)$ for $i = 0, \ldots, t-1$. (We say that the sequence $(f_n)_{n\geq 0}$ satisfies the polynomial

$$p(X) = X^r - p_1 X^{r-1} - p_2 X^{r-2} - \cdots - p_r$$

if

$$f_n = p_1 f_{n-1} + p_2 f_{n-2} + \cdots + p_r f_{n-r}, \qquad \text{for all } n \geq r.)$$

Then the sequence f defined by $f_n = f_{i,j}$, where $i = n \bmod t$ and $j = \lfloor n/t \rfloor$ is a linearly recursive sequence, satisfying the polynomial $p_0(X^t)\cdots p_{t-1}(X^t)$. The sequence f is the *interlacing* of the sequences $f_0, \ldots, f_{t-1}$. It is clear that the interlacing of a finite number of sequences, each of which has a linearly recursive inverse with respect to the Hadamard product, has a linearly recursive inverse with respect to the Hadamard product.

The main theorems, of this paper are the following.

THEOREM 1.1. *Let f be a linearly recursive sequence. Then f is Hadamard invertible if and only if f is everywhere nonzero, and except for a finite number of terms, is the interlacing of geometric series.*

THEOREM 1.2. *The linearly recursive sequences f and g satisfy $fg = 0$ if and only if f and g are the interlacing of t linearly recursive sequences f_i and g_i, except for a finite number of terms, and for each i, either $f_i = 0$ or $g_i = 0$.*

Let k be a field, let $k[X]$ be the algebra of polynomials in the variable X, and let $k[X]^*$ be vector space of k-linear functions on $k[X]$. Each $f \in k[X]^*$ can be identified with the sequence $(f_0, f_1, f_2, \ldots) = (f_n)_{n\geq 0}$, where $f_n = f(X^n)$. The continuous dual coalgebra $k[X]^\circ$ (see [9] for details) consists of those $f \in k[X]^*$

such that $f(J) = 0$ for some cofinite ideal $J \subseteq k[X]$. Any such ideal J is a principal ideal generated by a monic polynomial

$$p(X) = X^r - p_1 X^{r-1} - p_2 X^{r-2} - \cdots - p_r.$$

If $f(J) = 0$, where $J = (p(X))$, then the sequence f_n is linearly recursive, satisfying

$$f_n = p_1 f_{n-1} + p_2 f_{n-2} + \cdots + p_r f_{n-r}, \qquad \text{for all } n \geqq r.$$

Conversely, if the sequence f_n satisfies this recurrence relation, then f vanishes on the ideal $J = (p(X))$. If $p(X)$ is a polynomial such that $f(J) = 0$, where $J = (p(X))$, we say that the polynomial $p(X)$ is *associated* with the linearly recursive sequence (f_n), and that the linearly recursive sequence (f_n) *satisfies* $p(X)$.

The coalgebra structure of $k[X]^\circ$ depends on the algebra structure of $k[X]$. The algebra structure of $k[X]^\circ$ depends on the coalgebra structure of $k[X]$. In [5], these ideas were investigated, using the coalgebra structure of $k[X]$ under which $\Delta(X) = 1 \otimes X + X \otimes 1$ and $\varepsilon(X) = 0$, that is, with X primitive. In this case, identifying $k[X]^*$ as a formal power series algebra of series $f = \Sigma_{n \geq 0} f_n Z^{(n)}$, where $Z^{(n)}(X^p) = \delta_{np}$, the product is given by the Hurwitz product

$$Z^{(m)} Z^{(n)} = \binom{m+n}{m} Z^{(m+n)}.$$

The Hopf algebra $k[X]^\circ$ is a subalgebra of this divided-power series algebra.

In this paper we consider a different coalgebra structure on $k[X]$ under which $k[X]^\circ$ becomes a bialgebra but not a Hopf algebra. The algebra structure induced on the recursive sequences $k[X]^\circ$ by this coalgebra structure is the Hadamard product. For this coalgebra structure, we let $\Delta(X) = X \otimes X$ and $\varepsilon(X) = 1$, that is, we let X be grouplike. Since $\Delta(X^n) = X^n \otimes X^n$ for all $n \geqq 0$, the multiplication on $k[X]^*$ is given by $(f_n)(g_n) = (h_n)$ with $h_n = f_n g_n$, that is, the Hadamard product of the sequences (f_n) and (g_n). In this paper we determine the group of units of the algebra $k[X]^\circ$, that is, those linearly recursive sequences which are invertible with respect to the Hadamard product. Since a necessary condition for $f \in k[X]^\circ$ to be invertible is that $f_n \neq 0$ for all n, we can rephrase the problem: determine when the sequence (f_n^{-1}) is linearly recursive. We also determine the zero divisors in $k[X]^\circ$, that is, those linearly recursive sequences (f_n) and (g_n) such that $f_n g_n = 0$.

Since linearly recursive sequences occur throughout mathematics, the alge-

braic structure of the set of such sequences has been discussed by many authors. We do not list all possible related references here. We do wish to mention the article of van der Poorten [6] in which linearly recursive sequences are identified with power series expansions of rational functions. Since the product used in that paper is the usual one (which differs from the Hadamard product) we will not make use of the representation of linearly recursive sequences as rational functions here. The characterization we give for Hadamard-invertible linearly recursive sequences is not new: see for example [7]. We wish to thank J.-P. Bézivin for bringing the work of Reutenauer found in [7] to our attention. What is new in this paper are the algebraic methods which we use to prove the results, in particular, the natural application of Hopf-algebraic techniques. A general introduction to the theory of Hopf algebras can be found in [9]. A discussion of the relation between linearly recursive sequences and Hopf algebras can be found in [5].

All bialgebras considered in this paper are commutative and cocommutative. If the field k is algebraically closed, the structure of cocommutative Hopf algebras is well understood (see [9] for a complete presentation).

An example of a cocommutative Hopf algebra is the following: let G be a group, and let kG be a vector space with basis G. Define a multiplication on kG by extending the group multiplication linearly to all of kG; the unit in G is a unit for this multiplication. Define a comultiplication $\Delta : kG \to kG \otimes kG$ by letting $\Delta(g) = g \otimes g$ for $g \in G$ and extending linearly; the map $\varepsilon : kG \to k$ such that $\varepsilon(g) = 1$ for $g \in G$ is a counit for this multiplication. Let H be a cocommutative Hopf algebra, and define

$$\mathrm{G}(H) = \{h \in H \mid h \neq 0 \quad \text{and} \quad \Delta(h) = h \otimes h\}.$$

The elements of $\mathrm{G}(H)$ are called the grouplike elements of H. It can be shown that they are linearly independent over k, and form a group under multiplication. It follows that $k\,\mathrm{G}(H)$ is a Hopf subalgebra of H.

Define $\mathbf{u}_n$ and $\mathbf{u}$ as follows:

$$\mathbf{u}_0(H) = k1,$$

$$\mathbf{u}_{n+1}(H) = \{h \in H \mid \Delta(h) \in k1 \otimes H + H \otimes \mathbf{u}_n(H)\},$$

$$\mathbf{u}(H) = \bigcup_{n=0}^{\infty} \mathbf{u}_n(H).$$

It can be shown (see [9]) that $\mathbf{u}(H)$ is a Hopf subalgebra of H. If the

characteristic of k is $p > 0$, it can be shown that $\mathbf{u}_{p^r-1}(H)$ is a Hopf subalgebra for $r \geqq 0$.

The *primitive* elements of the Hopf algebra H are defined by

$$P(H) = \{h \in H \mid \Delta(h) = 1 \otimes h + h \otimes 1\}.$$

It can be shown that $P(H)$ is a Lie algebra, and that if k has characteristic 0 and $P(H)$ generates H as an algebra, then $H \cong U(P(H))$, where $U(L)$ denotes the universal enveloping algebra of the Lie algebra L. (See [9] for details.) If k has characteristic 0, it can be shown that $\mathbf{u}(H)$ is generated by $P(\mathbf{u}(H))$.

The proof of the following theorem can be found in [9].

THEOREM 1.3 (Harrison). *Let H be a commutative, cocommutative Hopf algebra over the algebraically closed field k. Then*

$$H \cong k\,\mathrm{G}(H) \otimes \mathbf{u}(H).$$

2. Continuous duals of polynomials

We consider the polynomial algebra $k[X]$ with coalgebra structure given by $\Delta(X^n) = X^n \otimes X^n$ and $\varepsilon(X^n) = 1$ for all $n \geqq 0$. This gives a bialgebra structure on $k[X]$. In order to use the structure theory of Hopf algebras, we embed $k[X]$ into the Hopf algebra $k[X, X^{-1}] \cong k\mathbf{Z}$. To define a Hopf algebra structure on $k[X, X^{-1}]$ we let $\Delta(X^n) = X^n \otimes X^n$ and $\varepsilon(X^n) = 1$ for all $n \in \mathbf{Z}$. (The antipode on $k[X, X^{-1}]$ is given by $S(X^n) = X^{-n}$ for all $n \in \mathbf{Z}$.)

As described in Section 1, $k[X]^\circ$ can be identified with the space of linearly recursive sequences over k, and is a bialgebra. Each $f \in k[X]^\circ$ is identified with the linearly recursive sequence $(f_n)_{n \geqq 0}$, where $f_n = f(X^n)$ for $n \geqq 0$. The product in $k[X]^\circ$ is the Hadamard product $fg = h$ where $h_n = f_n g_n$ for all $n \geqq 0$.

Similarly $k[X, X^{-1}]^*$ can be identified with the space of sequences $(f_n)_{n \in \mathbf{Z}}$, where $f_n = f(X^n)$ for $n \in \mathbf{Z}$. The product in $k[X, X^{-1}]^*$ is again the Hadamard product under this identification. The algebra $k[X, X^{-1}]$ is a principal ideal algebra, with nonzero ideals cofinite and generated by monic polynomials with nonzero constant term. Hence the elements of the subalgebra $k[X, X^{-1}]^\circ$ are the sequences $f = (f_n)_{n \in \mathbf{Z}}$ such that there exists a polynomial $p(X) = X^r - p_1 X^{r-1} - \cdots - p_r$, with $r > 0$ and $p_r \neq 0$ such that

$$f_n = p_1 f_{n-1} + \cdots + p_r f_{n-r} \qquad \text{for all } n \in \mathbf{Z}. \tag{1}$$

The recurrence relation given by Equation (1) can also be read as

$$f_m = p_r^{-1}(f_{m+r} - p_1 f_{m+r-1} - \cdots - p_{r-2} f_{m+2} - p_{r-1} f_{m+1}),$$

letting $n - r = m$, so that each term is a fixed linear combination of the r subsequent terms, as well as the r previous terms. We refer to this as *back-solving*. Since $k[X, X^{-1}]$ is a Hopf algebra, so is $k[X, X^{-1}]^\circ$.

We now consider the following split short exact sequence:

$$0 \to K \to k[X]^\circ \underset{\beta}{\overset{\alpha}{\rightleftarrows}} k[X, X^{-1}]^\circ \to 0.$$

The map α is defined as follows. Suppose $f \in k[X]^\circ$ is a recursive sequence. Then $f \in (k[X]/((p(X)))^*$ for some $p(X) \in k[X]$. Write $p(X) = X^k q(X)$ with $q(X)$ a polynomial relatively prime to X. Then by the Chinese Remainder Theorem we have

$$k[X]/(p(X)) \cong k[X]/(X^k) \oplus k[X]/(q(X)).$$

Also

$$K[X]/(q(X)) \cong k[X, X^{-1}]/(q(X)).$$

These two isomorphisms give an embedding

$$k[X, X^{-1}]/(q(X)) \subseteq k[X]/(p(X)).$$

This embedding gives a coalgebra homomorphism

$$(k[X]/(p(X)))^* \to (k[X, X^{-1}]/(q(X)))^*.$$

Since $k[X]^\circ$ is the union of the subcoalgebras $(k[X]/(p(X)))^*$ and $k[X, X^{-1}]^\circ$ is the union of the subcoalgebras $(k[X, X^{-1}]/(q(X)))^*$, we get a coalgebra homomorphism

$$\alpha : k[X]^\circ \to k[X, X^{-1}]^\circ.$$

We show below that α is also an algebra homomorphism.

In concrete terms, the map α is described as follows. If f is a recursive sequence which satisfies the polynomial $p(X) = X^k q(X)$, by back-solving we can find a doubly-infinite recursive sequence (which satisfies the polynomial $q(X)$) which agrees with f at all points except possibly for $f_0, \ldots, f_{k-1}$. This doubly-infinite recursive sequence is $\alpha(f)$. Note that $\alpha(f)$ is uniquely determined by f. To see that α is an algebra homomorphism, note that $\alpha(fg)_n = \alpha(f)_n \alpha(g)_n$ for all n sufficiently large, since the sequence $\alpha(f)_n$ agrees with the sequence f_n for n sufficiently large. Therefore $\alpha(fg)_n = \alpha(f)_n \alpha(g)_n$ for all n by back-solving from that point.

The map β is induced by the embedding $k[X] \to k[X, X^{-1}]$. It is simply the restriction of a doubly-infinite recursive sequence to the nonnegative integers.

Clearly β is a bialgebra homomorphism. Note that $\alpha\beta = I$. The kernel K of α is given by

$$K = \operatorname{Ker}\alpha = \{f \mid f((X^k)) = 0 \text{ for some } k \geqq 0\}.$$

That is, K is the set of sequences which are 0 almost everywhere.

More precisely, K is a bialgebra ideal in $k[X]^\circ$, and $k[X, X^{-1}]^\circ$ is isomorphic to a subbialgebra of $k[X]^\circ$, and we have

$$k[X]^\circ \cong k[X, X^{-1}]^\circ \oplus K. \tag{2}$$

We wish to determine the units in the algebra $k[X]^\circ$. If $f \in k[X]^\circ$ is a unit, then $\alpha(f) \in k[X, X^{-1}]^\circ$ is a unit. Conversely, suppose $\alpha(f)$ is a unit in $k[X, X^{-1}]^\circ$. Let $g = \alpha(f) \in k[X, X^{-1}]^\circ$. From Equation (2) we can write

$$f = g + z = g(1 + g^{-1}z)$$

so that, since $g = \alpha(f)$ is a unit, f is a unit if and only if $1 + g^{-1}z$ is a unit. But this is a recursive sequence which is 1 almost everywhere, so it is a unit in $k[X]^\circ$ if and only if it is nowhere 0.

This gives a method for deciding whether $f \in k[X]^\circ$ is a unit in terms of whether $\alpha(f) \in k[X, X^{-1}]^\circ$ is a unit:

PROPOSITION 2.1. *Let $f \in k[X]^\circ$. Then*

(1) *if $\alpha(f) \in k[X, X^{-1}]^\circ$ is not a unit, then f is not a unit;*

(2) *if $\alpha(f) \in k[X, X^{-1}]^\circ$ is a unit, and $f_0, \ldots, f_{k-1}$ are all nonzero, where X^k is the maximum power of X dividing some polynomial $p(X)$ associated with f, then f is a unit in $k[X]^\circ$.*

PROOF. Part (1) follows immediately from that fact that units are mapped into units by algebra homomorphisms. To prove part (2), we observe that if we write $p(X) = X^k q(X)$, then if we identify f with an element of $(k[X]/(p(X))^*$ and $g = \alpha(f)$ with an element of $(k[X, X^{-1}]/(q(X))^*$, we have that $f = g + z$, where $z \in (k[X]/(X^k))^*$, the set of sequences (z_n) such that $z_n = 0$ for $n \geqq k$, so that if $g^{-1} \in k[X, X^{-1}]^\circ$, and if $f_0 f_1, \ldots, f_{k-1} \neq 0$, then $f^{-1} \in k[X]^\circ$: if g^{-1} satisfies $r(X)$, then f^{-1} satisfies $X^k r(X)$. This completes the proof of the proposition.

Note that Proposition 2.1 gives us an effective method for determining whether $f \in k[X]^\circ$ is a unit, assuming that

(1) we have an effective method for determining a polynomial $p(X)$ which f satisfies;

(2) we have an effective method for determining whether a doubly infinite sequence $f \in k[X, X^{-1}]^\circ$ is a unit.

We will discuss item (2) in Section 4.

We can use Proposition 2.1 to show that the inverse of the Fibonacci sequence is not recursive. The Fibonacci sequence 1, 1, 2, ... in $k[X]^\circ$ maps to the sequence

$$\ldots, 2, -1, 1, 0, 1, 1, 2, \ldots$$

which is obviously not invertible.

We will prove the following theorems, which are just restatements of Theorems 1.1 and 1.2

THEOREM 2.2. *The sequence $f \in k[X]^\circ$ is invertible if and only if $f(X^n) \neq 0$ for $n \geqq 0$, and f agrees with an interlacing of finitely many geometric series, except for a finite number of terms.*

In fact, if f satisfies the polynomial $X^k q(X)$ with $q(X)$ not divisible by X, the finite number of exceptional points must lie among $f_0, \ldots, f_{k-1}$.

THEOREM 2.3. *Let f, g be linearly recursive sequences with $fg = 0$. Then except for a finite number of terms, f is the interlacing of the t sequences f_i, g is the interlacing of the t sequences g_i, for $i = 0, \ldots, t-1$, and there is a partition $\{0, \ldots, t-1\} = I \cup J$ such that $f_i = 0$ for all $i \in I$ and $g_i = 0$ for all $i \in J$.*

3. The Hopf algebra $k[X, X^{-1}]^\circ$

In this section we investigate the structure of the Hopf algebra $k[X, X^{-1}]^\circ$. We will prove two theorems, which imply Theorems 2.2 and 2.3.

THEOREM 3.1. *The sequence $f \in k[X, X^{-1}]^\circ$ is invertible if and only if f is an interlacing of finitely many nonzero geometric sequences.*

In proving this theorem, we may assume that the field k is algebraically closed. For if f is invertible, it is invertible when we extend the scalars to $\bar{k}$, the algebraic closure of k. If f is a linearly recursive sequence over k, and is a geometric series (ba^n) over $\bar{k}$, then $b \in k$, since $f_0 = b \in k$. Since $b \in k$ and $f_1 = ba \in k$, it follows that $a \in k$. Therefore f is a geometric sequence over k. It is obvious that if f is an interlacing of a finite set of sequences over $\bar{k}$, it is an interlacing of the same sequences over k.

The second theorem is the following.

THEOREM 3.2. *The sequences $f, g \in k[X, X^{-1}]^\circ$ satisfy $fg = 0$ if and only if for some $t > 0$, f is the interlacing of the t sequences f_i, g is the interlacing of the t sequences g_i, and there is a partition $\{0, \ldots, t-1\} = I \cup J$ such that $f_i = 0$ for all $i \in I$, and $g_i = 0$ for all $i \in J$.*

In proving this theorem it is clear that we may assume that k is algebraically closed. To prove Theorems 3.1 and 3.2 we must examine the structure of the Hopf algebra $k[X, X^{-1}]^\circ$.

We first identify the grouplike elements $G(k[X, X^{-1}]^\circ)$ and the irreducible Hopf subalgebra $\mathbf{u}(k[X, X^{-1}]^\circ)$.

Let $f \in G(k[X, X^{-1}]^\circ)$. Direct computation gives $f(X^{i+j}) = f(X^i)f(X^j)$, that is, $f_{i+j} = f_i f_j$ for $i, j \in \mathbf{Z}$. In particular, $f_0^2 = f_0$. If $f_0 = 0$, then $f_i = f_{0+i} = f_0 f_i = 0 f_i = 0$. Therefore $f_0 = 1$. Since $f_0 = f_1 f_{-1}$, we have that $f_1 \neq 0$. A simple application of mathematical induction gives that $f_n = f_1^n$ for $n \geqq 0$. Since $f_0 = f_n f_{-n}$, we have that $f_n = f_1^n$ for all $n \in \mathbf{Z}$. Let $\mathbf{e}(a)$ denote the geometric sequence $(a^n)_{n \in \mathbf{Z}}$. We have shown that if $f \in G(k[X, X^{-1}]^\circ)$, then $f = \mathbf{e}(f_1)$ and $f_1 \neq 0$. Note that $\mathbf{e}(ab) = \mathbf{e}(a)\mathbf{e}(b)$. This proves that the group $G(k[X, X^{-1}]^\circ)$ is isomorphic to the multiplicative group $k^\times$ of nonzero elements of k.

Recall that if k has characteristic 0, then $\mathbf{u}(k[X, X^{-1}]^\circ)$ is just the universal enveloping algebra of the Lie algebra of primitive elements of $k[X, X^{-1}]^\circ$. We now determine $P(k[X, X^{-1}]^\circ)$. If $f \in P(k[X, X^{-1}]^\circ)$, then $f_{m+n} = f(X^{m+n}) = f(X^m X^n) = \varepsilon(X^m)f(X^n) + F(X^m)\varepsilon(X^n) = f_m + f_n$. It follows that $f_n = nf_1$. We have proved that $P(k[X, X^{-1}]^\circ) = kD$, where $D(X^n) = n$, so that if k has characteristic 0, we have that $\mathbf{u}(k[X, X^{-1}]^\circ) \cong k[D]$.

For arbitrary k, $\mathbf{u}(k[X, X^{-1}]^\circ) = \bigcup_{n=0}^{\infty} \mathbf{u}_n(k[X, X^{-1}]^\circ)$. We will prove that $\mathbf{u}_n(k[X, X^{-1}]^\circ)$ is the set of sequences which satisfy the polynomial $(X-1)^{n+1}$. For $n = 0$, we have that $\mathbf{u}_0(k[X, X^{-1}]^\circ) = k1$, the set of constant sequences. On the other hand, the sequences to which the polynomial $X - 1$ is associated are exactly the constant sequences. Now suppose $n > 0$. Then $f \in \mathbf{u}_n(k[X, X^{-1}]^\circ)$ if and only if $\Delta(f) \in k1 \otimes k[X, X^{-1}]^\circ + k[X, X^{-1}]^\circ \otimes \mathbf{u}_{n-1}(k[X, X^{-1}]^\circ)$, which is true if and only if $\Delta(f)(p \otimes q) = 0$ for all $p \in (X-1)$, $q \in (X-1)^n$, which is true if and only if $f(((X-1)^{n+1})) = 0$.

Suppose now that the characteristic of k is $p > 0$. Then for $r \geqq 0$ we have that $\mathbf{u}_{p^r-1}$ is the set of sequences which satisfy $(X-1)^{p^r} = X^{p^r} - 1$, the set of periodic sequences with period p^r. This is clearly a separable algebra, since it has a basis of orthogonal idempotents $v_0, v_1, \ldots, v_{p^r-1}$ defined by

$$v_i(X^j) = \begin{cases} 1 & \text{if } j \equiv i \pmod{p^r}, \\ 0 & \text{otherwise.} \end{cases}$$

We will use the following lemmas in the proofs of Theorems 3.1 and 3.2.

LEMMA 3.3. *Let k be a field, and let A be an algebra over k with no nonzero nilpotent elements. Then the units of the polynomial algebra $A[X]$ all lie in A.*

PROOF. This is found in [1, page 11].

LEMMA 3.4. *Let F be a finitely generated free abelian group. Then the units of the group algebra kF are all of the form cg, where $c \in k$, $c \neq 0$, and $g \in F$.*

PROOF. This follows immediately from material in [4, Section 26].

LEMMA 3.5. *Let F be a finitely generated free abelian group. Then the group algebra kF has no nontrivial zero divisors. The polynomial algebra $kF[X]$ has no nontrivial zero divisors.*

PROOF. This follows immediately from material in [4, Section 26]. Since kF has no nontrivial zero divisors, neither does $kF[X]$.

The "if" portion of Theorem 3.1 is trivial. We now prove the "only if" portion. Suppose that k has arbitrary characteristic. Denote $\mathbf{u}_n(k[X, X^{-1}]^\circ)$ by $\mathbf{u}_n$ and $\mathbf{u}(k[X, X^{-1}]^\circ)$ by $\mathbf{u}$. Suppose that $f \in k[X, X^{-1}]^\circ$ is invertible. Let

$$p(X) = (X - b_1)^{f_1} \cdots (X - b_r)^{f_r}$$

be the polynomial of minimal degree associated with the sequence f, and let

$$q(X) = (X - c_1)^{g_1} \cdots (X - c_s)^{g_s}$$

be the polynomial of minimal degree associated with the sequence f^{-1}. Let $\{a_1, \ldots, a_t\}$ be the set of roots of the polynomials $p(X)$ and $q(X)$, and let e_i be the largest of the multiplicities with which a_i occurs in the polynomials $p(X)$ and $q(X)$. Then

$$f, f^{-1} \in \mathbf{e}(a_1)\mathbf{u}_{e_1 - 1} \oplus \cdots \oplus \mathbf{e}(a_t)\mathbf{u}_{e_t - 1}.$$

Let G be the subgroup of $k^\times$ generated by $\{a_1, \ldots, a_t\}$. Since G is a finitely generated abelian group, $G \cong K \times F$, where K is a finite group, and F is a finitely generated free group. Since K is isomorphic to a finite subgroup of $k^\times$, K is cyclic, and its order is not divisible by the characteristic of k.

If the characteristic of k is 0, then f and f^{-1} are in $kK \otimes kF \otimes k[D]$. Lemma 3.3 implies that f and f^{-1} are in $kK \otimes kF$.

If the characteristic of k is $p > 0$, let p^r be the smallest power of p satisfying $p^r \geqq e_i$ for $i = 1, \ldots, t$. In this case f and f^{-1} are in $kK \otimes kF \otimes \mathbf{u}_{p^r - 1}$.

Since the characteristic of k does not divide the order of K, kK is a semisimple algebra (see [3, Theorem (10.8)]). In particular, since k is algebraically closed and K is abelian, kK has a basis of orthogonal idempotents. We give an explicit description of these idempotents. Let $m = |K|$, and let $\zeta \in k$ be a primitive mth root of 1. Then

$$K = \{\mathbf{e}(\zeta^j) \mid j = 0, \ldots, m-1\}.$$

The character χ_i of K is defined by

$$\chi_i(\mathbf{e}(\zeta^j)) = \zeta^{ij},$$

for $i, j = 0, \ldots, m-1$. The orthogonal idempotents in the basis of kK are therefore given by

$$z_i = \frac{1}{m} \sum_{j=0}^{m-1} \zeta^{-ij} \mathbf{e}(\zeta^j).$$

(The proof of [3, Theorem (33.8)] works in this case, even though that theorem is stated only for characteristic 0.)

We now determine which linearly recursive sequence is represented by the idempotent z_i:

$$\begin{aligned} z_i(X^n) &= \frac{1}{m} \sum_{j=0}^{m-1} \zeta^{-ij} \zeta^{nj} \\ &= \frac{1}{m} \sum_{j=0}^{m-1} \zeta^{(n-i)j} \\ &= \delta_{n \bmod m,\, i}. \end{aligned}$$

In other words, the linearly recursive sequence represented by z_i has 1 in its $(i + xm)$th position, and has 0 elsewhere. Therefore the linearly recursive sequences in kK are the periodic sequences of period m.

Suppose that the characteristic of k is 0. Since $kK \otimes kF$ has no nonzero nilpotent elements, Lemma 3.3 implies that any invertible $f \in kK \otimes kF$. Since $kK = \bigoplus_{i=0}^{m-1} kz_i$, it follows that $kK \otimes kF = \bigoplus_{i=0}^{m-1} kFz_i$. It follows from Lemma 3.4 that if f is invertible,

$$f = \sum_{i=0}^{m-1} c_i \mathbf{e}(a_i) z_i,$$

with $a_i \in F$, $c_i \in k$ and $c_i \neq 0$. This says that f is the interlacing of the m geometric sequences $(c_i a_i^n)$.

A more direct way to see that a Hadamard invertible sequence f must be an interlacing of geometric sequences in characteristic 0 is as follows. For $0 \leqq i < m$ let $T_i : kK \times F \to kF$ be defined by

$$T_i(\mathbf{e}(a)) = a^i \mathbf{e}(a^m).$$

It is easily checked that T_i is an algebra homomorphism. If $f = \Sigma_l d_l \mathbf{e}(b_l) \in kK \times F$ is invertible, then $T_i(f)$ is invertible, and so must be of the form $c_i \mathbf{e}(a_i)$. We claim that f is the interlacing of the m geometric sequences $(c_i a_i^n)$. To see this, note that the $(i + jm)$th term of f is $\Sigma_l d_l b_l^{i+jm}$, which is the jth term of $T_i(f)$, and so equals $c_i a_i^j$. Therefore f is the claimed interlacing.

Suppose now that the characteristic of k is $p > 0$, and we have that f, $f^{-1} \in kK \otimes kF \otimes \mathbf{u}_{p^r-1}$. Let $A = kK \otimes \mathbf{u}_{p^r-1}$. The algebra A has a basis of orthogonal idempotents $w_l = z_i v_j$, where $i = 0, \ldots, m-1, j = 0, \ldots, p^r - 1$, and $l = ip^r + jm$. Note that w_l is the linearly recursive sequence which has 1 in its $(ip^r + jm + xmp^r)$th positions, and 0 in its other positions. Note that

$$A \otimes kF = \bigoplus_{l=0}^{mp^r-1} kFw_l,$$

and that $kFw_l \cong kF$. Therefore

$$f = \sum_{l=0}^{mp^r-1} c_l \mathbf{e}(a_l) w_l$$

with $a_l \in F$, $c_l \in k$ and $c_l \neq 0$. Therefore f is the interlacing of the mp^r geometric sequences $(c_l a_l^n)$. This completes the proof of Theorem 3.1.

To prove Theorem 3.2, we observe that as in the proof of Theorem 3.1 we may assume that f and $g \in \bigoplus_{i=0}^{t-1} kFw_i$ (if the characteristic of k is $p > 0$), or that f and $g \in \bigoplus_{i=0}^{t-1} kFz_i[D]$ (if the characteristic of k is 0). If the characteristic of k is $p > 0$, since $(fw_i)(gw_i) = 0$, by Lemma 3.5 $fw_i = 0$ or $gw_i = 0$. That is, we have a partition $\{0, \ldots, t-1\} = I \cup J$ such that $fw_i = 0$ if $i \in I$, and $gw_i = 0$ if $i \in J$. A similar argument with w_i replaced by z_i applies in the case where the characteristic of k is 0.

The decompositions $f = \Sigma\, fw_i$, $g = \Sigma\, gw_i$ (or in characteristic 0, $f = \Sigma\, fz_i$, $g = \Sigma\, gz_i$) correspond to representations of f and g as interlacing of sequences f_i and g_i. The fact that $fw_i = 0$ (or $fz_i = 0$) for $i \in I$ implies that $f_i = 0$ for $i \in I$. Similarly, $g_i = 0$ for $i \in J$. This completes the proof of Theorem 3.2.

4. Effectiveness of the determination of units in $k[X, X^{-1}]^\circ$

We now show that we have an effective means of deciding whether a recursive sequence $f \in k[X, X^{-1}]^\circ$ is Hadamard invertible. We have shown in Theorem 3.1 that f is Hadamard invertible if and only if it is an interlacing of geometric sequences. We must show that we can find from f alone a bound on the number of geometric sequences of which it is an interlacing, if it is Hadamard invertible.

We first prove a lemma which we will use in the proof of the main theorem of this section.

LEMMA 4.1. *Let F be a free subgroup of $k^\times$. A sequence $g \in k[X, X^{-1}]^\circ$ satisfying the polynomial $p(X)$, all of whose roots are in F, is Hadamard invertible if and only if it is a geometric sequence.*

PROOF. The "if" portion of the lemma is immediate. We now prove the "only if" portion. By Theorem 3.1, since g is invertible, it is the interlacing of s geometric sequences $g_0, \ldots, g_{s-1}$, with $g_i = d_i \mathbf{e}(b_i)$. Since $g \in kF$, we have

$$g = \sum_{j=1}^{t} c_j \mathbf{e}(a_j)$$

with the $a_j \in F$ distinct. Now

$$g_i = \sum_{j=1}^{t} c_j a_j^i \mathbf{e}(a_j^s) \qquad \text{for } i = 0, \ldots, s-1.$$

Therefore

$$\sum_{j=1}^{t} c_j a_j^i \mathbf{e}(a_j^s) = d_i \mathbf{e}(b_i) \qquad \text{for } i = 0, \ldots, s-1. \tag{3}$$

Since F is free and the a_j are distinct, it follows that the a_j^s are distinct. Now Equation (3), which holds in the group algebra of the group $k^\times$, implies that $s = 1$. Therefore g is a geometric sequence. This completes the proof of the lemma.

We now prove a theorem which allows the effective determination of whether a linear recursive sequence in $k[X, X^{-1}]^\circ$ is Hadamard invertible.

THEOREM 4.2. *Let the sequence $f \in k[X, X^{-1}]^\circ$ satisfy the polynomial $p(X)$. Suppose that the order of the torsion subgroup of the subgroup of $k^\times$ generated by the roots of $p(X)$ is m. If the charactersitic of k is $p > 0$, let p^r be the*

smallest power of p not less than the largest multiplicity of the roots of $p(X)$. *Then f is a unit if and only if f is the interlacing of m geometric sequences if the characteristic of k is* 0, *or* mp^r *geometric sequences if the characteristic of k is* $p > 0$.

PROOF. The "if" portion of the theorem is immediate. We now prove the "only if" portion. Let G be the subgroup of $k^\times$ generated by the roots of the polynomial $p(X)$. We know that $G \cong K \times F$, where K is a finite group, and F is a finitely generated free group. If the characteristic of k is 0, let $t = m$; if the characteristic of k is $p > 0$, let $t = mp^r$. The proof of the "only if" portion of Theorem 3.1 (which follows Lemma 3.5) can be used to show that f is the interlacing of t sequences $f_i \in kF$. Since f is an invertible linearly recursive sequence, it follows that the sequences f_i are invertible. By Lemma 4.1, the sequences f_i are geometric sequences. This completes the proof of the theorem.

Theorem 4.2 can be used effectively to determine whether $f \in k[X, X^{-1}]^\circ$ satisfying the minimal polynomial $p(X)$ is Hadamard invertible. To do so, we first determine the order m of the torsion subgroup of the subgroup of $k^\times$ generated by the roots of $p(X)$. (If the characteristic of k is $p > 0$, we also determine the smallest power p^r of p not less than the multiplicities of the roots of $p(X)$.) Examination of the first $3m$ (or $3mp^r$) terms of the series gives the polynomial $(X^m - a_1)\cdots(X^m - a_m)$ which is the polynomial which an interlacing of the m geometric series $(b_i a_i^m)$ must satisfy. Then we simply determine whether $p(X)$ divides this polynomial.

Note that $p(X)$ might properly divide the polynomial $(X^m - a_1)\cdots(X^m - a_m)$. For example, if the characteristic of k is not 2, the sequence

$$\ldots, 1, 1, 1, 2, 1, 1, 4, 1, 1, \ldots$$

given by

$$f_0, f_1, f_2 = 1$$

$$f_3 = 2$$

$$f_4, f_5 = 1$$

$$f_n = 3f_{n-3} - 2f_{n-6} \qquad \text{for } n \geqq 6$$

satisfies the polynomial $p(X) = X^6 - 3X^3 + 2 = (X^3 - 2)(X^3 - 1)$. It is the interlacing of three geometric sequences $1, 2, 4, \ldots, 1, 1, 1, \ldots$, and

$1, 1, 1, \ldots$, which tell us that it satisfies the polynomial $(X^3 - 2)(X^3 - 1)^2$ which is a proper multiple of $p(X)$.

We now give an example to illustrate the use of Theorem 4.2 to show that a sequence is not Hadamard invertible. Let the characteristic of k be 0, and let f be the sequence

$$\ldots, 1, 3, 7, 15, 31, \ldots$$

given by

$$f_0 = 1$$

$$f_1 = 3$$

$$f_n = 3f_{n-1} - 2f_{n-2} \qquad \text{for } n \geqq 2$$

Then f satisfies $p(X) = X^2 - 3X + 2 = (X - 1)(X - 2)$. The subgroup of $k^\times$ generated by the roots of $p(X)$ has torsion subgroup equal to $\{1\}$, so that if f is Hadamard invertible, f must be a geometric sequence, which it is clearly not. Therefore f is not Hadamard invertible.

References

1. M. F. Atyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

2. B. Benzaghou, *Algèbres de Hadamard*, Bull. Soc. Math. France **98** (1970), 209–252.

3. C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley–Interscience, New York, 1962.

4. D. S. Passman, *Infinite Group Rings*, Marcel Dekker, New York, 1971.

5. B. Peterson and E. J. Taft, *The Hopf algebra of linearly recursive sequences*, Æquationes Math. **20** (1980), 1–17.

6. A. J. van der Poorten, *Some facts that should be better known, especially about rational functions*, in *Number Theory and Applications* (R. A. Mollin, ed.), Kluwer Acad. Publ., Dordrecht, 1989.

7. C. Reutenauer, *Sur les éléments inversibles de l'algèbre de Hadamard des séries rationelles*, Bull. Soc. Math. France **110** (1982), 225–232.

8. C. Ronse, *Feedback Shift Registers*, Springer-Verlag, Berlin, 1984.

9. M. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.