The Energy Spreading PONS Transform and its Applications [1]

Jim Byrnes
Prometheus Inc.

Dedicated to the 80^{th} Anniversary of the Academy of Sciences of Armenia

1 Introduction

The author has two purposes in offering this Proceedings contribution. First is to share the development history and current status of *PONS*, the Prometheus Orthonormal Set, with the broader community of mathematicians. Second is to make that community aware of some of the many interesting (in the author's opinion) open PONS problems.

PONS is a suite of digital signal processing and data transmission algorithms whose genesis may be found in the Byrnes generalization [6] of the Shapiro Polynomials [37]. They are efficient, scalable to incorporate growth, robust to reduce the effects of transmission errors which inevitably occur, and secure to prevent unauthorized access and to ensure the privacy of communications.

It is straightforward to describe, in heuristic terms, what we mean by *energy spreading*. Namely, when a digital signal of any dimension is expanded in the PONS basis, each of the terms in the transform domain has approximately the same amount of energy. Various mathematical details may be found in publications including [6, 7, 11, 34]. Many published results may also be found at https://www.prometheus-us.com/PONS-papers/.

For a more mathematical point of view, consider that *energy* is represented by the L^2 norm. Thus, a reasonable way to think of energy spreading is to analyze the relative contributions to the L^2 norm of the transformed versions of a finite–energy signal coming from various sub–arcs of the unit circle. If energy is really *spread*, that contribution should only depend upon the length of the sub–arc, and not upon where in the unit circle it is located. Toward that end, in Section 4 we define and discuss the concepts of the *Fixed Arc Property* (FAP) and an *Energy Spreading Gauge* (ESG). FAP and ESG represent new research. The remainder of the paper is a review.

[1]PONS research over the years has been supported mainly by internal (IR&D) funds. In addition, Prometheus Inc. acknowledges the generous support received during this time from various US Department of Defense agencies, including the Air Force, Missile Defense Agency, DARPA and National Geospatial Intelligence Agency.

A further motivation for delving more deeply into energy spreading transforms is the large amount of recent work in the electrical engineering community on the application of PONS–type sequences to many areas, including wireless communications [14, 15, 23, 30, 31, 32], optical communications [27, 36], robust transmission of digital data [35], watermarking [13, 38], and radar [5, 17, 21, 26, 29, 40]. While these works have generated and continue to generate considerable interest in the applied community, we believe that the fundamental theory of energy–spreading transforms which underlies it all lacks a cohesive mathematical foundation. For example, most of the above–cited authors appear to be unaware of the ground–breaking work of H. S. Shapiro [37], who first constructed the *upper–flat* ± 1 polynomials, whose coefficient sets are *complementary sequences*, which form the mathematical backbone of many of their (and numerous other) contributions. Note that Shapiro's 1951 work (these *Shapiro Polynomials* were published eight years later by Rudin [33], who was a member of Shapiro's Masters Thesis Committee at MIT) predates that of Golay [20], which appears to be the generally accepted beginning of such ideas in the electrical engineering community, by 10 years. In fact the story begins even earlier than 1951, as Golay introduced the concept of complementary sequences in the context of multislit spectrometry in 1949 [18, 19].

An essentially identical situation has occurred in the study of certain Reed–Muller codes. Two basic facts known to Golay [20] and Shapiro [37], namely that:

- the value of the n^{th} term in the basic Shapiro sequence is $+1$ if the number of times that the block $\{1, 1\}$ occurs in the binary expansion of n is even and -1 if it is odd; and
- when the rows of the classic Walsh–Hadamard matrix are multiplied term–wise by the Shapiro sequence of the same length, the resulting Hadamard matrix consists entirely of pairs of ± 1 complementary sequences (hence, more specifically, is a PONS matrix, see Section 2);

have been restated by Davis and Jedwab [14, 15, 23, 30, 39] in coding theory language, thereby showing that PONS can be identified with a coset of the first–order Reed–Muller code $RM(1, m)$ inside the second–order code $RM(2, m)$ [1].

In addition to the engineering results on energy spreading transforms, a small sample of which is cited above, much mathematical work in harmonic analysis has flowed from the basic contributions of Golay and Shapiro [3, 4, 6, 8, 9, 10, 16, 24, 25, 28]. Thus, there is a long and rich history of work in this area in both the mathematics and engineering communities, with little interaction between them.

2 Mathematics of One–Dimensional PONS

We begin with a definition of the original symmetric PONS matrices. The original development of PONS is based on the Shapiro polynomials [37]. To prove a global uncertainty principle conjecture Byrnes expanded the Shapiro polynomials into a basis via the concatenation rule depicted below [6]. Working with the sequences formed by the polynomial coefficients, symmetric PONS matrices are obtained as follows. Starting with

$$P_1 := \begin{bmatrix} P_{1,1} \\ Q_{1,1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

construct the 2×2 matrix P_2 by combining the pair of rows of P_1 using the following four combination patterns:

$$P_2 := \begin{bmatrix} P_{2,1} \\ Q_{2,1} \\ P_{2,2} \\ Q_{2,2} \end{bmatrix} = \begin{bmatrix} P_{1,1} & Q_{1,1} \\ P_{1,1} & -Q_{1,1} \\ Q_{1,1} & P_{1,1} \\ -Q_{1,1} & P_{1,1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$

Generalizing to the $2^m \times 2^m$ case, combine each pair of rows in the same way to obtain

$$P_m := \begin{bmatrix} P_{m,1} \\ Q_{m,1} \\ P_{m,2} \\ Q_{m,2} \\ \vdots \\ P_{m,2^{m-1}-1} \\ Q_{m,2^{m-1}-1} \\ P_{m,2^{m-1}} \\ Q_{m,2^{m-1}} \end{bmatrix} = \begin{bmatrix} P_{m-1,1} & Q_{m-1,1} \\ P_{m-1,1} & -Q_{m-1,1} \\ Q_{m-1,1} & P_{m-1,1} \\ -Q_{m-1,1} & P_{m-1,1} \\ \vdots & \vdots \\ P_{m-1,2^{m-2}} & Q_{m-1,2^{m-2}} \\ P_{m-1,2^{m-2}} & -Q_{m-1,2^{m-2}} \\ Q_{m-1,2^{m-2}} & P_{m-1,2^{m-2}} \\ -Q_{m-1,2^{m-2}} & P_{m-1,2^{m-2}} \end{bmatrix}. \tag{2}$$

Properties of PONS Matrices

Here is a list of some of the important properties of these matrices:

Property 1. *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 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 1 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 2. *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,*

$$|A_{2r}(z)|^2 + |A_{2r+1}(z)|^2 = \text{ constant } (= 2L, \text{ in this case}) \tag{3}$$

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" [20].*

Property 3. *[Much related to Properties 1 and 2] Every row-polynomial* $A_r(z)$ *is QMF, that is,*

$$|A_r(z)|^2 + |A_r(-z)|^2 = \text{ constant } (= 2L \text{ in this case}) \tag{4}$$

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

Property 4 (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.*

Property 5 (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, which we call ERS (Equal Row Sums), is important but easy to check. 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 6 ("Bounded crest factor properties")**.** *In engineering terms the crest factor is the ratio of the peak to average power. Thus, mathematically in this discussion, the crest factor is the ratio of the sup norm to the* L^2 *norm of the polynomial on the unit circle. Briefly stated, not only does 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.

Property 7 ("Correlation properties")**.** *We devote the entire Section 2.1 to these all-important properties.*

2.1 Correlation results

Theorem 1. *Let* $(a_0, a_1, \dots a_{L-1})$ *be any row of any* $L \times L$ *PONS matrix (*$L = 2^m$*). Let*

$$c_j = \sum_{k=0}^{L-1-j} a_k a_{k+j} \quad (j = 1, 2, \dots L-1)$$

denote the j*-th out-of-phase aperiodic autocorrelation of that PONS row. Then we have the "maximal" estimate*

$$\max_{1 \leq j \leq L-1} |c_j| \leq K \cdot L^{0.73}$$

where K *is an absolute constant. (The exponent* 0.73... *arises from the computation of the spectral radius of some PONS-related matrix.)*

This is indeed a difficult result, and the exponent 0.73... can be proved to be optimal. The proof involves, in particular, heavy inequalities on norms of matrix products. Also the proof becomes somewhat less technical if, instead of the optimal exponent 0.73..., we only wish to obtain the (slightly less good) exponent 3/4.

Theorem 2. *Let* $(a_0, a_1, \dots a_{L-1})$ *be any row of any* $L \times L$ *PONS matrix (*$L = 2^m \geq 4$*). Let*

$$\gamma_j = \sum_{k \,(\text{modulo } L)} a_k a_{k+j} \quad (j = 1, 2, \dots L-1)$$

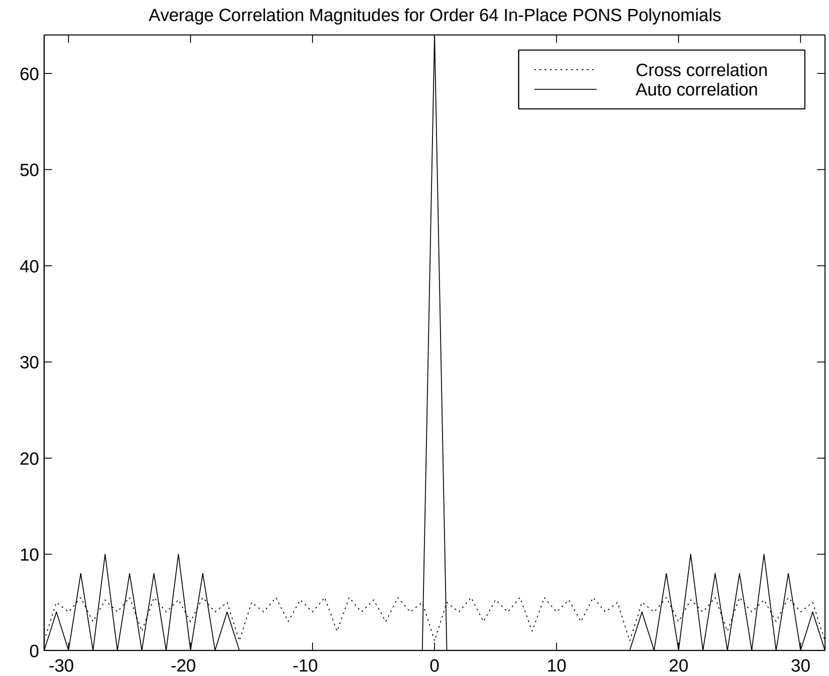

Figure 1: Average PONS periodic correlation magnitudes

denote the j-th out-of-phase periodic autocorrelation of that PONS row. Then

$$\gamma_j = \begin{cases} \pm 4c'_j & \text{if } L/4 < j < L/2 \\ 0 & \text{otherwise} \end{cases}$$

where the c'_j denote the aperiodic autocorrelations of some PONS row of length $L/4$.

Note that this means that three out of four of the periodic autocorrelations of every PONS sequence are zero, including all of the autocorrelations within a quarter length shift from 0 (see Figure 1). This generalizes to multidimensional PONS: For n-dimensional PONS, all but one out of every 4^n periodic autocorrelations are zero (again including all those close to the zero shift).

While the proof of this Theorem 2 is much easier than that of Theorem 1, the two theorems put together imply the estimate

$$\max_{1 \le j \le L-1} |\gamma_j| \le K' \cdot L^{0.73}$$

for the *periodic* autocorrelations, with the constant $K' = K \cdot 4^{-0.73}$.

Theorem 3. *Both for the periodic autocorrelations γ_j and the aperiodic autocorrelations c_j of any PONS row of length l, we have*

$$\sum_{j=1}^{L-1} |\gamma_j|^2 = \frac{1}{6}L^2 + \mathrm{O}(L) \quad \textit{and} \quad \sum_{j=1}^{L-1} |c_j|^2 = \frac{1}{6}L^2 + \mathrm{O}(L).$$

We simply mention that similar expressions for *cross-correlations* (both periodic and aperiodic) of any two distinct rows of the same PONS matrix oscillate between $\frac{4}{3}L^2 + \mathrm{O}(L)$ and $\frac{2}{3}L^2 + \mathrm{O}(L)$.

3 PONS Energy Spreading Applied to Signal Transmission

There are two inherent features of the PONS transform of a digital signal that make it useful under certain circumstances. First, energy spreading makes the transmitted PONS domain version of the signal appear to be white noise, thus naturally adding security to the communications system. Second, transmitting the PONS domain version of a signal as opposed to the original signal, and then reconstructing the signal by taking the inverse transform on the receive end, makes the transmission extremely robust to noise in the transmission channel.

We illustrate several of the above properties via an image processing example, using Figure 2 as our sample digital image. Figure 3, which appears to the eye to be white noise, is a PONS representation of Figure 2 containing exactly the same information as the original (since the PONS transform is invertible).

Suppose there is some kind of bursty noise which substantially degrades transmission of Figure 2 at isolated and unpredictable times. Figure 4 is an example of such a situation, where roughly 60% of the pixels have been lost.

Now suppose that the PONS transform has been applied before transmission, so that Figure 3 is transmitted in place of Figure 2. If the same exact burst error occurs during transmission as did with Figure 3, Figure 5 is received. However, when the inverse PONS transform is applied to Figure 5, Figure 7 results. Comparison of Figures 4 and 7 show a main advantage of energy spreading. Figure 2 is repeated as Figure 6 for easy comparison of the PONS reconstruction for 60 % pixel loss with the original (no pixel loss).

A live demonstration of this transmission robustness was the main feature of the author's Yerevan presentation. A movie illustrating this demonstration is prometheus-us.com/PONS-papers/pons-output.mp4. Contact the author if you would like to arrange a web meeting to see the demonstration running in real time.

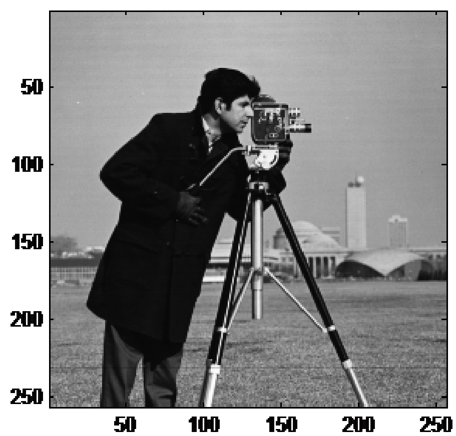

Figure 2: Original Image

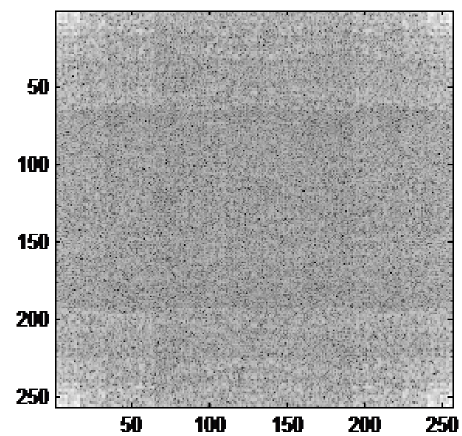

Figure 3: PONS of Original Image

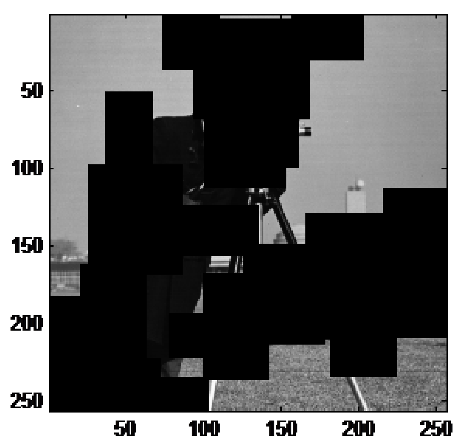

Figure 4: Image after 60% Loss

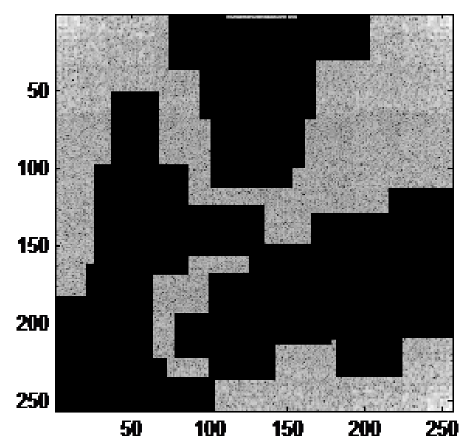

Figure 5: PONS after 60% Loss

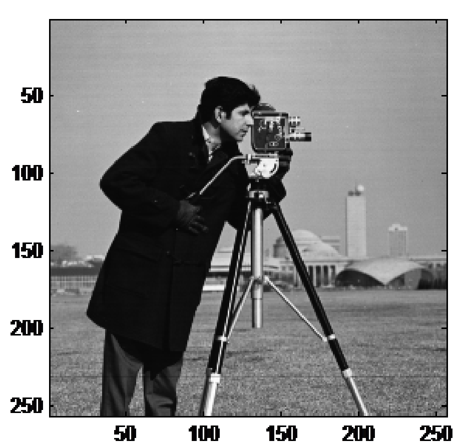

Figure 6: Original Image (Again)

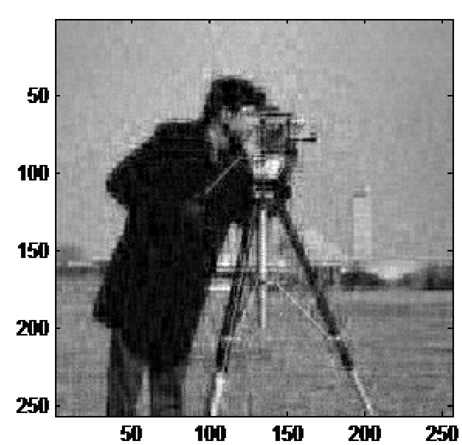

Figure 7: Reconstructed PONS of 60% Loss

4 Open Problems

FAP and ESG

Per Section 1, we describe the FAP and ESG. Let $E(f) = \int_0^1 |f(e^{2\pi it})|^2 dt$ (it is easier to put the 2π inside the argument). All functions are assumed to be square integrable and periodic with period 1. Let $\Gamma = [0, 1]$ and γ any subinterval of Γ. $|\gamma| =$ length of γ. Let $E_\gamma(f) = \int_\gamma |f(e^{2\pi it})|^2 dt$.

Our original definition of FAP (the set of all sequences $\{f_n\}$ of functions satisfying the "Fixed Arc Property") says that $\{f_n\} \in FAP$ if, given any $\gamma \subset \Gamma$, $E_\gamma(f_n) \sim |\gamma| E(f_n)$. Let $R_{n,\gamma}(f_n) = \frac{E_\gamma(f_n)}{|\gamma| E(f_n)}$. It seems that (at least) two definitions of FAP make sense:

Definition 1. *Weak Fixed Arc Property*

$\{f_n\} \in FAP_w$ if, given any $\epsilon > 0$ and any $\gamma \subset \Gamma$, $\exists N_{\epsilon,\gamma} = N \ni n > N \Rightarrow |R_{n,\gamma}(f_n) - 1| < \epsilon$.

Definition 2. *Strong Fixed Arc Property*

$\{f_n\} \in FAP_s$ if, given any $\epsilon > 0$ and any δ, $0 < \delta < 1$, $\exists N_{\epsilon,\delta} = N \ni n > N \Rightarrow |R_{n,\gamma}(f_n) - 1| < \epsilon$ for any $\gamma \subset \Gamma$ with $|\gamma| = \delta$.

It appears clear, but should be checked, that $FAP_s \subset FAP_w$. One problem is to construct an example of an $\{f_n\} \in FAP_w, \{f_n\} \notin FAP_s$.

Similarly, our definition of ESG (the set of all sequences $\{f_n\}$ of functions having an "Energy Spreading Gauge" $\{\delta_n\}$) can be stated in at least two ways. In both cases $\{\delta_n\}$ is assumed to be a sequence of non negative numbers ≤ 1 approaching 0.

Definition 3. *Weak Energy Spreading Gauge Property*

$\{f_n\} \in ESG_w$ if $\exists \{\delta_n\} \ni$, given any $\{\gamma_n\}$, $\gamma_n \subset \Gamma$, with $|\gamma_n| = \delta_n$, and given any $\epsilon > 0$, $\exists N_{\epsilon,\{\gamma_n\}} = N \ni n > N \Rightarrow |R_{n,\gamma_n}(f_n) - 1| < \epsilon$.

Definition 4. *Strong Energy Spreading Gauge Property*

$\{f_n\} \in ESG_s$ if $\exists \{\delta_n\} \ni$, given any $\epsilon > 0$, $\exists N_{\epsilon,\delta_n} = N \ni n > N \Rightarrow |R_{n,\gamma_n}(f_n) - 1| < \epsilon$ for any $\{\gamma_n\}$, $\gamma_n \subset \Gamma$, with $|\gamma_n| = \delta_n$.

As before, $ESG_s \subset ESG_w$. A second problem is to construct an example of an $\{f_n\} \in ESG_w$, $\{f_n\} \notin ESG_w$.

"Possible" proof that $FAP_s \subset ESG$:

Suppose $\{f_n\} \in FAP_s$. Let $0 < \Delta_1 < 1$. Choose $N_1 = N_{1,\Delta_1} \ni n > N_1 \Rightarrow |R_{n,\gamma_1}(f_n) - 1| < 1$ for any $\gamma_1 \subset \Gamma$ with $|\gamma_1| = \delta_1$. Let $\Delta_2 = \frac{1}{2}\Delta_1$. Choose $N_2 = N_{2,\Delta_2} \ni N_2 \geq N_1$ and $n > N_2 \Rightarrow |R_{n,\gamma_2}(f_n) - 1| < \frac{1}{2}$ for any $\gamma_2 \subset \Gamma$ with $|\gamma_2| = \Delta_2$. Continue. For each $k \geq 1$ let $\Delta_k = \frac{1}{k}\Delta_1$. Choose $N_k = N_{k,\Delta_k} \ni N_k \geq N_{k-1}$ and $n > N_k \Rightarrow |R_{n,\gamma_k}(f_n) - 1| < \frac{1}{k}$ for any $\gamma_k \subset \Gamma$ with $|\gamma_k| = \Delta_k$.

Define $\{\delta_n\}$ by:

$\{\Delta_1\Delta_1...\Delta_1\Delta_2\Delta_2...\Delta_2...\Delta_k\Delta_k...\Delta_k...\} = \{\delta_n\}_{n=1}^{\infty}$ where there are N_1 of the Δ_1 elements, $N_2 - N_1$ of the Δ_2 elements, ..., $N_k - N_{k-1}$ of the Δ_k elements, and so on.

Then given any $\epsilon > 0$, choose $k \ni \frac{1}{k} < \epsilon$. Then $n > N_k \Rightarrow |R_{n,\gamma_k}(f_n) - 1| < \frac{1}{k} < \epsilon$ for any $\gamma_k \subset \Gamma$ with $|\gamma_k| = \Delta_k$.

QED?

The author is not satisfied with this "proof" because Δ_k stays fixed as $n \to \infty$. So it apeears that the "arcs" are not getting smaller as $n \to \infty$. The third problem is to clarify this.

Possibly interesting example:

Let $\{\alpha_n\}$ be any sequence of positive integers increasing to ∞. Let $\tau_n = \frac{1}{1^2} + \frac{1}{2^2} + ... + \frac{1}{\alpha_n^2}$. *i. e.*, $\tau_n = \sum_{k=1}^{\alpha_n} \frac{1}{k^2}$. For each n, divide Γ into α_n equal subintervals, so each has length $\frac{1}{\alpha_n}$. For each n, now further divide each of these α_n subintervals into α_n equal sub-subintervals each of length $\frac{1}{\alpha_n^2}$. So the k^{th} one starts at $\frac{k}{\alpha_n} + \frac{0}{\alpha_n^2}$, $\frac{k}{\alpha_n} + \frac{1}{\alpha_n^2}$, and so on, and ends at $\frac{k}{\alpha_n} + \frac{\alpha_n}{\alpha_n^2} = \frac{k+1}{\alpha_n}$.

For each k, define $f_n(x) = \frac{1}{j}$ for $\frac{k}{\alpha_n} + \frac{j}{\alpha_n^2} \leq x < \frac{k}{\alpha_n} + \frac{j+1}{\alpha_n^2}$, $0 \leq j < \alpha_n$. *i. e.*, $f_n(x)$ is periodic with period $\frac{1}{\alpha_n}$; it is independent of which k^{th} sub-subinterval we are in.

Then for any real ρ, $\int_{\rho}^{\rho+\frac{1}{\alpha_n}} |f_n(e^{2\pi it})|^2 dt = \frac{1}{\alpha_n}\tau_n$ <u>independent of ρ</u>! Suppose $\{\delta_n\} = \{\frac{1}{\alpha_n}\}$ and $\gamma_n \subset \Gamma$ is any sub interval of length δ_n, say $\gamma_n = (\rho_n, \rho_n + \delta_n)$. $E(f_n) = \int_0^1 |f_n(e^{2\pi it})|^2 dt = \tau_n$ (because it $= \alpha_n \frac{1}{\alpha_n}\tau_n$) and $E_{\gamma_n}(f_n) = \int_{\rho_n}^{\rho_n+\frac{1}{\alpha_n}} |f_n(e^{2\pi it})|^2 dt = \frac{1}{\alpha_n}\tau_n$, so $R_{n,\gamma_n} = \frac{1}{\delta_n}\frac{E_{\gamma_n}(f_n)}{E(f_n)} = \frac{1}{\delta_n}\frac{\delta_n\tau_n}{\tau_n} = 1$ for every n. So $\{\delta_n\}$ is a strong ESG for $\{f_n\}$.

So, if we allow $\{f_n\}$ to be any sequence of $\mathcal{L}^2$ functions instead of restricting them to be polynomials, we can have non-ultraflat sequences whose ESG goes to 0 arbitrarily fast.

Fourier–PONS

As shown in [2, 12, 22], there is a close relationship between Walsh functions and Fourier analysis. Such a relationship has not yet been studied for PONS functions and polynomials. When developed, it will play an important role in both understanding the mathematics of PONS and in signal processing applications of PONS. Specific questions include:

- Determine if there are PONS–Fourier series analogous to Walsh–Fourier series, and (if there are) analyze their properties;
- Determine if the smooth PONS construction [8] yields a PONS–Fourier transform and, if not, determine a different construction of continuous PONS–type functions that does;
- Develop an inverse PONS–Fourier transform;
- Determine a product–convolution duality analogous to those that occur in Fourier analysis and Walsh–Fourier analysis;
- Develop a concept for PONS analogous to that of sequency [22] for Walsh functions;
- Determine signal processing applications of these Fourier–PONS ideas, related in particular to orthogonal frequency-division multiplexing (OFDM).

Quadriphase PONS

It is straightforward to construct PONS–type Hadamard matrices with entries ± 1, $\pm i$. While they satisfy the basic energy spreading property and important follow–on consequences, much work remains to determine and prove their deeper properties and to utilize them in signal processing. Specific questions include:

- Prove that the rows can be paired off into Golay complementary pairs;
- Determine if the row polynomials are QMFs;
- Determine if they satisfy the ERS property;
- Determine the crest factors of finite sections of each row polynomial;
- Determine the auto- and cross–correlation properties of the rows;

- Decide if there exist symmetric quadriphase PONS matrices;
- Determine approximately how many quadriphase PONS matrices exist for each particular size;
- Determine the spectral properties of quadriphase PONS matrices;
- Develop a factorization approach to fast quadriphase PONS transform algorithms;
- Develop radar and communications waveforms based upon quadriphase PONS matrices and determine their properties;
- Determine the robustness to noise and jamming of quadriphase PONS transforms;
- Determine if the rows can be employed to reduce the peak-to-average ratio (PAPR) in OFDM communications.

Two–dimensional PONS transforms

While the basic construction of PONS transforms for signals of any dimension has been developed and initial theorems have been proven [7], both the theory and applications are much less mature than for the 1D case. Concentrating on 2D transforms and applications for now, specific challenges include:

- Extend the description and quantification of the PONS energy spreading property to multidimensional signals;
- Develop the concepts of 2D Golay pairs (or sets) and QMF;
- Optimize the PONS decomposition and exact reconstruction algorithms so as to minimize the computational requirements for image processing;
- Investigate the possibility of combining PONS with other algorithms such as DCT or DPCM;
- Investigate whether the quality of various image compression schemes can be measured by comparing the accuracy of their respective PONS coefficients;
- Consider the design of a parallel image searching algorithm using PONS;
- Investigate the use of PONS components for feature recognition;
- Investigate the prediction of PONS-processed frames of moving images, and the possible determination of PONS coefficients, from other PONS data;
- Investigate PONS in a multidimensional multiresolution framework, explicitly analyzing the time-scale characteristics of PONS decomposition and synthesis and establishing the pyramid relationship between PONS coefficient matrices;

- Determine what corresponds in 2D to the ERS property.

5 Nonsense Required by Springer

On behalf of all authors, the corresponding author states that there is no conflict of interest.

My manuscript has no associated data.

References

[1] M. An, J. S. Byrnes, W. Moran, B. Saffari, H. S. Shapiro, and R. Tolimieri. PONS, Reed–Muller codes, and group algebras. In Jim Byrnes and Gerald Ostheimer, editors, *Proceedings 2003 NATO Advanced Study Institute on Computational Noncommutative Algebra and Applications*, pages 155–196, Il Ciocco, Italy, 2004. Kluwer Academic Publishers. URL: `https://nato-us.org`.

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

[3] G. Benke. Generalized Rudin-Shapiro systems. *J. Fourier Anal. Appl.*, 1(1):87–101, 1994.

[4] G. Bjorck and B. Saffari. New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries. *Comptes Rendus Academie Sciences Paris*, 320:319–324, 1995.

[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 and D.J. Newman. Null steering employing polynomials with restricted coefficients. *IEEE Trans. Antennas and Propagation*, 36(2):301–303, 1988.

[10] 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.

[11] 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.

[12] J.S. Byrnes and D.A. Swick. Instant Walsh functions. *SIAM-Review*, 12:131, 1970.

[13] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. Watermarking using the Prometheus Orthonormal Set—PONS, University of New Mexico, 2002. Preprint.

[14] J.A. Davis and J. Jedwab. Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes. *Electronics Letters*, 33(4):267–268, February 1997.

[15] 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.

[16] S. Eliahou, M. Kervaire, and B. Saffari. On Golay polynomial pairs. *Advances in Applied Mathematics*, 12:235–292, 1991.

[17] R.J. Evans, W. Moran, M. Viola, and A. Bolton. Clutter adaptive CFAR part I: Detection. In *Proceedings of the 2001 Workshop on Defence Appications of Signal Processing*, pages 290–294. DASP, September 2001.

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

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

[20] M.J.E. Golay. Complementary series. *IRE Trans. Inf. Theory*, 7:82–87, April 1961.

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

[22] Henning F. Harmuth. Applications of Walsh functions in communications. *IEEE-Spectrum*, pages 82–91, November 1969.

[23] T. Hunziker and U.P. Bernhard. Evaluation of coding and modulation schemes based on Golay complementary sequences for efficient OFDM transmission. In *Proc. IEEE Vehicular Technology Conference (VTC '98)*, volume II, pages 1631–1635, Ottawa, Canada, May 1998.

[24] A. la Cour-Harbo. On the Rudin–Shapiro transform. *Applied and Computational Harmonic Analysis*, 24(3):310–328, 2008.

[25] J.E. Littlewood. On polynomials $\sum \pm 1 z^m, \sum e^{\alpha_m i} z^m, \;\; z = e^{i\theta}$. *J. Lon. Math. Soc.*, 41:367–376, 1966.

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

[27] S. S. Muhammad, H. Mehmood, A. Naseem, and A. Abbas. Hybrid coding technique for pulse detection in an optical time domain reflectometer. *Radioengineering*, 21(1):624–631, April 2012.

[28] D.J. Newman and J.S. Byrnes. The L^4 norm of a polynomial with coefficients ± 1. *Amer. Math. Monthly*, 97(1):42–45, 1990.

[29] A. Ojha. Characteristics of complementary coded radar waveforms in noise and target fluctuation. In *IEEE Southeastcon '93*, pages 4–7, Charlotte, NC, USA, April 1993.

[30] K.G. Paterson. Generalized Reed-Muller codes and power control in OFDM modulation. *IEEE Trans. Information Theory*, 46(1):104–120, January 2000.

[31] 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.

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

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

[34] Ekaterina L. Rundblad, Valeriy Labunets, and Ilya Nikitin. A unified approach to Fourier-Clifford-Prometheus sequences, transforms and filter banks. In Jim Byrnes and Gerald Ostheimer, editors, *Proceedings 2003 NATO Advanced Study Institute on Computational Noncommutative Algebra and Applications*, pages 389–400, Il Ciocco, Italy, 2004. Kluwer Academic Publishers.

[35] W. Saengow and B. Thipakorn. Localized error mitigation in image transmission systems using PONS transform. In *Proceedings of Image and Vision Computing '00 New Zealand*, pages 298–303, Waikato, New Zealand, 2000.

[36] P. K. Sahu, S. C. Gowre, and S. Mahapatra. Optical time-domain reflectometer performance improvement using complementary correlated Prometheus orthonormal sequence. *IET Optoelectronics*, 2(3):128–133, June 2008.

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

[38] Michael J. Thurgood. Derivation of a closed form for the original PONS matrix and fast algorithms for generating the original and symmetric PONS matrices. Sc.M. thesis, University of New Mexico, 2002.

[39] 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.

[40] R. Wilson and J. 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.