On the classification of binary shifts of minimal commutant index

(conjugacy class/commutant index/subfactor index)

GEORGE 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 $\sigma, \rho$ on $R$ are said to be conjugate if there exists a $*$-automorphism $\gamma$ which intertwines $\sigma$ and $\rho$ 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 $\infty$) 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 $\sigma$ of any binary shift is a subset $X$ of the anticommutation set of $\sigma$ and a sequence $\{u_n : n \in \mathbb{Z}^+\}$ of symmetries generating $X$ and satisfying the generalized commutation relations

$$u_i u_j = (-1)^{\delta(i,j)} u_j u_i \tag{1}$$

for distinct $i, j$, where $g$ is the characteristic function of $X$. The mappings $\sigma(u_i) = u_{i+j}$ completely determine $\sigma$ as a unital $*$-endomorphism, and $\sigma$ is a shift in the sense that the inclusion of subfactors $R \supseteq \sigma(R) \supseteq \sigma^2(R) \supseteq \cdots$ 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 $\sigma$ and $\tau$. 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 $\{g(2), g(1), 0, g(1), g(2), \ldots\}$ of the "bistream" $\{0, g(1), g(2), \ldots\}$ 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 bistream corresponding to $X$ is eventually periodic if and only if the corresponding binary shift $\sigma$ 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 $\mathcal{M}_n, n \in \mathbb{N}$, be the group algebra over $\mathbb{C}$ generated by the first $n$ generators $u_0, u_1, \ldots, u_{n-1}$. $\mathcal{M}_n$ consists of the linear combinations of words $u(k_0) = I$ and $u_i u_j \cdots u_k$ in the generators. Using $I$, one may assume the words are presented in ordered form, i.e., $i_0 \leq i_1 \leq \cdots \leq i_m$, and since the $u_i$’s are symmetries, one may also assume that $i_0, i_1, \ldots, i_m$ are distinct. Hence $\mathcal{M}_n$ has dimension $2^{n+1}$ over $\mathbb{C}$. It is clear that $\mathcal{M}_n \subset \mathcal{M}_{n+1}$ is a unital isometric embedding for all $n$.

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

Let $\sigma$ be the unital $*$-endomorphism on $R$ by $\sigma(u_i) = u_{i+1}, i \in \mathbb{Z}^+$. $\sigma$ 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 $\sigma$ is a subfactor of $R$ of subfactor
Corollary 2.2 (from ref. 9, theorem 2.1). A binary shift of finite commutant index restricts to a binary shift \( \sigma \) on the subfactor \( R_s \) of \( R \) generated by the sequence \( \{w, \sigma(w), \sigma^2(w), \ldots \} \). The derived shift \( \sigma \) has commutant index \( k \). The anticommutation set \( X_k \subset \mathbb{N} \) associated with \( \sigma \) is a subset of \( \{1, 2, \ldots, k - 1\} \) which includes \( k - 1 \). \( R_s \) has subfactor index \( 2^m \) in \( R \).

Remark 2.3: Since by the theorem above a binary shift \( \sigma \) 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 \( \sigma \) is a binary shift of commutant index 2. Suppose \( w \) generates the 2-dimensional algebra \( \sigma^2(R) \cap R \).

Definition 2.4. Let \( b = (b_0, b_1, \ldots) \) be a bitstream in \( GF(2) \). Then a vector \( c = (c_0, c_1, \ldots) \) in entries in \( GF(2) \) is said to antimult \( b \) if \( \sum_{i=0}^{k} c_i b_i = 0 \) for all \( k \in \mathbb{Z}^+ \).

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

In the next section we shall establish the following uniqueness result: if \( \sigma, \rho \) are binary shifts of commutant index 2 with generators \( \{u_i \}_{i=0}^{n} \) and \( \{v_i \}_{i=0}^{n} \), respectively, and if \( J = [k_0, \ldots, k_m] \) is a vector over \( GF(2) \) such that \( u_i v_j = \sum_{l=0}^{m} u_i^l v_j^l \) (respectively, \( v_i u_j = \sum_{l=0}^{m} v_i^l u_j^l \)) is a qword for \( \sigma \) (respectively, \( \rho \)), then \( \sigma \) and \( \rho \) are conjugate. We shall require the following results for the proof.

Theorem 2.6 (from ref. 1, theorem 3.6). A pair of binary shifts are conjugate if and only if their anticommutation sets are identical.

Theorem 2.7 (from ref. 2, theorem 3.4). Let \( a = (a_0, a_1, \ldots) \) be a bitstream over \( GF(2) \) with periodic reflected sequence. Then there is a nonzero vector \( k = [k_0, k_1, \ldots, k_m] \) over \( GF(2) \) with the following properties:

(i) \( k \) annihilates \( a \).

(ii) \( k \) is flip-symmetric, i.e., \( k = [k_m, k_{m-1}, \ldots, k_0] \).

(iii) if \( s \) is any other nonzero vector annihilating \( a \) then there are \( c_i \in GF(2) \) such that \( s = c_0 [k_0, k_1, \ldots, k_m, 0, \ldots, 0] + c_1 [0, k_0, k_1, \ldots, k_m, 0, \ldots, 0] + \cdots + c_m [0, 0, 0, \ldots, k_0, k_1, \ldots, k_m] \).

3. Reciprocal Polynomials and Qwords

Let \( \sigma \) 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 \( p(x) = c_{0} + c_{1} x + c_{2} x^2 + \cdots + c_{n} x^n \) in \( F[x] \) and for \( a \) in the word in the generators \( u_i, i \in \mathbb{Z}^+ \), let \( (z, p) \) denote the element \( z^i \sigma(z)^i \cdots \sigma^j(z)^j \) of \( R \). Then the following identities are easily verified for words \( z, z' \) and polynomials \( p, q \) (cf., ref. 6, definition 4.4):

\[
\langle z, p \rangle (z, q) = \langle z, p + q \rangle \quad [3.1]
\]

\[
\langle (z, p), q \rangle = \langle z, pq \rangle \quad [3.2]
\]

\[
\langle (z, p), (z', q) \rangle = \langle z', z \rangle \cdot \langle z, p \rangle \quad [3.3]
\]
It follows that

with

satisfies the following system:

where

is a complete conjugacy invariant, and hence the assertion

corresponds to binary shifts of commutant index 2 whose word has length \( n + 1 \). By Theorem 2.1 such a word \( w \) in the generators \( \{ u_k : k \in \mathbb{Z}^+ \} \) has the form \( w = u_k^a u_1^a \cdots u_n^a \), 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:

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

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

\[
\begin{bmatrix}
  a_0 & a_1 & a_2 & a_3 & \cdots & a_m \\
  a_1 & a_0 & a_1 & a_2 & \cdots & a_{m-1} \\
  a_2 & a_1 & a_0 & a_1 & \cdots & a_{m-2} \\
  \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  a_m & a_{m-1} & a_{m-2} & \cdots & a_0 \\
\end{bmatrix}
\]

By ref. 13, there are \( 2^{n-3} \) choices of \( a_1, \ldots, a_{n-2} \) such that \( A_{n-2} \) is invertible. Assuming \( a_0 \) 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 \( a \) 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 \( a \) 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 \( a_0, a_1, \ldots, a_{n-2}, a_n \). We require

\( k_1 = 1 \), however. By Cramer’s Rule \( k_1 \) is the determinant of the matrix

\[
\begin{bmatrix}
  a_0 & a_1 & \cdots & a_{n-2} & a_1 + 1 \\
  a_1 & a_0 & a_1 & a_2 & a_1 + 0 \\
  a_2 & a_1 & a_0 & a_3 & a_2 + 0 \\
  \vdots & \vdots & \vdots & \vdots & \vdots \\
  a_{n-2} & a_{n-3} & a_{n-4} & a_{n-4} & a_{n-3} + 0 \\
  a_{n-1} & a_{n-2} & a_{n-3} & a_{n-1} & a_{n-1} + 0 \\
\end{bmatrix}
\]

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, 0, 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 $C_i$, $i = 0, 1, \ldots, n$, 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 $C_0$ 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 $C_0 = \sum_{j=0}^{n-1} s_j C_j$. Hence the last column of $A$ coincides with $\sum_{j=0}^{n-1} s_j C_j$. But $C_1, C_2, \ldots, C_{n-1}$ 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 $s_n C_n = C_n = [a_n, \ldots, a_n]^T$. 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 $det(B) = 0$.

Proof: Obvious.

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

**Lemma 4.2.** If $n \in \mathbb{N}$ is odd there are $2^{n-1}$ reciprocal polynomials of degree $n$ with constant coefficient 1. If $n$ is even there are $2^n$ 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 $\prod_{i=1}^{t} f_i(x)$ where $a_i$ are reciprocal.

**Proof:** (a) It is straightforward to show that if $f$ is any polynomial with constant coefficient 1 then $f(x)f^r(x)$ 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 $\prod h_i(x)$ of its irreducible factors. Since $p$ has constant coefficient 1 so do all of the $h_i$’s. Let $deg(h_1) = n$, then since $n = deg(p) = \sum n_k$ we have (see Definition 3.1), $p(x) = p'(x) = x^n p(\frac{1}{x}) = x^n \prod h_i(\frac{1}{x}) = \prod h_i(x)$. 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 $n \cong 3$. Among the $2^{n-1}$ polynomials in $F[x]$ with constant coefficient 1 there are $2^n$ 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 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 $x^3 + x^2 + x + 1 = (x + 1)^2$ are both reciprocal, hence partially reciprocal. Hence there are two polynomials of each type and $pr(2) = 2 = 2^{1-2}$.

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 $n = 5$ even, say $n = 2r$, we claim that $z(n) = z(2r) = \frac{1}{2}(4^r - 4) + 2$ and for $n = 2r + 1$, $z(2r + 1) = \frac{1}{2}(4^r - 4) + 2$. 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
Since all degree 2 polynomials with constant coefficient 1 are reciprocal, and since \( \deg(gh) \neq 1 \) is not a factor of \( h(x) \). Also if \( f(x) \) is partially reciprocal then \( \deg(g) \equiv 2 \); obviously \( \deg(g) \equiv 1 \) 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

\[
pr(n) = \sum_{j=2}^{n-3} s(j)z(n-j) + s(n)z(0)
\]

\[
= \sum_{j=2}^{2m-3} s(j)z(2m-j) + s(2m)
\]

\[
= \sum_{j=2}^{2m-3} s(j)z(2m-j) + 2^m
\]

\[
= I + II, \text{ where}
\]

\[
I = \sum_{k=1}^{m-2} s(2k)z(2(m-k)) + 2^m
\]

\[
= \sum_{k=1}^{m-2} 2^k \left( \left( \frac{1}{3} \right) (2 \cdot 4^{m-k} - 4) - 2 \right) + 2^m, \quad \text{and}
\]

\[
II = \sum_{k=1}^{m-2} s(2k+1)z(2m-(2k+1))
\]

\[
= \sum_{k=1}^{m-2} s(2k+1)z(2(m-k-1) + 1)
\]

\[
= \sum_{k=1}^{m-2} 2^k \left( \left( \frac{1}{3} \right) (4^{m-k-1} - 4) + 2 \right)
\]

\[
So \, pr(n) = I + II = \sum_{k=1}^{m-2} 2^k \left( \left( \frac{1}{3} \right) (2 \cdot 4^{m-k} - 4) + 2 \right) + 2^m
\]

\[
= \sum_{k=1}^{m-2} 2^k \cdot 4^{m-k-1} + 2^m
\]

\[
= \sum_{k=1}^{m-2} 2^k \cdot 4^{m-2k-2} + 2^m
\]

\[
= \sum_{k=1}^{m-2} 2^{2m-2k-2} + 2^m
\]

\[
= 2^{2m-2}.
\]

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 \( n = 2m+1 \), \( pr(n) = \sum_{j=2}^{m-1} s(j)z(n-j) + s(n)z(0) = I + II \), where

\[
I = \sum_{k=1}^{m-1} s(2k)z(2m+1-2k)
\]

\[
= \sum_{k=1}^{m-1} 2^k \cdot z(2(m-k) + 1)
\]

\[
= \sum_{k=1}^{m-1} 2^k \cdot \left( \left( \frac{1}{3} \right) \cdot (4^{m-k} - 4) + 2 \right) + 2^{m-1}z(3)
\]

\[
= \sum_{k=1}^{m-1} 2^k \cdot \left( \left( \frac{1}{3} \right) \cdot (4^{m-k} - 4) + 2 \right) + 2^m, \quad \text{and}
\]

\[
II = \sum_{k=1}^{m-2} s(2k+1)z(2m-2k) + s(2m+1)
\]

\[
= \sum_{k=1}^{m-2} 2^k \cdot \left( \left( \frac{1}{3} \right) (2 \cdot 4^{m-k} - 4) + 2 \right) + 2^{m}, \quad \text{so}
\]

\[
I + II = \sum_{k=1}^{m-2} 2^k \left( \left( \frac{1}{3} \right) (2 \cdot 4^{m-k} + 4^{m-k} - 4) + 2 \right) + 2^{m+1}
\]

\[
= \sum_{k=1}^{m-2} 2^k \left( \left( \frac{1}{3} \right) (4^{m-k} + 4^{m-k} - 4) + 2 \right) + 2^{m+1}
\]

\[
= \sum_{k=1}^{m-2} 2^k \cdot 4^{m-k} + 2^{m+1}
\]

\[
= \sum_{k=1}^{m-2} 2^{2m-2k-2} + 2^{m+1}
\]

\[
= \sum_{k=1}^{m-2} 2^{2m-2k-1} + 2^{m+1}
\]

\[
= 2^{2m-1}.
\]

So far we have shown that if we assume \( z(2r) = \left( \frac{1}{3} \right) (2 \cdot 4^{r-1} + 4) - 2 \) for all \( r \) such that \( 2r < n \) and \( z(2r+1) = \left( \frac{1}{3} \right) (4^{r} - 4) + 2 \) 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

\[
z(n) = 2^{n-2} - z(n-1)
\]

\[
= 2^{2k-1} - z(2k)
\]

\[
= 2^{2k-1} - \left( \left( \frac{1}{3} \right) (2 \cdot 4^{k-1} + 4) - 2 \right)
\]

\[
= \left( \frac{1}{3} \right) (3 \cdot 2^{2k-1} - 2 \cdot 4^{k-1} - 4) + 2 \]

\[
= \left( \frac{1}{3} \right) \left( 3 \cdot 2^{2k-1} - 2 \cdot 2^{2k-2} - 4 \right) + 2
\]

\[
= \left( \frac{1}{3} \right) \left( 4^{k} - 4 \right) + 2.
\]
If \( n \) is even then similarly, for \( z = 2k \),
\[
z(n) = 2^{n-2} - z(n-1) = 2^{2k-2} - z(2k-1) = 2^{2k-2} - z(2(k-1) + 1) = 2^{2k-2} - \left( \frac{1}{3} \right)(4^{k-1} - 4) - 2 = 4^{k-1} - \left( \frac{1}{3} \right)(4^{k-1} - 4) - 2 = \left( \frac{1}{3} \right)(2 \cdot 4^{k-1} - 4) - 2
\]
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 \( \geq 3 \) and conjugacy classes of binary shifts of commutant index 2 whose qwords have length \( \geq 4 \). 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 \( u_0^k u_1^{k_1} \cdots u_n^{k_n} \).

**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 bit-strings. 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 \( u_0^k u_1^{k_1} \cdots u_n^{k_n} \). 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 \( w = u_0^k u_1^{k_1} \cdots u_n^{k_n} = (u_0, p) \) be a qword corresponding to a representative \( \sigma \) 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.