On the classification of binary shifts of finite commutant index

Geoffrey L. Price†

Department of Mathematics 9E, United States Naval Academy, Annapolis, MD 21402

Edited by Richard V. Kadison, University of Pennsylvania, Philadelphia, PA, and approved October 19, 1999 (received for review October 8, 1999)

We provide a complete classification up to conjugacy of the binary shifts of finite commutant index on the hyperfinite *II_1* factor. There is a natural correspondence between the conjugacy classes of these shifts and polynomials over *GF*(2) satisfying a certain duality condition.

conjugacy class | subfactor index

1. Introduction

Let R denote the hyperfinite II_1 factor. A pair of *-automorphisms σ, ρ on R are said to be conjugate if there exists a *-automorphism γ on R that satisfies $\gamma \circ \sigma(A) = \rho \circ \gamma(A)$ for all A in R. The notion of conjugacy carries over to the setting of unital *-endomorphisms on R. In this situation, it turns out that the Jones index $[R : \sigma(R)]$ of the subfactor $\sigma(R)$ in R is a numerical conjugacy invariant, as is the commutant (or relative commutant) index: this is the first positive integer k (or ∞) for which the relative commutant algebra $\sigma^k(R)' \cap R$ is nontrivial.

In ref. 1 R. T. Powers introduced a family of unital *-endomorphisms on R known as binary shifts. The range $\sigma(R)$ of each binary shift σ is a subfactor of index 2. As a result, the minimal possible commutant index for a binary shift is 2 (ref. 2). Powers has shown in ref. 1 that there exist binary shifts of any specified commutant index $k \in \{\infty, 2, 3, \ldots\}$. In particular, he showed that for any finite commutant index there are at most countably many conjugacy classes but that there are uncountably many conjugacy classes having infinite commutant index (see *Theorem 2.4*).

In ref. 3, we gave a complete classification of the conjugacy classes of binary shifts of commutant index 2. We showed that there is a natural correspondence between the conjugacy classes of these shifts and polynomials with coefficients in $GF(2)$ that satisfy a certain duality condition (see *Theorem 2.7*). These are the polynomials that have constant coefficient 1 and that have no self-reciprocal factors (see *Definition 2.2*) of degree greater than 1. In this paper, we show that there is an analogous correspondence between binary shifts of any finite commutant index $k \geq 2$ and polynomials over $GF(2)$ with constant coefficient 1 and no self-reciprocal factors of degree exceeding $2k-3$. Unlike the case for $k = 2$, the correspondence for higher commutant indices is not one-to-one, but we produce a recursion formula **5.1** that relates the number of conjugacy classes of binary shifts of commutant index k that are associated with each of the polynomials of the form described above. As a consequence, we can provide precise information, for example, on the number of binary shifts of fixed finite commutant index that are associated with any irreducible polynomial $p(x)$ over $GF(2)$.

2. Preliminaries

In this section, we present Powers' construction of the binary shifts on R. We also state some of the results that are known about binary shifts and that are relevant to their classification up to conjugacy. In particular, we shall exploit the close connections existing between the theory of recurring linear sequences and binary shifts. See ref. 4, chapter 6, for an extensive bibliography on the subject of recurring linear sequences.

Let X be a (finite or infinite) subset of $\mathbb{N}$, with characteristic function $g: \mathbb{N} \to \{0, 1\}$. Let $\{u_0, u_1, \ldots\}$ be a sequence of hermitian unitary operators (or generators) that satisfy the commutation relations

$$u_i u_{i+j} = (-1)^{g(j)} u_{i+j} u_i,\ i, j \in \mathbb{Z}^+. \qquad \textbf{[2.1]}$$

One may define words in the generators by setting, for finite ordered subsets $J = \{j_0, j_1, \ldots, j_m\}$ of distinct nonnegative integers, $u(J) = u_{j_0} u_{j_1} \cdots u_{j_m}$, and $u(\emptyset) = I$, the identity. In fact, because the u_j values are hermitian and satisfy **2.1**, any product of the generators may be rewritten as either $+u(J)$ or $-u(J)$ for some finite ordered subset $J \subset \mathbb{Z}^+$. (See ref. 5 for a concrete realization of these generators as operators on a Hilbert space.) For $n \in \mathbb{N}$, let $\mathfrak{A}_n$ be the finite-dimensional group algebra over $\mathbb{C}$ consisting of linear combinations of the words in the generators $\{u_0, u_1, \ldots, u_{n-1}\}$. Note that $\mathfrak{A}_n$ has dimension 2^n, the number of words in the generators. Because $\mathfrak{A}_n \subset \mathfrak{A}_{n+1}$ for all $n \in \mathbb{N}$, one may obtain an $AF-$algebra by taking the uniform closure of the union $\bigcup_{n=1}^{\infty} \mathfrak{A}_n$. Following the terminology of ref. 1, definition 3.2, we refer to $\mathfrak{A}$ as the binary shift algebra associated with X. The binary shift itself is the unital *-homomorphism on $\mathfrak{A}$ defined uniquely by the mappings $\sigma(u_j) = u_{j+1}$ on the generators. We shall refer to X as the *anticommutation set*, to $\mathbf{a} = \{a_0, a_1, \ldots\}$, where $a_j = g(j)$, as the *bitstream*, and to $\check{\mathbf{a}} = \{\ldots, a_2, a_1, a_0, a_1, a_2, \ldots\}$ as the *reflected bitstream* associated with σ.

If the reflected bitstream is periodic, it is easy to see that $\mathfrak{A}$ has a nontrivial center. In fact, if $\check{\mathbf{a}}$ has period length p the word $u_0 u_p$ (as well as its shifts) lies in the center. On the other hand, $\mathfrak{A}$ has trivial center if $\check{\mathbf{a}}$ is not periodic.

THEOREM 2.1 (from ref. 1, theorem 3.9; ref. 6, theorem 2.3; and ref. 7, corollary 5.5). *Let $\mathfrak{A}$ be the binary shift algebra with anticommutation set X and corresponding bitstream given by $a_j = g(j)$, $j \in \mathbb{Z}^+$. Then the following conditions are equivalent.*

(i) *$\check{\mathbf{a}}$ is not periodic.*
(ii) *The center of $\mathfrak{A}$ consists of scalar multiples of the identity.*
(iii) *For any nontrivial word w, $wu_j = -u_j w$ for some u_j.*
(iv) *$\mathfrak{A}$ has a unique normalized trace.*
(v) *$\mathfrak{A}$ is isomorphic to the UHF algebra of type 2^∞.*

Hence if any of the above conditions hold, then in the trace representation of $\mathfrak{A}$, the weak operator closure of $\mathfrak{A}$ is isomorphic to the hyperfinite II_1 algebra R.

It is straightforward to see that the binary shift σ on $\mathfrak{A}$ extends to a unital *-homomorphism on R that we shall also denote by σ. Then we have the following results for binary shifts on R.

THEOREM 2.2 (from ref. 1, theorem 3.6). *A pair of binary shifts on R are conjugate if and only if they are defined via the same bitstream.*

THEOREM 2.3 (ref. 1 and ref. 2, example 2.3.2). *For any binary shift on R the subfactor $\sigma(R)$ has Jones index $[R : \sigma(R)] = 2$.*

This paper was submitted directly (Track II) to the PNAS office.

†E-mail: glp@usna.edu.

As a consequence of the previous theorem the minimal commutant index for a binary shift is 2 (ref. 2, corollary 2.2.4). On the other hand, if $X = \{k-1\}$, then $u_0 \in \sigma^k(R)' \cap R$, $\sigma^{k-1}(R)' \cap R = \mathbb{C}I$, so the associated binary shift has commutant index k. Hence, there exist examples of binary shifts for any finite commutant index $k \geq 2$. The following theorem characterizes those binary shifts with finite commutant index.

THEOREM 2.4 (from ref. 8, theorem 2.1, and ref. 9, theorem 5.8). *A binary shift on R has finite commutant index if and only if its bitstream* **a** *is eventually periodic. For a binary shift σ of finite commutant index k and generators u_j, $j \in \mathbb{Z}^+$, there is a word $w = u(j_0, j_1, \ldots, j_n)$ such that*

(*i*) *$j_0 = 0$, i.e., w "starts" with u_0, and*
(*ii*) *for any $s \geq 0$, $\sigma^{k+s}(R)' \cap R$ is a 2^s−dimensional algebra generated by the words $w, \sigma(w), \ldots, \sigma^r(w)$.*

Definition 2.1: Let σ be a binary shift on R with generators u_j, $j \in \mathbb{Z}^+$. Let z be a word in the generators, and let $p(x) = c_0 + c_1x + \cdots + c_nx^n$ be a polynomial with coefficients in $GF(2)$, then $\langle z, p\rangle$ shall denote the word $z^{c_0}\sigma(z)^{c_1}\cdots\sigma^n(z)^{c_n}$ in R.

Suppose $p(x)$ is the polynomial for which $w = \langle u_0, p\rangle$ in the preceding theorem. In the study of binary shifts of commutant index 2 in ref. 3, we described connections among polynomials $p(x)$, words $w = \langle u_0, p\rangle$ generating relative commutant algebras, and conjugacy classes of shifts. *Theorem 2.7* describes this connection. To state the theorem, we need to identify polynomials that possess a special symmetry.

Definition 2.2: A polynomial $p(x)$ with coefficients in $GF(2)$ and constant term 1 is called *reciprocal* or *self-reciprocal* if its coefficients are flip-symmetric (4, 10), i.e., $p(x) = c_0 + c_1x + \cdots + c_nx^n = c_n + c_{n-1}x + \cdots + c_0x^n$.

Remark 2.1: Note that if a polynomial $p(x) = c_0 + c_1x + \cdots + c_nx^n$ with constant coefficient 1, then $p^*(x) = x^n p(\frac{1}{n}) = c_n + c_{n-1}x + \cdots + c_0x^n$. Hence, $p(x)$ is reciprocal if and only if $p(x) = p^*(x)$.

The following results about reciprocal polynomials will be used in the next section.

LEMMA 2.5. *If $h(x)$ is a polynomial with constant coefficient 1, then $h^*(x)h(x)$ is reciprocal. The product of reciprocal polynomials is reciprocal.*

Proof: Obvious. □

THEOREM 2.6 (see ref. 3, theorem 4.3). *Any polynomial $p(x)$ with constant coefficient 1 has a unique reciprocal divisor of maximal degree.*

THEOREM 2.7. *Let $p(x)$ be a polynomial over $GF(2)$ with constant coefficient 1. Then there exists a binary shift of commutant index 2 and generators u_j, $j \in \mathbb{Z}^+$ such that $\langle u_0, p\rangle$ generates $\sigma^2(R)' \cap R$ if and only if $p(x)$ has no reciprocal factors of degree exceeding 1. Moreover there is a one-to-one correspondence between such polynomials and the family of binary shifts of commutant index 2.*

It is possible to show that among those polynomials of degree $n \geq 3$ whose constant coefficient is 1 there are 2^{n-2} that satisfy the hypotheses of the theorem, (ref. 3, theorem 4.4). Hence, there are countably many conjugacy classes of binary shifts of commutant index 2. *Corollary 5.5* establishes the same conclusion for any finite commutant index.

Although we are interested in analyzing binary shifts on R, it is useful for that purpose to understand the structure of the $AF-$algebras $[\bigcup_{n=1}^{\infty} \mathfrak{A}_n]^-$ that have nontrivial centers.

THEOREM 2.8. *Let* **a** *be a bitstream for which* $\check{\mathbf{a}}$ *is periodic. Let $\mathfrak{A}$ be the corresponding $AF-$algebra, and let τ be the trace on $\mathfrak{A}$ that vanishes on nontrivial words. Let M be the von Neumann algebra obtained by completing $\mathfrak{A}$ in the weak operator closure with respect to τ. Then there exists a word $w = \langle u_0, p\rangle = u_0^{c_0}u_1^{c_1}\cdots u_n^{c_n}$ such that*

(*i*) *$c_0 = 1$,*
(*ii*) *$p(x)$ is reciprocal, and*
(*iii*) *the center of M is generated by w and its shifts.*

Hence the center of M is isomorphic to the algebra of continuous functions on the Cantor set.

Suppose **a** is a bitstream in $GF(2)$ with $a_0 = 0$. Then for each $n \in \mathbb{N}$ one may construct an nxn Toeplitz matrix A_n whose first row consists of the first n elements of **a**, viz.,

$$A_n = \begin{bmatrix} a_o & a_1 & a_2 & a_3 & \cdots & a_{n-1} \\ a_1 & a_o & a_1 & a_2 & \cdots & a_{n-2} \\ a_2 & a_1 & a_o & a_1 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & \cdots & a_o \end{bmatrix} \qquad \textbf{[2.2]}$$

Because A_n is a skew-symmetric matrix, it has even rank (this holds true even for matrices over $GF(2)$ (ref. 11, theorem IV.11). The sequence of Toeplitz matrices associated with a bitstream has a rather remarkable property.

THEOREM 2.9 (from ref. 7, theorem 5.4). *Let $\nu(A_n)$ denote the nullity of the $n \times n$ Toeplitz matrix above. If* $\check{\mathbf{a}}$ *is not periodic, the sequence $\{\nu(A_n) : n \in \mathbb{N}\}$ consists of the concatenation of strings of non-negative integers of the form $1, 2, \ldots, m-1, m, m-1, \ldots, 2, 1, 0$. If* $\check{\mathbf{a}}$ *is periodic, then the nullity sequence consists of finitely many strings of the above mentioned form followed by the sequence $1, 2, \ldots$.*

THEOREM 2.10 (From ref. 12, corollary 2.10; see also ref. 13). *For any even positive integer n there are $2^{n-2}nxn$ invertible Toeplitz matrices of the form above.*

Finally, it will be helpful to use the following properties of the operations $\langle z, p\rangle$ for a word z in the generators of a binary shift on R and for polynomials $p(x)$ with coefficients in $GF(2)$ (see ref. 6, section 4):

$$\langle z, p\rangle\langle z, q\rangle = \pm\langle w, p+q\rangle \qquad \textbf{[2.3.1]}$$

$$\langle\langle w, p\rangle, q\rangle = \pm\langle w, pq\rangle \qquad \textbf{[2.3.2]}$$

3. Bitstreams and Polynomials

In this section, we prove some elementary results about bitstreams over finite fields that are based on some well-known results from the theory of linear recurring sequences (ref. 4, chapter 6). Our results stem from important connections that exist between eventually periodic bitstreams with entries in a finite field and polynomials with coefficients in the same field. Here we deal exclusively with the finite field $GF(2)$. We shall say that a polynomial $p(x) = c_0 + c_1x + \cdots + c_nx^n$ *annihilates* a bitstream **a** if for all $j \in \mathbb{Z}^+$, $\sum_{l=0}^{n} c_la_{j+l} = 0$. If a bitstream is eventually periodic, i.e., if there exists a positive integer s such that $a_k = a_{k+s}$ for all $k \geq N$, some N, then the polynomial $x^N + x^{N+s}$ annihilates **a**. In particular, one has the following result.

LEMMA 3.1 (cf. ref. 4, theorem 6.11). *A bitstream* **a** *over $GF(2)$ is eventually periodic if and only if it is annihilated by some polynomial $p(x)$ with coefficients in $GF(2)$.* **a** *is periodic if and only if it is annihilated by a polynomial with constant coefficient* 1.

If **a** and **b** are bitstreams, then define addition by $\mathbf{a} + \mathbf{b} = \mathbf{c}$, where $c_j = a_j + b_j$ for all $j \in \mathbb{Z}^+$. Defining scalar multiplication in the obvious way, one sees that the set of periodic (respectively, eventually periodic bitstreams) forms a vector space over $GF(2)$: for if **a** is periodic (respectively, eventually periodic) with period s and **b** is periodic (respectively, eventually periodic) with period t, then **c** is periodic (respectively, eventually periodic) with period a divisor of st (4). The same is true for doubly infinite periodic sequences, and also for the subset consisting of those reflected bitstreams $\check{\mathbf{a}} = \{\ldots, a_2, a_1, a_0, a_1, a_2, \ldots\}$, $a_0 = 0$, which are periodic. Thus we have the following:

MATHEMATICS

LEMMA 3.2. *With the addition and multiplication operations as defined above, the set of periodic reflected bitstreams forms a vector space over* $GF(2)$.

Definition 3.1 (cf. ref. 4, section 6.5): For a polynomial $p(x)$ with coefficients in $GF(2)$ and constant coefficient 1, let $S(p)$ be the vector space of periodic reflected bitstreams annihilated by $p(x)$.

PROPOSITION 3.3. *Suppose* $\check{\mathbf{a}}$ *is a periodic reflected bitstream in* $S(p)$. *If* $r(x)$ *is the maximal reciprocal factor of* $p(x)$ *then* $\check{\mathbf{a}} \in S(r)$.

Proof: Because the reflected bitstream $\check{\mathbf{a}}$ is symmetric about its entry $a_0 = 0$, it is clear that $p(x)$ annihilates $\check{\mathbf{a}}$ if and only if $p^*(x)$ does too (see *Remark 2.1*). Hence $\check{\mathbf{a}} \in S(p) \cap S(p^*)$. But for any pair p, q of polynomials, $S(p) \cap S(q) = S(gcd(p,q))$, by ref. 4, theorem 6.54. Clearly r divides the polynomial $d = gcd(p, p^*)$. Suppose $p(x)/r(x) = \prod h_i(x)$, where the h_i values are irreducible, then clearly $d(x) = r(x) \cdot gcd(\prod h_i(x), \prod h_i{}^*(x))$. But if $h(x)$ is an irreducible factor of both $\prod h_i(x)$ and $\prod h_i{}^*(x)$, then $h(x) = h_i(x) = h_j{}^*(x)$ for some i and j. But then by *Lemma 2.5*, $h_i(x)h_j(x) = h_i(x)h_i{}^*(x)$ is reciprocal, which contradicts the maximality of the degree of r. Hence $r = gcd(p, p^*) = S(p) \cap S(p^*)$ annihilates $\check{\mathbf{a}}$.

PROPOSITION 3.4. *Let* $r(x)$ *be a reciprocal polynomial with constant coefficient* 1 *and degree either* $2l$ *or* $2l+1$, $l \in \mathbb{Z}^+$, *The vector space of periodic reflected bitstreams annihilated by* $r(x)$ *has dimension* l.

Proof: Let $\check{\mathbf{c}} = \{\ldots, c_2, c_1, c_0, c_1, c_2, \ldots\}$ be a periodic reflected bitstream (with $c_0 = 0$). Because r is reciprocal of degree $2l$ or $2l+1$, and $\check{\mathbf{c}}$ is symmetric about c_0, r annihilates $\check{\mathbf{c}}$ if and only if it annihilates $\{c_l, c_{l-1}, \ldots, c_1, c_0, c_1, \ldots\}$. Because degree$(r) \in \{2l, 2l+1\}$, it is clear that $c_1, c_2, \ldots, c_l$ may be chosen arbitrarily but that $c_{l+1}, c_{l+2}, \ldots$ depend on the choice of c_1 through c_l.

COROLLARY 3.5. *If* $r(x)$ *is a reciprocal polynomial with constant coefficient* 1 *and degree either* $2l$ *or* $2l+1$, $l \in \mathbb{Z}^+$, *there are exactly* 2^l *periodic reflected bitstreams annihilated by* $r(x)$.

Definition 3.2: Let $k \geq 2$ be a fixed positive integer. Let $w = u_0^{c_0} u_1^{c_1} \cdots u_n^{c_n}$, with $c_0 = 1$, be a word in the generators u_j, $j \in \mathbb{Z}^+$ of a binary shift σ. Then w is called a qkword if $w \in \sigma^k(R)' \cap R$ but $w \notin \sigma^{k-1}(R)' \cap R$.

Remark 3.1: Suppose $\mathbf{a}$ is a bitstream and w is a word of the form above. By using **2.1** repeatedly, it follows that for $j \in \mathbb{Z}^+$, $wu_j = (-1)^{a_j c_0 + a_{j-1} c_1 + \cdots + a_{|n-j|} c_n} u_j w$. Hence w is a qkword if and only if there exists a bitstream $\mathbf{a}$ satisfying the following linear system.

$$
\begin{aligned}
a_{k-1}c_0 + a_{k-2}c_1 + a_{k-3}c_2 + \cdots + a_{|n-k-1|}c_n &= 1 \\
a_k c_0 + a_{k-1}c_1 + a_{k-2}c_2 + \cdots + a_{|n-k|}c_n &= 0 \\
a_{k+1}c_0 + a_k c_1 + a_{k-1}c_2 + \cdots + a_{|n-k+1|}c_n &= 0 \\
&\vdots
\end{aligned}
\qquad \textbf{[3.1]}
$$

The first equation holds because w must anticommute with u_{k-1} and the remaining equations hold because w commutes with $u_k, u_{k+1}, \ldots$.

Remark 3.2: As $[R : \sigma(R)] = 2$, $\sigma(R)' \cap R = \mathbb{C}I$ (ref. 2, corollary 2.2.4), so there are no q1words.

We shall see below that for fixed values $c_0, c_1, \ldots, c_n$ it is possible to have more than one bitstream $\mathbf{a}$ that satisfies **3.1**. For that reason, we shall need the following terminology.

Definition 3.3: Let $p(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial with constant coefficient 1. If the linear system above is satisfied then $p(x)$ is said to *meet* $\mathbf{a}$ *at the integer* k. If there is an integer k for which $p(x)$ meets $\mathbf{a}$, then we say that $(p, \mathbf{a})$ are a *binary pair*.

Remark 3.3: Note that if $(p, \mathbf{a})$ meet at k then if σ is the binary shift on R with generators u_j, $j \in \mathbb{Z}^+$ and bitstream $\mathbf{a}$, $w = \langle u_0, p\rangle \in \sigma^k(R)' \cap R$, $w \notin \sigma^{k-1}(R)' \cap R$. Hence w is a qkword and σ is a binary shift of commutant index $\leq k$. On the other hand, since 2 is the minimal possible commutant index for a binary shift, if a binary pair $(p, \mathbf{a})$ meet at 2 then σ has commutant index 2.

THEOREM 3.6. *Let* $k \geq 2$ *and* $n > 2k-2$ *be fixed integers. Then for any polynomial* $p(x)$ *of degree n and constant coefficient* 1 *there are at most* 2^{k-2} *distinct bitstreams* $\mathbf{a} = \{a_0, a_1, \ldots\}$ (*with* $a_0 = 0$) *which meet* $p(x)$ *at k.*

Proof: We sketch the induction proof. By using the remark above, a restatement of *Theorem 2.7* shows that any polynomial of any degree n with constant coefficient 1 can meet at most one bitstream $\mathbf{a}$ at the integer 2. Suppose the assertion holds for $j = 2, \ldots, k-1$, and suppose $\mathbf{a}, \mathbf{b}$ are bitstreams that meet $p(x)$ at k. Then if $\mathbf{s} = \mathbf{a} + \mathbf{b}$, it follows that either (i) the reflected bitstream $\check{\mathbf{s}}$ of $\mathbf{s}$ is periodic and annihilated by $p(x)$, or (ii) $p(x)$ meets $\mathbf{s}$ at j for some $j \in \{2, 3, \ldots, k-1\}$. One obtains the result by combining the induction assumption with the count, in *Corollary 3.5*, of the number of periodic reflected bitstreams annihilated by a reciprocal polynomial. □

4. Counting Polynomials with Symmetry

In this section, we complete the analysis necessary to enumerate the binary shifts of finite commutant index on the hyperfinite II_1 factor R. As in ref. 3, where a classification was made of the binary shifts of commutant index 2, we establish a natural connection between binary shifts of finite commutant index and polynomials over $GF(2)$ that satisfy a certain symmetry condition. In the course of making this connection, it is convenient first to study the family of binary pairs that meet at a fixed integer $k \geq 2$ (see *Definition 3.3*) and subsequently to match these pairs with binary shifts. In *Lemmas 4.1* and *4.2* we show that a polynomial $p(x)$ with constant coefficient 1 meets a bitstream at k if and only if $p(x)$ has no reciprocal factors of degree $\geq 2k-2$. Using these results, we are able to provide a recursion formula that counts, for each polynomial $p(x)$ above, the number of binary shifts σ of commutant index k, with generating family u_j, $j \in \mathbb{Z}^+$ of hermitian unitaries for which $\langle u_0, p\rangle$ generates the first nontrivial relative commutant algebra $\sigma^k(R)' \cap R$.

Recall that a polynomial $p(x) = c_0 + c_1 x + \cdots + c_n x^n$ with constant coefficient $c_0 = 1$ meets a bitstream $\mathbf{a}$ at an integer k if and only if the coefficients of $p(x)$ satisfy the infinite system **3.1** of linear equations over F. The first equation follows from **2.1** because $w = \langle u_0, p\rangle$ must anticommute with u_{k-1}. The remaining equations are satisfied because w commutes with the generators $u_k, u_{k+1}, \ldots$. If $n < 2k-2$, then $|n-k-1| < k-1$, and we observe that because $c_0 = 1$, for any choice of $a_1, a_2, \ldots, a_{k-2}$, there is one and only one choice of $a_{k-1}, a_k, \ldots$ such that the system holds. Hence w is a qkword which corresponds to exactly 2^{k-2} distinct bitstreams $\mathbf{a}$. This establishes the first assertion of the following result. We omit the analysis of the case $n = 2k-2$, whose proof we shall present elsewhere.

LEMMA 4.1. *If* $k \geq 2$ *and* $n < 2k-2$, *any polynomial of degree n with constant coefficient* 1 *meets at k with* 2^{k-2} *distinct bitstreams. If* $n = 2k-2$ *then there are* $2^{n-1} - 2^{n-k+1}$ *polynomials of degree n with constant coefficient* 1 *which meet at k with some bitstream. These are the polynomials which are not reciprocal. Each of these polynomials meets at k with* 2^{k-2} *distinct bitstreams.*

The analysis pertaining to polynomials of degree exceeding $2k-2$ is considerably more difficult, and we devote the remainder of this section to studying this case. As we shall see below, whether a polynomial of degree $n \geq 2k-2$ meets a bitstream at the integer k is determined by the degree of its maximal reciprocal factor. Polynomials with reciprocal factors of high degree will not correspond to qkwords, and therefore we will be led to counting the number of polynomial of fixed degree $n \geq 2k-2$ having maximal reciprocal factors exceeding a certain degree (see *Theorem 4.4*).

LEMMA 4.2. *Let $k \geq 2$. No polynomial $p(x)$ with coefficients in $GF(2)$, constant coefficient 1, and a reciprocal factor of degree $\geq 2k-2$ meets at k with any bitstream.*

Proof: Suppose $p(x) = q(x)r(x)$, where $r(x)$ is a reciprocal polynomial of degree $m \geq 2k-2$, and suppose $p(x)$ meets at k with some bitstream $\mathbf{a}$. Then there is a binary shift σ with generators u_j, $j \in \mathbb{Z}^+$, say, such that $w = \langle u_0, p\rangle$ is a qkword for σ. Let $z = \langle u_0, q\rangle$, then by **2.3** $w = \langle u_0, p\rangle = \langle u_0, qr\rangle = \pm\langle\langle u_0, q\rangle, r\rangle = \pm\langle z, r\rangle$. It is straightforward to see that if $z_j = \sigma^j(z)$, $j \in \mathbb{Z}^+$, then σ restricts to a binary shift on the von Neumann algebra M generated by the z_j values and $w \in \sigma^k(M)' \cap M$ but $w \notin \sigma^{k-1}(M)' \cap M$. Hence w anticommutes with z_{k-1} so that if $\mathbf{b}$ is the bitstream for the restricted binary shift on M and $r(x) = l_0 + l_1x + \cdots + l_mx^m$,

$$b_{k-1}l_0 + b_{k-2}l_1 + \cdots + b_{m-k+1}l_m = 1.$$

If $m = 2k-2$, then because $r(x)$ is reciprocal the left side becomes

$$b_{k-1}l_0 + b_{k-2}l_1 + \cdots + b_1l_{k-2} + b_0l_{k-1} + b_1l_{k-2} + b_{k-1}l_0,$$

which is 0, a contradiction. If $m > 2k-2$, then because $r(x)$ is reciprocal the equation may be rewritten as

$$b_{k-1}l_m + b_{k-2}l_{m-1} + \cdots + b_{m-k+1}l_0 = 1,$$

which implies that w anticommutes with z_{m-k+1}, also a contradiction (since $m-k+1 \geq k$ and $w \in \sigma^k(M)' \cap M$). By contradiction w cannot be a qkword. Equivalently, $p(x)$ does not meet at k with any bitstream. □

Remark 4.1: We shall see below (*Corollary 4.8*) that for $n \geq 2k-2$ all other polynomials with constant coefficient 1 meet at k with at least one bitstream. In fact, they meet at k with exactly 2^{k-2} bitstreams.

Below we shall count the number of polynomials of fixed degree $n \geq 2k-2$ which have maximal reciprocal factors of degree $\geq 2k-2$. To make this calculation, we require both a definition and a result from ref. 3.

Definition 4.1 (cf. ref. 3, definition 4.1): A polynomial $f(x) \in F[x]$ with constant coefficient 1 is *completely free* if $f(x)$ has no reciprocal factors except for the constant polynomial 1. $z(n)$ denotes the number of completely free polynomials of degree n with constant coefficient 1.

THEOREM 4.3 (from ref. 3, theorem 4.4). *Let $r \geq 1$ be a fixed integer. If $n = 2r$, then $z(n) = \frac{1}{3}(2\cdot 4^{r-1}+4)-2$ and if $n = 2r+1$ then $z(n) = \frac{1}{3}(4^r-4)+2$.*

Combining this result with a calculation similar to the one that appears in in ref. 3, theorem 4.4, one establishes the following.

THEOREM 4.4. *With the same notation as above, there are, for $n > 2k-2$, exactly 2^{n-k} polynomials of degree n with constant coefficient 1 whose maximal reciprocal factor has degree $\geq 2k-2$. If $n = 2k-2$ there are $2^{n-(k-1)} = 2^{k-1}$ such polynomials.*

COROLLARY 4.5. *With the same notation as above, let $n \geq 2k-2$ be a fixed integer. If $n = 2k-2$ then the number of polynomials of degree n with constant coefficient 1 which meet at k is at most $2^{n-1}-2^{k-1}$ (equivalently, the maximum number of polynomials of coefficient 1 for which $\langle u_0, p\rangle$ is a qkword is $2^{n-1}-2^{k-1}$). If $n > 2k-2$ there are at most $2^{n-1}-2^{n-k}$ such polynomials.*

Proof: Combine the preceding with *Lemma 4.2.* □

Definition 4.2: For a fixed nonnegative integer n and an integer $k \geq 2$, we denote by $BP(n,k)$ the number of binary pairs $(p, \mathbf{a})$ such that $p(x)$ meets $\mathbf{a}$ at k.

THEOREM 4.6. *Let $k \geq 2$ be an integer. Then for all integers $n > 2k-2$, $BP(n,k) \geq (2^{n-1}-2^{n-k})\cdot 2^{k-2}$.*

Proof: We omit the details of the proof, which relies on the unimodality properties of the nullity sequence $\{\nu(A_m) : m \in \mathbb{N}\}$ of the *mxm* Toeplitz matrices associated with any bitstream $\mathbf{a} = \{a_j : j \in Z^+\}$ (see *Theorem 2.9*; also see refs. 7 and 12–14). □

COROLLARY 4.7. *Let $k \geq 2$ be an integer. Then*

(*i*) $BP(0,k) = 2^{k-2}$.

(*ii*) $BP(n,k) = 2^{n-1}\cdot 2^{k-2}$ *if* $1 \leq n < 2k-2$.

(*iii*) $BP(n,k) = (2^{n-1}-2^{n-k+1})\cdot 2^{k-2}$ *if* $n = 2k-2$.

(*iv*) $BP(n,k) = (2^{n-1}-2^{n-k})\cdot 2^{k-2}$ *if* $n > 2k-2$.

Proof: The first three equations are obtained by combining the results of *Lemmas 4.1* and *4.2*. So suppose $n > 2k-2$. By *Theorem 3.4* there are 2^{n-k} polynomials of degree $n > 2k-2$ with constant coefficient 1 having a reciprocal factor of degree $\geq 2k-2$. By *Lemma 4.2* none of these polynomials meets with any bitstream at the integer k. Therefore, among all polynomials of degree n with constant coefficient 1, there are at most $2^{n-1} - 2^{n-k}$ that meet some bitstream at k. By *Theorem 3.6* each such polynomial meets at k with at most 2^{k-2} distinct bitstreams. Hence $BP(n,k) \leq (2^{n-1}-2^{n-k})\cdot 2^{k-2}$. But by the preceding theorem, $BP(n,k) \geq (2^{n-1}-2^{n-k})\cdot 2^{k-2}$. □

The following result follows as a corollary to the proof of the preceding corollary.

COROLLARY 4.8. *The following are equivalent for any polynomial $p(x)$ with constant coefficient 1 over $GF(2)$, and any integer $k \geq 2$.*

(*i*) *$p(x)$ meets at least one bitstream at k.*

(*ii*) *$p(x)$ meets exactly 2^{k-2} bitstreams at k.*

(*iii*) *$p(x)$ has no reciprocal factors of degree $\geq 2k-2$.*

5. Conjugacy Classes of Binary Shifts

As a consequence of the preceding results, we are now in a position to establish a correspondence between the conjugacy classes of binary shifts of finite commutant index and the family of polynomials over $GF(2)$ with constant coefficient 1. Specifically we provide an algorithm that can be used to compute, for any polynomial $p(x)$ over $GF(2)$ with constant coefficient 1, and any integer $k \geq 2$, the number of binary shifts σ of commutant index k associated with $p(x)$ in the sense that $w = \langle u_0, p\rangle$ generates $\sigma^k(R)' \cap R$, (where u_j, $j \in \mathbb{Z}^+$ are the generators for σ). In *Corollary 4.8*, it is shown that for a fixed index $k \geq 2$, any polynomial $p(x)$ meets either 2^{k-2} bitstreams at k or it meets no bitstreams at k. In terms of binary shifts, by using *Remark 3.3*, this means that for a polynomial $p(x)$ there are either 2^{k-2} binary shifts σ for which $\langle u_0, p\rangle$ is a qkword, or no such binary shifts. Note, however, that if $w = \langle u_0, p\rangle$ is a qkword for some binary shift σ, it is not necessarily the case that σ has commutant index k. As an elementary example, consider the polynomial $p(x) = x+1$ and the binary shift σ with bitstream $\{0,1,0,0,0,\ldots\}$. Then $\langle u_0, p\rangle = u_0u_1$ is a q3word. On the other hand, σ is a binary shift of commutant index 2, with the word u_0 generating the relative commutant algebra $\sigma^2(R)' \cap R$. What is needed, therefore, is a way to determine how many of the bitstreams $\mathbf{a}$ which meet $p(x)$ at k actually correspond to binary shifts of commutant index k. The following three results provide the key.

THEOREM 5.1. *Let $\mathbf{a}$ be an eventually periodic but not mirror-periodic bitstream, i.e., the reflected bitstream $\check{\mathbf{a}}$ is not periodic. Let σ, with generators $\{u_j : j \in \mathbb{Z}^+\}$, be the binary shift on R corresponding to $\mathbf{a}$. Let $k \in \{2,3,\ldots\}$ be the commutant index of σ. Then if $p(x)$ is such that the word $w = \langle u_0, p\rangle$ generates $\sigma^k(R)' \cap R$,*

(*i*) *$(p, \mathbf{a})$ is a binary pair,*

(*ii*) *$(p, \mathbf{a})$ meets at the integer k,*

(*iii*) *if $f(x)$ is a polynomial with constant coefficient 1, then $(pf, \mathbf{a})$ meets at $k + \deg(f)$,*

(*iv*) *if $(g, \mathbf{a})$ is a binary pair for some polynomial g with constant coefficient 1, then p is a factor of g and $(g, \mathbf{a})$ meets at $k + \deg(g/p)$.*

Proof: First note that σ is indeed a binary shift on R, because $\check{\mathbf{a}}$ is not periodic (*Theorem 2.1*). Also, σ has finite commutant index, because $\mathbf{a}$ is eventually periodic (*Theorem 2.4*). Let

MATHEMATICS

$p(x) = c_0 + c_1x + \cdots + c_nx^n$, then $w = u_0^{c_0}u_1^{c_1}\cdots u_n^{c_n}$. Because w anticommutes with u_{k-1} and commutes with $u_k, u_{k+1}, \ldots$, the infinite linear system **3.1** is satisfied. Hence $(p, \mathbf{a})$ is a binary pair meeting at the integer k. This proves *i* and *ii*. To see *iii*, note that if $f(x) = l_0 + l_1x + \cdots + l_mx^m$ with $l_0 = 1 = l_m$ then by **2.3**, $\langle u_0, pf\rangle = \pm\langle\langle u_0, p\rangle, f\rangle = \pm\langle w, f\rangle = \pm w^{l_0}\sigma(w)^{l_1}\cdots\sigma^m(w)^{l_m}$. It follows that $\langle u_0, pf\rangle$ anticommutes with u_{k-1+m} and commutes with $u_{k+m}, u_{k+m+1}, \ldots$ whence *iii*.

To see *iv*, let $y = \langle u_0, g\rangle$. Because $(g, \mathbf{a})$ is a binary pair, there is an integer k_0 where they meet. It follows that the word y anticommutes with u_{k_0-1} and commutes with $u_{k_0}, u_{k_0+1}, \ldots$, i.e., $y \notin \sigma^{k_0-1}(R)' \cap R$ but $y \in \sigma^{k_0}(R)' \cap R$. Because σ has commutant index k, then $k \le k_0$ and $y \notin \sigma^{k_0-1}(R)' \cap R$, $y \in \sigma^{k_0}(R)' \cap R = \{w, \sigma(w), \ldots, \sigma^{k_0-k}(w)\}''$. We conclude that there is a polynomial $h(x)$ of degree $k_0 - k$ and constant coefficient 1 such that $y = \pm\langle w, h\rangle$. But then $\langle u_0, g\rangle = y = \pm\langle w, h\rangle = \pm\langle\langle u_0, p\rangle, h\rangle = \pm\langle u_0, ph\rangle$, so $p(x)h(x) = g(x)$. Hence, $p(x)$ is a factor of $g(x)$. That $(g, \mathbf{a})$ meet at $k + \deg(g/p)$ now follows from *iii*. □

As an immediate corollary we have the following.

COROLLARY 5.2. *Suppose σ is a binary shift on the hyperfinite II_1 factor R with corresponding bitstream $\mathbf{a} = \{a_0, a_1, \ldots\}$. Suppose there are an integer k_0 and a polynomial $g(x) \in F[x]$, with constant coefficient* 1, *such that g is paired at k_0 with* $\mathbf{a}$. *Then σ has finite commutant index. In particular there is a unique polynomial p with constant coefficient* 1 *such that p and* $\mathbf{a}$ *are paired at k, the commutant index of σ. Moreover,*

(*i*) *p is a factor of g, and*

(*ii*) *if the polynomial g/p has degree s, then $k + s = k_0$.*

COROLLARY 5.3. *Suppose σ is a binary shift on R with finite commutant index k and corresponding bitstream* $\mathbf{a}$. *Then for $s \ge 0$ there are exactly 2^{s-1} binary pairs $(g, \mathbf{a})$ which meet at the integer $k + s$. Each such polynomial g has the form $g(x) = p(x)f(x)$ where $p(x)$ is the unique polynomial which meets* $\mathbf{a}$ *at k, and $f(x)$ is a polynomial with constant coefficient* 1 *of degree s.*

Proof: The result follows from the preceding result and the fact that there are exactly 2^{s-1} distinct polynomials of degree s with constant coefficient 1. □

Definition 5.1: Let $p(x)$ be a polynomial with constant coefficient 1 in $GF(2)$. For any integer $k \ge 2$ let $C(p, k)$ denote the family of binary shifts σ of commutant index k on R for which the word $w = \langle u_0, p\rangle$ in the generators of σ generates the first nontrivial relative commutant algebra $\sigma^k(R)' \cap R$.

Remark 5.1:

(*i*) Restating *Theorem 2.7* (see also *Remark 3.3*) in terms of this notation, we have $C(p, 2) = \emptyset$ if $p(x)$ has any reciprocal divisors of degree exceeding 1 and $|C(p, 2)| = 1$, otherwise.

(*ii*) Because there are no q1words, by *Remark 3.2*, $C(p, 1) = \emptyset$.

(*iii*) Let $p(x) = 1$. Then $C(p, k)$, for $k \ge 2$, consists of all binary shifts of commutant index k for which the word $w =< u_0, p >= u_0$ generates $\sigma^k(R)' \cap R$. It is not difficult to show that these are the binary shifts each of whose bitstreams $\mathbf{a} = \{a_0, a_1, \ldots\}$ satisfies $a_{k-1} = 1, a_k = a_{k+1} = \cdots = 0$. Note that, as $a_1, a_2, \ldots, a_{k-2}$ may be chosen arbitrarily, there are 2^{k-2} such binary shifts, i.e., $|C(p, k)| = 2^{k-2}$.

The following result gives a recursive formula for computing the cardinality of $C(p, k)$.

THEOREM 5.4. *Let $k \ge 2$ be a fixed integer. Let $p(x)$ be a polynomial of degree n with constant coefficient* 1. *If $p(x)$ has a reciprocal factor $r(x)$ with $\deg(r(x)) \ge 2k - 2$ then $C(p, k) = \emptyset$. Otherwise, for each $j = 0, 1, \ldots, n-1$ let $q_{j1}, q_{j2}, \ldots, q_{jm_j}$ be the distinct factors of $p(x)$ of degree j. Then*

$$\left|C(p, k)\right| = 2^{k-2} - \sum_{\substack{\max(\{0,\, 2+n-k\}) \le j \le n-1 \\ 1 \le i \le m_j}} \left|C(q_{ji}, k - (n - j))\right| \quad \textbf{[5.1]}$$

Proof: If $p(x) = 1$, statement *iii* of the remark indicates that $|C(p, k)| = 2^{k-2}$. It is clear that the summation in this case is 0 and the formula holds in this situation. If $k = 2$ and $p(x)$ has no reciprocal factors of degree > 1, then by statement *iii* the formula should be 1. Because $C(p, 1) = \emptyset$ by statement *ii*, the formula holds in this case. So we may assume that $p(x)$ has degree ≥ 1 and that $k \ge 3$. Let $p(x)$ be a polynomial of degree n with constant coefficient 1. By *Lemma 4.2* (see also *Remark 3.3*), $C(p, k) = \emptyset$ if $p(x)$ has a reciprocal factor of degree $\ge 2k - 2$, so we may assume that the maximal reciprocal factor of $p(x)$ has degree $< 2k - 2$. Suppose $|C(q, l)|$ is known, for all polynomials $q(x)$ of degree $< n$ and all $l \in \{2, 3, \ldots, k-1\}$. Suppose $\mathbf{a}$ is a bitstream that meets $p(x)$ at k. Let σ be the corresponding binary shift on R. Then either $\sigma \in C(p, k)$ or by *Corollary 5.2* there is an $l \in \{2, \ldots, k-1\}$ such that σ has commutant index $l < k$. In the latter case there is a unique polynomial $q(x)$ for which $\sigma \in C(q, l)$. Suppose $\deg(q) = j \le n - 1$. By *Corollary 5.2* $q(x)$ is a proper factor of $p(x)$ and $k = l + \deg(p/q) = l + n - j$, so $l = k - (n - j)$. Because $C(q, l) = 0$ unless $l \ge 2$, we must have $k - (n - j) \ge 2$, or $j \ge 2 + (n - k)$. Of course $j \ge 0$ also. On the other hand, $q(x)$ is a proper factor of $p(x)$, so $j = \deg(q) < \deg(p) = n$, hence $\max(\{0, 2 + (n - k)\}) \le j \le n - 1$. Hence every binary shift σ of commutant index less than k, for which $\langle u_0, p\rangle$ is a qkword (where $\{u_j : j \in \mathbb{Z}^+\}$ are the generators of σ) is accounted for in the summation in the formula above.

Conversely, suppose $q(x)$ is a proper factor of $p(x)$, and suppose $\sigma \in C(q, k - \deg(p/q)) = C(p, k - n + \deg(q))$. Let $\mathbf{a}$ be the bitstream corresponding to σ. Then by *Corollary 4.8* and *Theorem 5.1*, $\mathbf{a}$ is one of the 2^{k-2} bitstreams that meet $p(x)$ at k. Hence, the summation in the formula subtracts from the 2^{k-2} bitstreams corresponding to $p(x)$ any bitstream associated with a binary shift σ of commutant index $< k$ for which $\langle u_0, p\rangle$ is a qkword. Hence the right side of the formula above counts all binary shifts σ of commutant index equal to k for which $\langle u_0, p\rangle$ generates $\sigma^k(R)' \cap R$. □

COROLLARY 5.5. *There are countably many conjugacy classes of binary shifts of any finite commutant index.*

COROLLARY 5.6. *Let $p(x)$ be an irreducible polynomial over $GF(2)$ of degree $n \ge 1$. Let $k \ge 2$ be an integer. If $p(x)$ is reciprocal then*

(*i*) $|C(p, k)| = 0$ *if* $n \ge 2k - 2$,

(*ii*) $|C(p, k)| = 2^{k-2}$ *if* $k - 1 \le n < 2k - 2$, *and*

(*iii*) $|C(p, k)| = 2^{k-2} - 2^{k-n-2}$ *if* $0 < n \le k - 2$.

If $p(x)$ is not reciprocal then

(*iv*) $|C(p, k)| = 2^{k-2}$ *if* $n \ge k - 1$, *and*

(*v*) $|C(p, k)| = 2^{k-2} - 2^{k-n-2}$ *if* $0 < n \le k - 2$.

Proof: Statement *i* follows immediately from the first assertion of the theorem. Otherwise, because 1 is the only proper factor of $p(x)$ the formula in the theorem reduces to $|C(p, k)| = 2^{k-2} - |C(1, k - n)|$. If $n \ge k - 1$, then $|C(1, k - n)| = 0$, so *ii* and *iv* follow. If $0 < n \le k - 2$, then $|C(1, k - n)| = 2^{k-n-2}$ by *iii* of the remark preceding the theorem, and $|C(p, k)| = 2^{k-2} - |C(1, k - n)| = 2^{k-2} - 2^{k-n-2}$, giving *iii* and *v*. □

What follows is an algorithm for determining the bitstreams of those binary shifts that lie in $C(p, k)$, for any polynomial $p(x)$ over $GF(2)$ with constant coefficient 1. If $p(x) = 1$, then $C(p, k)$, by *Remark 5.1(iii)*, consists of binary shifts whose bitstreams are of the form $\mathbf{a} = \{0, a_1, a_2, \ldots, a_{k-2}, 1, 0, 0, \ldots\}$. Suppose $p(x)$ has degree $n > 0$ and suppose $k \ge 2$. Suppose moreover that $p(x)$ has no reciprocal factors of degree $\ge 2k - 2$. Assuming the bitstreams for all binary shifts in

$C(q, l)$, $\deg(q(x)) < n$, $l \leq n-1$, have been determined we find the bitstreams associated with the binary shifts in $C(p, k)$.

To do this we first seek any bitstream $\mathbf{a}$ that meets $p(x)$ at k. If $q(x)$ is a factor of $p(x)$ such that $C(q, k - deg(p/q)) \neq \emptyset$ then by *Theorem 5.1* the bitstream associated with a binary shift in this set meets $p(x)$ at k. If no such factor $q(x)$ exists we find $\mathbf{a}$ as follows. If $\deg(p(x)) \leq 2k-2$ then we may obtain $\mathbf{a}$ as in the proof of *Lemma 4.1.* If $\deg(p(x)) > 2k-2$ then we can find a bitstream $\mathbf{a}$ by solving the system consisting of the first $n+1$ equations in the infinite system **3.1**. Having done that, the remaining elements $\{a_{n-k}, a_{n-k+1}, \ldots\}$ are obtained from the remaining equations in **2.1** using the fact that $c_0 = 1$. For the next step, let $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \ldots, \mathbf{s}^{(m)}$ be the bitstreams constructed as in the proof of *Theorem 3.6.* For $1 \leq j \leq m$ let $\mathbf{b}^{(j)} = \mathbf{a} + \mathbf{s}^{(j)}$. [From that theorem it was determined that $m \leq 2^{k-2}$. From the computation of $BP(n, k)$ in *Corollaries 4.7* and *4.8*, however, it turns out that $m = 2^{k-2}$.) By the theorem, we have found all of the bitstreams that meet $p(x)$ at k. Note that all of these bitstreams correspond to binary shifts in $C(p, k)$. For if not, the proof of the theorem above implies that one of these bitstreams meets with some factor $q(x)$ of $p(x)$ at the integer $k - \deg(p/q)$, which is not the case for the situation we are currently considering.

Because a bitstream is a complete conjugacy invariant for binary shifts on R, the procedure above leads to the following.

THEOREM 5.7. *The algorithm above gives a complete classification of the binary shifts of finite commutant index up to conjugacy.*

It is a pleasure to thank Alexis Alevras and Robert T. Powers for helpful conversations. We are also grateful to Professor Powers for writing a very enlightening computer program related to the classification of binary shifts. This work was supported in part by a research grant from the National Science Foundation.

1. Powers, R. T. (1988) *Can. J. Math.* **40,** 86–114.
2. Jones, V. F. R. (1983) *Invent. Math.* **72,** 1–25.
3. Price, G. L. (1999) *Proc. Natl. Acad. Sci. USA* **96,** 8839–8844.
4. Lidl, R. & Neiderreiter, H. (1994) *Introduction to Finite Fields and Their Applications* (Cambridge Univ. Press).
5. Vik, S. *Math. Scand.*, in press.
6. Price, G. L. (1987) *Can. J. Math.* **39,** 492–511.
7. Powers, R. T. & Price, G. L. (1994) *J. Funct. Anal.* **121,** 275–295.
8. Bures, D. & Yin, H. *Pacific J. Math.* **142,** 245–257.
9. Price, G. L. (1998) *J. Funct. Anal.* **156,** 121–169.
10. Carlitz, L. (1967) *J. Reine Angew. Math.* **226,** 212–220.
11. Newman, M. (1972) *Integral Matrices* (Academic, New York).
12. Culler, K. & Price, G. L. (1996) *Linear Algebra Appl.* **248,** 317–325.
13. Price, G. L. & Truitt, G. H. (1999) *Linear Algebra Appl.* **294,** 49–66.
14. Price, G. L. (1998) *J. Operator Theory* **39,** 177–195.