PONS, REED-MULLER CODES, AND GROUP ALGEBRAS

Myoung An, Jim Byrnes, William Moran, B. Saffari, Harold S. Shapiro, and Richard Tolimieri
Prometheus Inc.
21 Arnold Avenue
Newport, RI 02840
jim@prometheus-inc.com

Abstract In this work we develop the family of Prometheus orthonormal sets (PONS) in the framework of certain abelian group algebras. Classical PONS, considered in 1991 by J. S. Byrnes, turned out to be a rediscovery of the 1960 construction by G. R. Welti [28], and of subsequent rediscoveries by other authors as well.

This construction highlights the fundamental role played by group characters in the theory of PONS. In particular, we will relate classical PONS to idempotent systems in group algebras and show that signal expansions over classical PONS correspond to multiplications in the group algebra.

The concept of a splitting sequence is critical to the construction of general PONS. We will characterize and derive closed form expressions for the collection of splitting sequences in terms of group algebra operations and group characters.

The group algebras in this work are taken over direct products of the cyclic group of order 2. PONS leads to idempotent systems and ideal decompositions of these group algebras. The relationship between these special systems and ideal decompositions, and the analytic properties of PONS, is an open research topic. A second open research topic is the extension of this theory to group algebras over cyclic groups of order greater than 2.

Keywords: character basis, companion row, crest factor, FE, Fejer dual, functional equation, generating function, generating polynomial, Golay, group algebra, Hadamard matrix, PONS, QMF, Reed-Muller Codes, Shapiro transform, Shapiro sequence, splitting property, splitting sequence, symmetric PONS, Thue-Morse sequence, Welti codes, Walsh-Hadamard matrices.

1. Introduction

PONS, the *Prometheus Orthonormal Set,* has undergone considerable refinement, development, and extension since it was considered in [6]. First it turned out to be a rediscovery of Welti's 1960 construction [28] and of subsequent rediscoveries by others as well. Its application as an energy spreading transform for one-dimensional digital signals is discussed in [10], with further details of this aspect presented in the patent [9]. The construction of a smooth basis with PONS-like properties is given in [8], thereby answering in the affirmative a question posed by Ingrid Daubechies in 1991. A conceptually clear definition of the PONS sequences that comprise the original symmetric PONS matrix, via polynomial concatenations, is also given in [8]. An application to image processing of a preliminary version of multidimensional PONS can be found in [7]. An in-depth study of multidimensional PONS is currently being prepared. Proofs of the results given below will appear elsewhere.

2. Analytic Theory of One-Dimensional PONS (Welti)

First we provide an account of some of the most basic mathematical concepts and results on *one-dimensional* PONS (Welti) sequences and the related PONS (Welti) matrices.

2.1 Shapiro Transforms of Unimodular Sequences

The whole mathematical theory of the PONS system, and also its applications to signal processing, turn out to derive from *one* fundamental idea, that of the *Shapiro transform of a unimodular sequence*. We begin by describing it.

Let $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ be *any* infinite sequence of unimodular complex numbers. Then a sequence (P_m, Q_m) of polynomial pairs (with unimodular coefficients and common length 2^m) is inductively defined as follows: $P_0(x) = Q_0(x) = 1$, and:

$$\begin{cases} P_{m+1}(x) &= P_m(x) + \alpha_m x^{2^m} Q_m(x) \\ Q_{m+1}(x) &= P_m(x) - \alpha_m x^{2^m} Q_m(x) \end{cases} \quad \text{for all integers } m \geq 0. \quad (1)$$

Since $P_m(x)$ is a truncation of $P_{m+1}(x)$ for *every* $m \geq 0$, it follows that there is an *infinite* sequence $(\beta_0, \beta_1, \beta_2, \ldots)$ of unimodular complex numbers which *only* depends on the given sequence $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ and such that for each $m \geq 0$ the *first* polynomial P_m of the pair (P_m, Q_m) is always the partial sum of length 2^m (i.e., of degree $2^m - 1$) of the *unique*

power series $\sum_{k=0}^{\infty} \beta_k x^k$. Note that such a property does *not* hold for the polynomials Q_m, since Q_m is not a truncation of Q_{m+1}.

The explicit construction of the Shapiro transform $(\beta_k)_{k\geq 0}$ in terms of the original unimodular sequence $(\alpha_m)_{m\geq 0}$ is as follows: Let $k = \sum_{r\geq 0} \delta_r \cdot 2^r$ denote the expansion of an arbitrary integer $k \geq 0$ in base 2 (so that the "*binary digits*" δ_r take only the values 0 and 1, and $\delta_r = 0$ for all $r > \log k/\log 2$). Then we have

$$\beta_k = \epsilon_k \prod_{r\geq 0} \alpha_r^{\delta_r} \tag{2}$$

where

$$\epsilon_k = (-1)^{\sum_{r\geq 0} \delta_r \delta_{r+1}} \quad \text{(the classical Shapiro sequence [25])}. \tag{3}$$

We call $(\beta_k)_{k\geq 0}$ the *Shapiro transform* of the sequence $(\alpha_m)_{m\geq 0}$. In particular, when $\alpha_m = 1$ for all $m \geq 0$, we have $\beta_k = \epsilon_k$ (the classical Shapiro sequence).

The "*Shapiro transform power series*" $\sum_{k=0}^{\infty} \beta_k z^k$ and the related polynomial pairs (P_m, Q_m) have, respectively, all the remarkable properties of the classical Shapiro power series $\sum_{k=0}^{\infty} \epsilon_k z^k$ and those of the classical Shapiro polynomial pairs. (We will recall these properties in the following section, on the "original PONS matrix"). In addition, all the *unimodular complex* numbers $\alpha_0, \alpha_1, \alpha_2, \ldots$ are at our disposal, which can be useful in many situations. For our present purposes (PONS constructions) the parameters $\alpha_0, \alpha_1, \alpha_2, \ldots$ will only take the values ± 1. But the case when $\alpha_m = \pm 1$ or $\pm i$ can also be useful in signal processing (and leads to PONS-type Hadamard matrices with entries ± 1, $\pm i$). Other choices of the unimodular parameters $\alpha_0, \alpha_1, \alpha_2, \ldots$ have other interesting applications that will be dealt with elsewhere.

2.2 The Original PONS (Welti) Matrix of Order 2^m

Before giving, in section 2.4, several (essentially equivalent) definitions of PONS matrices in full generality, and indicating structure theorems for such general PONS matrices, we start by recalling the *original PONS matrix* constructed in 1991 and published in 1994 [6]. Indeed, the proofs of structure results for *general* PONS matrices make use (in the inductive arguments) of properties of this original matrix of order 2^m, which we will denote by P_{2^m}. (There is no risk of confusion with the previously defined *polynomial* P_m).

The original way of defining the P_{2^m} uses an inductive method based on the *concatenation rule*:

$$\begin{pmatrix} A \\ B \end{pmatrix} \to \begin{pmatrix} A & B \\ A & -B \\ B & A \\ B & -A \end{pmatrix} \tag{4}$$

where A and B are two consecutive matrix rows. More precisely, we start with the 2×2 matrix

$$P_2 := \begin{pmatrix} + & + \\ + & - \end{pmatrix}$$

(where, henceforth, we write $+$ instead of $+1$ and $-$ instead of -1, to ease notation). Thus the two rows of P_2 are $A = (++)$ and $B = (+-)$. Then the rule (4) means that the first row of the next matrix, P_4, is the concatenation of A and B, which here is $(+++-)$; the second row of P_4 is the concatenation of $A = (++)$ and $-B := (-+)$, which is therefore $(++-+)$; the third row of P_4 is the concatenation of B and A, i.e., $(+-++)$; and finally the fourth row of P_4 is the concatenation of $B = (+-)$ and $-A := (--)$. Thus

$$P_4 := \begin{pmatrix} + & + & + & - \\ + & + & - & + \\ + & - & + & + \\ + & - & - & - \end{pmatrix}.$$

To obtain the next matrix P_8, we first take the pair A, B to be the first two rows of P_4 (in that order) and use the concatenation rule (4) to obtain the first four rows of P_8. Then we take the pair A, B to be the next two rows of P_4 (in that order), and use the concatenation rule (4) to obtain the next four rows of P_8. Thus

$$P_8 := \begin{pmatrix} + & + & + & - & + & + & - & + \\ + & + & + & - & - & - & + & - \\ + & + & - & + & + & + & + & - \\ + & + & - & + & - & - & - & + \\ + & - & + & + & - & + & + & + \\ + & - & + & + & + & - & - & - \\ + & - & - & - & + & - & + & + \\ + & - & - & - & - & + & - & - \end{pmatrix}.$$

Similarly, the first two rows of P_8 and the concatenation rule (4) yield the first four rows of P_{16}, and so on. Already, from this definition, one can deduce many fundamental properties held by P_{2^m}, $(m = 1, 2, 3, \ldots)$.

We list some of them and indicate later on that many of these properties also hold for the most general PONS (Welti) matrices that we shall define and characterize below. In addition, some of these properties (for example, the extremely important *bounded crest-factor property for all finite sections*) will also be seen to be valid for some very broad classes of Hadamard matrices generalizing the PONS (Welti) matrices.

We note that, in the context of codewords, a basically identical matrix to P_L was constructed by Welti [28]. Several additional authors [16, 18, 26, 29] have also reported on these *Welti codes* and their application to radar, and others [5, 3, 4, 21, 22, 19, 20] have discussed communications applications of similar constructions.

2.3 Some Properties of the Original PONS (Welti) matrix P_L, $(L = 2^m)$

As we said, most of the properties below will be seen to hold for the most general PONS matrices (that we shall define later, in section 2.4) and even for some very broad generalizations of PONS.

PROPERTY 1 *P_L, with $L = 2^m$, is a Hadamard matrix of order 2^m.*

PROPERTY 2 *Suppose the rows of P_L are ordered from 0 to $L-1$ (i.e., the first row has rank 0 and the last row has rank $L-1$). Denote by $A_r(z)$ the polynomial "associated" to the r-th row (i.e., $A_r(z) = \sum_{k=0}^{L-1} a_k z^k$ if $(a_0, a_1, \ldots a_{L-1})$ denotes the r-th row, $r = 0, 1, \ldots L-1$). It is well known [2] that, with this notation, $A_1(z) = (-1)^{m+1} A_0^*(-z)$ where $A^*(z) = z^{\deg A}\overline{A}(1/z)$ denotes the "inverse" of the polynomial $A(z)$. This is a famous identity on the classical Shapiro pairs. Property 2 is that a similar identity $A_{2r+1}(z) = \lambda_{m,r} A_{2r}^*(-z)$ holds for all $r = 0, 1, \ldots L/2$, where $\lambda_{m,r}$ is an extremely interesting number (with values ± 1) expressible in terms of the "Morse sequence". The Morse sequence is the sequence of coefficients in the Taylor (or power series) expansion of the infinite product $\prod_{s=0}^{\infty} \left(1 - z^{2^s}\right)$.*

PROPERTY 3 *With the previous notation, for every $r = 0, 1, \ldots L/2$ the polynomials $A_{2r}(z)$ and $A_{2r+1}(z)$ are "Fejér-dual" (or "dual" for short), that is,*

$$|A_{2r}(z)|^2 + |A_{2r+1}(z)|^2 = \text{ constant } (= 2L, \text{ in this case}) \qquad (5)$$

for all $z \in \mathbb{C}$ with $|z| = 1$. Equivalently, the $(2r)$-th row and the $(2r+1)$-st row are always "Golay complementary pairs" [15].

PROPERTY 4 *[Much related to Properties 2 and 3] Every row-polynomial $A_r(z)$ is QMF, that is,*

$$|A_r(z)|^2 + |A_r(-z)|^2 = \text{ constant } (= 2L \text{ in this case}) \tag{6}$$

for all $z \in \mathbb{C}$ with $|z| = 1$.

PROPERTY 5 (THE "SPLITTING PROPERTY" OF ROWS) *For every $r = 0, 1, \ldots, L-1$, the two "halves" of the row-polynomial $A_r(z)$ are dual, each of these two halves has dual halves, each of these halves (i.e., "quarters" of $A_r(z)$) has dual halves, and so on. This "splitting property" is, by far, the most important property, in view of its applications to "energy spreading". It extends to general PONS matrices and to a broader class of PONS-related Hadamard matrices that we will consider later.*

PROPERTY 6 (THE "QMF-SPLITTING PROPERTY") *This is a finer form of the "QMF property" (Property 4) and an analog of the "splitting property" just described. We will postpone its definition until we come to the structure results for general PONS matrices (in section 2.4).*

PROPERTY 7 (THE "HYBRID SPLITTING PROPERTY") *This is also a finer form of the "QMF property (above Property 4), and is as follows: Every row-polynomial $A_r(z)$ is QMF, i.e., (6) holds; and if we split $A_r(z)$ into two halves of equal length, then each of those halves is QMF. If we split these halves into halves of equal length, these in turn are QMF, and so on. We will return to this property in section 2.4 when we deal with the structure results for general PONS matrices.*

PROPERTY 8 (THE "CONSTANT ROW-SUMS PROPERTY") *If m is even, then each row-sum of P_L (with $L = 2^m$) has the constant value $\sqrt{L} = 2^{m/2}$. If m is odd, then the row sums are either zero or $\sqrt{2L} = 2^{(m+1)/2}$. This property is important but easy to check. However, this is a very special case of the deep (and still partly open) problem of the values of row-polynomials at various roots of unity.*

PROPERTY 9 ("BOUNDED CREST FACTOR PROPERTIES") *Not only is it true that every row-polynomial have crest factor $\leq \sqrt{2}$, but also every finite section of such a polynomial has crest factor not exceeding some absolute constant C. (Good values of C are known, but the optimal value of C is still an open problem.) We point out that these extremely important properties (for "energy spreading") are closely related to Property 5 (splitting properties of rows).*

PROPERTY 10 ("DUAL-COMPANION UNIQUENESS") *Every row has exactly one "companion row", that is, if $A_r(z)$ and $A_s(z)$ denote the associated row-polynomials, then $|A_r(e^{it})| = |A_s(e^{it})|$ for all $t \in \mathbb{R}$. These*

two rows are "mirror images" of each other, except for a possible multiplication by -1. This possible sign change, and also the distribution of the location of s in terms of r, are quite surprising and can be expressed, here also, in terms of the Morse sequence. As a corollary, every row has exactly two "duals" (or, equivalently, two rows which are Golay-complements to it [15]).

2.4 General Definition of PONS (Welti) Matrices

In section 2.3 we described the original PONS matrix and some of its properties. Before considering any other special PONS matrices (such as, typically, the *symmetric* PONS matrices the very existence of which is really surprising), we will give a *general definition* of PONS matrices and also consider some of their useful generalizations. It is convenient to start by considering three very broad classes of finite sequences of length 2^m. These have an independent interest, with or without regard to Hadamard or PONS matrices.

So, let $S = (a_0, a_1, \ldots a_{L-1})$ denote any complex-valued sequence of length $L = 2^m$, $(m \geq 1)$. Its "*associated polynomial*" (or "*generating polynomial*") is

$$P(z) := \sum_{k=0}^{L-1} a_k z^k.$$

The two "halves" of $P(z)$ are:

$$A(z) = \sum_{k=0}^{L/2-1} a_k z^k \quad \text{and} \quad B(z) = \sum_{k=L/2}^{L-1} a_k z^k.$$

Definition 11 *The sequence S is said to have the "splitting property" (or to be a "splitting sequence") if its generating polynomial $P(z)$ has "dual" halves, that is,*

$$|A(e^{it})|^2 + |B(e^{it})|^2 = \text{ constant } (= \|P\|_2^2 = \sum_{k=0}^{L-1} |a_k|^2, \text{ necessarily}),$$

and if each of the halves $A(z)$ and $B(z)$ has dual halves, and so on.

Definition 12 *The sequence S is said to have the "QMF splitting property" (or to be a "QMF splitting sequence") if, first of all, it is QMF, which means that $P(z)$ and $P(-z)$ are dual, or, equivalently, that the even-index component $C(z) := \sum_{k=0}^{L/2-1} a_{2k} z^k$ and the odd-index component $D(z) := \sum_{k=0}^{L/2-1} a_{2k+1} z^k$ are dual; and if, in turn, both of $C(z)$ and $D(z)$ are QMF; and so on.*

DEFINITION 13 *The sequence S is said to have the "hybrid splitting property" (or to be a "hybrid splitting sequence") if it is QMF (i.e., $P(z)$ and $P(-z)$ are dual), and if it has QMF halves (i.e., $A(z)$ and $A(-z)$ are dual and also $B(z)$ and $B(-z)$ are dual), and if each of the halves has QMF halves, and so on.*

We point out that these are three (overlapping but) *pairwise distinct* classes, even if S is assumed to only take the values ± 1 (as long as $L \geq 16$). The smallest $L = 2^m$ for which one can find examples of ± 1 sequences of length L satisfying one of the above conditions and not the other two is precisely $L = 16$. However, we have the following two theorems:

THEOREM 14 *For any integer $m \geq 4$, there are Hadamard matrices of order $L = 2^m$ all of whose rows satisfy the requirements of any of the above three definitions, but not those of the other two.*

Thus we obtain three *pairwise distinct* (and very broad) classes of Hadamard matrices of order $L = 2^m$, ($L \geq 16$), which we call respectively:

(A) the class of $2^m \times 2^m$ Hadamard matrices with "*splitting rows*".

(B) the class of $2^m \times 2^m$ Hadamard matrices with "*QMF-splitting rows*".

(C) the class of $2^m \times 2^m$ Hadamard matrices with "*hybrid splitting rows*".

Our Theorem 15, stated below, says that the intersection of *any two* of the above three classes of Hadamard matrices is contained in the third class. (This will lead to the notion *and* complete identification of all "*general PONS matrices*"). We note that none of the classical Walsh-Hadamard matrices [1] lies in any of these three classes.

THEOREM 15 (UNIQUENESS AND STRUCTURE THEOREM) for General PONS Matrices *Suppose that all the rows of some $2^m \times 2^m$ Hadamard matrix P have any two of the above three properties (A), (B), (C).*

Then all the rows of P also have the third property, that is, all three of (A), (B) and (C) are satisfied by all the rows. In that case the rows of P constitute some permutation of the rows of the "original PONS matrix" P_L, with $L = 2^m$, after some of these rows have possibly been multiplied by -1.

REMARK 16 *The converse of Theorem 15 is obvious, in view of the properties of Shapiro transforms of ± 1 sequences.*

The proof of Theorem 15 is non-trivial. It is done by induction, and it uses (as a lemma) Property 10 of the "*original PONS matrix*" P_L and the fact that each row-polynomial $A_r(z)$ has *exactly two* duals $A_t(z)$ which are of the form $\pm A_r(-z)$ or $\pm A_r^*(-z)$. This lemma, in turn, rests on another lemma which involves the exact computation of the greatest common divisor between any two row-polynomials of P_L.

DEFINITION 17 *A general PONS (Welti) matrix of order* 2^m *is any* $2^m \times 2^m$ *Hadamard matrix satisfying the conditions of Theorem 15.*

COROLLARY 18 *All the rows of any* $2^m \times 2^m$ *general PONS matrix have all those properties of rows of the original PONS matrix* P_L *which are invariant by permutations of rows and sign changes.*

At this stage we mention the following result which also illustrates some structural difference between the PONS matrices and its generalizations.

PROPOSITION 19 *The largest length of runs of equal consecutive terms in any PONS-matrix row is 4. The largest length of runs of equal consecutive terms in any row of a "splitting Hadamard matrix" is 6.*

2.5 Symmetric PONS Matrices

If the "concatenation rule" (4) of section 2.2 is replaced by the new concatenation rule

$$\begin{pmatrix} A \\ B \end{pmatrix} \rightarrow \begin{pmatrix} A & B \\ A & -B \\ B & A \\ -B & A \end{pmatrix} \tag{7}$$

with the same starting matrix

$$P_2 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

then the result is a sequence of $2^m \times 2^m$ *symmetric* matrices which are, by construction and in view of the above Theorem 15, PONS matrices. A consequence of this extremely unexpected result is that, by standard operations on rows and suitable choice of the parameters α_j of section 2.2, we obtain *on the order of* 2^m symmetric $2^m \times 2^m$ PONS matrices.

3. Shapiro Sequences, Reed-Muller Codes, and Functional Equations

We begin our journey into the more algebraic aspects of PONS sequences by discussing their surprising relation to Reed-Muller codes.

Let $\mathbb{Z}_2^{2^m}$ be the set of binary 2^m-tuples, $m \geq 1$.

For each n, $1 \leq n \leq 2^m - 1$, and each j, $1 \leq j \leq m$, let $\delta_{j,n}$ be the coefficient of 2^{j-1} in the binary expansion of n and define $\delta_{0,n}$ to be $1, 0 \leq n \leq 2^m - 1$, so that

$$n = \sum_{j=1}^{m} 2^{j-1} \delta_{j,n}.$$

Define vectors $\vec{g}_j$ by

$$\vec{g}_j = \vec{g}_j(m) = \langle\, \delta_{j,0}\, \delta_{j,1}\, \delta_{j,2} \ldots\, \delta_{j,2^m-1} \,\rangle,$$

$$\vec{g}_0 = \vec{g}_0(m) = \langle\, 1\, 1\, 1 \ldots\, 1 \,\rangle.$$

and the matrix $\mathbf{G}_m$ by

$$\mathbf{G}_m = \{\vec{g}_0, \vec{g}_1, \ldots, \vec{g}_m\}$$

Example: $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_0$	1	1	1	1	1	1	1	1
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1

$$\begin{aligned} \mathbf{G}_3 = \{ \quad & \langle\, 1\,1\,1\,1\,1\,1\,1\,1 \,\rangle, \quad \langle\, 0\,1\,0\,1\,0\,1\,0\,1 \,\rangle, \\ & \langle\, 0\,0\,1\,1\,0\,0\,1\,1 \,\rangle, \quad \langle\, 0\,0\,0\,0\,1\,1\,1\,1 \,\rangle \quad \} \end{aligned}$$

The $\vec{g}_m$ are discretized versions of the Rademacher functions.

Claim. The elements of $\mathbf{G}_m$ are linearly independent.
The *Reed-Muller code* of rank m and order 0 is

$$RM(0, m) = \{\langle 0\,0 \ldots\, 0\rangle, \langle 1\,1 \ldots\, 1\rangle\},$$

where each vector (*codeword*) has 2^m entries. $RM(1, m)$ is the subgroup of $\mathbb{Z}_2^{2^m}$ generated by the codewords in $\mathbf{G}_m$, *i.e.*, the vector space over $\mathbb{Z}_2$ spanned by these codewords. $RM(1, m)$ contains 2^{m+1} codewords.
Define *multiplication* $\cdot$ on $\mathbb{Z}_2^{2^m}$ by

$$\langle x_0\, x_1 \ldots\, x_{2^m-1}\rangle \cdot \langle y_0\, y_1 \ldots\, y_{2^m-1}\rangle = \langle x_0 y_0\, x_1 y_1 \ldots\, x_{2^m-1} y_{2^m-1}\rangle.$$

Augment $\mathbf{G}_m$ with all products $\vec{g}_i \cdot \vec{g}_j$, $1 \leq i < j \leq m$, to form $\mathbf{G}_m^{(2)}$.

Example: $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_0$	1	1	1	1	1	1	1	1
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1
$\vec{g}_1 \cdot \vec{g}_2$	0	0	0	1	0	0	0	1
$\vec{g}_1 \cdot \vec{g}_3$	0	0	0	0	0	1	0	1
$\vec{g}_2 \cdot \vec{g}_3$	0	0	0	0	0	0	1	1

$$\mathbf{G}_3^{(2)} = \mathbf{G}_3 \cup \{\langle 0\,0\,0\,1\,0\,0\,0\,1 \rangle, \langle 0\,0\,0\,0\,0\,1\,0\,1 \rangle, \langle 0\,0\,0\,0\,0\,0\,1\,1 \rangle\}.$$

Claim. The $1 + m + \binom{m}{2}$ elements of $\mathbf{G}_m^{(2)}$ are linearly independent.
$RM(2, m)$ is the subgroup of $\mathbb{Z}_2^{2^m}$ generated by the codewords in $\mathbf{G}_m^{(2)}$.
$RM(2, m)$ contains $2^{1+m+\binom{m}{2}}$ codewords.
Augmenting $\mathbf{G}_m^{(2)}$ with all products of the form $\vec{g}_i \cdot \vec{g}_j \cdot \vec{g}_k$, $1 \le i < j < k \le m$, and continuing as above we get $\mathbf{G}_m^{(3)}$, $RM(3, m)$, *etc.*

Theorem. $RM(k, m)$ for $m \ge 1$, $0 \le k \le m$ is a subgroup of $\mathbb{Z}_2^{2^m}$ consisting of 2^N codewords, where $N = \sum_{i=0}^{k} \binom{m}{i}$. The minimum *Hamming weight* (*i.e.*, number of ones) of the nonzero codewords in $RM(k, m)$ is 2^{m-k}.

Proof. Exercise, or see Handbook of Coding Theory, V. Pless and W.C. Huffman, Editors, Vol. 1, pp. 122–126.
Let's examine a particular element $\vec{S}_m \in RM(2, m)$ given by

$$\vec{S}_m = \sum_{j=1}^{m-1} \vec{g}_j \cdot \vec{g}_{j+1} = \langle s_0\, s_1\, \ldots\, s_{2^m-1} \rangle.$$

Example. $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1
$\vec{S}_3$	0	0	0	1	0	0	1	0

Let $\phi(n)$ be the number of times that the *block* $B = [1\,1]$ occurs in the binary expansion of n, $0 \le n \le 2^m - 1$.

Claim.

$$s_n = \begin{cases} 0 & \text{if } \phi(n) \text{ is even} \\ 1 & \text{if } \phi(n) \text{ is odd.} \end{cases}$$

Let $\mathcal{G}_m = \{\vec{\gamma}_0, \vec{\gamma}_1, \vec{\gamma}_2, \ldots, \vec{\gamma}_{2^m-1}\}$ be the subgroup of $RM(1,m)$ generated by $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_m$.

Example. $m = 3$

	n	0	1	2	3	4	5	6	7
	$\vec{g}_1$	0	1	0	1	0	1	0	1
	$\vec{g}_2$	0	0	1	1	0	0	1	1
	$\vec{g}_3$	0	0	0	0	1	1	1	1
$\mathcal{G}_3$	$\vec{\gamma}_0 = 0\cdot\vec{g}_1 + 0\cdot\vec{g}_2 + 0\cdot\vec{g}_3$	0	0	0	0	0	0	0	0
	$\vec{\gamma}_1 = 1\cdot\vec{g}_1 + 0\cdot\vec{g}_2 + 0\cdot\vec{g}_3$	0	1	0	1	0	1	0	1
	$\vec{\gamma}_2 = 0\cdot\vec{g}_1 + 1\cdot\vec{g}_2 + 0\cdot\vec{g}_3$	0	0	1	1	0	0	1	1
	$\vec{\gamma}_3 = 1\cdot\vec{g}_1 + 1\cdot\vec{g}_2 + 0\cdot\vec{g}_3$	0	1	1	0	0	1	1	0
	$\vec{\gamma}_4 = 0\cdot\vec{g}_1 + 0\cdot\vec{g}_2 + 1\cdot\vec{g}_3$	0	0	0	0	1	1	1	1
	$\vec{\gamma}_5 = 1\cdot\vec{g}_1 + 0\cdot\vec{g}_2 + 1\cdot\vec{g}_3$	0	0	1	1	0	0	1	1
	$\vec{\gamma}_6 = 0\cdot\vec{g}_1 + 1\cdot\vec{g}_2 + 1\cdot\vec{g}_3$	0	0	1	1	1	1	0	0
	$\vec{\gamma}_7 = 1\cdot\vec{g}_1 + 1\cdot\vec{g}_2 + 1\cdot\vec{g}_3$	0	1	1	0	1	0	0	1

We now switch gears slightly, by rewriting all codewords in $RM(k,m)$ by mapping $0 \to 1$, $1 \to -1$. Since $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_m$ are discretized versions of the Rademacher functions, $\vec{\gamma}_0, \vec{\gamma}_1, \ldots, \vec{\gamma}_{2^m-1}$, are discretized versions of the Walsh functions. That is, $\mathcal{G}_m$ is the $2^m \times 2^m$ Sylvester Hadamard matrix, which we relabel H_m.

Example.

$$H_3 = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{matrix}$$

Now $s_n = (-1)^{\phi(n)}$.

Since we have

$$s_{2n} = s_n, \quad s_{2n+1} = \begin{cases} s_n & \text{if } n \text{ is even} \\ -s_n & \text{if } n \text{ is odd} \end{cases},$$

the binary expansion of $2n$ is the binary expansion of n shifted one slot to the left with a 0 added on the right and the binary expansion of $2n+1$ is the binary expansion of n shifted one slot to the left with a 1

added on the right. If n is even this does not change $\phi(n)$. If n is odd (*i.e.*, n *ends in* 1) then $\phi(2n+1) = \phi(n) + 1$.

■

Consider the *generating function* of $\{s_n\}$,

$$g(z) = \sum_{n=0}^{\infty} s_n z^n.$$

It can be shown that $g(z)$ satisfies the functional equation (FE) (Brillhart and Carlitz)

$$g(z) = g(z^2) + zg(-z^2).$$

Iterate this FE:

$$\begin{aligned} g(z^2) &= g(z^4) + z^2 g(-z^4) \\ g(-z^2) &= g(z^4) - z^2 g(-z^4), \quad \text{so} \\ g(z) &= (1+z)g(z^4) + z^2(1-z)g(-z^4). \end{aligned}$$

Repeat:

$$\begin{aligned} g(z^4) &= g(z^8) + z^4 g(-z^8) \\ g(-z^4) &= g(z^8) - z^4 g(-z^8), \quad \text{so} \\ g(z) &= (1+z+z^2-z^3)g(z^8) + z^4(1+z-z^2+z^3)g(-z^8). \end{aligned}$$

Continuing we see that, beginning with

$$g(z) = A(z)g(z^{2^m}) + z^{2^{m-1}} B(z) g(-z^{2^m})$$

and applying

$$\begin{aligned} g(z^{2^m}) &= g(z^{2^{m+1}}) + z^{2^m} g(-z^{2^{m+1}}) \\ g(-z^{2^m}) &= g(z^{2^{m+1}}) - z^{2^m} g(-z^{2^{m+1}}) \end{aligned}$$

we get at the next step

$$\begin{aligned} g(z) = \left[A(z) + z^{2^{m-1}} B(z)\right] g(z^{2^{m+1}}) \\ + z^{2^m} \left[A(z) - z^{2^{m-1}} B(z)\right] g(-z^{2^{m+1}}) \quad . \end{aligned}$$

Renaming the initial $A(z)$ and $B(z)$ to $P_0(z)$ and $Q_0(z)$, respectively, and naming the (polynomial) coefficients of $g(z^{2^m})$ and $g(-z^{2^m})$ $P_{m-1}(z)$ and $Q_{m-1}(z)$, respectively, $m \geq 1$, the above yields

$$\begin{aligned} P_0(z) &= Q_0(z) = 1 \\ P_m(z) &= P_{m-1}(z) + z^{2^{m-1}} Q_{m-1}(z) \\ Q_m(z) &= P_{m-1}(z) - z^{2^{m-1}} Q_{m-1}(z) \quad . \end{aligned}$$

Thus, the $\{P_m(z)\}_{m=0}^{\infty}$ and $\{Q_m(z)\}_{m=0}^{\infty}$ are precisely the Shapiro Polynomials! $P_m(z)$ and $Q_m(z)$ are each polynomials of degree $2^m - 1$ with coefficients ± 1. For each m, the first 2^m coefficients of $g(z)$ are exactly the coefficients of $P_m(z)$. Therefore, for each m, the 2^m-truncation

$$\langle\, s_0\, s_1\, \ldots\, s_{2^m-1}\,\rangle$$

of the *Shapiro sequence* $\{s_j\}_{j=0}^{\infty}$ is an element of $RM(2,m)$.
Why might that be important?

Recall the fundamental property of the Shapiro polynomials, namely that for each m P_m and Q_m are complementary:

$$|P_m(z)|^2 + |Q_m(z)|^2 = 2^{m+1} \quad \text{for all } |z| = 1.$$

Consequently P_m and Q_m each have *crest factor* (the ratio of the sup norm to the L^2 norm on the unit circle) bounded by $\sqrt{2}$ *independent of* m. *i.e.*, P_m and Q_m are *energy spreading*. So the coefficients of P_m are an energy spreading second order Reed-Muller codeword. Related results may be found in [11, 27].
Also, letting $\vec{h}_j$, $0 \le j \le 2^m - 1$, denote the rows of $\mathbf{H}_m$, the matrix $\mathbf{P}_m$ whose rows are $\vec{S}_m \cdot \vec{h}_j$, is a *PONS matrix*. Its 2^m rows can be split into 2^{m-1} pairs of complementary rows, with each row having crest factor (bounded by) $\sqrt{2}$.
Since each $\vec{h}_j \in RM(1,m)$ and $\vec{S}_m \in RM(2,m)$, the (rows of the) PONS matrix is a coset of the subgroup $RM(1,m)$ of $RM(2,m)$.
Thus we have constructed 2^m (really 2^{m+1} by considering $-\mathbf{H}_m$) energy spreading second order Reed-Muller codewords.

Note that blocks other than $B = [1\,1]$ appear in connection with higher-order Reed-Muller codes. For example, the block $[1\,1\,1]$ yields codewords in $RM(3,m)$. The generating functions of these blocks satisfy similar (although more complicated) FE's. An open question is whether these FE's yield corresponding crest factor bounds for subsets of $RM(k,m)$, $k \ge 3$, resulting in higher-order energy spreading Reed-Muller codes.
Blocks and FE's

Let $B = [\beta_1\, \beta_2\, \ldots\, \beta_r]$, $\beta_j = 0$ or 1, $\beta_1 = 1$ be a *binary block* and $N = N(B) = \beta_r + 2\beta_{r-1} + \ldots + 2^{r-1}\beta_1$ be the integer whose binary expansion is B. Let $\Psi_B(n)$ be the number of occurrences of B in the binary expansion of n and let $f_B(z)$ be the generating function of Ψ_B,

$$f_B(z) = \sum_{n=0}^{\infty} \Psi_B(n) z^n \quad .$$

Theorem. $f_B(z)$ satisfies the FE

$$f_B(z) = (1+z)f_B(z^2) + \frac{z^{N(B)}}{1-z^{2^r}} \quad .$$

Now consider the *parity sequence* of $\Psi_B(n)$, $\delta_B(n) = (-1)^{\Psi_B(n)}$, and its generating function $g_B(z) = \sum_{n=0}^{\infty} \delta_B(n) z^n$. For the general case it will again be useful to split g_B into its even and odd parts,

$$E_B(z) = \sum_{n=0}^{\infty} \delta_B(2n) z^{2n}$$
$$O_B(z) = \sum_{n=0}^{\infty} \delta_B(2n+1) z^{2n+1}$$

Previous example: $B = [11]$, $\delta_B(n)$ is the Shapiro sequence, $g_B(z)$ satisfies the FE $g_B(z) = g_B(z^2) + z g_B(-z^2)$.

Example: $B = [1]$.
As before, $\Psi_B(2n) = \Psi_B(n)$ and $\Psi_B(2n+1) = \Psi_B(n)+1$ so that (writing δ_n for $\delta_B(n)$ to ease notation) $\delta_{2n} = \delta_n$, $\delta_{2n+1} = -\delta_n$. Hence $E_B(z) = g_B(z^2)$, $O_B(z) = -z g_B(z^2)$, and we have the FE $g_B(z) = (1-z) g_B(z^2)$. Iterating, $g_B(z) = (1-z)(1-z^2)(1-z^4)\ldots$ and δ_n is the Thue-Morse sequence $[1\,-1\,-1\,1\,-1\,1\,1\,-1\,\ldots]$. We drop the subscript B from now on.

Example: $\beta_r = 0$.
$\Psi(2n+1) = \Psi(n)$, so $\delta_{2n+1} = \delta_n$, so $O(z) = z g(z^2)$. Since $g(z) - g(-z) = 2O(z)$ we have the FE $g(z) = g(-z) + 2z g(z^2)$.

Example: $\beta_r = 1$.
As above, now $g(z) = -g(-z) + 2g(z^2)$.
Example (a typical case?): $B = [1\,1\,0\,0\,1\,0], r = 6$.

$\Psi(2n+1) = \Psi(n)$. $\Psi(2n) = \Psi(n)$ unless the binary expansion of n ends in $[1\,1\,0\,0\,1]$, *i.e.*, unless $n \equiv K \pmod{2^5}$, where $K = 2^4 + 2^3 + 2^0 = 25$, in which case $\Psi(2n) = \Psi(n) + 1$. So

$$\delta_{2n+1} = \delta_n, \quad \delta_{2n} = \begin{cases} -\delta_n & \text{if } n \equiv 25 (\mathrm{mod}\, 32) \\ \delta_n & \text{otherwise} \end{cases} \quad .$$

So $O(z) = z g(z^2)$.

$$E(z) = \sum_{n=0}^{\infty} \delta_{2n} z^{2n} = \sum_{n=0}^{\infty} \delta_n z^{2n} - 2 \sum_{n \equiv 25 (\mathrm{mod}\, 32)} \delta_n z^{2n}$$

$$= g(z^2) - 2 \sum_{j=0}^{\infty} \delta_{32j+25} z^{64j+50} = g(z^2) - 2z^{50} F(z)$$

where $F(z) = \sum_{j=0}^{\infty} \delta_{32j+25} z^{64j}$.
But $\delta_{32j+25} = \delta_{2(16j+12)+1} = \delta_{16j+12} = \delta_{2(8j+6)} = \delta_{8j+6} = \delta_{2(4j+3)} = \delta_{4j+3} = \delta_{2(2j+1)+1} = \delta_{2j+1} = \delta_j$, where we have used the fact that neither $8j+6$ nor $4j+3$ can be congruent to $25 (\mathrm{mod}\, 32)$. So $F(z) = \sum_{j=0}^{\infty} \delta_j z^{64j} = g(z^{64})$, and we have the FE

$g(z) = (1+z) g(z^2) - 2z^{50} g(z^{64})$.

How *typical* is this example? Do we always get *Full Reduction* (FR) of the index of δ?
Consider the general case:

$$B = [\beta_1\, \beta_2\, \ldots\, \beta_r]$$
$$N = \beta_r + 2\beta_{r-1} + \ldots + 2^{r-1}\beta_1$$
$$K = \beta_{r-1} + 2\beta_{r-2} + \ldots + 2^{r-2}\beta_1 \quad .$$

Case I: $\beta_r = 0$. As above,

$$\delta_{2n+1} = \delta_n, \quad \delta_{2n} = \begin{cases} -\delta_n & \text{if } n \equiv K (\mathrm{mod}\, 2^{r-1}) \\ \delta_n & \text{otherwise} \end{cases} \quad .$$

$$O(z) = z g(z^2), \quad E(z) = g(z^2) - 2z^{2K} \sum_{j=0}^{\infty} \delta_{2^{r-1}j+K} z^{2^r j} \quad .$$

To get FR the index $I(1) = I_{j,K}(1) = 2^{r-1}j + K$ must reduce to j by repeated applications of the mapping $\mu(n)$:

$$\mu(2n+1) = n, \quad \mu(2n) = n \quad \text{unless } n \equiv K (\mathrm{mod}\, 2^{r-1}).$$

Let $\{I(1), I(2), \ldots\}$ be the succession of indices that we get by repeating μ (assuming it works), and let I denote one of these indices. Whether $I = 2n+1$ or $I = 2n$, reduction to n occurs by dropping the last binary digit on the right of I and shifting what's left 1 slot to the right. For reduction to fail at the first step, $I(1)$ must be of the form $2n$ where $n \equiv K (\mathrm{mod}\, 2^{r-1})$, or $n = 2^{r-1}m + K$ for some integer m, or $2n = 2^r m + 2K$.
The binary expansion (BE) of K is $(\beta_1\, \beta_2\, \ldots\, \beta_{r-1})$ so that of $2K$ is $(\beta_1\, \beta_2\, \ldots\, \beta_{r-1}\, 0)$.

So for the first reduction $I(1) \to I(2)$ to fail the BE of $I(1)$ must end in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}\,0)$. This is possible (*i.e.*, there are integers j which make it possible) iff the BE of $I(1)$ ends in $(\beta_2\,\beta_3\,\ldots\,\beta_{r-1}0)$, or (since the BE of $I(1)$ ends in that of K)

$$(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}) = (\beta_2\,\beta_3\,\ldots\,\beta_{r-1}0) \quad .$$

Assuming this equation does not hold we get $I(2)$ whose BE ends in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-2})$. As above, $I(2) \to I(3)$ fails iff the BE of $I(2)$ ends in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}\,0)$ which is possible (again, there are integers j which make it possible) iff $I(2)$ ends in $(\beta_3\,\beta_4\,\ldots\,\beta_{r-1}\,0)$, or

$$(\beta_1\,\beta_2\,\ldots\,\beta_{r-2}) = (\beta_3\,\beta_4\,\ldots\,\beta_{r-1}\,0) \quad .$$

Call the block $B = [\beta_1\,\beta_2\,\ldots\,\beta_r]$ *nonrepeatable* if

$$[\beta_1\,\beta_2\,\ldots\,\beta_\nu] \neq [\beta_{r-(\nu-1)}\,\beta_{r-(\nu-2)}\,\ldots\,\beta_r]$$

for each ν, $1 \leq \nu \leq r-1$.

Theorem. FR works iff B is nonrepeatable. When FR works we get the FE $g(z) = (1+z)g(z^2) - 2z^{2K}g(z^{2^r})$.

Case II: $\beta_r = 1$. The above argument works when B is nonrepeatable up to the last step, yielding:

Theorem. If $[\beta_1\,\beta_2\,\ldots\,\beta_\nu] \neq [\beta_{r-(\nu-1)}\,\beta_{r-(\nu-2)}\,\ldots\,\beta_r]$ for each ν, $2 \leq \nu \leq r-1$, and $\beta_1 = \beta_r = 1$, then reduction works up until the final step and we get the FE

$$g(z) = (1+z)g(z^2) - 2z^{2K+1-2^{r-1}}\left[g(z^{2^{r-1}}) - g(z^{2^r})\right] \quad .$$

Other cases are not so neat.

Example. $B = [1\,1\,0\,1\,1\,1]$.

The FE is

$$g(z) = (1+z)g(z^2) - 2z^7g(z^{16}) + 2z^7g(z^{32}) + 2z^{23}g(z^{64}) \quad .$$

Example. $B = [1\,0\,1\,1\,0\,1]$.

The FE is

$$g(z) = (1+z)g(z^2) - 2z^5[g(z^8) - (1+z^8)g(z^{16})] - 2z^{13}[g(z^{32}) - g(z^{64})].$$

The general "1-1" case, $\beta_1 = \beta_r = 1$.

$$\delta_{2n} = \delta_n, \quad \delta_{2n+1} = \begin{cases} -\delta_n & \text{if } n \equiv K (\mathrm{mod}\, 2^{r-1}) \\ \delta_n & \text{otherwise} \end{cases},$$

$$K = \beta_{r-1} + 2\beta_{r-2} + \ldots + 2^{r-2}\beta_1\,,$$

$$E(z) = g(z^2)\,,$$

$$O(z) = zg(z^2) - 2 \sum_{\substack{n \equiv K \\ (\mathrm{mod}\, 2^{r-1})}} \delta_n z^{2n+1} = zg(z^2) - 2G_B(z)$$

$$\text{where} \quad G_B(z) = \sum_{j=0}^{\infty} \delta_{2^{r-1}j+K} z^{2^r j + 2K + 1}.$$

Basic idea: Reduce the subscript of δ as much as possible, express $G_B(z)$ in terms of $G_B(z^{2^p})$ for some $p > 0$, replace $G_B(z^{2^p})$ by using $-2G_B(z^{2^p}) = O(z^{2^p}) - z^{2^p} g(z^{2^{p+1}}) = g(z^{2^p}) - g(z^{2^{p+1}}) - z^{2^p} g(z^{2^{p+1}})$ and then repeat to get the desired expression for $O(z) = g(z) - g(z^2)$.
The result for the "fully repeatable" case, $\beta_j = 1$, $1 \le j \le r$, is:

$$g(z) = (1-z)g(z^2) + 2z[g(z^4) + z^2 g(z^8) + z^6 g(z^{16}) + \ldots + z^{2^{r-2}-2} g(z^{2^{r-1}}) + z^{2^{r-1}-2} g(z^{2^r})].$$

4. Group Algebras

Consider a finite abelian group A with group composition written as multiplication. The *group algebra* $\mathbf{C}A$ is the vector space of formal sums

$$f = \sum_{u \in A} f(u)u, \qquad f(u) \in \mathbf{C},$$

with algebra multiplication defined by

$$fg = \sum_{v \in A} \left(\sum_{u \in A} f(u) g(u^{-1}v) \right) v, \qquad f,\, g \in \mathbf{C}A.$$

Identifying $u \in A$ with the formal sum u, we can view A as a subset of $\mathbf{C}A$. $\mathbf{C}A$ is a commutative algebra with identity. In this section we consider group algebras over direct products of the cyclic group of order 2.

Denote the direct product of N copies of the cyclic group of order 2 by

$$C_2(x_0, \ldots, x_{N-1})$$

and its group algebra by

$$A_2(x_0, \ldots, x_{N-1}).$$

$C_2(x_0, \ldots, x_{N-1})$ is the set of monomials

$$x_0^{j_0} \cdots x_{N-1}^{j_{N-1}}, \quad j_n = 0,\, 1, \quad 0 \le n < N,$$

with multiplication defined by

$$x_n^2 = 1, \quad 0 \le n < N, \tag{8}$$

$$x_m x_n = x_n x_m, \quad 0 \le m,\, n < N. \tag{9}$$

We call the factors x_n, for $0 \le n <$*N*, the *generators* of $C_2(x_0, \ldots, x_{N-1})$. For example,

$$C_2(x_0) = \{1, x_0\}$$

and

$$C_2(x_0, x_1) = \{1, x_0, x_1, x_0 x_1\}.$$

$A_2(x_0, \ldots, x_{N-1})$ is the algebra of polynomials

$$f = \sum_{j_0=0}^{1} \cdots \sum_{j_{N-1}=0}^{1} f(j_0, \ldots j_{N-1}) x_0^{j_0} \cdots x_{N-1}^{j_{N-1}},$$

with multiplication defined by (8) and (9). For example in $A_2(x_0)$ the algebra multiplication is given by

$$(a_0 + a_1 x_0)(b_0 + b_1 x_0) = c_0 + c_1 x_0,$$

where

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 \\ a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

and in $A_2(x_0, x_1)$ the algebra multiplication is given by

$$(a_0 + a_1 x_0 + a_2 x_1 + a_3 x_0 x_1)(b_0 + b_1 x_0 + b_2 x_1 + b_3 x_0 x_1) = \\ c_0 + c_1 x_0 + c_2 x_1 + c_3 x_0 x_1,$$

where

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

In general multiplication in $A_2(x_0, \ldots, x_{N-1})$ can be described by the action of a $2^N \times 2^N$ block circulant matrix having 2×2 circulant blocks.

The monomials

$$x_0^{j_0} \cdots x_{N-1}^{j_{N-1}}, \quad j_n = 0, 1, \quad 0 \le n < N,$$

define a basis, the *canonical basis* of the vector space $A_2(x_0, \ldots, x_{N-1})$. The basis is ordered by the lexicographic ordering on the exponents. For example, as listed,

$$1, x_0$$

is the canonical basis of $A_2(x_0)$ and

$$1, x_0, x_1, x_0 x_1$$

is the canonical basis of $A_2(x_0, x_1)$.

A nonzero element $\tau \in \mathbf{C}A$ is called a character of A if $\tau(1) = 1$ and

$$v\tau = \tau(v^{-1})\tau, \quad v \in A.$$

Denote the collection of characters of A by A^*. The characters of

$$C_2(x_0, \ldots, x_{N-1})$$

are the set of products in $A_2(x_0, \ldots, x_{N-1})$

$$(1 + \epsilon_0 x_0) \cdots (1 + \epsilon_{N-1} x_{N-1}), \quad \epsilon_n = \pm 1, \quad 0 \le n < N.$$

The characters of $C_2(x_0)$ are

$$1 + x_0, \, 1 - x_0.$$

The characters of $C_2(x_0, \ldots, x_{N-1})$ form a basis of the vector space $A_2(x_0, \ldots, x_{N-1})$, called the *character basis*. The characters are ordered such that the matrix H_{2^N} of the character basis relative to the canonical basis is the N-fold tensor product

$$H_{2^N} = H_2 \otimes \cdots \otimes H_2,$$

where

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

is the 2×2 Fourier transform matrix. The matrix of the character basis of $C_2(x_0)$

$$1 + x_0, \, 1 - x_0$$

is H_2 and the matrix of the character basis of $C_2(x_0, x_1)$

$$(1 + x_0)(1 + x_1), \, (1 - x_0)(1 + x_1), \, (1 + x_0)(1 - x_1), \, (1 - x_0)(1 - x_1)$$

is

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

The set of group-translates of the characters of $C_2(x_0)$

$$(1 \pm x_0)x_1^{k_1} \cdots x_{N-1}^{k_{N-1}}, \quad k_n = 0, 1, \quad 0 \le n < N,$$

forms a basis of $A_2(x_0, \ldots, x_{N-1})$, called the *translate-character* basis. The translate-character basis is ordered by first forming the set of pairs

$$(1 + x_0)x_1^{k_1} \cdots x_{N-1}^{k_{N-1}}, \quad (1 - x_0)x_1^{k_1} \cdots x_{N-1}^{k_{N-1}} \tag{10}$$

and then lexicographically ordering the exponents in the set of pairs. The matrix of the translate-character basis relative to the canonical basis is the N-fold matrix direct sum

$$H_2 \oplus \cdots \oplus H_2.$$

The translate-character basis of $A_2(x_0, x_1)$ is

$$1 + x_0, \quad 1 - x_0, \quad (1 + x_0)x_1, \quad (1 - x_0)x_1.$$

The translate-character basis will be especially important in the development of PONS. The main reason is contained in the following discussion.

Consider $f \in A_2(x_0, \ldots, x_{N-1})$ such that

$$f(j_0, \ldots, j_{N-1}) = \pm 1, \quad j_n = 0, 1, \quad 0 \le n < N.$$

The coefficients of the expansion of f over the translate-character basis are ± 1 or 0 and for each exponent set

$$k_1, \ldots, k_{N-1}, \quad k_n = \pm 1, \quad 0 \le n < N,$$

exactly one element in the pair (10) has nonzero coefficient. For example the element in $A_2(x_0, x_1)$

$$f = f_0 + f_1 x_0 + f_2 x_1 + f_3 x_0 x_1$$

can be written as

$$f = f_0(1 + f_0 f_1 x_0) + f_2(1 + f_2 f_3 x_0)x_1.$$

If f_0, f_1, f_2, $f_3 = \pm 1$, then $f_0 f_1$, $f_2 f_0 = \pm 1$.

5. Reformulation of Classical PONS

We reformulate the classical PONS construction procedure as described in Section 2.2 using group algebra operations, and we distinguish these orthonormal bases within the group algebra framework. For the purpose of this work we will modify P_{2^N}, the $2^N \times 2^N$ PONS matrix, by row permutation and row multiplication by -1.

Specifically we explore certain relationships between PONS matrices and character basis matrices. In particular, we show that a PONS matrix is completely determined by its 0-th row and the equivalent size character basis matrix. For a classical PONS matrix, the 0-th row can be constructed arithmetically and provides an example of a splitting sequence. The concept of a splitting sequence will be developed in a group algebra framework in the next section.

By the original PONS construction as given in Section 2.2 the 4×4 PONS matrix is

$$\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

Interchanging the 1st and 2nd row we have the matrix

$$P_4 = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

The component-wise product of any two rows of P_4 is a row of the character basis matrix H_4. In fact

$$P_4 = H_4 D_4,$$

where D_4 is the diagonal matrix formed by the 0-th row of P_4.

In general, by row permutation the classical $2^N \times 2^N$ PONS matrix can be transformed into the matrix

$$P_{2^N} = H_{2^N} D_{2^N},$$

where D_{2^N} is the diagonal matrix formed by the 0-th row of the classical PONS matrix.

The 0-th row of the original 4×4 PONS matrix can be defined arithmetically. From the binary representation of the integers $0 \leq n < 4$

$$0\,0, \quad 0\,1, \quad 1\,0, \quad 1\,1$$

we see that -1 is placed in the position having two 1's. Once D_{2^N} is constructed independently of the original construction, we can define the $2^N \times 2^N$ PONS matrix as

$$P_{2^N} = H_{2^N} D_{2^N}.$$

In the following sections we will place this result in the group algebra setting.

Several other definitions are possible. For example

$$D_{2^N} H_{2^N} D_{2^N}$$

can be viewed as a *symmetrical form* of the $2^N \times 2^N$ PONS matrix.

6. Group Algebra of Classical PONS

For an integer $N > 0$, we will use group algebra operations to define a PONS sequence of size 2^N. The first 2^n, $n \leq N$, terms of this sequence are the same as the elements in the 0-th row of the classical $2^n \times 2^n$ PONS matrix. PONS sequences will be identified with elements in the group algebra having special properties. Below we will extend these results to give a group algebra characterization of general binary splitting sequences.

Denote the elements of the canonical basis of $A_2(x_0, \ldots, x_{n-1})$ by v_0, v_1, ..., v_{2^n-1}. For $\mathbf{a} \in \mathbf{C}^{2^n}$

$$\mathbf{a} = (a_0, a_1, \ldots, a_{2^n-1})$$

identify $\mathbf{a}$ with the element a in $A_2(x_0, \ldots, x_{n-1})$

$$a = \sum_{r=0}^{2^n-1} a_r v_r.$$

If $n = 4$,

$$a = a_0\, 1 + a_1 x_0 + a_2 x_1 + a_3 x_0 x_1.$$

Set

$$\alpha_2 = 1 + x_0, \qquad \alpha_2^* = 1 - x_0$$

and

$$\alpha_4 = \alpha_2 + \alpha_2^* x_1, \qquad \alpha_4^* = \alpha_2 - \alpha_2^* x_1.$$

α_4 corresponds to the sequence

$$1 \;\; 1 \;\; 1 \;\; -1$$

which is the 0-th row of P_4.

Set

$$\alpha_{2^n} = \alpha_{2^{n-1}} + \alpha^*_{2^{n-1}} x_{n-1}$$

and

$$\alpha^*_{2^n} = \alpha_{2^{n-1}} - \alpha^*_{2^{n-1}} x_{n-1}.$$

The sequence corresponding to α_{2^n} is the 0-th row of P_{2^n}.

We will study the group algebra properties of the elements α_{2^n} and $\alpha^*_{2^n}$. The key to understanding the reason for expansions over the translate-character basis is contained in the character product formula

$$\alpha_2^2 = 2(1 + x_0), \quad (\alpha_2^*)^2 = 2(1 - x_0) \tag{11}$$

$$\alpha_2 \alpha_2^* = 0. \tag{12}$$

Implications of these formulas will be seen throughout this work.

Since

$$\alpha_4^2 = \alpha_2^2 + 2\alpha_2 \alpha_2^* x_1 + (\alpha_2^*)^2,$$

we have by (9) and (12)

$$\alpha_4^2 = 2(1 + x_0) + 2(1 - x_0) = 4. \tag{13}$$

In the same way

$$(\alpha_4^*)^2 = 4. \tag{14}$$

Since

$$\alpha_4 \alpha_4^* = \alpha_2^2 - (\alpha_2^*)^2,$$

by (9)

$$\alpha_4 \alpha_4^* = 2(1 + x_0) - 2(1 - x_0) = 4x_0. \tag{15}$$

We can write the important factorization

$$\alpha_4^* = \alpha_4 x_0. \tag{16}$$

By (16)

$$\alpha_8 = \alpha_4 + \alpha_4^* x_2 = \alpha_4(1 + x_0 x_2) \tag{17}$$

and

$$\alpha_8^* = \alpha_4(1 - x_0 x_2). \tag{18}$$

Since

$$(1 + x_0 x_2)^2 = 2(1 + x_0 x_2), \quad (1 - x_0 x_2)^2 = 2(1 - x_0 x_2),$$

and

$$(1 + x_0 x_2)(1 - x_0 x_2) = 0,$$

we have

$$\alpha_8^2 = 8(1 + x_0x_2), \quad (\alpha_8^*)^2 = 8(1 - x_0x_2),$$

and

$$\alpha_8\alpha_8^* = 0.$$

α_4 and α_8 have very different group algebra properties reflecting the expansion of α_4

$$\alpha_4 = 1 + x_0 + (1 - x_0)x_1$$

in terms of the *conjugate* characters $1 + x_0$ and $1 - x_0$ and the expansion of α_8

$$\alpha_8 = \alpha_4(1 + x_0x_2)$$

in which the character $1 + x_0x_2$ is a factor. This result is general for α_{2^n} depending on whether n is even or odd.

Arguing as above

$$\alpha_{16} = \alpha_8 + \alpha_8^* x_3 = \alpha_4 \left[(1 + x_0x_2) + (1 - x_0x_2)x_3\right],$$

$$\alpha_{16}^* = \alpha_8 - \alpha_8^* x_3 = \alpha_4 \left[(1 + x_0x_2) - (1 - x_0x_2)x_3\right]$$

from which we have

$$\alpha_{16}^2 = (\alpha_{16}^*)^2 = 16,$$

$$\alpha_{16}\alpha_{16}^* = 16x_0x_2,$$

$$\alpha_{16}^* = \alpha_{16}x_0x_2.$$

The same arguments show

$$\alpha_{32} = \alpha_{16} + \alpha_{16}^* x_4 = \alpha_{16}(1 + x_0x_2x_4)$$

$$\alpha_{32}^* = \alpha_{16}(1 - x_0x_2x_4).$$

In general if n is odd

$$\alpha_{2^n} = \alpha_{2^{n-1}}(1 + x_0x_2 \cdots x_{n-1}),$$

$$\alpha_{2^n}^* = \alpha_{2^{n-1}}(1 - x_0x_2 \cdots x_{n-1})$$

and

$$\alpha_{2^n}^2 = 2^n(1 + x_0x_2 \cdots x_{n-1}), \quad (\alpha_{2^n}^*)^2 = 2^n(1 - x_0x_2 \cdots x_{n-1})$$

$$\alpha_{2^n}\alpha_{2^n}^* = 0.$$

If n is even

$$\alpha_{2^n} = \alpha_{2^{n-2}} \left[(1 + x_0x_2 \cdots x_{n-2}) + (1 - x_0x_2 \cdots x_{n-2})x_{n-1}\right],$$

$$\alpha^*_{2^n} = \alpha_{2^{n-2}} \left[(1 + x_0 x_2 \cdots x_{n-2}) - (1 - x_0 x_2 \cdots x_{n-2}) x_{n-1} \right]$$

and

$$\alpha^2_{2^n} = (\alpha^*_{2^n})^2 = 2^n,$$

$$\alpha_{2^n} \alpha^*_{2^n} = 2^n x_0 x_2 \cdots x_{n-2}$$

$$\alpha^*_{2^n} = \alpha_{2^n} x_0 x_2 \cdots x_{n-2}.$$

An important implication of these formulas is that if n is odd, α_{2^n} is not invertible in the group algebra while if n is even, α_{2^n} is invertible with inverse $2^{-n}\alpha_{2^n}$.

7. Group Algebra Convolution

In this section we relate *convolution* in $A_2(x_0, \ldots, x_{N-1})$ by the PONS element α_{2^N} with the PONS matrix P_{2^N}.

Consider

$$\alpha \in A_2(x_0, \ldots, x_{N-1}).$$

The mapping $\mathcal{C}_{2^N}(\alpha) : A_2(x_0, \ldots, x_{N-1}) \longrightarrow A_2(x_0, \ldots, x_{N-1})$ defined by

$$\mathcal{C}_{2^N}(\alpha)\beta = \alpha\beta, \quad \beta \in A_2(x_0, \ldots, x_{N-1})$$

is a linear mapping of $A_2(x_0, \ldots, x_{N-1})$ called *convolution* by α. The matrix of $\mathcal{C}_{2^N}(\alpha)$ relative to the canonical basis is

$$\mathcal{C}_{2^N}(\alpha) = \left[\alpha(y^{-1}x)\right]_{x,y \in C_2(x_0,\ldots,x_{N-1})}.$$

For

$$\alpha_4 = 1 + x_0 + x_1 - x_0 x_1$$

the matrix $\mathcal{C}_4(\alpha_4)$ can be formed from the products

$$\begin{aligned} x_0\alpha_4 &= 1 + x_0 - x_1 + x_0 x_1 \\ x_1\alpha_4 &= 1 - x_0 + x_1 + x_0 x_1 \\ x_0 x_1 \alpha_4 &= -1 + x_0 + x_1 + x_0 x_1. \end{aligned}$$

$$\mathcal{C}_4(\alpha_4) = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$

Note that, as described in Section 2.5, the above is the 4×4 *s*ymmetric PONS matrix.

We have defined the 4×4 PONS matrix as

$$P_4 = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

Convolution by α_4 and P_4 are related by

$$\mathcal{C}_4(\alpha_4) = D_4 P(4,2) P_4, \tag{19}$$

where D_4 is the diagonal matrix formed by the 0-th row of P_4 and $P(4,2)$ is the 4×4 stride by 2 permutation matrix

$$P(4,2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since $P_4 = H_4 D_4$,

$$\mathcal{C}_4(\alpha_4) = D_4 P(4,2) H_4 D_4.$$

In group algebra terminology, $P(4,2)$ is the matrix relative to the canonical basis of the automorphism of $A_2(x_0, x_1)$ defined by the group automorphism of $C_2(x_0, x_1)$

$$x_0 \longrightarrow x_1, \quad x_1 \longrightarrow x_0.$$

By (19), up to row permutation and multiplication by -1, convolution by the classical PONS element α_4 in $A_2(x_0, x_1)$ coincides with the action of the 4×4 PONS matrix P_4. This will be the case whenever N is even and 2^N is the length of the classical PONS element. The length 16 case will be considered below.

For N odd, since

$$\alpha_8^2 = 8(1 + x_0 x_2)$$

and α_8 is not an invertible element in $A_2(x_0, x_1, x_2)$, convolution by α_8 in $A_2(x_0, x_1, x_2)$ cannot coincide with P_8 even after row permutation and multiplication by -1.

Set

$$J_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad J_{2^N} = I_N \otimes J_2.$$

Since

$$\alpha_8 = \alpha_4(1 + x_0 x_2)$$

and

$$\mathcal{C}_8(1 + x_0x_2) = \begin{bmatrix} I_4 & J_4 \\ J_4 & I_4 \end{bmatrix},$$

we have

$$\mathcal{C}_8(\alpha_8) = \begin{bmatrix} I_4 & J_4 \\ J_4 & I_4 \end{bmatrix} (I_2 \otimes \mathcal{C}_4(\alpha_4)).$$

By (19)

$$\mathcal{C}_8(\alpha_8) = \begin{bmatrix} D_4 & J_4D_4 \\ J_4D_4 & D_4 \end{bmatrix} (I_2 \otimes P(4,2)) (I_2 \otimes P_4). \tag{20}$$

$$P_8 = H_8D_8,$$

where

$$H_8 = (H_2 \otimes I_4)(I_2 \otimes H_4)$$

and

$$D_8 = (D_4 \otimes I_2)(I_2 \otimes D_4).$$

By (19)

$$P_8 = (H_2 \otimes I_4) \left((I_2 \otimes H_4)(D_4 \otimes I_2)(I_2 \otimes H_4^{-1})\right) (I_2 \otimes P_4).$$

Direct computation shows

$$(I_2 \otimes H_4)(D_4 \otimes I_2)(I_2 \otimes H_4^{-1}) = (I_2 \otimes P(4,2))(I_4 \oplus J_4)(I_2 \otimes P(4,2)),$$

where $\oplus$ is the matrix direct sum.

These results show that

$$\mathcal{C}_8(\alpha_8)P_8^{-1} = \begin{bmatrix} D_4 & J_4D_4 \\ J_4D_4 & D_4 \end{bmatrix} (I_4 \oplus J_4)(H_2^{-1} \otimes I_4)(I_2 \otimes P(4,2)).$$

Since

$$J_4D_4J_4 = D_4^* = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix},$$

we have the main result relating $\mathcal{C}_8(\alpha_8)$ and P_8

$$\mathcal{C}_8(\alpha_8) = \frac{1}{2} \begin{bmatrix} D_4 + D_4^* & D_4 - D_4^* \\ (D_4 + D_4^*)J_4 & (D_4^* - D_4)J_4 \end{bmatrix} (I_2 \otimes P(4,2))P_8.$$

A direct computation shows

$$\mathcal{C}_8(\alpha_8) = D_8Q_8(I_2 \otimes P(4,2))P_8,$$

where $D_8 = D_4 \oplus D_4^*$ and

$$Q_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Q_8 is a singular matrix. In fact if

$$\mathbf{w} = P_8\mathbf{v},$$

then $\mathcal{C}_8(\alpha_8)\mathbf{v}$ computes only the components

$$w_0,\ w_2,\ w_5,\ w_7.$$

The computation of the remaining components is given by $\mathcal{C}_8(\alpha_8^*)\mathbf{v}$.

Since

$$\alpha_{16} = \alpha_4\left[(1 + x_0x_2) + (1 - x_0x_2)x_3\right],$$

convolution by α_{16} in $A_2(x_0, x_1, x_2, x_3)$can be written as

$$\mathcal{C}_{16}(\alpha_{16}) = \begin{bmatrix} \mathcal{C}_8(1 + x_0x_2) & \mathcal{C}_8(1 - x_0x_2) \\ \mathcal{C}_8(1 - x_0x_2) & \mathcal{C}_8(1 + x_0x_2) \end{bmatrix} \mathcal{C}_{16}(\alpha_4).$$

Arguing as before

$$\mathcal{C}_{16}(\alpha_{16}) = \begin{bmatrix} X_8 & X_8^* \\ X_8^* & X_8 \end{bmatrix} (I_4 \otimes D_4P(4,2))(I_4 \otimes P_4),$$

where

$$X_8 = \begin{bmatrix} I_4 & J_4 \\ J_4 & I_4 \end{bmatrix}, \quad X_8^* = \begin{bmatrix} I_4 & -J_4 \\ -J_4 & I_4 \end{bmatrix}.$$

$$P_{16} = H_{16}D_{16},$$

where

$$H_{16} = (H_4 \otimes I_4)(I_4 \otimes H_4)$$

and

$$D_{16} = (D_4 \otimes I_4)(I_2 \otimes D_4 \otimes I_2)(I_4 \otimes D_4).$$

We can now write

$$P_{16} = (P_4 \otimes I_4)(I_4 \otimes H_4)(I_2 \otimes D_4 \otimes I_2)(I_4 \otimes H_4^{-1})(I_4 \otimes P_4).$$

By direct computation

$$(I_4 \otimes H_4)(I_2 \otimes D_4 \otimes I_2)(I_4 \otimes H_4^{-1})$$

$$= (I_4 \otimes P(4,2))(I_4 \oplus J_4 \oplus I_4 \oplus J_4)(I_4 \otimes P(4,2)).$$

Combining the preceding formulas

$$\mathcal{C}_{16}(\alpha_{16})P_{16}^{-1}$$

$$= \begin{bmatrix} X_8 & X_8^* \\ X_8^* & X_8 \end{bmatrix} (I_4 \otimes D_4)(I_4 \oplus J_4 \oplus I_4 \oplus J_4)(P_4^{-1} \otimes I_4)(I_4 \otimes P(4,2)).$$

Since

$$P_4^{-1} \otimes I_4 = \begin{bmatrix} I_4 & I_4 & I_4 & I_4 \\ I_4 & -I_4 & I_4 & -I_4 \\ I_4 & I_4 & -I_4 & -I_4 \\ -I_4 & I_4 & I_4 & -I_4 \end{bmatrix}$$

and

$$J_4 D_4 J_4 = D_4^*,$$

we can derive the main result relating $\mathcal{C}_{16}(\alpha_{16})$ and P_{16}.

$$\mathcal{C}_{16}(\alpha_{16}) = Y_{16}(I_4 \otimes P(4,2))P_{16},$$

where

$$Y_{16} = \frac{1}{2} \begin{bmatrix} D_4 + D_4^* & D_4 - D_4^* & 0 & 0 \\ 0 & 0 & (D_4 + D_4^*)J_4 & (D_4^* - D_4)J_4 \\ D_4 - D_4^* & D_4 + D_4^* & 0 & 0 \\ 0 & 0 & (D_4 - D_4^*)J_4 & -(D_4 + D_4^*)J_4 \end{bmatrix}.$$

Direct computation shows that

$$Y_{16} = D_{16}Q_{16},$$

where Q_{16} is the permutation matrix

$$Q_{16} = \left[\begin{array}{cccc|cccc|cccc|cccc}
1&0&0&0&0&0&0&0&\multicolumn{8}{c}{\multirow{4}{*}{0}}&\multicolumn{4}{c}{\multirow{4}{*}{0}}\\
0&1&0&0&0&0&0&0&\multicolumn{8}{c}{}&\multicolumn{4}{c}{}\\
0&0&0&0&0&0&1&0&\multicolumn{8}{c}{}&\multicolumn{4}{c}{}\\
0&0&0&0&0&0&0&1&\multicolumn{8}{c}{}&\multicolumn{4}{c}{}\\
\hline
\multicolumn{8}{c|}{\multirow{4}{*}{0}}&\multicolumn{8}{c|}{\multirow{4}{*}{0}}&0&1&0&0&0&0&0&0\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&1&0&0&0&0&0&0&0\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&0&0&0&0&0&0&0&1\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&0&0&0&0&0&0&1&0\\
\hline
0&0&0&0&1&0&0&0&\multicolumn{8}{c|}{\multirow{4}{*}{0}}&\multicolumn{8}{c}{\multirow{4}{*}{0}}\\
0&0&0&0&0&1&0&0&\multicolumn{8}{c|}{}&\multicolumn{8}{c}{}\\
0&0&1&0&0&0&0&0&\multicolumn{8}{c|}{}&\multicolumn{8}{c}{}\\
0&0&0&1&0&0&0&0&\multicolumn{8}{c|}{}&\multicolumn{8}{c}{}\\
\hline
\multicolumn{8}{c|}{\multirow{4}{*}{0}}&\multicolumn{8}{c|}{\multirow{4}{*}{0}}&0&0&0&0&0&1&0&0\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&0&0&0&0&1&0&0&0\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&0&0&0&1&0&0&0&0\\
\multicolumn{8}{c|}{}&\multicolumn{8}{c|}{}&0&0&1&0&0&0&0&0
\end{array}\right].$$

From these formulas

$$\mathcal{C}_{16}(\alpha_{16}) = D_{16}Q_{16}(I_4 \otimes P(4,2))P_{16}.$$

The permutation matrix Q_{16} corresponds to the automorphism of the algebra $A_2(x_0, x_1, x_2, x_3)$ induced by the group automorphism defined by

$$x_0 \longrightarrow x_0$$
$$x_1 \longrightarrow x_1x_3$$
$$x_2 \longrightarrow x_3$$
$$x_3 \longrightarrow x_0x_2.$$

Combined with the automorphism defining $(I_4 \otimes P(4,2))$

$$x_0 \longrightarrow x_1$$
$$x_1 \longrightarrow x_0$$
$$x_2 \longrightarrow x_2$$
$$x_3 \longrightarrow x_3$$

the permutation matrix $Q_{16}(I_4 \otimes P(4,2))$ corresponds to the automorphism of the algebra defined by

$$x_0 \longrightarrow x_1x_3$$
$$x_1 \longrightarrow x_0$$
$$x_2 \longrightarrow x_3$$
$$x_3 \longrightarrow x_0x_2.$$

8. Splitting Sequences

The concept of a splitting sequence was discussed in Sections 2.3 and 2.4. In this section we will describe the binary splitting sequences using group algebra operations. We begin by establishing notation.

The characters of $C_2(x_0)$ are

$$1 + x_0, \quad 1 - x_0. \tag{21}$$

The expressions

$$\pm(1 + x_0), \quad \pm(1 - x_0)$$

will be denoted by λ with or without subscripts. Typically

$$\lambda = a(1 + \epsilon x_0), \tag{22}$$

where $a = \pm 1$ and $\epsilon = \pm 1$. a is called the *coefficient* of λ and ϵ is called the *sign* of λ. In general

$$\lambda_1 \lambda_2 = 0$$

if and only if $sign(\lambda_1) = -sign(\lambda_2)$. λ is called a *directed character* of $C_2(x_0)$.

Identify sequences of length 2^N with linear combinations over the canonical basis of $A_2(x_0, \ldots, x_{N-1})$. A sequence of length 4

$$b_0, b_1, b_2, b_3$$

is identified with the element

$$\alpha = b_0 + b_1 x_0 + b_2 x_1 + b_3 x_0 x_1$$

in $A_2(x_0, x_1)$.

Only sequences of ± 1 will be considered. Every sequence of length 2^N of ± 1 uniquely determines a sequence of directed characters

$$\lambda_0, \lambda_1, \ldots, \lambda_{N-1}$$

and consequently a sequence of signs, the n-th sign equal to the sign of λ_n, and a sequence of coefficients, the n-th coefficient equal to the coefficient of λ_n. If

$$\alpha = -(1 + x_0) + (1 - x_0)x_1,$$

then the corresponding sequence of directed characters is

$$-(1 + x_0), \quad 1 - x_0,$$

the corresponding sequence of signs is

$$+\,-$$

and the corresponding sequence of coefficients is

$$-\,+\,.$$

The splitting condition on sequences of ± 1 places conditions on the sign patterns of splitting sequences. The following tables describe the sign patterns for $N = 2$, 3 and 4.

Table 1. Sign patterns for splitting sequences

$N=2$	$-+ \quad +-$
$N=3$	$-+-+ \quad -++- \quad +-+- \quad +--+$
$N=4$	$-+-+-+-+ \quad -+-++-+- \quad -++--++-$
	$+-+-+-+- \quad +-+--+-+ \quad +--+-+--+$

Consider a length 4 splitting sequence α_4 and write

$$\alpha_4 = \lambda_0 + \lambda_1 x_1,$$

where λ_0, λ_1 are directed characters. The length 4 splitting condition implies

$$\lambda_0^2 + \lambda_1^2 = 1.$$

By the character product formula

$$\lambda_0 \lambda_1 = 0. \tag{23}$$

Condition (23) is also sufficient for splitting, proving the following result.

THEOREM 20 *α_4 is a splitting sequence of length 4 if and only if α_4 has the form*

$$\alpha_4 = \pm((1 + x_0) \pm (1 - x_0)x_1)$$

or

$$\alpha_4 = \pm((1 - x_0) \pm (1 + x_0)x_1).$$

The splitting sequences of length 4 having sign pattern

$$+\,-$$

are given by

$$\alpha_4 = \pm((1 + x_0) \pm (1 - x_0)x_1)$$

while those having sign pattern

$$- +$$

are given by

$$\alpha_4 = \pm((1 - x_0) \pm (1 + x_0)x_1).$$

COROLLARY 21 *If α_4 is a splitting sequence of length 4, then $\alpha_4^2 = 4$.*

The condition $\alpha_4^2 = 4$ is also sufficient for a sequence of ± 1 of length 4 to be a splitting sequence.

Consider a splitting sequence α_8 of length 8 given by the directed characters

$$\lambda_0,\ \lambda_1,\ \lambda_2,\ \lambda_3. \tag{24}$$

α_8 can be written

$$\alpha_8 = \alpha_4 + \alpha_4^* x_2,$$

where

$$\alpha_4 = \lambda_0 + \lambda_1 x_1, \quad \alpha_4^* = \lambda_2 + \lambda_3 x_1,$$

are splitting sequences of length 4. The length 4 splitting condition implies

$$\alpha_4^2 + (\alpha_4^*)^2 = 8.$$

There are 4 cases to consider. Suppose α_4 and α_4^* have sign pattern

$$- +\,.$$

The length 8 splitting condition implies that the coefficients of the directed characters in (24) satisfy

$$-a_0 a_1 - a_2 a_3 = 0.$$

Since

$$\alpha_4 \alpha_4^* = 2a_0 a_2 (1 - x_0) + 2a_1 a_3 (1 + x_0),$$

we have

$$\alpha_4 \alpha_4^* = \pm 4 x_0$$

and

$$\alpha_8 = \alpha_4 (1 \pm x_0 x_2). \tag{25}$$

The same argument shows that if α_4 and α_4^* have the sign pattern

$$+ -,$$

then α_8 has the same form.

Suppose α_4 has the sign pattern

$$-+$$

and α_4^* has the sign pattern

$$+\ -\ .$$

The splitting condition implies

$$-a_0a_1 + a_2a_3 = 0.$$

Since

$$\alpha_4\alpha_4^* = (2a_0a_3(1 - x_0) + 2a_1a_2(1 + x_0))x_1,$$

we have

$$\alpha_4\alpha_4^* = \pm 4x_1$$

and

$$\alpha_8 = \alpha_4(1 \pm x_1x_2). \tag{26}$$

The same result holds if we reverse the patterns of α_4 and α_4^*.

Since (25) and (26) define splitting sequences whenever α_4 is a splitting sequence of length 4, we have the following result.

THEOREM 22 *α_8 is a splitting sequence of length 8 if and only if α_8 has one of the two forms*

$$\alpha_8 = \alpha_4(1 \pm x_0x_2)$$

or

$$\alpha_8 = \alpha_4(1 \pm x_1x_2),$$

where α_4 is an arbitrary splitting sequence of length 4.

As the proof shows, the splitting sequences of length 8 having sign pattern

$$-\ +\ -+, \quad +\ -\ +\ -$$

are given by

$$\alpha_4(1 \pm x_0x_2)$$

while those having sign patterns

$$-\ +\ +-, \quad +\ -\ -\ +$$

are given by

$$\alpha_4(1 \pm x_1x_2).$$

COROLLARY 23 *If α_8 is a splitting sequence of length 8, then*

$$\alpha_8^2 = 8(1 \pm x_0x_2)$$

or

$$\alpha_8^2 = 8(1 \pm x_1 x_3).$$

Consider a splitting sequence α_{16} of length 16 and write

$$\alpha_{16} = \alpha_8 + \alpha_8^* x_3,$$

where α_8 and α_8^* are length 8 splitting sequences. The splitting condition on α_{16} implies

$$\alpha_8^2 + (\alpha_8^*)^2 = 16.$$

By Theorem 22

$$\alpha_8 \alpha_8^* = 0. \tag{27}$$

Suppose α_8 has sign pattern

$$+ \; - \; + \; - \; .$$

By Theorem 22 α_8 has the form

$$\alpha_8 = \alpha_4(1 \pm x_0 x_2),$$

where α_4 is a length 4 splitting sequence having sign pattern

$$+ \; - \; .$$

Consider the case

$$\alpha_8 = \alpha_4(1 + x_0 x_2).$$

If α_4 is given by the directed characters

$$\lambda_0 \, \lambda_1,$$

then α_8 is given by the directed characters

$$\lambda_0 \, \lambda_1 \, \lambda_0 \; - \lambda_1. \tag{28}$$

By (27)

$$\alpha_8^* = \alpha_4^*(1 - x_0 x_2).$$

There are two cases. Suppose α_4^* has sign pattern

$$+ -$$

and is given by the directed characters

$$\lambda_2 \, \lambda_3.$$

α_8^* is given by the directed characters

$$\lambda_2\,\lambda_3\ -\lambda_2\,\lambda_3. \tag{29}$$

The splitting condition on α_{16} applied to (28) and (29) implies

$$-a_0a_1 + a_2a_3 = 0.$$

Since

$$\alpha_4\alpha_4^* = 2a_0a_2(1+x_0) + 2a_1a_3(1-x_0),$$

we have

$$\alpha_4\alpha_4^* = \pm 4$$

and

$$\alpha_{16} = \alpha_4[(1+x_0x_2) \pm (1-x_0x_2)x_3].$$

Suppose α_4^* has sign pattern

$$-\ +\,.$$

α_8^* is given by the directed characters

$$\lambda_2\,\lambda_3\,\lambda_2\ -\lambda_3 \tag{30}$$

and has sign pattern

$$-\ +\ -\ +\,.$$

The splitting condition on α_{16} applied to (28) and (30) implies

$$-a_0a_1 + a_2a_3 = 0.$$

Since

$$\alpha_4\alpha_4^* = 2a_0a_3(1+x_0)x_1 + 2a_1a_2(1-x_0)x_1,$$

we have

$$\alpha_4\alpha_4^* = \pm 4x_1$$

and

$$\alpha_{16} = \alpha_4[(1+x_0x_2) \pm (1-x_0x_2)x_1x_3].$$

Similar arguments prove the following result.

THEOREM 24 *α_{16} is a splitting sequence of length 16 if and only if α_{16} has one of the following forms.*

$$\begin{array}{lll}
\text{Type 1.} & & \alpha_4[(1+x_0x_2)\pm(1-x_0x_2)x_3] \\
 & & \alpha_4[(1-x_0x_2)\pm(1+x_0x_2)x_3] \\
\text{Type 2.} & & \alpha_4[(1+x_0x_2)\pm(1-x_0x_2)x_1x_3] \\
 & & \alpha_4[(1-x_0x_2)\pm(1+x_0x_2)x_1x_3] \\
\text{Type 3.} & & \alpha_4[(1+x_1x_2)\pm(1-x_1x_2)x_3] \\
 & & \alpha_4[(1-x_1x_2)\pm(1+x_1x_2)x_3] \\
 & & \alpha_4[(1+x_1x_2)+(1-x_1x_2)x_0x_3] \\
 & & \alpha_4[(1-x_1x_2)+(1+x_1x_2)x_0x_3],
\end{array}$$

where α_4 is a length 4 splitting sequence.

The length 16 splitting sequences in Theorem 24 have been organized according to their sign patterns.

$$\begin{array}{ll}
\text{Type 1} & - + - + - + - + \\
 & + - + - + - + - \\
\text{Type 2} & - + - + + - + - \\
 & + - + - - + - + \\
\text{Type 3} & - + + - - + + - \\
 & + - - + + - - + .
\end{array}$$

COROLLARY 25 *If α_{16} is a length 16 splitting sequence, then $\alpha_{16}^2 = 16$.*

The condition

$$\alpha_{16}^2 = 16$$

is not sufficient for α_{16} to be a splitting sequence.

A similar argument proves the following result.

THEOREM 26 *The splitting sequences of length 32 have one of the following forms.*

Type 1 *$\alpha_{16}(1 \pm x_0x_2x_4)$, where α_{16} is Type 1.*

Type 2 *$\alpha_{16}(1 \pm x_1x_3x_4)$, where α_{16} is Type 1.*

Type 3 *$\alpha_{16}(1 \pm x_0x_2x_4)$, $\alpha_{16}(1 \pm x_1x_3x_4)$, where α_{16} is Type 2.*

Type 4 *$\alpha_{16}(1 \pm x_1x_2x_4)$, $\alpha_{16}(1 \pm x_0x_3x_4)$, where α_{16} is Type 3.*

The classification of length 32 splitting sequences into types corresponds to the sign patterns of the type.

Type 1	− + − + − + − + − + − + − + − +
	+ − + − + − + − + − + − + − + −
Type 2	− + − + − + − + + − + − + − + −
	+ − + − + − + − − + − + − + − +
Type 3	− + − + + − + − − + − + + − + −
	+ − + − − + − + + − + − − + − +
Type 4	+ − − + + − − + + − − + + − − +
	− + + − − + + − − + + − − + + −

9. Historical Appendix on PONS

What we have been calling PONS was actually first introduced by G. R. Welti [28], and subsequently rediscovered on several occasions by independent authors. However closely related (and most important) work had already been done, independently by Golay [13, 14] in 1949–1951 and by H. S. Shapiro [25] in 1951.

A remarkable feature of these various rediscoveries is that all of them emerged in *entirely different* contexts, radars, *etc.* In this short appendix, we briefly comment on some of these works, leaving out many aspects of this history which would have required a detailed study and considerable space to present it. For a much more complete study of this history, see [24].

In his 1949–1951 papers [13] and [14], M. J. E. Golay introduced the general concept of "complementary pairs" of finite sequences all of whose entries are ± 1. This was motivated by a highly non-trivial application to *infra-red spectrometry*. Neither Golay nor any of his fellow engineers ever used the language and properties of generating polynomials, until the 1980's.

In 1951, H. S. Shapiro [25] introduced what became known, after 1963, as the "Rudin-Shapiro" polynomial pairs. Shapiro's work was entirely in pure mathematics (specifically, complex and Fourier analysis). The use of Rudin's name in "Rudin-Shapiro" polynomials is utterly unjustified, and seems due to an unfortunate "original mistake" in the 1963 book [17] by J.-P. Kahane and R. Salem.

In 1959 G. R. Welti wrote the paper [28] which appeared in print in 1960. In spite of its title, of particular interest for our present purpose is the *first half* of the paper (on binary sequences), in which Welti intro-

duced *exactly* what J. S. Byrnes and others called "PONS matrices" in the 1990's. (However, the approach and motivation of Byrnes was completely different from those of Welti). Welti was unaware of the works of Golay and Shapiro. He obtained the first row of Welti's matrix (*i.e.*, the Shapiro sequence) by a method entirely different from that of Shapiro, and he obtained the remaining rows as Hadamard products of the first row with the rows of the Walsh matrix.

Also in 1959, W. Rudin (who had been a member of Shapiro's MIT thesis committee!) wrote a paper [23] in which he claimed to have "rediscovered" the Shapiro polynomial pairs. This was *not* a rediscovery. As we said earlier, full details of this matter will be given in [24].

In 1961, Golay [15], who in turn was unaware of the works of Shapiro and Welti (and even that of Rudin), obtained all the Welti rows (*i.e.*, the PONS rows), by a method quite close to that of Shapiro.

In 1981, Mendes France and Tenenbaum [12] (who had never seen Shapiro's 1951 work [25] but had heard of it only via Rudin's "rediscovery" [23], and also were unaware of the works of Golay and Welti), rediscovered all the Welti rows and named them "paper-folding sequences". This was a work in pure mathematics, related to fractal dimensions of plane curves.

In the early 1990's, J. S. Byrnes (who was aware of the works of Shapiro [25] and Rudin [23] but not of those of Golay, Welti, and Mendes France & Tenenbaum) rediscovered [6] the Welti matrices (which he later on named "PONS matrices"), in yet another context of pure mathematics: His motivation was to use them as a tool to prove an "uncertainty principle conjecture" of H. S. Shapiro. However, unlike the previous instances of discovery/rediscovery of these objects in a *pure mathematics* context, PONS soon became a tool for radar signal processing as well.

These various discoveries and re-discoveries have given rise to an enormous amount of further research and new open problems, many of which are deep. The ongoing research on such subjects is very active. We hope to return to these matters elsewhere.

We finish this appendix with two remarks on *this paper*. The first remark is that we left out the subject of *correlation properties* of PONS sequences. The reason is that these correlation properties are sometimes very good and sometimes very bad (and proving how bad they can be is itself a difficult task). We will return to these correlation matters elsewhere. The second remark is that the heterogeneous aspect of this paper is due to the fact that it was written over several years by several authors with different views. (According to some historians, the Old Testament was written by various authors who were sometimes several centuries apart!)

References

[1] K.G. Beauchamp. *Applications of Walsh and Related Functions*. Academic Press, London, 1984.

[2] J. Brillhart and L. Carlitz. Note on the shapiro polynomials. *Proc. AMS*, 25:114–118, 1970.

[3] S.Z. Budisin. New complementary pairs of sequences. *Electronics Letters*, 26(13):881–883, 21 June 1990.

[4] S.Z. Budisin. Efficient pulse compressor for Golay complementary sequences. *Electronics Letters*, 27(3):219–220, 31 January 1991.

[5] S.Z. Budisin, B.M. Popović, and L.M. Indjin. Designing radar signals using complementary sequences. *Proc. IEE Conf. RADAR 87*, pages 593–597, Oct. 1987.

[6] J.S. Byrnes. Quadrature mirror filters, low crest factor arrays, functions achieving optimal uncertainty principle bounds, and complete orthonormal sequences — a unified approach. *Applied and Computational Harmonic Analysis*, 1:261–266, 1994.

[7] J.S. Byrnes. A low complexity energy spreading transform coder. In Y. Zeevi and R. Coifman, editors, *Signal and Image Representation in Combined Spaces*, Haifa, 1997.

[8] J.S. Byrnes, W. Moran, and B. Saffari. Smooth PONS. *The Journal of Fourier Analysis and Applications*, 6(6):663–674, 2000.

[9] J.S. Byrnes, M.A. Ramalho, G.K. Ostheimer, and I. Gertner. Discrete one dimensional signal processing method and apparatus using energy spreading coding. U.S. Patent number 5,913,186, 1999.

[10] J.S. Byrnes, B. Saffari, and H.S. Shapiro. Energy spreading and data compression using the Prometheus orthonormal set. In *Proc. 1996 IEEE Signal Processing Conf.*, Loen, Norway, 1996.

[11] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Information Theory*, 45(7):2397–2417, November 1999.

[12] M. Mendes France and G. Tenenbaum. Dimensions des courbes planes, papiers pliés et suites de Rudin-Shapiro. *Bull. Soc. Math. France*, 109:207–215, 1981.

[13] M.J.E. Golay. Multislit spectrometry. *J. Optical Society Am.*, 39:437, 1949.

[14] M.J.E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Optical Society Am.*, 41:468, 1951.

[15] M.J.E. Golay. Complementary series. *IEEE Trans. Information Theory*, 7:82–87, April 1961.

[16] John E. Gray and Soon H. Leong. On a subclass of Welti codes and Hadamard matrices. *IEEE Trans. Electromagnetic Compatibility*, 12(2):167–170, 1990.

[17] J.-P. Kahane and G. Tenenbaum. *Ensembles parfaits et séries trigonométriques*. Hermann, Paris, 1963.

[18] Hans Dieter Lüke. Sets of one and higher dimensional Welti codes and complementary codes. *IEEE Trans. Aerospace and Electronic Systems*, 21(2):170–178, March 1985.

[19] B.M. Popović. Power efficient multitone signals with flat amplitude spectrum. *IEEE Trans. Communications*, 39(7):1031–1033, July 1991.

[20] B.M. Popović. New RACH preambles with low autocorrelation sidelobes and reduced detector complexity. In *Proc. of the 4th CDMA International Conference, Vol. 2*, pages 157–161, September 1999.

[21] B.M. Popović. Spreading sequences for multicarrier CDMA systems. *IEEE Trans. Communications*, 47(6):918–926, June 1999.

[22] B.M. Popović, N. Suehiro, and P.Z. Fan. Orthogonal sets of quadriphase sequences with good correlation properties. *IEEE Trans. Information Theory*, 48(4):956–959, April 2002.

[23] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.

[24] B. Saffari. History of Shapiro polynomials and Golay complementary pairs. (In preparation).

[25] H.S. Shapiro. Extremal problems for polynomials and power series. Sc.M. thesis, Massachusetts Institute of Technology, 1951.

[26] R. J. Turyn. Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression and surface wave-encoding. *Journal of Combinatorial Theory*, 16:313–333, 1974.

[27] S. R. Weller, W. Moran, and J. S. Byrnes. On the use of the PONS sequences for peak-to-mean power control in OFDM. In *Proc. of the Workshop on Defense Applications in Signal Processing*, pages 203–209, LaSalle, Illinois, USA, August 1999.

[28] G. R. Welti. Quaternary codes for pulsed radar. *IRE Trans. Inf. Theory*, 6:400–408, 1960.

[29] Roland Wilson and John Richter. Generation and performance of quadraphase Welti codes for radar and synchronization of coherent and differentially coherent PSK. *IEEE Trans. Communications*, 27(9):1296–1301, September 1979.