Proc. Natl. Acad. Sci. USA
Vol. 96, pp. 8839–8844, August 1999
Mathematics

On the classification of binary shifts of minimal commutant index

(conjugacy class / commutant index / subfactor index)

GEOFFREY L. PRICE

Department of Mathematics 9E, United States Naval Academy, Annapolis, MD 21402-5000

Edited by Richard V. Kadison, University of Pennsylvania, Philadelphia, PA, and approved May 6, 1999 (received for review May 1, 1999)

ABSTRACT **We provide a complete classification up to conjugacy of the binary shifts of commutant index 2 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.**

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 which intertwines σ and ρ in the sense that $\gamma \circ \sigma(A) = \rho \circ \gamma(A)$ for all $A \in R$. This notion carries over to the more general setting of unital $*$-endomorphisms on R. In general it is difficult to determine whether a pair of $*$-endomorphisms are conjugate, even when they are automorphisms. On the other hand, it is quite straightforward to see that the subfactor index $[R : \sigma(R)]$ of $\sigma(R)$ and the commutant index, i.e., the first positive integer k (or ∞) such that $\sigma^k(R)' \cap R$ is nontrivial, are numerical conjugacy invariants for unital $*$-endomorphisms on R.

In ref. 1, R. T. Powers initiated a study of a family of unital $*$-endomorphisms on R called binary shifts. The range $\sigma(R)$ of any binary shift σ is a subfactor of R of subfactor index 2. Corresponding to each binary shift is a subset X of $\mathbb{N}$, the *anticommutation set* of σ and a sequence $\{u_n : n \in \mathbb{Z}^+\}$ of symmetries generating R and satisfying the generalized commutation relations

$$u_i u_j = (-1)^{g(|i-j|)} u_j u_i \qquad [1]$$

for distinct i, j, where g is the characteristic function of X. The mappings $\sigma(u_i) = u_{i+1}$ completely determine σ as a unital $*$-endomorphism, and σ is a shift in the sense that the inclusion of subfactors $R \supset \sigma(R) \supset \sigma^2(R) \supset \cdots$ has trivial intersection.

In ref. 1, it was shown that a pair of binary shifts are conjugate if and only if the same subset X of $\mathbb{N}$ determines the commutation relations (**1**) of the sequences of symmetries for both σ and τ. In ref. 2, we showed that a sequence of symmetries with commutation relations determined by X generates the hyperfinite II_1 factor if and only if the reflected sequence $\{\ldots, g(2), g(1), 0, g(1), g(2), \ldots\}$ of the "bitstream" $\{0, g(1), g(2), \ldots\}$ is not periodic. In what follows we shall always assume that X is aperiodic in this sense. Among such sets we have shown that the bitstream corresponding to X is eventually periodic if and only if the corresponding binary shift σ on R has finite commutant index. Combining these results one sees that there are countably many conjugacy classes of binary shifts with finite commutant index and uncountably many with infinite commutant index.

In this paper we consider those binary shifts with commutant index 2, the minimal possible commutant index (3) and show that there are countably many such shifts. Specifically we exhibit a one-to-one correspondence between such shifts and the subset of polynomials $p(x)$ over $GF(2)$ with constant coefficient 1 whose self-reciprocal factors (see *Definition 3.1*) have degree at most 1. For $n \geq 2$ we show that the number of such polynomials of degree n is 2^{n-2} and therefore exactly half of the polynomials over $GF(2)$ with constant coefficient 1 correspond to binary shifts of commutant index 2.

In ref. 4, A. Connes completely classified the outer conjugacy classes of $*$-automorphisms on R. Powers used the terminology *cocycle conjugacy* to describe the analogous notion for unital $*$-endomorphisms R. It is quite straightforward to show that there are countably many cocycle conjugacy classes of binary shifts of finite commutant index. In ref. 5, we have shown that all binary shifts of commutant index 2 are cocycle conjugate (see also ref. 6 for results on shifts of higher commutant index). On the other hand, very little is known about the cocycle conjugacy classes of binary shifts of infinite commutant index.

2. Preliminaries

In this section we recall some results on the structure of binary shifts that we shall need in determining the conjugacy classes of those shifts with commutant index 2. We refer to refs. 1 and 6–8 for a more detailed discussion of these results. Let $\{a_0, a_1, \ldots\}$ be a bitstream of $0's$ and $1's$ with $a_0 = 0$. We shall assume that the reflected sequence $\{\ldots, a_2, a_1, a_0, a_1, a_2, \ldots\}$ is not periodic. As is mentioned in the previous section it is sometimes useful to view the elements $a_n, n \in \mathbb{N}$ as the values $g(n)$ of the characteristic function g of a subset X of $\mathbb{N}$. Also as in the previous section, one can choose a sequence of hermitian unitary elements $\{u_0, u_1, \ldots\}$ which satisfy the generalized commutation relations (**1**) (see also ref. 1, definition 3.2, and ref. 6, section 3). Let $\mathfrak{A}_n, n \in \mathbb{N}$, be the group algebra over $\mathbb{C}$ generated by the first n generators $u_0, u_1, \ldots, u_{n-1}$. $\mathfrak{A}_n$ consists of the linear combinations of words $u(\phi) = I$ and $u_{i_0} u_{i_1} \ldots u_{i_m} = u(i_0, i_1, \ldots, i_m)$ in the generators. Using **1**, one may assume the words are presented in ordered form, i.e., $i_0 \leq i_1 \leq \ldots \leq i_m$, and since the u_i's are symmetries, one may also assume that $i_0, i_1, \ldots, i_m$ are distinct. Hence $\mathfrak{A}_n$ has dimension 2^n over $\mathbb{C}$. It is clear that $\mathfrak{A}_n \subset \mathfrak{A}_{n+1}$ is a unital isometic embedding for all n.

The linear functional τ uniquely determined by $\tau(I) = 1, \tau(u(i_0, \ldots, i_m)) = 0$ defines a trace on the algebra $\mathfrak{A} = \bigcup_{n=1}^{\infty} \mathfrak{A}_n$. Assuming that the reflected sequence derived from the bitstream is not periodic, it follows by combining (ref. 1, theorem 3.9, and ref. 6, theorem 2.3) that for any nontrivial word u in $\mathfrak{A}$ there is a word u' in $\mathfrak{A}$ such that $uu' = -u'u$. This shows that τ is the unique normalized trace on $\mathfrak{A}$. It follows that the completion of $\mathfrak{A}$ in its GNS representation defined by τ is the hyperfinite II_1 factor R.

Let σ be the unital $*$-endomorphism on R by $\sigma(u_i) = u_{i+1}, i \in \mathbb{Z}^+$. σ is the *binary shift* on R associated with the sequence $\{u_0, u_1, \ldots\}$ of symmetries generating R.

THEOREM 2.1 (from ref. 2, theorem 5.6, corollary 5.7). *The range $\sigma(R)$ of a binary shift σ is a subfactor of R of subfactor*

PNAS is available online at www.pnas.org.

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

index 2. A binary shift has finite commutant index if and only if its bitstream is eventually periodic. If σ has commutant index $k < \infty$ then there is a word w in the generators $\{u_0, u_1, \ldots\}$ of R satisfying the following conditions.

(*i*) w generates $\sigma^k(R)' \cap R$.
(*ii*) the words $w, \sigma(w), \ldots, \sigma^r(w)$ generate $\sigma^{k+r}(R)' \cap R$, for all $r \in \mathbb{N}$.
(*iii*) $w = u(i_0, i_1, \ldots, i_m)$ for some set $I = \{i_0 < \cdots < i_m\}$ with $i_0 = 0$.

COROLLARY 2.2 (from ref. 9, theorem 2.1). *A binary shift of finite commutant index restricts to a binary shift σ_∞ on the subfactor R_∞ of R generated by the sequence $\{w, \sigma(w), \sigma^2(w), \ldots\}$. The derived shift σ_∞ has commutant index k. The anticommutation set $X_\infty \subset \mathbb{N}$ associated with σ_∞ is a subset of $\{1, 2, \ldots, k-1\}$ which includes $k-1$. R_∞ has subfactor index 2^m in R.*

Remark 2.3: Since by the theorem above a binary shift σ has subfactor index 2, i.e., $[R : \sigma(R)] = 2$, the minimal commutant index for a binary shift is 2 (ref. 3, corollary 2.2.4).

In what follows we consider exclusively the situation in which σ is a binary shift of commutant index 2. Suppose w generates the 2-dimensional algebra $\sigma^2(R)' \cap R$. If $w = u_0$ then $X_\infty = X = \{1\}$ and $\sigma_\infty = \sigma$. Suppose $w \neq u_0$, then $w = u(i_0, i_1, \ldots, i_m) = u(I)$ for some positive integer m. Then w commutes with $u_2, u_3, \ldots$, and since $w \notin \sigma(R)' \cap R = \mathbb{C}$ it anticommutes with u_1. Write $w = u_0^{k_0} u_1^{k_1} \cdots u_m^{k_m}$ where $k_0 = 1 = k_m$ and $k_j = 1$ if $j \in I$, $k_j = 0$ if $j \notin I$. Since w anticommutes with u_1 we have, using **1**, that $a_1k_0 + a_0k_1 + a_1k_2 + \cdots + a_{n-1}k_n = 1 \, mod \, 2$. Since w also commutes with $u_2, u_3, \ldots$, we obtain the following linear system of equations over $GF(2)$:

$$\begin{aligned} a_1k_0 + a_0k_1 + a_1k_2 + \cdots + a_{m-1}k_m &= 1 \\ a_2k_0 + a_1k_1 + a_0k_2 + \cdots + a_{m-2}k_m &= 0 \\ a_3k_0 + a_2k_1 + a_1k_2 + \cdots + a_{m-3}k_m &= 0 \\ &\vdots \end{aligned} \qquad \textbf{[2]}$$

Definition 2.4: Let $\mathbf{b} = (b_0, b_1, \ldots)$ be a bitstream in $GF(2)$. Then a vector $\mathbf{c} = [c_0, \ldots, c_n]$ with entries in $GF(2)$ is said to annihilate $\mathbf{b}$ if $\sum_{i=0}^{n} c_i b_{i+k} = 0$ for all $k \in \mathbb{Z}^+$.

Definition 2.5: Let σ be a binary shift of commutant index 2 whose associated sequence of hermitian unitary generators is $\{u_0, u_1, \ldots\}$. Then the word w in the u_i's which generates $\sigma^2(R)' \cap R$ is called the *qword* associated with σ.

In the next section we shall establish the following uniqueness result: if σ, ρ are binary shifts of commutant index 2 with generators $\{u_i\}_{i=0}^{\infty}, \{v_i\}_{i=0}^{\infty}$, respectively, and if $\mathbf{k} = [k_0, \ldots, k_m]$ is a vector over $GF(2)$ such that $u_0^{k_0} u_1^{k_1} \cdots u_m^{k_m}$ (respectively, $v_0^{k_0} v_1^{k_1} \cdots v_m^{k_m}$) is a qword for σ (respectively, ρ), then σ and ρ are conjugate. We shall require the following results for the proof.

THEOREM 2.5 (from ref. 1, theorem 3.6). *A pair of binary shifts are conjugate if and only if their anticommutation sets are identical.*

THEOREM 2.6 (from ref. 2, theorem 3.4). *Let $\mathbf{a} = \{a_0, a_1, \ldots\}$ be a bitstream over GF(2) with periodic reflected sequence. Then there is a nonzero vector $\mathbf{k} = [k_0, k_1, \ldots, k_m]$ over $GF(2)$ with the following properties:*

(*i*) $\mathbf{k}$ annihilates $\mathbf{a}$.
(*ii*) $\mathbf{k}$ is flip-symmetric, i.e., $\mathbf{k} = [k_m, k_{m-1}, \ldots, k_0]$
(*iii*) if $\mathbf{s}$ is any other nonzero vector annihilating $\mathbf{a}$ then there are $c_i \in GF(2)$ such that $\mathbf{s} = c_0[k_0, k_1, \ldots, k_m, 0, \ldots, 0] + c_1[0, k_0, k_1, \ldots, k_m, 0, \ldots, 0] + \cdots + c_r[0, \ldots, 0, k_0, k_1, \ldots, k_m]$.

3. Reciprocal Polynomials and Qwords

Let σ be a binary shift of commutant index 2 on R with generating sequence of symmetries $\{u_0, u_1, \ldots\}$. Let $F = GF(2)$ and let $F[x]$ be the ring of polynomials over F. For $p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ in $F[x]$ and for z a word in the generators u_i, $i \in \mathbb{Z}^+$, let $\langle z, p \rangle$ denote the element $z^{c_0}\sigma(z)^{c_1} \cdots \sigma^n(z)^{c_n}$ of R. Then the following identities are easily verified for words z, z' and polynomials p, q (cf., ref. 6, definition 4.4):

$$\langle z, p \rangle \langle z, q \rangle = \pm \langle z, p + q \rangle \qquad \textbf{[3.1]}$$

$$\langle \langle z, p \rangle, q \rangle = \pm \langle z, pq \rangle \qquad \textbf{[3.2]}$$

$$\langle z, p \rangle \langle z', p \rangle = \pm \langle zz', p \rangle \qquad \textbf{[3.3]}$$

Let w be the qword for σ. By *iii* of *Theorem 2.1*, $w = \langle u_0, p \rangle$ for some polynomial $p(x) \in F[x]$ with constant coefficient 1. We show in *Theorem 5.1* that p must have a special form. We need the following definition, (cf. ref. 10, definition 3.12):

Definition 3.1: If $p(x) = k_0x^n + k_1x^{n-1} + \cdots + k_n$ is a polynomial with $k_0 \neq 0$, its reciprocal polynomial $p^*(x)$ is $x^n p(1/x) = k_nx^n + k_{n-1}x^{n-1} + \cdots + k_0$. A polynomial p is called self-reciprocal (or sometimes just reciprocal) if $p = p^*$.

For results on the number of irreducible self-reciprocal polynomials of a given degree over a finite field see refs. 11 and 12.

LEMMA 3.1. *Let z be a nontrivial word in the generators of a binary shift σ of commutant index 2. Let $r(x) \in F[x]$ be any reciprocal polynomial of degree > 1 and with constant coefficient 1. Then $\langle z, r \rangle$ is not a qword for σ.*

Proof: Let $y = \langle z, r \rangle$ where r is as above, and suppose y is a qword, i.e., $y \in \sigma^2(R)' \cap R$. By *Theorem 2.1(iii)*, y "starts" with the initial generator u_0. Hence z does, too, and r must be a polynomial with constant coefficient 1. Now suppose first that $z = u_0$. Since y is a word in the generators of σ, it either commutes or anticommutes with u_1. If y commutes with u_1, then $y \in \sigma(R)' \cap R$, since $\sigma(R) = \{u_1, u_2, \ldots\}$. But $\sigma(R)' \cap R$ is trivial since $[R : \sigma(R)] = 2$ (ref. 3, corollary 2.2.4). Hence y anticommutes with u_1. Writing $r(x) = k_mx^m + k_{m-1}x^{m-1} + \cdots + k_0$ with $m > 1$, then since $u_1y = -yu_1$, it follows from **2** that $k_0a_1 + k_1a_0 + k_2a_1 + \cdots + k_ma_{m-1} = 1$, where $\mathbf{a} = \{a_0, a_1, \ldots\}$ is the bitstream defining the commutation relations for the generators of σ. If $m = 2$, however, the above equation is $k_0a_1 + k_1a_0 + k_2a_1 = 1$, which is absurd since $k_0 = k_2 (= 1)$ and $a_0 = 0$. If $m > 2$, then since r is reciprocal, the equation above may be rewritten as $k_ma_1 + k_{m-1}a_0 + k_{m-2}a_1 + \cdots + k_0a_{m-1} = 1$, i.e., y anticommutes with u_{m-1}. But $u_{m-1} \in \sigma^2(R)$ and $y \in \sigma^2(R)' \cap R$, a contradiction. Hence $y = \langle u_0, r \rangle \notin \sigma^2(R)' \cap R$.

Next suppose $z = \langle u_0, q \rangle$ for some polynomial q with constant coefficient 1. Let M be the von Neumann subalgebra of R generated by the elements $z_j = \sigma^j(z)$, $j \in \mathbb{Z}^+$. Then it is straightforward to see that σ restricts to a binary shift on M with generators z_j, and that $y \in \sigma^2(M)' \cap M$. Applying the argument above with the u_j's replaced with the z_j's and the bitstream $\mathbf{a}$ for σ replaced with the bitstream $\mathbf{b}$ for the restriction of σ to M, one obtains a similar contradiction as above for y, and therefore $y = \langle z, r \rangle \notin \sigma^2(R)' \cap$. ■

THEOREM 3.2. *Let σ be a binary shift of commutant index 2. If $p(x) \in F[x]$ has a reciprocal factor of degree > 1 then $\langle v, p \rangle$ is not a qword for σ for any word v in the generators of σ.*

Proof: Suppose p is a polynomial with a reciprocal factor r of degree > 1, and suppose $y = \langle v, p \rangle$ is a qword. Since $v = \langle u_0, q \rangle$ for some polynomial q and since $\langle v, p \rangle = \langle \langle u_0, q \rangle, p \rangle = \pm \langle u_0, pq \rangle$ by **3.2**, we may assume by replacing p with pq if necessary that $v = u_0$ and thus $y = \langle u_0, p \rangle$. Since y "starts" with u_0 by *iii* of *Theorem 1.1*, p, and thus r, must have constant coefficient 1. Let s be the polynomial such that

$p = rs$, then $y = \langle u_0, p\rangle = \langle u_0, rs\rangle = \pm\langle\langle u_0, s\rangle, r\rangle$ so applying the previous lemma to $z = \langle u_0, s\rangle$ shows that $y = \pm\langle z, r\rangle$ cannot be a qword. ■

Using the preceding results we can now show the following uniqueness result which shows that if $p \in F[x]$ and $\langle u_0, p\rangle, \langle v_0, p\rangle$ are qwords for binary shifts σ, ρ of commutant index 2, then σ and ρ are conjugate.

THEOREM 3.3. *For $m \in \mathbb{Z}^+$ let $p(x) = k_0 + k_1x + \cdots + k_mx^m$ be a polynomial in $F[x]$ with $k_0 = k_m = 1$. Then up to conjugacy there is at most one binary shift σ of commutant index 2 whose qword w has the form $\langle u_0, p\rangle$, where $\{u_i : i \in \mathbb{Z}^+\}$ is the sequence of symmetries associated with σ.*

Proof: If $p(x) = 1$ then $\langle u_0, p\rangle = u_0$. It is easy to show that if u_0 generates $\sigma^2(R)' \cap R$ then σ has anticommutation set $X = \{1\}$. By *Theorem 2.5* the anticommutation set is a complete conjugacy invariant, and hence the assertion holds for polynomials of degree 0. If $p(x) = x + 1$, then $w = \langle u_0, p\rangle = u_0u_1$. It is straightforward to show, using **2**, that the only conjugacy class of binary shifts of commutant index 2 having a qword of this form is the one associated with the anticommutation set $X = \mathbb{N}$. If deg $p = 2$ then either $p(x) = x^2 + x + 1$ or $x^2 + 1$, but it is a simple matter, using relations **2**, to show that no binary shift of commutant index 2 has a qword of the form $u_0u_1u_2$ or u_0u_2.

We may suppose therefore that p is a polynomial of degree ≥ 3. Suppose σ and ρ are nonconjugate binary shifts of commutant index 2, each of whose qwords is associated with the polynomial p. Let $\mathbf{a} = \{a_0, a_1, \ldots\}$ (respectively, $\mathbf{b} = \{b_0, b_1, \ldots\}$) be the bitstream associated with σ (respectively, with ρ). Let $\mathbf{c} = \{c_0, c_1, \ldots\}$ be given by $c_i = a_i + b_i$ for all $i \in \mathbb{Z}^+$. Since σ and ρ are not conjugate $\mathbf{a} \neq \mathbf{b}$ so $\mathbf{c}$ is nontrivial. Moreover, since both $\mathbf{a}$ and $\mathbf{b}$ satisfy **2** it follows that $\mathbf{c}$ satisfies the following system:

$$\begin{aligned} &c_1k_0 + c_0k_1 + c_1k_2 + \cdots + c_{m-1}k_m = 0\\ &c_2k_0 + c_1k_1 + c_0k_2 + \cdots + c_{m-2}k_m = 0\\ &c_3k_0 + c_2k_1 + c_1k_2 + \cdots + c_{m-3}k_m = 0\\ &\qquad\vdots \end{aligned} \qquad \textbf{[4]}$$

Let $\{v_0, v_1, \ldots\}$ be a sequence of symmetries whose bitstream satisfies **4**. From **4** the word $w = \langle v_0, p\rangle$ commutes with all symmetries $v_i, i \in \mathbb{N}$. By assumption $k_0 = 1$ so that w starts with v_0. But then, since w must commute with itself it follows that w also commutes with v_0. Hence the von Neumann algebra N generated by the sequence $\{v_i : i \in \mathbb{Z}^+\}$ has a nontrivial center. By *Theorem 2.6* there is a reciprocal polynomial r with constant coefficient 1 such that $z = \langle v_0, r\rangle$ and its shifts generate the center of N. It follows that for some n there are elements $l_0, \ldots, l_n \in GF(2)$, with $l_0 = 1$, such that $w = z^{l_0}\sigma(z)^{l_1} \cdots \sigma^n(z)^{l_n}$. Hence $w = \pm\langle z, q\rangle$ where $q(x) = l_0 + l_1x + \cdots + l_nx^n$. By **3**, $w = \pm\langle z, q\rangle = \pm\langle\langle v_0, r\rangle, q\rangle = \pm\langle v_0, rq\rangle$. Since $w = \langle v_0, p\rangle$ then $p = rq$ so that the reciprocal polynomial r is a factor of p. Let $\{s_0, \ldots, s_d\}$ be the coefficients of r. Since z lies in the center of N it commutes with $v_i \in \mathbb{Z}^+$. From this it follows that the vector $\mathbf{s} = [s_0, \ldots, s_d]$ annihilates the bitstream $\mathbf{c}$. Since $\mathbf{c} \neq \mathbf{0}$ it follows that $d > 1$. Hence p has a reciprocal factor of degree greater than 1, which contradicts *Theorem 3.2*. By contradiction there is at most one conjugacy class of binary shifts of commutant index 2 whose qword has the form $\langle u_0, p\rangle$. ■

Definition 3.2: If $w = u(i_0, i_1, \ldots, i_m)$ is a word in the generators of a binary shift σ with $i_0 < i_1 < \cdots < i_m$ then its *length* is $i_m - i_0 + 1$.

THEOREM 3.4. *For any integer $n \geq 3$ there are at least 2^{n-2} nonconjugate binary shifts of commutant index 2 whose qword has the form $u_0^{k_0}u_1^{k_1} \cdots u_n^{k_n}$ with $k_0 = 1 = k_n$.*

Proof: If $n = 3$ then straightforward computations using **2** show that the only qwords are of the form $u_0u_1u_3$ and $u_0u_2u_3$. So we may suppose $n \geq 4$. For fixed $n \geq 4$ we shall produce 2^{n-2} distinct bitstreams $\mathbf{a} = \{a_0, a_1, \ldots\}$ with $a_0 = 0$ which correspond to binary shifts of commutant index 2 whose qword has length $n + 1$. By *Theorem 2.1* such a qword w in the generators $\{u_k : k \in \mathbb{Z}^+\}$ has the form $w = u_0^{k_0}u_1^{k_1} \cdots u_n^{k_n}$ where $k_0 = 1 = k_n$, and the exponents $k_0, k_1, \ldots, k_n$ satisfy **2**.

Suppose n is odd. Since we are assuming k_0 and k_n to be 1, the first $n - 1$ equations of **2** may be rewritten as follows:

$$\begin{bmatrix} a_o & a_1 & a_2 & a_3 & \cdots & a_{n-2}\\ a_1 & a_o & a_1 & a_2 & \cdots & a_{n-3}\\ a_2 & a_1 & a_o & a_1 & \cdots & a_{n-4}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{n-2} & a_{n-3} & a_{n-4} & \cdots & \cdots & a_0 \end{bmatrix} \cdot \begin{bmatrix} k_1\\ k_2\\ k_3\\ \vdots\\ k_{n-1} \end{bmatrix} = \begin{bmatrix} a_1 + a_{n-1} + 1\\ a_2 + a_{n-2}\\ a_3 + a_{n-3}\\ \vdots\\ a_{n-1} + a_1 \end{bmatrix}.$$

For a bitstream $\mathbf{a}$ as above and for each $m \in \mathbb{N}$ let A_m be the $(m + 1) \times (m + 1)$ Toeplitz matrix:

$$\begin{bmatrix} a_o & a_1 & a_2 & a_3 & \cdots & a_m\\ a_1 & a_o & a_1 & a_2 & \cdots & a_{m-1}\\ a_2 & a_1 & a_o & a_1 & \cdots & a_{m-2}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ a_m & a_{m-1} & a_{m-2} & \cdots & \cdots & a_o \end{bmatrix}.$$

By ref. 13, there are 2^{n-3} choices of $a_1, \ldots, a_{n-2}$ such that A_{n-2} is invertible. Assuming $\mathbf{a}$ has been chosen so that A_{n-2} is invertible, we can of course solve the matrix equation above. Note that this equation can be solved regardless of the choice of the entry a_{n-1}, which appears only on the right side of the equation. Once $a_0 = 0$ and $a_1, a_2, \ldots, a_{n-2}, a_{n-1}$ have been chosen, however, it is clear that the remaining equations in **2** can be solved by one and only one choice of each of the entries $a_n, a_{n+1}, \ldots$. Hence for n odd there are at least 2^{n-2} choices of $\mathbf{a}$ such that **2** has a solution.

Now suppose n is even. Since $k_0 = 1$ the first n equations of **2** may be written as follows:

$$A_{n-1} \cdot \begin{bmatrix} k_1\\ k_2\\ \vdots\\ k_n \end{bmatrix} = \begin{bmatrix} a_1\\ a_2\\ \vdots\\ a_n \end{bmatrix} + \begin{bmatrix} 1\\ 0\\ \vdots\\ 0 \end{bmatrix}.$$

Suppose the elements $a_0, a_1, \ldots, a_{n-1}$ of $\mathbf{a}$ have been chosen so that the matrices $A_{n-3}, A_{n-2}, A_{n-1}$ have nullities $2, 1, 0$, respectively. Since A_{n-1} is invertible $k_1, k_2, \ldots, k_n$ are uniquely determined by $a_0, a_1, \ldots, a_{n-1}, a_n$. We require $k_n = 1$, however. By Cramer's Rule k_n is the determinant of the matrix

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_1 + 1\\ a_1 & a_0 & \cdots & a_{n-3} & a_2 + 0\\ a_2 & a_1 & \cdots & a_{n-4} & a_3 + 0\\ \vdots & \vdots & \ldots & \vdots & \vdots\\ a_{n-2} & a_{n-3} & \cdots & a_0 & a_{n-1} + 0\\ a_{n-1} & a_{n-2} & \cdots & a_1 & a_n + 0 \end{bmatrix}.$$

Let A (respectively, B) be the matrix obtained from the one above by replacing its last column with entries $a_1, a_2, \ldots, a_{n-1}, a_n$ (respectively, with $1, 0, \ldots, 0$). Observe that the determinant of the matrix above agrees with $det(A) + det(B)$. We show that $det(A) = 1$. To see this

recall from ref. 13, theorem 2.6 (see also ref. 7) that since A_{n-1} is invertible the matrix A_n has nullity 1 regardless of the choice of a_n. Moreover, the unique nontrivial element of the right kernel of A_n is of the form $[s_0, s_1, \ldots, s_n]^T$ with $s_0 = 1 = s_n$. Hence if we label the columns of the Toeplitz matrix A_n by C_i, $i = 0, \ldots, n$, then

$$\sum_{j=0}^{n} s_j C_j = [0, 0, \ldots, 0]^T,$$

and therefore

$$C_n = \sum_{j=0}^{n-1} s_j C_j.$$

Note that the last column of A coincides with the column $\tilde{C}_0$ obtained by deleting the initial entry of the initial column C_0 of A_n. Deleting the initial entries of the other columns of A_n we get $\tilde{C}_0 = \sum_{j=1}^{n} s_j \tilde{C}_j$. Hence the last column of A coincides with $\sum_{j=1}^{n} s_j \tilde{C}_j$. But $\tilde{C}_1, \tilde{C}_2, \ldots, \tilde{C}_{n-1}$ coincide with the first $n-1$ columns of A so that A has the same determinant as the matrix obtained by replacing the last column of A with $s_n \tilde{C}_n = \tilde{C}_n = [a_{n-1}, \ldots, a_0]^T$. But this matrix is A_{n-1} which is invertible and therefore has determinant 1 over $GF(2)$. Hence $k_n = 1$ if and only if $det(B) = 0$.

$Det(B)$ coincides with the determinant of the matrix M below:

$$\begin{bmatrix} a_1 & a_0 & a_1 & a_2 & \cdots & a_{n-3} \\ a_2 & a_1 & a_0 & a_1 & \cdots & a_{n-4} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-2} & a_{n-3} & a_{n-4} & a_{n-5} & \cdots & a_0 \\ a_{n-1} & a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_1 \end{bmatrix}$$

The matrix A_{n-3} occupies the top right corner of M. Since A_{n-3} has nullity 2 its rank is $n-4$. Hence the rank of M is at most $n-2$. Hence $det(M) = 0$ and $k_n = 1$.

We use results from ref. 13 to show that there are 2^{n-3} choices for $a_0, a_1, \ldots, a_{n-1}$ (with $a_0 = 0$) such that $A_{n-3}, A_{n-2}, A_{n-1}$ have nullities 2, 1, 0, respectively. Let $\rho(S)$ be the rank of any square matrix S over $GF(2)$. By ref. 13, corollary 2.10, there are 2^{n-2} n-tuples $[a_0, a_1, \ldots, a_{n-1}]$ for which A_{n-1} is invertible. If A_{n-1} is invertible then (by ref. 13, theorem 2.7) $\rho(A_{n-3})$ is either $n-4$ or $n-2$. The number of invertible matrices A_{n-3}, i.e., matrices for which $\rho(A_{n-3})$ is $n-2$, is 2^{n-4} (ref. 13, corollary 2.10). For A_{n-3} invertible $\rho(A_{n-2}) = n-2$ regardless of the choice of a_{n-2}, but there is only one choice of a_{n-1} such that A_{n-1} is invertible (ref. 13, proof of corollary 2.10). Thus there are 2^{n-3} n-tuples $[a_0, a_1, \ldots, a_{n-1}]$ such that $\rho(A_{n-3}) = n-2$, $\rho(A_{n-2}) = n-2$,and $\rho(A_{n-1}) = n$. Thus subtracting 2^{n-3} from the number 2^{n-2} of n-tuples for which A_{n-1} is invertible yields the number of n-tuples satisfying $\rho(A_{n-3}) = n-4$, $\rho(A_{n-2}) = n-2$, $\rho(A_{n-1}) = n$. Hence there are 2^{n-3} such n-tuples. Since $det(A) = 1$ regardless of the choice of a_n, we see that a_n may be chosen arbitrarily but that all subsequent elements of the bitstream are determined. Hence for even $n \geq 4$ there are at least 2^{n-2} choices of bitstreams **a** such that the qword of the corresponding binary shift of commutant index 2 has length n. This completes the proof. ■

Remark: If $n = 0$ then u_0 is a qword for a binary shift of commutant index 2 whose bitstream **a** is $\{0, 1, 0, 0, \ldots\}$. For $n = 1$ $u_0 u_1$ is a qword for the the shift with bitstream $\{0, 1, 1, \ldots\}$. It is straightforward to show that there are no qwords corresponding to $n = 2$.

From *Theorem 2.1* any qword for a binary shift of commutant index 2 with generators $\{u_0, u_1, \ldots\}$ starts with u_0. In Section 5 we shall show that for $n \geq 3$ there are exactly 2^{n-2} qwords w of length $n+1$, i.e., there are 2^{n-2} polynomials p over $GF(2)$ of degree n such that for some set $\{u_0, u_1, \ldots\}$ of generators of a binary shift of commutant 2, $w = \langle u_0, p \rangle$ is a qword. As a key step in proving this result we devote the next section to determining the number of polynomials of degree n over $GF(2)$ with constant coefficient 1 which have nontrivial reciprocal factors.

4. Polynomials with Reciprocal Factors

Let σ be a binary shift of commutant index 2 and with corresponding sequence of symmetries $\{u_0, u_1, \ldots\}$. In *Theorem 3.2* we showed that if $\langle u_0, p \rangle = w$ is the qword for σ that p has no reciprocal factors of degree > 1. In this section we count the number of polynomials over $GF(2)$ with constant coefficient 1 which have a reciprocal factor of degree ≥ 2, and use this result in the next section to classify σ up to conjugacy.

Definition 4.1: We shall say that a polynomial $p \in GF(2)$ with constant coefficient 1 is *free* if any reciprocal factor of p has degree < 2. If p has a reciprocal factor of degree ≥ 2 it is said to be *partially reciprocal*.

LEMMA 4.1. *The product of reciprocal polynomials is reciprocal.*

Proof: Obvious. ■

LEMMA 4.2. *If $n \in \mathbb{N}$ is odd there are $2^{\frac{1}{2}(n-1)}$ reciprocal polynomials of degree n with constant coefficient* 1*. If n is even there are $2^{\frac{1}{2}n}$ of degree n of this form.*

Proof: Obvious. ■

Although the following result is well-known we have not been able to locate a complete proof. See ref. 10, chapter 3, for related results.

THEOREM 4.3. *A polynomial $p(x) \in F[x]$ with constant coefficient* 1 *is reciprocal if and only if it can be written as a product of irreducible factors of the form $\prod q_i(x) \cdot \prod f_j(x) f_j^*(x)$, where the q_i's are reciprocal.*

Proof: It is straightforward to show that if f is any polynomial with constant coefficient 1 then $f(x)f^*(x)$ is reciprocal. Hence any polynomial of the form in the statement of the theorem is reciprocal. Now suppose p is reciprocal of degree at least 1. Write $p(x)$ as the product $\prod h_k(x)$ of its irreducible factors. Since p has constant coefficient 1 so do all of the h_k's. Let $deg(h_k) = n_k$, then since $n = deg(p) = \sum n_k$ we have (see *Definition 3.1*), $p(x) = p^*(x) = x^n p(\frac{1}{x}) = x^n \prod h_k(\frac{1}{x}) = \prod x^{n_k} h_k(\frac{1}{x}) = \prod h_k^*(x)$. Using this computation along with the fact that $F[x]$ is a unique factorization domain shows that p has the desired form. ■

THEOREM 4.4. *Let $n \geq 3$. Among the 2^{n-1} polynomials in $F[x]$ with constant coefficient* 1 *there are 2^{n-2} which are free and 2^{n-2} which are partially reciprocal.*

Proof: We prove the result using induction on the degree of the polynomials over $GF(2)$. Let $pr(n)$ denote the number of partially reciprocal polynomials of degree n with constant coefficient 1. There are 4 polynomials of degree $n = 3$ with constant coefficient 1: the polynomials x^3+x+1 and x^3+x^2+1 are free (and irreducible) and the polynomials $x^3 + 1 = (x+1)(x^2+x+1)$ and $x^3+x^2+x+1 = (x+1)^3$ are both reciprocal, hence partially reciprocal. Hence there are two polynomials of each type and $pr(2) = 2 = 2^{3-2}$.

Let $s(n)$ be the number of reciprocal polynomials of degree n with constant coefficient 1 and let $z(n)$ be the number of free polynomials with constant coefficient 1 not divisible by $x+1$. From the previous paragraph $z(3) = 2$. For $n = 4$ the only such polynomials are the irreducible polynomials $x^4 + x + 1$ and $x^4 + x^3 + 1$. For n even, say $n = 2r$, we claim that $z(n) = z(2r) = \frac{1}{3}(2 \cdot 4^{r-1} + 4) - 2$ and for $n = 2r+1$, $z(2r+1) = \frac{1}{3}(4^r - 4) + 2$. We establish these equations by induction in the process of proving our first induction claim.

Let $m > 1$ and suppose the values of $pr(n)$ and $z(n)$ are valid for all $n < 2m$. Using *Theorem 4.3* any degree n polynomial $f(x)$ with constant coefficient 1 can be factored as

$g(x)h(x)$ where g is reciprocal and h is free. Since $x+1$ is reciprocal we may assume that any factor of $x+1$ of $f(x)$ is included as a factor of $g(x)$ and therefore we may assume that $x+1$ is not a factor of $h(x)$. Also if $f(x)$ is partially reciprocal then $deg(g) \geq 2$: obviously $deg(g) \geq 1$ when $f(x)$ is partially reciprocal but if $deg(g) = 1$ then $g(x) = x+1$ and $g(x)h(x)$ is free. Also if $f(x)$ is partially reciprocal then $deg(h) \neq 2$ since all degree 2 polynomials with constant coefficient 1 are reciprocal, and $deg(h) \neq 1$ since $h(x)$ is not divisible by $x+1$. Therefore, if $deg(g) = j$ and $deg(h) = n-j$, then we may assume $j \neq 0, 1, n-2, n-1$, and

$$\begin{aligned} pr(n) &= \sum_{j=2}^{n-3} s(j)z(n-j) + s(n)z(0) \\ &= \sum_{j=2}^{2m-3} s(j)z(2m-j) + s(2m) \\ &= \sum_{j=2}^{2m-3} s(j)z(2m-j) + 2^m \\ &= I + II, \text{ where} \end{aligned}$$

$$\begin{aligned} I &= \sum_{k=1}^{m-2} s(2k)z(2(m-k)) + 2^m \\ &= \sum_{k=1}^{m-2} 2^k \left(\left(\frac{1}{3}\right)(2 \cdot 4^{m-k-1} + 4) - 2 \right) + 2^m, \text{ and} \end{aligned}$$

$$\begin{aligned} II &= \sum_{k=1}^{m-2} s(2k+1)z(2m-(2k+1)) \\ &= \sum_{k=1}^{m-2} s(2k+1)z(2(m-k-1)+1) \\ &= \sum_{k=1}^{m-2} 2^k \left(\left(\frac{1}{3}\right)(4^{m-k-1} - 4) + 2 \right) \end{aligned}$$

$$\begin{aligned} \text{So } pr(n) = I + II &= \sum_{k=1}^{m-2} 2^k \left(\left(\frac{1}{3}\right)(2 \cdot 4^{m-k-1} + 4^{m-k-1}) \right) + 2^m \\ &= \sum_{k=1}^{m-2} 2^k \cdot 4^{m-k-1} + 2^m \\ &= \sum_{k=1}^{m-2} 2^k \cdot 2^{2m-2k-2} + 2^m \\ &= \sum_{k=1}^{m-2} 2^{2m-k-2} + 2^m \\ &= 2^{2m-2}. \end{aligned}$$

To handle the odd case, let $m > 1$ and suppose the values of $pr(n)$ and $z(n)$ are valid for all $n < 2m+1$. Then we have, for $n = 2m+1$, $pr(n) = \sum_{j=2}^{n-3} s(j)z(n-j) + s(n)z(0) = I + II$, where

$$\begin{aligned} I &= \sum_{k=1}^{m-1} s(2k)z(2m+1-2k) \\ &= \sum_{k=1}^{m-1} 2^k \cdot z(2(m-k)+1) \\ &= \sum_{k=1}^{m-2} 2^k \cdot \left(\left(\frac{1}{3}\right) \cdot (4^{m-k} - 4) + 2 \right) + 2^{m-1} z(3) \\ &= \sum_{k=1}^{m-2} 2^k \cdot \left(\left(\frac{1}{3}\right) \cdot (4^{m-k} - 4) + 2 \right) + 2^m, \text{ and} \end{aligned}$$

$$\begin{aligned} II &= \sum_{k=1}^{m-2} s(2k+1)z(2m-2k) + s(2m+1) \\ &= \sum_{k=1}^{m-2} 2^k \cdot \left(\left(\frac{1}{3}\right)(2 \cdot 4^{m-k-1} + 4) - 2 \right) + 2^m, \text{ so} \end{aligned}$$

$$\begin{aligned} I + II &= \sum_{k=1}^{m-2} 2^k \left(\left(\frac{1}{3}\right)(2 \cdot 4^{m-k-1} + 4^{m-k}) + 2^{m+1} \right. \\ &= \sum_{k=1}^{m-2} 2^k \left(\left(\frac{1}{3}\right)(6 \cdot 4^{m-k-1}) + 2^{m+1} \right. \\ &= \sum_{k=1}^{m-2} 2^{k+1} 4^{m-k-1} + 2^{m+1} \\ &= \sum_{k=1}^{m-2} 2^{k+1} 2^{2m-2k-2} + 2^{m+1} \\ &= \sum_{k=1}^{m-2} 2^{2m-k-1} + 2^{m+1} \\ &= 2^{2m-1}. \end{aligned}$$

So far we have shown that if we assume $z(2r) = (\frac{1}{3})(2 \cdot 4^{r-1} + 4) - 2$ for all r such that $2r < n$ and $z(2r+1) = (\frac{1}{3})(4^r - 4) + 2$ for all r such that $2r+1 < n$, that $pr(n) = 2^{n-2}$. To complete the induction we must show that $z(n)$ has the asserted value. First note that by the induction assumptions we have shown that $pr(n) = 2^{n-2}$, i.e., the number of polynomials of degree n with constant coefficient 1 which are partially reciprocal is 2^{n-2}. Since there are 2^{n-1} degree n polynomials with constant coefficient 1 there are 2^{n-2} free polynomials of degree n and constant coefficient 1. Let $p(x)$ be a free polynomial of degree n which has factor $x+1$. If $q(x)$ satisfies $(x+1)q(x) = p(x)$, $q(x)$ is free of degree $n-1$. Hence $p(x)$ is the product of $x+1$ with a free polynomial of degree $n-1$. Conversely, if q is free, of degree $n-1$, with constant coefficient 1, and relatively prime to $x+1$, then $p(x) = (x+1)q(x)$ is free. Hence

$$z(n) = 2^{n-2} - z(n-1).$$

Now suppose first that n is odd, say $n = 2k+1$. Then the number of free polynomials of degree n with factor $x+1$ and constant coefficient 1 is equal to the number of free polynomials of degree $n-1$ with constant coefficient 1 which do not have $x+1$ as a factor, i.e., $z(n-1) = z(2k)$. Therefore, $z(n) = z(2k+1)$, the number of free polynomials of degree $n = 2k+1$ with constant coefficient 1 which are relatively prime to $x+1$, is equal to

$$\begin{aligned} z(n) &= 2^{n-2} - z(n-1) \\ &= 2^{2k-1} - z(2k) \\ &= 2^{2k-1} - \left(\left(\frac{1}{3}\right)(2 \cdot 4^{k-1} + 4) - 2 \right) \\ &= \left(\frac{1}{3}\right)(3 \cdot 2^{2k-1} - 2 \cdot 4^{k-1} - 4) + 2 \\ &= \left(\frac{1}{3}\right)(3 \cdot 2^{2k-1} - 2 \cdot 2^{2k-2} - 4) + 2 \\ &= \left(\frac{1}{3}\right)(4^k - 4) + 2. \end{aligned}$$

If n is even then similarly, for $z = 2k$,

$$\begin{aligned} z(n) &= 2^{n-2} - z(n-1) \\ &= 2^{2k-2} - z(2k-1) \\ &= 2^{2k-2} - z(2(k-1)+1) \\ &= 2^{2k-2} - \left(\frac{1}{3}\right)(4^{k-1} - 4) - 2 \\ &= 4^{k-1} - \left(\frac{1}{3}\right)(4^{k-1} - 4) - 2 \\ &= \left(\frac{1}{3}\right)(2 \cdot 4^{k-1} - 4) - 2 \end{aligned}$$

This completes the proof. ■

5. Reciprocal Polynomials and Conjugacy

Using the results of the previous two sections we may now show the connection between conjugacy classes of binary shifts of commutant index 2 and free polynomials (see *Definition 4.1*).

THEOREM 5.1. *A one-to-one correspondence exists between free polynomials of degree* ≥ 3 *and conjugacy classes of binary shifts of commutant index 2 whose qwords have length* ≥ 4. *The correspondence associates a free polynomial* $k_0 + k_1 x + k_2 x^2 + \cdots + k_n x^n$ *with constant coefficient* $k_0 = 1$ *with the conjugacy class of binary shifts whose qword has the form* $u_0^{k_0} u_1^{k_1} \cdots u_n^{k_n}$.

Proof: By *Theorem 2.5* any two binary shifts in the same conjugacy class are generated by sequences of symmetries whose commutation relations are the same. Hence any two binary shifts in the same conjugacy class have identical bitstreams. Since the equations **2** determine the form of the corresponding qword for these shifts, it follows that any two binary shifts of commutant index 2 in the same conjugacy class have qwords of the same form. On the other hand, (by *Theorem 3.3*) for any $n+1$-tuple $[k_0, k_1, \ldots, k_n]$ over $GF(2)$ there is up to conjugacy at most one binary shift of commutant index 2 whose qword has the form $u_0^{k_0} u_1^{k_1} \cdots u_n^{k_n}$. Hence the form of a qword determines the conjugacy class of the shift to which the qword corresponds.

Suppose $n \geq 3$. By *Theorem 3.4* there are at least 2^{n-2} distinct conjugacy classes of binary shifts of commutant index 2 whose qwords have length $n+1$. Let $w = u_0^{k_0} u_1^{k_1} \cdots u_n^{k_n} = \langle u_0, p \rangle$ be a qword corresponding to a representative σ of one of these conjugacy classes. By *Theorem 3.2* the polynomial p is not partially reciprocal. Hence p is free. By *Theorem 4.4* there are exactly 2^{n-2} free polynomials of degree n with constant coefficient 1. Hence there are at most 2^{n-2} conjugacy classes of shifts whose qwords have length $n+1$. Thus there are exactly 2^{n-2} conjugacy classes of binary shifts of commutant index 2 whose qwords have length $n+1$, each of which corresponds to a free polynomial of degree n with constant coefficient 1. ■

I am grateful to Robert T. Powers and Erling Størmer for helpful conversations. This work was supported in part by research grants from the National Science Foundation and the National Security Agency.

1. Powers, R. T. (1988) *Can. J. Math.* **40,** 86–114.
2. Price, G. L. (1987) *Can. J. Math.* **39,** 492–511.
3. Jones, V. F. R. (1983) *Invent. Math.* **72,** 1–25.
4. Connes, A. (1975) *Ann. Sci. Ec. Norm. Sup.* **8,** 383–420.
5. Price, G. L. (1998) *J. Operator Theory* **39,** 177–195.
6. Price, G. L. (1998) *J. Funct. Anal.* **156,** 121–169.
7. Powers, R. T. & Price, G. L. (1994) *J. Funct. Anal.* **121,** 275–295.
8. Vik, S. (2000) *Math. Scand.*, in press.
9. Bures, D. & Yin, H. (1988) *J. Operator Theory* **20,** 91–106.
10. Lidl, R. & Neiderreiter, H. (1983) *Introduction to Finite Fields and Their Applications* (Addison-Wesley, Reading, MA).
11. Carlitz, L. (1967) *J. Reine Angew. Math.* **226,** 212–220.
12. Miller, R. L. (1978) *Discrete Math.* **22,** 25–33.
13. Culler, K. & Price, G. L. (1996) *Linear Algebra Appl.* **248,** 317–325.