Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions

Matthew G. Parker*and C. Tellambura†

March 6, 2001

5.3.01, M.G.Parker, ConstaBent2.tex

Abstract

A Golay Complementary Sequence (CS) has a Peak-to-Average-Power-Ratio (PAPR) ≤ 2.0 for its one-dimensional continuous Discrete Fourier Transform (DFT) spectrum. Davis and Jedwab showed that all known length 2^m CS, (GDJ CS), originate from certain quadratic cosets of Reed-Muller $(1, m)$. These can be generated using the Rudin-Shapiro construction. This paper shows that GDJ CS have a PAPR ≤ 2.0 under <u>all</u> $2^m \times 2^m$ unitary transforms whose rows are unimodular linear (Linear Unimodular Unitary Transforms (LUUTs)), including one- and multi-dimensional generalised DFTs. In this context we define Constahadamard Transforms (CHTs) and show how all LUUTs can be formed from tensor combinations of CHTs. We also propose tensor cosets of GDJ sequences arising from Rudin-Shapiro extensions of near-complementary pairs, thereby generating many more infinite sequence families with tight low PAPR bounds under LUUTs. We then show that GDJ CS have a PAPR $\leq 2^{m-\lfloor \frac{m}{2} \rfloor}$ under all $2^m \times 2^m$ unitary transforms whose rows are linear (Linear Unitary Transforms (LUTs)). Finally we present a radix-2 tensor decomposition of any $2^m \times 2^m$ LUT.

*M.G.Parker is with the Code Theory Group, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: matthew@ii.uib.no. Web: http://www.ii.uib.no/~matthew/MattWeb.html

†C.Tellambura is with the School of Computer Science and Software Engineering, Monash University, Clayton, Victoria 3168, Australia. E-mail: chintha@dgs.monash.edu.au. Phone/Fax: +61 3 9905 3196/5146

Keywords: Complementary, Bent, Reed-Muller, PAPR, Nonlinear, Golay, Fourier, Multidimensional, Quadratic, Rudin-Shapiro, Covering Radius, DFT, Transform, Unitary

Some preliminary definitions:
Z_n is the set of integers $\{0, 1, \ldots, n-1\}$.
For length N vectors $\mathbf{s}$,$\mathbf{f}$, where $\mathbf{s} \in Z_P^N$, $\mathbf{f} \in Z_n^N$, and s_j, f_j are sequence elements of $\mathbf{s}$ and $\mathbf{f}$, respectively, $0 \leq j < N$, we define,
Correlation: $\mathbf{s} \odot \mathbf{f} = \sum_{j=0}^{N-1} \epsilon^{\mu s_j - \lambda f_j}$, where
$\epsilon = \exp(2\pi\sqrt{-1}/\mathrm{lcm}(P,n))$, $\mu = \frac{\mathrm{lcm}(P,n)}{P}$, $\lambda = \frac{\mathrm{lcm}(P,n)}{n}$, where lcm means 'least common multiple'.
Orthogonal: $\mathbf{s}$ and $\mathbf{f}$ are 'Orthogonal' to each other if $\mathbf{s} \odot \mathbf{f} = 0$.
(Almost) Orthogonal:[1] $\mathbf{s}$ and $\mathbf{f}$ are '(Almost) Orthogonal' to each other if $0 \leq |\mathbf{s} \odot \mathbf{f}| \leq \sqrt{2N}$.
Roughly Orthogonal: $\mathbf{s}$ and $\mathbf{f}$ are 'Roughly Orthogonal' to each other if $0 \leq |\mathbf{s} \odot \mathbf{f}| \leq B$, for some pre-chosen B significantly less than N.
Unimodular: A sequence is unimodular if every element in the sequence has magnitude 1.
A **Function** representation for a sequence will be used interchangeably with the sequence representation itself, where the sequence describes the function. A function, $\mathbf{s}$, will be defined over m binary variables, x_i, and outputs to Z_P. More precisely,

$$\mathbf{s} : \{0,1\}^m \rightarrow \{0, 1, \ldots, P-1\}$$

$\mathbf{s}$ is then represented by a sequence, also called $\mathbf{s}$, under a lexicographical ordering of the variables. More precisely,

$$s(x_0 = k_0, x_1 = k_1, \ldots, x_{m-1} = k_{m-1}) = s_j$$

where $j = \sum_{i=0}^{m-1} k_i 2^i$, $k_i \in \{0,1\}$. For instance, for $m = 3$, choosing $\mathbf{s} = 2(x_0x_1 + x_0x_2) + x_1$ with output over Z_4 gives the following function $\leftrightarrow$ sequence equivalence:

x_2	x_1	x_0	$\mathbf{s}$	
0	0	0	0	
0	0	1	0	
0	1	0	1	equivalent to
0	1	1	3	the sequence
1	0	0	0	$\mathbf{s} = 00130211$
1	0	1	2	
1	1	0	1	
1	1	1	1	

[1]This definition is related to the definition of 'Quasi-Orthogonality' found in [34].

Sequence representations for linear functions, x_i, are of the form $x_0 = 0101010101\ldots$, $x_1 = 001100110011\ldots$, $x_2 = 0000111100001111\ldots$, and so on.
In Sections 2-6 we refer to a sequence, $\mathbf{s}$, by its integer representation over Z_P^N. In Sections 7-8 we refer to the <u>same</u> sequence, $\mathbf{s}$, by its unimodular complex-modulated form, such that $\mathbf{s} = (\epsilon^{s_0}, \epsilon^{s_1}, \ldots, \epsilon^{s_{N-1}})$, where $\epsilon = \exp(2\pi\sqrt{-1}/P)$. Moreover we widen the discussion to include non-unimodular sequences, i.e. sequences whose complex-modulated form does not necessarily have elements with magnitude 1.
Tensor Sum: In this paper the (left) tensor sum is the additive version of the better-known (left) Tensor Product. The tensor sum of vectors (a,b,...,x) and (c,d,....,z) is here defined by $\oplus$ as,

$$(a, b, ..., x) \oplus (c, d, ...z) =$$
$$(a + c, b + c, ..., x + c, a + d, b + d, ..., x + d, ...a + z, b + z, ...x + z)$$

We equate the Tensor Sum $(a, b) \oplus (c, d) \oplus (e, f) \oplus \ldots$ mod n with linear functions of single binary variables: $q(x_0) + r(x_1) + s(x_2) + \ldots$ with output over Z_n, which in turn represents the element-by-element addition of sequences: $abababab... + ccddccdd... + eeeeffff...$, mod n.
The (left) Tensor Sum of Matrices is also defined by $\oplus$ as follows. Let $\mathbf{A}$ be an $m \times n$ matrix, and $\mathbf{B}$ be a $p \times q$ matrix with elements $A_{i,j}$, $B_{i,j}$, respectively. Let $B_{i,j} + \mathbf{A}$ be the $m \times n$ matrix,

$$\begin{pmatrix} B_{i,j} + A_{0,0} & B_{i,j} + A_{0,1} & \ldots & B_{i,j} + A_{0,n-1} \\ B_{i,j} + A_{1,0} & B_{i,j} + A_{1,1} & \ldots & B_{i,j} + A_{1,n-1} \\ \ldots & \ldots & \ldots & \ldots \\ B_{i,j} + A_{m-1,0} & B_{i,j} + A_{m-1,1} & \ldots & B_{i,j} + A_{m-1,n-1} \end{pmatrix}$$

Then $\mathbf{A} \oplus \mathbf{B} =$

$$\begin{pmatrix} B_{0,0} + \mathbf{A} & B_{0,1} + \mathbf{A} & \ldots & B_{0,q-1} + \mathbf{A} \\ B_{1,0} + \mathbf{A} & B_{1,1} + \mathbf{A} & \ldots & B_{1,q-1} + \mathbf{A} \\ \ldots & \ldots & \ldots & \ldots \\ B_{p-1,0} + \mathbf{A} & B_{p-1,1} + \mathbf{A} & \ldots & B_{p-1,q-1} + \mathbf{A} \end{pmatrix}$$

Tensor Product: The (left) Tensor Product [14] of vectors and of matrices is identical to the previous definition of (left) Tensor Sum, but with $\oplus$ and $+$ (addition) replaced by $\otimes$ and $\times$ (multiplication), respectively.
Tensor Permutation: A tensor permutation of m binary variables, x_i, takes x_i to $x_{\pi(i)}$, where the permutation π is any permutation of the integers in Z_m.

Definitions:

Definition 1 [2] $\mathbf{L_m}$ *is the infinite set of length* 2^m *sequences representing all linear functions in* m *binary variables with output over* ***all*** *alphabets,* Z_n, $1 \leq n \leq \infty$,

$$\mathbf{L_m} = \{\beta \oplus (0, \alpha_0) \oplus (0, \alpha_1) \oplus \ldots \oplus (0, \alpha_{m-1})\}, \ \ mod\ n$$

where $\oplus$ *means 'tensor sum',* $\beta, \alpha_j \in Z_n\ \forall j$, $\gcd(\beta, n) = \gcd(\alpha_j, n) = 1$.

Definition 2 $\mathbf{F1}$ *is the infinite set of length* N *sequences representing all one-dimensional Fourier functions with output over* ***all*** *alphabets,* Z_n, $1 \leq n \leq \infty$,

$$\mathbf{F1} = \{(0, \delta, 2\delta, 3\delta, \ldots, (N-1)\delta), \ \ mod\ n \\ 1 \leq n \leq \infty, 0 \leq \delta < n, \gcd(\delta, n) = 1\}$$

Definition 3 $\mathbf{F1_m}$ *is the infinite set of length* 2^m *sequences representing all one-dimensional Fourier functions in* m *binary variables with output over* ***all*** *alphabets,* Z_n, $1 \leq n \leq \infty$,

$$\mathbf{F1_m} = \{(0, \delta) \oplus (0, 2\delta) \oplus (0, 4\delta) \oplus \ldots \oplus (0, 2^{m-1}\delta), \ \ mod\ n \\ 1 \leq n \leq \infty, 0 \leq \delta < n, \gcd(\delta, n) = 1\}$$

$\mathbf{F1_m} \subset \mathbf{L_m}$. *Note also that* $\mathbf{F1_m}$ *is a special case of* $\mathbf{F1}$ *for the case when* $N = 2^m$.

Definition 4 $\mathbf{Fm_m}$ *is the infinite set of all* m*-dimensional linear Fourier functions in* m *binary variables with output over* ***all*** *alphabets,* Z_n, $1 \leq n \leq \infty$, n *even,*

$$\mathbf{Fm_m} = \{(0, \delta + c_0) \oplus (0, \delta + c_1) \oplus (0, \delta + c_2) \oplus \ldots \oplus (0, \delta + c_{n-1}) \\ mod\ n, 2 \leq n \leq \infty, n\ \ even, 0 \leq \delta < n/2, \gcd(\delta, n) = 1, c_i \in \{0, n/2\}\}$$

$\mathbf{Fm_m} \subset \mathbf{L_m}$.

Definition 5 *A* $2^m \times 2^m$ *Linear Unimodular Unitary Transform (LUUT)* $\mathbf{L}$ *has rows taken from* $\mathbf{L_m}$ *such that* $\mathbf{L}\mathbf{L}^\dagger = 2^m\mathbf{I_m}$, *where* $\dagger$ *means conjugate transpose,* $\mathbf{I_t}$ *is the* $2^t \times 2^t$ *identity matrix, and a row,* $\mathbf{u}$, *of* $\mathbf{L}$ *'times' a column,* $\mathbf{v}$, *of* $\mathbf{L}^\dagger$ *is computed as* $\mathbf{u} \odot (-\mathbf{v})$.

[2] The gcd constraint in Definition 1 and in subsequent similar definitions is to avoid degenerate cases (multiple representations).

Definition 6 $\mathbf{G_m}$ *is the infinite set of length* 2^m *normalised complex sequences, representing all complex-modulated linear functions in* m *binary variables with output over* C*.*

$$\mathbf{G_m} = \{(\chi) \otimes (\phi_0, \theta_0) \otimes (\phi_1, \theta_1) \otimes \ldots \otimes (\phi_{m-1}, \theta_{m-1})\}$$

where $\chi, \phi_j, \theta_j \in C$*,* $\forall j$*, such that* $|\chi|^2 = 1$*, and* $|\phi_j|^2 + |\theta_j|^2 = 2$*, and* $\otimes$ *means tensor-product.* C *is the infinite set of complex numbers. The sum of the magnitude-squareds of the elements of a sequence in* $\mathbf{G_m}$ *is* $N = 2^m$*.*

Definition 7 *A* $2^m \times 2^m$ *Linear Unitary Transform (LUT)* $\mathbf{G}$ *has rows taken from* $\mathbf{G_m}$ *such that* $\mathbf{G}\mathbf{G}^\dagger = 2^m \mathbf{I_m}$*, where a row,* $\mathbf{u}$*, of* $\mathbf{G}$ *'times' a column,* $\mathbf{v}$*, of* $\mathbf{G}^\dagger$ *is computed as* $\sum_{i=0}^{2^m-1} u_i v_i^*$*. LUUTs are a special case of LUT.*

1 Introduction

Length $N = 2^m$ Complementary Sequences (CS) are known to be (Almost) Orthogonal to $\mathbf{F1_m}$ (Definition 3) [11, 12, 13, 2, 9],i.e. they have a (near) flat Fourier spectrum. For example, Fig 1 shows the one-dimensional (2000-point) Fourier power spectra of the binary length 16 Complementary pair of sequences, $\mathbf{s_0} = x_0x_3 + x_3x_1 + x_1x_2 + x_1 + x_2 + 1 = 0110010100000011$ and $\mathbf{s_1} = x_0x_3 + x_3x_1 + x_1x_2 + x_1 + x_2 + x_0 + 1 = 1001010111110011$ which both have a worst case PAPR of 1.97. It is evident from the figure that their power sum is 2.00 everywhere. Length 2^m CS over Z_{2^h}, as formed using the Davis-Jedwab construction, $\mathbf{DJ_{m,h}}$, are also Roughly Orthogonal to each other [16, 9, 26, 33, 21], i.e. they form a codeset with reasonable Euclidean distance. For example, here are the 48 codewords in $\mathbf{DJ_{3,1}}$, having a minimum Hamming Weight of $2^{m-2} = 2$ between codewords, and where each codeword in the set has PAPR = 2.00,

00010010, 00011101, 00100001, 00101110, 01000111, 01001000, 01110100, 01111011
11101101, 11100010, 11011110, 11010001, 10111000, 10110111, 10001011, 10000100
00000110, 00001001, 00110101, 00111010, 01010011, 01011100, 01100000, 01101111
11111001, 11110110, 11001010, 11000101, 10101100, 10100011, 10011111, 10010000
00010100, 00011011, 00100111, 00101000, 01000001, 01001110, 01110010, 01111101
11101011, 11100100, 11011000, 11010111, 10111110, 10110001, 10001101, 10000010

We refer to $\mathbf{DJ_{m,\infty}}$ as $\mathbf{DJ_m}$. This paper shows that $\mathbf{DJ_m}$ is (Almost) Orthogonal to $\mathbf{L_m}$ (Definition 1), and therefore each member of $\mathbf{DJ_m}$ has a Peak-to-Average Power Ratio (PAPR) ≤ 2.0 under all $2^m \times 2^m$ LUUTs (Definition 5). The properties of $\mathbf{DJ_m}$ are shown to follow directly from a generalisation of the Rudin-Shapiro construction [29, 28, 13, 16, 17, 30]. We then define the set of ConstaHadamard Transforms (CHTs), a subset

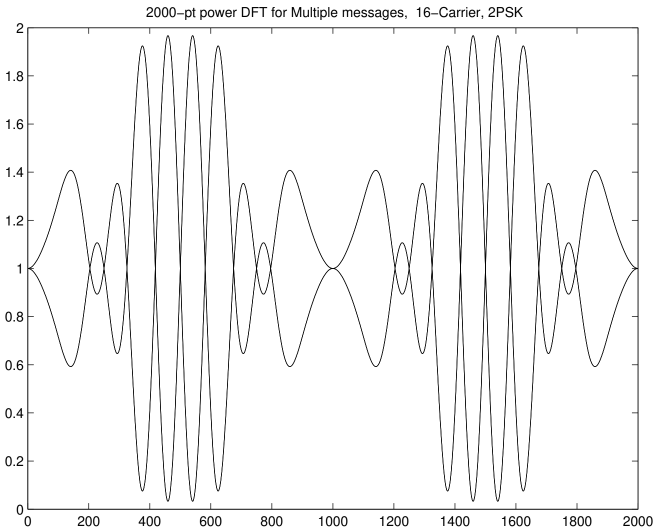

Figure 1: The Power Spectra of $\mathbf{s_0} = x_0x_3 + x_3x_1 + x_1x_2 + x_1 + x_2 + 1$ and $\mathbf{s_1} = x_0x_3 + x_3x_1 + x_1x_2 + x_1 + x_2 + x_0 + 1$

of LUUTs, whose rows cover all members of $\mathbf{L_m}$. $\mathbf{DJ_m}$ consequently has a PAPR ≤ 2.0 under all CHTs. We identify Hadamard and Negahadamard Transforms (HT,NHT) as being from a subclass of CHTs whose rows cover all members of $\mathbf{Fm_m}$ (Definition 4). In particular we show that $\mathbf{DJ_{m,1}}$ is both Bent and Negabent for m even, $m \neq 2 \bmod 3$ [23], under the HT and NHT respectively. We also show how Z_n-linearity of a sequence can be tested using appropriate CHTs. We then propose tensor cosets of $\mathbf{DJ_m}$, where we identify near-complementary seed pairs whose power sum has a PAPR $\leq v$ under certain subsets of LUUTs, where v is small. We grow sequence sets from these pairs by repeated application of Rudin-Shapiro such that these sets also have a PAPR $\leq v$ under certain subsets of LUUTs. In this way we extend the work of [16, 9, 26] by proposing further infinite sequence families with tight one-dimensional Fourier PAPR bounds, and of degree higher than quadratic. We also confirm and extend the recent results of [5] who construct families of Bent sequences using Bent sequences as seed pairs, although not in the context of Rudin-Shapiro [25]. We then show that $\mathbf{DJ_m}$ has PAPR $\leq 2^{m-\lfloor \frac{m}{2} \rfloor}$ under **all** LUTs (Definition 7). Finally we show that LUTs always have a convenient radix-2 tensor decomposition.

The (almost) orthogonality between $\mathbf{DJ_m}$ and $\mathbf{L_m}$ (Theorem 2) has, in one sense, been implicitly stated before. More specifically, Frank [10] and

Van Nee [33] have highlighted the polyphase properties of CS, namely that any phase shift of an orthogonal subset of a CS maintains the sequence as a CS. Also Davis and Jedwab [9] have implicitly used the polyphase property to extend their codesets from codes over Z_2 to codes over Z_{2^h}, $h \rightarrow \infty$. In all this work the idea is that any linear offset of a CS is also a CS under the **one-dimensional** Fourier Transform, where the linear offset is defined over **any** alphabet. However, the immediate implication that CS have PAPR ≤ 2.00 under **all** tensor-decomposable unitary transforms (including one and multidimensional DFTs) has not, to our knowledge been stated or exploited (Corollary 1). In other words, applying the polyphase property of CS not only widens the choice of CS possible but it all also widens the choice of unitary transform under which the sequence is a CS. So one contribution of this paper is to identify the complete class of unitary transforms under which length 2^m CS have an (Almost) Flat spectrum. To our knowledge the result of Theorem 6 relating to the (Roughly Flat) spectra of CS under a wider class of unitary transforms is completely new, and will have implications for the decoding complexity and/or cryptographic strength of CS under a generalised linear correlation attack.

2 Complementary Sequences (CS)

Let $\mathbf{s}$ be a length-N sequence (vector) over Z_P, and let s_j be the jth element in $\mathbf{s}$, such that $s_j = 0$, $0 > j \geq N$.

Definition 8 *The (one-dimensional) Aperiodic Autocorrelation Function (ACF) of* $\mathbf{s}$ *is given by,*

$$A_{\mathbf{s}}(k) = \sum_{j=0}^{N-1} \epsilon^{s_j - s_{j+k}}, \qquad -N < k < N$$

where $\epsilon = \exp(2\pi\sqrt{-1}/P)$.

Definition 9 $\mathbf{s0}$ *and* $\mathbf{s1}$ *are Golay Complementary Pairs of Sequences if they satisfy,*

$$A_{\mathbf{s0}}(k) + A_{\mathbf{s1}}(k) = 0, \qquad k \neq 0$$

i.e. if their Aperiodic ACFs sum to a delta-function. $\mathbf{s0}$ *and* $\mathbf{s1}$ *are then referred to as Complementary Sequences (CS). Binary CS are known for* *even lengths $2^a 10^b 26^c$, $a, b, c \geq 0$, where the length is the sum of at most two squares. This paper mainly considers power-of-two lengths for alphabets Z_{2^h}, but adaptations to other lengths (using non-power-of-two kernel sequences) and other alphabets can easily be envisaged [10].*

The one-dimensional Fourier power spectrum of $\mathbf{s}$, for $\mathbf{s}$ of length N defined over some Z_P^N, is then given by $|\mathbf{s} \odot \mathbf{f}|^2$, $\forall \mathbf{f} \in \mathbf{F1}$. By Parseval's Theorem, the average value of the one-dimensional Fourier power spectrum of $\mathbf{s}$ is N. Definition 9 implies that the one-dimensional Fourier power spectra of $\mathbf{s0}$ and $\mathbf{s1}$ sum to a constant value of $2N$ at all frequencies (e.g. Fig 1). Therefore,

Implication 1 *The PAPR of the one-dimensional Fourier power spectrum of a CS, $\mathbf{s}$, is constrained by,*

$$1.0 \leq PAPR(\mathbf{s}) \leq \frac{2N}{N} = 2.0$$

The Aperiodic ACF of Definition 8 is implicitly one-dimensional, hence the one-dimensional spectral property described in Implication 1. However this paper shows that Golay-Davis-Jedwab (GDJ) CS have good properties beyond the one-dimensional case.

2.1 Golay-Davis-Jedwab (GDJ) Complementary Sequences

Theorem 1 *[9] $\mathbf{s}$ is a GDJ CS if of length 2^m and expressible in Algebraic Normal Form as a function of m binary variables with output over Z_{2^h} as,*

$$\mathbf{s}(x_0, x_1, \ldots, x_{m-1}) = 2^{h-1} \sum_{k=0}^{m-2} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=0}^{m-1} c_k x_k + d \qquad (1)$$

where π is a permutation of the symbols $\{0, 1, \ldots, m-1\}$, $c_k, d \in Z_{2^h}$, and the x_k are linear binary functions with output over Z_{2^h}. We refer to the set of GDJ CS over Z_{2^h} as $\mathbf{DJ_{m,h}}$, and refer to $\mathbf{DJ_{m,\infty}}$ as $\mathbf{DJ_m}$.

The first term on the right-hand side of (1) determines the quadratic coset leader, and the second term determines the component from Reed-Muller (RM)$(1, m)$. There are $(\frac{m!}{2})2^{h(m+1)}$ sequences in $\mathbf{DJ_{m,h}}$, and $\mathbf{DJ_{m,h}}$ has a minimum Hamming Distance $\geq 2^{m-2}$. Thus, for distinct $\mathbf{s0}, \mathbf{s1} \in \mathbf{DJ_{m,1}}$, $\mathbf{s0} \odot \mathbf{s1} \leq 2^{m-1}$, i.e. $\mathbf{DJ_{m,1}}$ is roughly orthogonal.

3 Distance of $\mathbf{DJ_m}$ from $\mathbf{L_m}$

Theorem 2 $\mathbf{DJ_m}$ *is (Almost) Orthogonal to* $\mathbf{L_m}$.

Proof: We prove for $\mathbf{DJ_{m,1}}$ by using the Rudin-Shapiro construction [29, 28] to simultaneously construct $\mathbf{DJ_{m,1}}$ and $\mathbf{L_m}$. We then extend the proof to $\mathbf{DJ_m}$. Let $\mathbf{s0_j}$, $\mathbf{s1_j}$ be a CS pair in $\mathbf{DJ_{m,1}}$. More specifically, let $\mathbf{s0_0}$, $\mathbf{s1_0}$ be the length 1 sequences,

$$\mathbf{s0_0} = (0), \qquad \mathbf{s1_0} = (1)$$

where $\mathbf{s0_0}, \mathbf{s1_0} \in \mathbf{DJ_{0,1}}$. The Rudin-Shapiro sequence construction is as follows:

$$\mathbf{s0_j} = \mathbf{s0_{j-1}}|\mathbf{s1_{j-1}}, \qquad \mathbf{s1_j} = \mathbf{s0_{j-1}}|\overline{\mathbf{s1_{j-1}}} \tag{2}$$

where $\mathbf{s0_j}, \mathbf{s1_j} \in \mathbf{DJ_{j,1}}$, $\overline{\mathbf{s}}$ means binary negation of sequence $\mathbf{s}$, and $|$ means sequence concatenation.

Example 1: $\mathbf{s0_1} = 01, \mathbf{s1_1} = 00 \Rightarrow \mathbf{s0_2} = 0100, \mathbf{s1_2} = 0111$.

More generally we generate the $\mathrm{RM}(1,m) \cup \mathrm{RM}(0,m)$ coset of $x_0x_1 + x_1x_2 + \ldots + x_{m-2}x_{m-1}$ using all 2^m combinations of m iterations of the two constructions,

$$\begin{array}{lll} A: & \mathbf{s0_j} = \mathbf{s0_{j-1}}|\mathbf{s1_{j-1}}, & \mathbf{s1_j} = \mathbf{s0_{j-1}}|\overline{\mathbf{s1_{j-1}}} \\ & \text{and} & \\ B: & \mathbf{s0_j} = \overline{\mathbf{s0_{j-1}}}|\mathbf{s1_{j-1}}, & \mathbf{s1_j} = \overline{\mathbf{s0_{j-1}}}|\overline{\mathbf{s1_{j-1}}} \end{array} \tag{3}$$

Algebraically, constructions (3) become,

$$\begin{array}{ll} A: & \begin{array}{l} \mathbf{s0_j}(x) = x_{j-1}(\mathbf{s0_{j-1}}(x') + \mathbf{s1_{j-1}}(x')) + \mathbf{s0_{j-1}}(x') \\ \mathbf{s1_j}(x) = \mathbf{s0_j}(x) + x_{j-1} \end{array} \\ & \text{and} \\ B: & \begin{array}{l} \mathbf{s0_j}(x) = x_{j-1}(\mathbf{s0_{j-1}}(x') + \mathbf{s1_{j-1}}(x') + 1) + \mathbf{s0_{j-1}}(x') + 1 \\ \mathbf{s1_j}(x) = \mathbf{s0_j}(x) + x_{j-1} \end{array} \\ & \text{where } x = (x_0, x_1, \ldots, x_{j-1}), x' = (x_0, x_1, \ldots, x_{j-2}) \end{array} \tag{4}$$

Example 2: $\mathbf{s0_0} = 0, \mathbf{s1_0} = 1 \Rightarrow \mathbf{s0_1} = 01, \mathbf{s1_1} = 00$ by the first construction, and $\mathbf{s0_1} = 11, \mathbf{s1_1} = 10$ by the second construction, thereby covering the four sequences in $\mathrm{RM}(1,1) \cup \mathrm{RM}(0,1)$.

Finally we generate the complete set $\mathbf{DJ_{m,1}}$ from this coset by permutation of the indices, i, of x_i (tensor permutation) over Z_m. There are $\frac{m!}{2}$ distinct tensor permutations, (ignoring reversals).

Example 3: Let $\mathbf{s0_3} = x_0x_1 + x_1x_2 + x_2 + 1 = 11100010$. Permuting $x_0 \to x_1$, $x_1 \to x_0$, $x_2 \to x_2$, gives $\mathbf{s0'_3} = x_0x_1 + x_0x_2 + x_2 + 1 = 11100100$, where $\mathbf{s0_3}, \mathbf{s0'_3} \in \mathbf{DJ_{m,1}}$.
We now prove Theorem 2 for construction (2), where the extension of the proof to construction (3) with subsequent tensor permutation is straightforward. Let $\mathbf{f_j}$ be a sequence in $\mathbf{L_j}$ (Definition 1), and let $\mathbf{f_0}$ be the length 1 sequence, $\mathbf{f_0} = (\beta)$, where $\beta \in Z_n, 1 \leq n \leq \infty$. Let p_j, q_j be complex numbers satisfying,

$$p_j = \mathbf{f_j} \odot \mathbf{s0_j}, \qquad q_j = \mathbf{f_j} \odot \mathbf{s1_j} \tag{5}$$

Let,

$$\mathbf{f_j} = \mathbf{f_{j-1}} \oplus (0, \alpha_{j-1}), \ \bmod n \tag{6}$$

$\alpha_{j-1} \in Z_n, 1 \leq n \leq \infty$, $\gcd(\alpha_{j-1}, n) = 1$.
Using (6) $\forall \alpha_j$ we generate the complete set, $\mathbf{L_j}$. Combining (5), (2) and (6) we have,

$$p_j = \mathbf{f_{j-1}} \odot \mathbf{s0_{j-1}} + \epsilon^{\alpha_{j-1}} \mathbf{f_{j-1}} \odot \mathbf{s1_{j-1}} = p_{j-1} + \epsilon^{\alpha_{j-1}} q_{j-1} \tag{7}$$

$$q_j = \mathbf{f_{j-1}} \odot \mathbf{s0_{j-1}} - \epsilon^{\alpha_{j-1}} \mathbf{f_{j-1}} \odot \mathbf{s1_{j-1}} = p_{j-1} - \epsilon^{\alpha_{j-1}} q_{j-1} \tag{8}$$

where $\epsilon = \exp(2\pi\sqrt{-1}/n)$. Applying the relation,

$$|\phi p + \theta q|^2 + |\phi p - \theta q|^2 = 2(|\phi|^2|p|^2 + |\theta|^2|q|^2) \tag{9}$$

for the special case $|\phi|^2 = |\theta|^2 = 1$, to (7) and (8) we get,

$$|p_j|^2 + |q_j|^2 = 2(|p_{j-1}|^2 + |q_{j-1}|^2) = 2^j(|p_0|^2 + |q_0|^2)$$

Noting that $|p_0|^2 = |q_0|^2 = 1$, it follows that,

$$|p_j|^2 \leq 2^{j+1}, \qquad |q_j|^2 \leq 2^{j+1} \tag{10}$$

Noting that length $N = 2^j$, and combining (5) and (10) proves Theorem 2 for a subset of $\mathbf{DJ_{m,1}}$ comprising the sequences generated by (2). It is straightforward to extend the proof to the RM$(1, m)$ coset of $x_0x_1 + x_1x_2 + \ldots\ x_{m-2}x_{m-1}$ by replacing construction (2) with constructions (3). Further extension to the complete set $\mathbf{DJ_{m,1}}$ follows by observing that identical tensor-permuting of $\mathbf{f}$ and $\mathbf{s}$ leaves the argument of (7) - (10) unchanged. We further extend the proof to $\mathbf{DJ_m}$ by the following argument.

Let $\mathbf{R}$ be the set of all linear functions in m binary variables with output to Z_{2^∞} but not to Z_2. Then,

$$\mathbf{DJ_m} = \mathbf{DJ_{m,1}} \cup (\mathbf{DJ_{m,1}} + \mathbf{R})$$

Then the orthogonality between $\mathbf{DJ_m}$ and $\mathbf{L_m}$ is given by,

$$\mathbf{DJ_m} \odot \mathbf{L_m} = \{\mathbf{DJ_{m,1}} \odot \mathbf{L_m}, (\mathbf{DJ_{m,1}} + \mathbf{R}) \odot \mathbf{L_m}\}$$

But $\mathbf{L_m}$ includes $\mathbf{R}$ and $\mathbf{L_m} = \mathbf{L_m} + \mathbf{R}$. Therefore,

$$(\mathbf{DJ_{m,1}} + \mathbf{R}) \odot \mathbf{L_m} = (\mathbf{DJ_{m,1}} + \mathbf{R}) \odot (\mathbf{L_m} + \mathbf{R}) = \mathbf{DJ_{m,1}} \odot \mathbf{L_m}$$

∎

4 Transform Families With Rows From $\mathbf{L_m}$

Corollary 1 *Theorem 2 implies that sequences from $\mathbf{DJ_m}$ have an (Almost) flat spectrum under all $2^m \times 2^m$ transforms with rows taken from $\mathbf{L_m}$. In particular they have a PAPR ≤ 2.0 under all LUUTs.*

This section highlights two important LUUT sub-classes, firstly the one-dimensional Consta-Discrete Fourier Transforms (CDFTs), and secondly the m-dimensional Constahadamard Transforms (CHTs). We show that CHTs partition $\mathbf{L_m}$ into disjoint groups of 2^m sequences per matrix. An $N \times N$ Consta-DFT (CDFT) matrix has rows from $\mathbf{F1}$ and is defined over Z_n by,

$$\begin{pmatrix} 0 & d & 2d & \ldots & (N-1)d \\ 0 & d+k & 2(d+k) & \ldots & (N-1)(d+k) \\ . & . & . & . & . \\ 0 & d+(N-1)k & 2(d+(N-1)k) & \ldots & (N-1)(d+(N-1)k) \end{pmatrix} \quad (11)$$

$1 \leq n \leq \infty$, $N|n$, $k = \frac{n}{N}$, $d \in Z_k$, $\gcd(d,k) = 1$, (including the case $d = 0$, $k = 1$, which is the $N \times N$ DFT).

A radix-2 $N = 2^m$-point CHT matrix has rows from $\mathbf{L_m}$ over Z_n and is defined by the m-fold tensor sum of CHT kernels,

$$\begin{pmatrix} 0 & \delta_0 \\ 0 & \delta_0 + \frac{n}{2} \end{pmatrix} \oplus \begin{pmatrix} 0 & \delta_1 \\ 0 & \delta_1 + \frac{n}{2} \end{pmatrix} \oplus \ldots \oplus \begin{pmatrix} 0 & \delta_{m-1} \\ 0 & \delta_{m-1} + \frac{n}{2} \end{pmatrix}$$
$$= \oplus_{i=0}^{m-1} \begin{pmatrix} 0 & \delta_i \\ 0 & \delta_i + \frac{n}{2} \end{pmatrix}$$

$2 \leq n \leq \infty, n$ even, $0 \leq \delta_i < \frac{n}{2}$ $\gcd(\delta_i, \frac{n}{2}) = 1$, (including the case $\delta_i = 0$, $n = 2$). The rows of $\mathbf{A}$ and $\mathbf{A'}$ are disjoint for $\mathbf{A}$, $\mathbf{A'} \in \{2^m \times 2^m$ CHT matrices $\}$, $\mathbf{A} \neq \mathbf{A'}$, and the rows of all CHT matrices cover all members of

$\mathbf{L_m}$. The Hadamard Transform (HT) is $\oplus^m \mathbf{H}$, where $\mathbf{H} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ over Z_2, and the Negahadamard Transform (NHT) is $\oplus^m \mathbf{N}$, where $\mathbf{N} = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}$ over Z_4. Both HT and NHT originate from a subclass of CHTs whose rows are from $\mathbf{Fm_m}$, i.e. where all δ's are the same. Previous papers have focussed on proving Theorem 2 for the subset $\mathbf{F1_m}$ of $\mathbf{L_m}$, in other words showing that $\mathbf{DJ_m}$ has a PAPR ≤ 2.0 under all CDFTs [3]. A new contribution of this paper is that we have proved Theorem 2 for all of $\mathbf{L_m}$. In other words, we have shown that $\mathbf{DJ_m}$ has a PAPR ≤ 2.0 under all LUUTs, including all CHTs and CDFTs.

4.1 The (Almost) Constabent Properties of $\mathbf{DJ_m}$

Definition 10 *[23] A length 2^m sequence, $\mathbf{s}$, is Bent, Negabent, Constabent, if it has a PAPR $= 1.0$ under the HT, NHT, and CHT, respectively. It is (Almost) Bent, (Almost) Negabent, (Almost) Constabent, if it has a PAPR ≤ 2.0 under the HT, NHT, and CHT, respectively.*

From Theorem 2, $\mathbf{DJ_m}$ is (Almost) Constabent. More particularly,

Theorem 3 *[23] $\mathbf{DJ_{m,1}}$ is Bent for m even, and (Almost) Bent, with PAPR $= 2.0$, for m odd.*

Theorem 4 *[23] $\mathbf{DJ_{m,1}}$ is Negabent for $m \neq 2$ mod 3, and (Almost) Negabent, with PAPR $= 2.0$, for $m = 2$ mod 3.*

Corollary 2 *[23] $\mathbf{DJ_{m,1}}$ is Bent and Negabent for m even, $m \neq 2$ mod 3.*

Proof of Theorem 3: The restriction to rows of the HT constrain α_{j-1} to be 0 and 1 over Z_2 in (6), (7), and (8). We are left with the recurrence relationship,

$$p_j = p_{j-1} + q_{j-1}, \qquad q_j = p_{j-1} - q_{j-1}$$

Self-substitution gives $p_j = 2p_{j-2}$, $q_j = 2q_{j-2}$. With $p_0 = 1$, $q_0 = -1$ we get $p_1 = 0$, $q_1 = 2$, and $p_j = 2^{\lfloor \frac{j}{2} \rfloor} p_{j \bmod 2}$, $q_j = 2^{\lfloor \frac{j}{2} \rfloor} q_{j \bmod 2}$. The HT output for a length 2^j sequence constructed using (3) comprises elements of magnitude $|p_j|$ and $|q_j|$. The theorem follows by observing that the PAPR is $\max(\frac{|p_j|^2}{2^j}, \frac{|q_j|^2}{2^j})$ ∎

[3] Although the Bent nature of $\mathbf{DJ_{m,1}}$ has also been noted previously [19, 9].

Proof of Theorem 4: The restriction to rows of the NHT constrain α_{j-1} to be 1 and 3 over Z_4, in (6), (7), and (8). We are left with the recurrence relationship,

$$p_j = p_{j-1} + iq_{j-1}, \qquad q_j = p_{j-1} - iq_{j-1}$$

where $i = \sqrt{-1}$. Self-substitution gives $p_j = 2(1+i)p_{j-3}$, $q_j = 2(1+i)q_{j-3}$. With $p_0 = 1$, $q_0 = -1$ we get $p_1 = 1-i$, $q_1 = 1+i$, $p_2 = 0$, $q_2 = 2(1+i)$, and $p_j = 2(1+i)^{\lfloor \frac{j}{3} \rfloor} p_{j \bmod 3}$, $q_j = 2(1+i)^{\lfloor \frac{j}{3} \rfloor} q_{j \bmod 3}$. The NHT output for a length 2^j sequence constructed using (3) comprises elements of magnitude $|p_j|$ and $|q_j|$. The theorem follows by observing that the PAPR is $\max(\frac{|p_j|^2}{2^j}, \frac{|q_j|^2}{2^j})$
∎

The orders, 2 and 3, of the normalised recurrence relationships in the proofs of Theorems 3 and 4, respectively, are simply the multiplicative orders of the normalised complex modular versions of the Hadamard and Negahadamard kernel matrices, respectively. In other words, for complex modulated HT,

$$(\frac{1}{\sqrt{2}})^2 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and, for complex modulated NHT,

$$(\frac{1}{\sqrt{2}})^3 \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^3 = \frac{1+i}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where $i = \sqrt{-1}$. The full order of the NHT is 24, to eliminate the complex scalar rotation. This analysis of PAPR 'orders' as j increases is related to the analysis of [3] regarding the change in Rudin-Shapiro sequence weight as length increases. Table 1 shows some PAPRs for $\mathbf{DJ_{m,1}}$ for small values of m using the HT and NHT. The HT results relate to the binary Covering Radius

Table 1: PAPRs for Binary GDJ Complementary Sequences Using the HT and NHT

m	0	1	2	3	4	5	6	7	8	9
HT PAPR	1.0	2.0	1.0	2.0	1.0	2.0	1.0	2.0	1.0	2.0
NHT PAPR	1.0	1.0	2.0	1.0	1.0	2.0	1.0	1.0	2.0	1.0

problem for RM$(1, m)$ which seeks to determine the maximum Hamming distance, d, a length 2^m binary vector can be from RM$(1,m)$ [15, 20, 6]. For m even, $d = 2^{m-1} - 2^{\frac{m-2}{2}}$. For $m = 3,5,7$, $d = 2^{m-1} - 2^{\frac{m-1}{2}}$. For $m = 9,11,13$, d is known to satisfy $2^{m-1} - 2^{\frac{m-1}{2}} \leq d \leq 2^{m-1} - 2^{\frac{m-2}{2}}$, and for odd $m \geq 15$ d is known to satisfy $2^{m-1} - 2^{\frac{m-1}{2}} < d \leq 2^{m-1} - 2^{\frac{m-2}{2}}$. The PAPR of a binary sequence under the HT is related to d by,

$$\text{PAPR} = \frac{4(2^{m-1} - d)^2}{2^m}$$

Therefore, in the terminology of this paper, the best possible PAPR of a binary sequence under the HT is 1.0 for m even, 2.0 for $m = 3,5,7$, $1.0 \leq$ PAPR ≤ 2.0 for $m = 9,11,13$, and $1.0 \leq$ PAPR < 2.0 for odd $m \geq 15$. Therefore the set $\mathbf{DJ_{m,1}}$ is optimally distant from RM$(1,m)$ for all even m and odd $m < 9$, maybe optimally distant from RM$(1,m)$ for $m = 9,11,13$, and near-optimally distant from RM$(1,m)$ for odd $m \geq 15$.

A sequence which is (Almost) Orthogonal to, say, $\mathbf{F1_m}$ is not always (Almost) Orthogonal to $\mathbf{Fm_m}$, and vice versa. For instance, there are 64 binary sequences of length 8 which are (Almost) Orthogonal to $\mathbf{F1_m}$. However, only 48 of these sequences are (Almost) Orthogonal to $\mathbf{Fm_m}$, and these form the set $\mathbf{DJ_{3,1}}$. The other 16 sequences, namely,

00001101, 00011010, 01001111, 01011000, 10100111, 10110000, 11100101, 11110010,
00010110, 00111101, 01000011, 01101000, 10010111, 10111100, 11000010, 11101001,

have, for instance, a PAPR of 4.5 under the HT, and a PAPR of 2.5 under the NHT.

The results relating to the HT spectra of $\mathbf{DJ_{m,1}}$ and the associated construction of $\mathbf{DJ_{m,1}}$ have also recently been described in Theorems 4 and 5 of [5], (although not in the context of CS or the Rudin-Shapiro construction). We have further shown the (Almost) Negabent and (Almost) Constabent properties of such sequences, and the generalisation of the construction to Z_{2^h}. We have also shown the equivalence of these sequences to the (one-dimensional) GDJ CS, and their (Almost) Orthogonality to all unimodular linear functions.

4.2 Partitioning $\mathbf{L_m}$ Using CHTs

It will now be explained by example how the set of CHTs can partition $\mathbf{L_m}$ space, and how to test for Z_n-linearity. Consider, as an example, the set of matrices whose rows cover all Z_4-linear functions. The rows of HT and NHT comprise only a <u>subset</u> of the complete set of Z_4-linear functions. There are, in total, 4^m Z_4-linear functions (ignoring constant integer offsets, β) and the rows of the HT and NHT each comprise 2^m of these Z_4-linear functions. The complete set of Z_4-linear functions can be covered by the rows of all 2^m tensor sum combinations of $\mathbf{H}$ and $\mathbf{N}$. For instance, for $m = 3$ we cover all Z_4-linear functions by using the following 8 transform matrices:

$$\begin{array}{cccc} \mathbf{H} \oplus \mathbf{H} \oplus \mathbf{H}, & \mathbf{H} \oplus \mathbf{H} \oplus \mathbf{N}, & \mathbf{H} \oplus \mathbf{N} \oplus \mathbf{H}, & \mathbf{H} \oplus \mathbf{N} \oplus \mathbf{N}, \\ \mathbf{N} \oplus \mathbf{H} \oplus \mathbf{H}, & \mathbf{N} \oplus \mathbf{H} \oplus \mathbf{N}, & \mathbf{N} \oplus \mathbf{N} \oplus \mathbf{H}, & \mathbf{N} \oplus \mathbf{N} \oplus \mathbf{N} \end{array}$$

where $\mathbf{H} = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$ and $\mathbf{N} = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}$, both over Z_4.

For instance, the rows of $\mathbf{N} \oplus \mathbf{H} \oplus \mathbf{N}$ are the 8 linear functions $\{1,3\}x_0 + \{0,2\}x_1 + \{1,3\}x_2$ over Z_4.

Although $\mathbf{DJ_{m,1}}$ can be both Bent and Negabent, it is never Z_4-Bent (i.e. $\mathbf{DJ_{m,1}}$ cannot have a PAPR $= 1.0$ under all Z_4-linear transforms). For example, Table 2 shows the PAPR of $\mathbf{DJ_{4,1}}$ under all 16 tensor sum combinations of $\mathbf{H}$ and $\mathbf{N}$, where $\mathbf{N} \oplus \mathbf{H} \oplus \mathbf{N} \oplus \mathbf{N}$ is represented by **NHNN**, and so on. Table 2 shows that, although $\mathbf{DJ_{4,1}}$ is Bent (**HHHH**) and Negabent (**NNNN**), it is not Z_4-Bent. For instance, it has a PAPR $= 2.0$ using **HHNN**.

Table 2: PAPRs for Length-16 Binary GDJ Complementary Sequences Using all Z_4-Linear Transforms

Transform	**HHHH**	**HHHN**	**HHNH**	**HHNN**
PAPR	1.0	1.0	1.0	2.0
Transform	**HNHH**	**HNHN**	**HNNH**	**HNNN**
PAPR	1.0	1.0	1.0	2.0
Transform	**NHHH**	**NHHN**	**NHNH**	**NHNN**
PAPR	1.0	2.0	1.0	1.0
Transform	**NNHH**	**NNHN**	**NNNH**	**NNNN**
PAPR	2.0	1.0	2.0	1.0

We cover all Z_n-linear functions for any even n in a similar way (odd n is included as a subset of Z_{2n}-linear functions). In general the matrix partitions are the $(\frac{n}{2})^m$ different tensor sum combinations of appropriate CHT kernels. For example, when $n = 6$ we use three CHTs, $\mathbf{H} = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$, $\mathbf{S} = \begin{pmatrix} 0 & 1 \\ 0 & 4 \end{pmatrix}$

, and $\mathbf{T} = \begin{pmatrix} 0 & 2 \\ 0 & 5 \end{pmatrix}$ over Z_6. For $m = 2$ we can test the Z_6-linearity of $\mathbf{s}$ using 9 transforms, **HH**,**HS**,**HT**,**SH**,**SS**,**ST**,**TH**,**TS**,**TT**. It is evident from the above discussion that each member of $\mathbf{L_m}$ occurs as a row of one of these matrix partitions.

5 Complementary Sets

[9, 26] also present constructions for Complementary Sets of unimodular sequences over Z_{2^h} with PAPR $\leq 2^v$, for some $v > 1$. In each case we can show that these sequences have a PAPR $\leq 2^v$ under all LUUTs by use of Rudin-Shapiro-type equations. For instance, the relation,

$$\begin{gathered} |p+q+r+s|^2 + |p-q+r-s|^2 + |p+q-r-s|^2 \\ +|p-q-r+s|^2 = 4(|p|^2 + |q|^2 + |r|^2 + |s|^2) \end{gathered}$$

can be used to construct complementary sets of four sequences with PAPR ≤ 4.0 under all unimodular linear functions. [9, 26] have highlighted the one-dimensional spectral properties of these sequences. Theorem 6 of [5] has further highlighted the HT spectral properties of these sequences. The extension to larger sets of sequences, defined by further Rudin-Shapiro-type (orthogonal) equations is straightforward, but we leave the full investigation of the properties of these sequences to further work, leaving this paper to concentrate just on sequence pair constructions.

6 Seeded Extensions of $\mathbf{DJ_m}$

$\mathbf{DJ_m}$ is recursively constructed using the initial length 1 CS pair, $\mathbf{s0_0} = (0)$ and $\mathbf{s1_0} = (1)$. $\mathbf{DJ_m}$ is (Almost) Orthogonal to $\mathbf{L_m}$ precisely because $|\mathbf{f} \odot \mathbf{s0_0}|^2 + |\mathbf{f} \odot \mathbf{s1_0}|^2 = 2.0$, $\forall \mathbf{f} \in \mathbf{L_0}$. We can, instead, take any pair of length-t starting sequences $\mathbf{s0_0}$ and $\mathbf{s1_0}$, such that,

$$|\mathbf{f} \odot \mathbf{s0_0}|^2 + |\mathbf{f} \odot \mathbf{s1_0}|^2 \leq vt, \qquad \forall \mathbf{f} \in \mathbf{E_0} \tag{12}$$

where $\mathbf{E_0}$ is any desired set of length-t sequences, and v is a real value ≥ 2.0. Applying Rudin-Shapiro to these starting sequences then constructs a sequence family with PAPR $\leq v$.

Example 4. There are twelve entries in Table 8 which refer to an infinite sequence family called ${}_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$ where each sequence in the family has a PAPR $\leq v = 2.9425$ under all CDFTs. For Tables 4 to 12 $\mathbf{E_0} = \mathbf{F1_3}$. The notation and construction will become clearer as this section progresses but we first show why ${}_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$ ensures a PAPR $\leq v = 2.9425$ under all CDFTs. For example, the first entry for ${}_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$ in Table 8 describes a 'seed' with form,

$$\Theta = \tau pqr + \tau(pr + p + r) + pq + pr + q + r$$

Fixing the 'glue' variable, τ, to 0 and 1, respectively, splits the seed into a pair of sequences,

$$\mathbf{s_0} = pq + pr + q + r \qquad \text{and } \mathbf{s_1} = pqr + pq + p + q$$

We can then, for instance, assign $p = x_0, q = x_1, r = x_2$, thereby describing two length 8 starting sequences over three variables ($t = 8$). (Note here that, with $p = x_i, q = x_j, r = x_k$, we require $j - i = 1$ and $k - j = 1$, which is implied by the $1,1$ superscript of ${}_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$). We find that the sum of the power spectra of $\mathbf{s_0}$ and $\mathbf{s_1}$ has a worst-case peak of 2.9425, as required and shown in Fig 2. In this paper we propose the construction of 'seeds' by computer

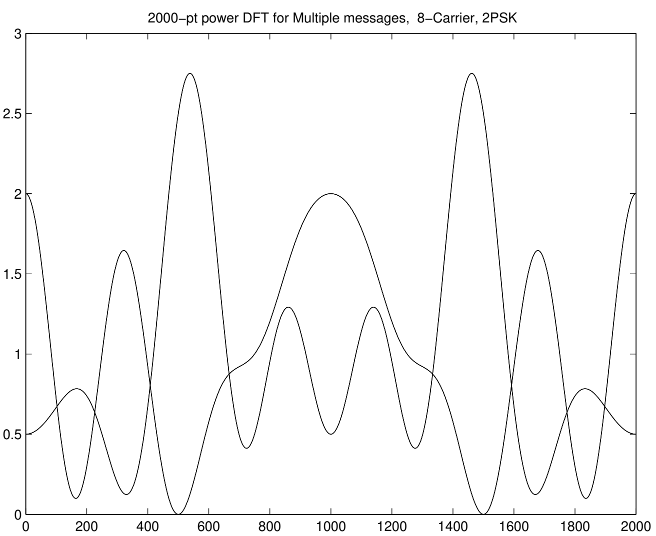

Figure 2: The Power Spectra of $\mathbf{s_0} = pq + pr + q + r$ and $\mathbf{s_1} = pqr + pq + p + q$

search for pairs of sequences with a low spectral power sum. The seed is then formed by 'joining' the sequence pair using a 'glue' variable, $\tau = x_g$.

Subsequent Rudin-Shapiro extension 'grows' on a quadratic extension which is connected to the seed at the glue variable, x_g. We now describe the seed construction more formally.

Let $t = w2^u$, w odd. We can therefore define a function for our length t starting sequences using u binary variables and one w-state variable, y. We first define an ordered subset of u integers, $\mathbf{U} = \{q_0, q_1, \ldots, q_{u-1}\}$, $\mathbf{U} \subset \mathbf{Z_m}$, $q_i \neq q_k$, $i \neq k$. We also define $\mathbf{Z'_m} = \mathbf{Z_m} \not\cap \mathbf{U}$. $\mathbf{x_U}$ is the set of binary variables $\{x_{q_0}, x_{q_1}, \ldots, x_{q_{u-1}}\}$ over which, along with y, a starting sequence is described, $\mathbf{x_{Z'_m}}$ is the set of binary variables $\{x_0, x_1, \ldots, x_{m-1}\} \not\cap \mathbf{x_U}$ over which $\mathbf{DJ_{m-u,h}}$ is described, and $\mathbf{x_{Z_m}} = \mathbf{x_U} \cup \mathbf{x_{Z'_m}}$, where $\mathbf{x_{Z_m}}$ is a set of m binary variables with output over Z_{2^h}. $\mathbf{s0_0}$ and $\mathbf{s1_0}$ are functions of y and $\mathbf{x_U}$, where y has w states. $\mathbf{s0_1}$ and $\mathbf{s1_1}$ are functions of y, $\mathbf{x_U}$, and x_g, $g \in \mathbf{Z'_m}$. We refer to x_g as the 'glue' variable. We then identify sets of seed functions $\mathbf{\Theta}(y, \mathbf{x_U}, x_g)$ derived from $\mathbf{s0_0}, \mathbf{s1_0}$ which satisfy (12) for certain fixed (preferably small) υ. We illustrate the seed construction in Fig 3, further developing the line graph representation of [26]. Each black dot symbolises a function variable. The line between two dots (variables) indicates a quadratic component comprising the variables at either end of the line. For example, a line with four consecutive black dots, x_i, x_j, x_k, x_l, indicates the quadratic extension $x_ix_j + x_jx_k + x_kx_l$.

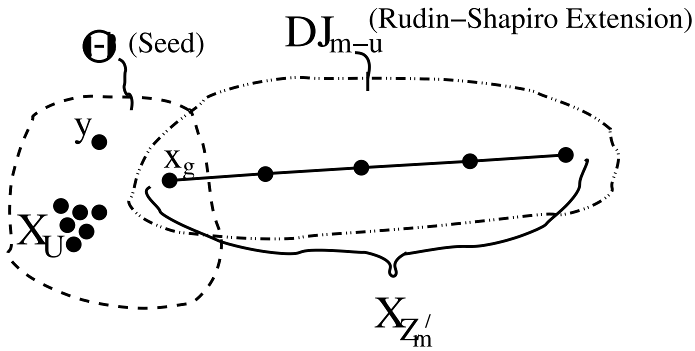

Figure 3: Seeded $\mathbf{DJ_m}$

Theorem 5 *The length $t2^{m-u} = w2^m$ sequence family $\mathbf{\Gamma}(y, \mathbf{x_{Z_m}}) = \mathbf{\Theta}(y, \mathbf{x_U}, x_g) + \mathbf{DJ_{m-u}}(\mathbf{x_{Z'_m}})$ has a correlation $\leq \sqrt{\upsilon t 2^{m-u}}$ with the length $t2^{m-u}$ sequence set $\mathbf{E_0} \oplus \mathbf{L_{m-u}}$, where υ is given by (12), and $g \in \mathbf{Z'_m}$.*

Proof: Similar to the proof for Theorem 2, but now $|p_0|^2 + |q_0|^2 \leq \upsilon t$, and the starting sequence pairs are length t, not 1. ∎

Theorem 5 allows us to construct favourable 'tensor cosets' [4] of $\mathbf{DJ_m}$ by first identifying a starting pair of sequences with desirable correlation properties, i.e. a pair which satisfy (12) for small υ, and where $\mathbf{E_0}$ may be, say, $\mathbf{F1_u}$, $\mathbf{Fm_u}$, $\mathbf{L_u}$, or something else. We don't consider $\mathbf{\Theta}$ which are, themselves, line graph extensions of smaller seeds, $\mathbf{\Theta}'$, i.e. $\mathbf{\Theta}$ satisfying the following degenerate form are forbidden: $\mathbf{\Theta}(y, \mathbf{x_U}, x_g) = \mathbf{\Theta}'(y, \mathbf{x_{U'}}, x_a) + x_a x_b + x_b x_c + \ldots + x_q x_g$, for some $a, b, c, \ldots, q, g \notin \mathbf{U}'$ but $\in \mathbf{U}$. For each algebraic form $\mathbf{\Theta}$, we can identify certain tensor symmetry operations on $\mathbf{x_U}$ which leave PAPR invariant. The specific symmetry depends on the choice of $\mathbf{E_0}$.

Lemma 1 *If* $\mathbf{E_0} = \mathbf{Fm_u}$ *the PAPR associated with Rudin-Shapiro extensions of a specific* $\mathbf{\Theta}(y, \mathbf{x_U}, x_g)$ *is invariant for all possible choices and orderings of* $\mathbf{U}$ *where* $|\mathbf{U}| = u$ *is fixed.*

Proof: From Definition 4, each tensor component of $\mathbf{f} \in \mathbf{Fm_m}$ is of the form, $(0, \delta + c)$, so swapping x_i with x_k simply swaps $(0, \delta + c)$ with $(0, \delta + c')$ to give another function, $\mathbf{f}' \in \mathbf{Fm_m}$. ∎

We now give a few example constructions which all follow from Theorem 5, coupled with Theorems 3 and 4.

Corollary 3 [5] *Let* $\mathbf{s0_0}(\mathbf{x_U})$ *and* $\mathbf{s1_0}(\mathbf{x_U})$ *be any two length* $t = 2^u$ *Bent Functions in u binary variables with output over* Z_2*, where u is even. Then* $\mathbf{\Gamma}(\mathbf{x_{Z_m}})$ *comprises (Almost) Bent functions, and when* $h = 1$*, comprises Bent functions for* $m - u$ *even and functions with PAPR* $= 2.0$ *under the HT for* $m - u$ *odd.*

Example 5: Let $\mathbf{s0_0}(\mathbf{x_U}) = x_0x_1 + x_1x_2 + x_2x_3$, $\mathbf{s1_0}(\mathbf{x_U}) = x_0x_1 + x_0x_2 + x_2x_3$ with output over Z_2. $\mathbf{s0_0}$,$\mathbf{s1_0}$ are in $\mathbf{DJ_{4,1}}$ so both are Bent. However they do not form a complementary pair. By $j = m - u$ applications of (4) with output over Z_{2^h} and with tensor permutation we can use these two sequences to generate the (Almost) Bent family,

$$\mathbf{\Gamma}(\mathbf{x_{Z_m}}) = 2^{h-1}(x_g(x_{q_1}x_{q_2} + x_{q_0}x_{q_2}) + x_{q_0}x_{q_1} + x_{q_1}x_{q_2} + x_{q_2}x_{q_3} + \sum_{k=0}^{3} b_k x_{q_k}) + 2^{h-1}\sum_{k=0}^{j-1} x_{r_k}x_{r_{k+1}} + \sum_{k=0}^{j-1} c_k x_{r_k} + d$$
$$= \mathbf{\Theta}(\mathbf{x_U}, x_g) + \mathbf{DJ_{j,h}}(\mathbf{x_{Z'_m}})$$

where $\mathbf{U} = \{q_0, q_1, \ldots, q_{u-1}\}$, $\mathbf{Z'_m} = \{r_0, r_1, \ldots, r_{m-u-1}\}$, $q_i \neq q_k$, $r_i \neq r_k$,

[4] By 'tensor-coset' we do **not** mean the well-known construction $p(x, y) = q(x) + r(y)$, which ensures that $p(x, y)$ is Bent given $q(x)$ and $r(y)$ Bent. In contrast, seed constructions of this section are not tensor decomposable.

[5] This corollary has also recently been presented in Theorems 4 and 5 of [5], but not in the context of Rudin-Shapiro constructions.

$i \neq k$, $b_k \in Z_2$, $c_k, d \in Z_{2^h}$, $g \in \mathbf{Z'_m}$. The members of $\mathbf{x_{Z_m}}$ are binary variables with output over Z_{2^h}. By Lemma 1 all possible configurations/permutations are achieved by all possible assignments of q_i, r_i to $\mathbf{Z_m}$. For $h = 1$ $\mathbf{\Gamma}(\mathbf{x_{Z_m}})$ is Bent for j even, and has a PAPR $= 2.0$ under the HT for j odd.

Corollary 4 *Let $\mathbf{s0_0}(x)$ and $\mathbf{s1_0}(x)$ be any two length $t = 2^u$ Bent and Negabent Functions in u binary variables with output over Z_2, where u is even, and $u \neq 2$ mod 3. Then $\mathbf{\Gamma}(\mathbf{x_{Z_m}})$ comprises (Almost) Bent and (Almost) Negabent functions in $m = u + j$ binary variables with output over Z_{2^h} and, when $h = 1$, comprises Bent and Negabent functions for $j = 0$ mod 6.*

Example 5 is also an example for Corollary 4.

Corollaries 3 and 4 and a similar one for Negabent sequences allows us to 'seed' many more Bent, Negabent and Bent/Negabent sequences with degree higher than quadratic. Table 3 shows the degrees of Bent, Negabent, and Bent/Negabent functions we can construct using seeds constructed from $\mathbf{DJ_{u,1}}$, where the total number of binary variables is m.

Table 3: The Degrees of $\mathbf{DJ_{u,1}}$-Seeded Bent,Negabent,Bent/Negabent Functions With Output Over Z_2

m	0	1	2	3	4	5	6	7	8	9	10
B	0		2		2		2, 3		2, 3, 4		2, 3, 4, 5
N	0	1		2	2		2, 3	2, 3		2, 3, 4	2, 3, 4
B/N	0				2		2				2, 3

B: Degrees for Bent, N: Degrees for Negabent, B/N: Degrees for Bent/Negabent

6.1 Families with Low PAPR Under all CDFTs

We now identify, computationally, sets of length-t sequence pairs over Z_2 which, by the application of (4), can be used to generate families of length $N = t2^{m-u}$ sequences over Z_{2^h} which have a PAPR $\leq v$ under **all** length-N CDFTs. In particular we find pairs of length $t = 2^u$, and present sets of length 2^m with PAPR $\leq v \leq 4.0$ in Tables 4 - 12. In [9, 26] constructions are provided for quadratic cosets of RM$(1, m)$ with PAPR upper bounds $\leq 2^k$, $k \geq 1$ under all length-N CDFTs. The seeded constructions of this paper further refine these PAPR upper bounds to include non-powers-of-two. We also present low PAPR constructions not covered in [9, 26], including those higher than quadratic.

Corollary 5 *Let* $\mathbf{s0_0}$ *and* $\mathbf{s1_0}$ *be length* $t = 2^u$ *binary sequences whose one-dimensional continuous Fourier power spectrum sum is found, computationally, to have a maximum* $= \upsilon t$*. Then the set of length* 2^m *sequences over* Z_{2^h}*, constructed from* $\mathbf{s0_0}$*,* $\mathbf{s1_0}$*, has a one-dimensional continuous Fourier PAPR* $\leq \upsilon$*. Tables 4 - 12 show such sets for* $u = 0, 1, 2, 3$ *and* $\mathbf{U} \subset \{0, 1, 2, 3, 4\}$*, for the cases* $\upsilon \leq 4.0$*.*

For the CHT examples previously discussed all choices and orderings of seed variables left PAPR invariant (Lemma 1). In the case of CDFT PAPR, however, Lemma 1 does not hold. But tensor shifts of variables do leave PAPR invariant. This leads us to modify our definition as follows. $\mathbf{U}$ is now the ordered subset of u integers, $\mathbf{U} = \{z+q_0, z+q_1, \ldots, z+q_{u-1}\}$ for integers z, q_i such that $\mathbf{U} \subset \mathbf{Z_m}$ and $q_i < q_{i+1}$. The following Lemma describes the invariance of CDFT PAPR under tensor shift.

Lemma 2 *If* $\mathbf{E_0} = \mathbf{F1_u}$ *then the PAPR associated with Rudin-Shapiro extensions of a specific* $\mathbf{\Theta}(y, \mathbf{x_U}, x_g)$ *is invariant for all possible shifts of* $\mathbf{U}$*, i.e. for all possible values of* z*, given fixed* q_i*.*

Proof: From Definition 3, each tensor component of $\mathbf{f} \in \mathbf{F1_m}$ is of the form, $(0, 2^i\delta)$, so replacing x_i with x_{i+1} is equivalent to replacing δ with $\delta/2$, where the shifted version of $\mathbf{f}$ is also in $\mathbf{F1_m}$ ∎

For example, it is found, computationally, that the normalised sum of the power spectrums of $\mathbf{s0_0} = x_0x_1+x_1+x_0$, and $\mathbf{s1_0} = x_0x_1$ under the continuous one-dimensional Fourier Transform has a maximum of 3.5396. Then one seed is $(x_g+1)(x_0x_1+x_1+x_0)+x_gx_0x_1+b_0x_0+b_1x_1 = x_0x_1+x_g(x_0+x_1)+b_0x_0+b_1x_1$, $b_0, b_1 \in \{0, 1\}$. Let p be the first element in $\mathbf{x_u}$ (x_0 in our example), q be the second (x_1 in our example), and $\tau = x_g$. One can then find this seed in Table 6 which also represents seeds derived from this seed via Lemma 2. Here is the complete set having PAPR ≤ 3.5396,

$$
\begin{aligned}
&{}_{\mathbf{3a}}\mathbf{\Gamma^1} = {}_{\mathbf{3a}}\mathbf{\Theta}(\mathbf{x_U}, x_g) + \mathbf{DJ_{m-u,h}}(\mathbf{x_{Z'_m}}), \quad \mathbf{U} = \{z, z+1\}, g \in \mathbf{Z'_m} \\
&\text{where} \\
&{}_{\mathbf{3a}}\mathbf{\Theta}(p, q, \tau) = 2^{h-1}(pq + \tau(q+p) + b_1q + b_0p), \quad b_0, b_1 \in \{0, 1\}
\end{aligned}
$$

where x_i outputs over $Z_{2^h}, \forall i$. The e of ${}_{\mathbf{e}}\mathbf{\Gamma^{s_0}}$ and ${}_{\mathbf{e}}\mathbf{\Theta}$ is an arbitrary categorisation label for the specific seed, and the s_i of ${}_{\mathbf{e}}\mathbf{\Gamma^{s_0,s_1,\ldots,s_{u-2}}}$ describe the tensor-shift-invariant pattern of variable indices associated with this seed, where $s_{i-1} = q_i - q_{i-1}$. For instance, for our example, ${}_{\mathbf{3a}}\mathbf{\Gamma^1}$, we could choose

$\mathbf{U} = \{2,3\}$, where the seed is built from the ANF form ${}_{\mathbf{3a}}\mathbf{\Theta}$, thus the ANF form $x_2x_3 + x_0(x_3 + x_2) + x_2 + x_0x_4 + x_4x_5 + x_1x_5 + x_1 + 1$ has a PAPR ≤ 3.5396, where we have constructed our seed over x_2, x_3, and x_0, 'attached' the line graph $x_1x_5 + x_5x_4 + x_4x_0$ to it, connecting at $x_g = x_0$, and added the linear terms $x_2 + x_1 + 1$. As another example, the following set has PAPR ≤ 3.8570,

$${}_{\mathbf{3a}}\mathbf{\Gamma^2} = {}_{\mathbf{3a}}\mathbf{\Theta}(\mathbf{x_U}, x_g) + \mathbf{DJ_{m-u,h}}(\mathbf{x_{Z'_m}}), \quad \mathbf{U} = \{z, z+2\}, g \in \mathbf{Z'_m}$$

${}_{\mathbf{3a}}\mathbf{\Gamma^2}$ has exactly the same algebraic structure as ${}_{\mathbf{3a}}\mathbf{\Gamma^1}$, but ${}_{\mathbf{3a}}\mathbf{\Theta}$ is, instead, constructed over x_0, x_2, x_g. The sets ${}_{\mathbf{3a}}\mathbf{\Gamma^s}$ are quadratic sets so, when $h = 1$, the union of the sets ${}_{\mathbf{3a}}\mathbf{\Gamma^s}$ with $\mathbf{DJ_{m,1}}$ is a set of binary quadratic forms, so retains minimum Hamming distance of 2^{m-2}. Tables 4 - 12 show $\mathbf{\Gamma}$-sets using 1,2,3,4-variable seeds with PAPR ≤ 4.0. We use reversal symmetry to halve the number of inequivalent representatives for some $\mathbf{\Gamma}$ sets, (indicated by 'with R'). Reversal symmetry for functions of binary variables is equivalent to replacing each x_i with $x_i + 2^{h-1}$. Reversal does not change the algebraic degree of the seeds, $\mathbf{\Theta}$.

Table 4: Rudin-Shapiro Extensions Using $u + 1 = 1$-Variable Seeds (the set $\mathbf{DJ_{m,h}}$)

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(\tau)}{2^{h-1}}$	υ	χ
${}_{\mathbf{0}}\mathbf{\Gamma}$	0	2.00	0

Table 5: Rudin-Shapiro Extensions Using $u + 1 = 2$-Variable Seeds

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(x_z,x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,\tau)}{2^{h-1}}$	υ	χ
${}_{\mathbf{1}}\mathbf{\Gamma}$	b_0p	4.00	0

$b_0 \in \{0, 1\}$

${}_{\mathbf{1}}\mathbf{\Gamma}$ of Table 5 is an alternative derivation for the PAPR ≤ 4.0 bound of the complementary set of Section 5. The χ-value of each $\mathbf{\Gamma}$-set, as shown in Tables 4 - 12, is a threshold on or below which a given $\mathbf{\Gamma}$-set overlaps with other $\mathbf{\Gamma}$-sets, i.e. where Rudin-Shapiro extensions of $\mathbf{\Theta}$ equal Rudin-Shapiro extensions of $\mathbf{\Theta}'$, $\mathbf{\Theta} \neq \mathbf{\Theta}'$. Consider a seed extension of the form

Table 6: Rudin-Shapiro Extensions Using $u+1 = 3$-Variable Seeds, All Cosets of RM$(1,1)$ in p

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U},x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,\tau)}{2^{h-1}}$	υ	χ
${}_{\mathbf{2}}\mathbf{\Gamma^1}$	$pq\tau+$ $\{pq+q,q\}$ with R	3.0000	0
${}_{\mathbf{3}}\mathbf{\Gamma^1}$	$pq+b_1q$	3.5396	1
${}_{\mathbf{3a}}\mathbf{\Gamma^1}$	$pq+\tau(q+p)+b_1q$	3.5396	0
${}_{\mathbf{3}}\mathbf{\Gamma^2}$		3.8570	1
${}_{\mathbf{3a}}\mathbf{\Gamma^2}$		3.8570	0
${}_{\mathbf{3}}\mathbf{\Gamma^3}$		3.9622	1
${}_{\mathbf{3a}}\mathbf{\Gamma^3}$		3.9622	0
${}_{\mathbf{3}}\mathbf{\Gamma^4}$		3.9904	1
${}_{\mathbf{3a}}\mathbf{\Gamma^4}$		3.9904	0
${}_{\mathbf{3}}\mathbf{\Gamma^5}$		3.9976	1
${}_{\mathbf{3a}}\mathbf{\Gamma^5}$		3.9976	0
${}_{\mathbf{4}}\mathbf{\Gamma^1}$	$\tau(p+q)+b_1q$	4.0000	1
${}_{\mathbf{4}}\mathbf{\Gamma^2}$		4.0000	
${}_{\mathbf{4}}\mathbf{\Gamma^3}$		4.0000	
${}_{\mathbf{4}}\mathbf{\Gamma^4}$		4.0000	
${}_{\mathbf{4}}\mathbf{\Gamma^5}$		4.0000	

$b_1 \in \{0,1\}$

shown in Fig 4. The seed shows three subsidiary quadratic extensions other than the primary extension. These subsidiary extensions qualify as Rudin-Shapiro extensions if they have no quadratic offshoots and if their constituent variables do not occur elsewhere in the seed (other than in linear terms). In Fig 4 the maximum length of a subsidiary quadratic extension comprises 4 variables. We therefore set $\chi = 4$ for this seed and state that $\mathbf{\Gamma}$, the Rudin-Shapiro extension of $\mathbf{\Theta}$, only becomes **active** when extended by χ variables from x_g, i.e. when $m-u = \chi+1$. Consider Fig 5. Here $\chi = 3$ and $\mathbf{\Gamma}$ becomes active only when extended by $\chi = 3$ variables. Only enumerating active $\mathbf{\Gamma}$ avoids repeated counts. However, this way of counting does not deal with the case when two or more $\mathbf{\Gamma}$ are identical, inactive, and all extended by $\chi - 1$ variables for their respective χ. At the moment we can only count these cases by hand or by computer. χ is an indication of the level of extension required

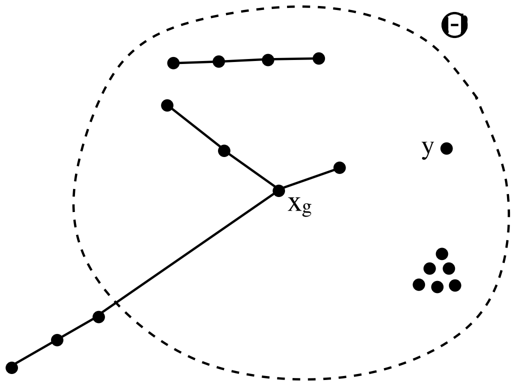

Figure 4: Seed with Subsidiary Quadratic Extensions, $\chi = 4$

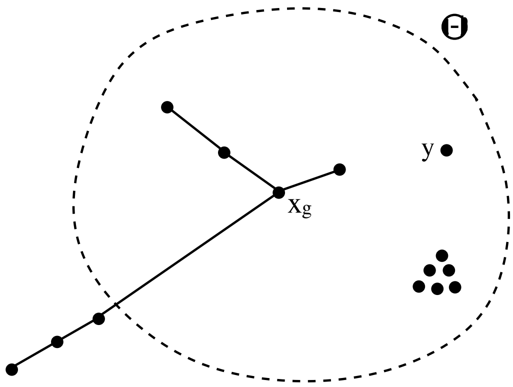

Figure 5: Seed with Subsidiary Quadratic Extensions, $\chi = 3$

before a certain $\mathbf{\Gamma}$-set is wholly disjoint from other $\mathbf{\Gamma}$-sets under consideration. The lack of disjointness between $\mathbf{\Gamma}$-sets makes sequence enumeration for a union of $\mathbf{\Gamma}$-sets non-trivial at extensions $\leq \chi$. This is an important drawback of the seed extension technique.

The size of each $\mathbf{\Gamma}$-set is shown in Tables 13 - 14, where all sizes are given relative to the size, D, of $\mathbf{DJ_{m,h}}$.

6.1.1 Some Comments on Code Rate Versus PAPR Versus Distance

In the following we define a quadratic, cubic, quartic code, etc..., as being a codeset comprising functions with degrees ≤ 2, ≤ 3, ≤ 4, ...etc, respectively.

The underlying aim of [9, 26] is to find a largest possible family of sequences, $\mathbf{S}$, roughly orthogonal to the set $\mathbf{F1_m}$ and roughly orthogonal to every other member of $\mathbf{S}$. As discussed in [27], these three aims, PAPR vs Distance vs Rate, work against each other. The solution of [9, 26] in a binary context proposes $\mathbf{S}$ comprising selected $\mathrm{RM}(2,m)$ cosets of $\mathrm{RM}(1,m)$, thereby ensuring Hamming Distance $\geq 2^{m-2}$ for binary sequences of length 2^m. The complete set of $\mathrm{RM}(2,m)$ cosets of $\mathrm{RM}(1,m)$ is a significant proportion of $Z_2^{2^m}$ up to about $m = 5$, so for $2 \leq m \leq 5$ one can obtain quadratic codes with good PAPR/distance/code rate trade-off. [9, 26] propose quadratic codes comprising the infinite family $\mathbf{DJ_{m,1}}$ together with further $\mathrm{RM}(2,m)$ cosets of $\mathrm{RM}(1,m)$ identified computationally to have low worst-case PAPR over the whole coset. This computational search is practical up to about $m = 6$, where there are 2^{22} sequences with algebraic degree $= 2$ to search, of which about 2^{16} are from $\mathbf{DJ_{m,1}}$. A hardware implementation requires a ROM to store those coset leaders not in $\mathbf{DJ_{m,1}}$. Using the results of [26] one can reduce the size of this ROM by constructing some of these sequences using the infinite family derived from complementary sets of size 4 with PAPR ≤ 4.00 (this family is also $\mathbf{_1\Gamma}$ of Table 6). Our paper further introduces infinite quadratic families $\mathbf{_3\Gamma}$, $\mathbf{_{3a}\Gamma}$, $\mathbf{_4\Gamma}$,$\mathbf{_{18}\Gamma}$, $\mathbf{_{18a}\Gamma}$, $\mathbf{_{19}\Gamma}$, $\mathbf{_{19a}\Gamma}$,$\mathbf{_{20}\Gamma}$, $\mathbf{_{20a}\Gamma}$,$\mathbf{_{21}\Gamma}$, $\mathbf{_{22}\Gamma}$, $\mathbf{_{23}\Gamma}$, $\mathbf{_{24}\Gamma}$,$\mathbf{_{25}\Gamma}$, which also have PAPRs ≤ 4.0. The inclusion of these sets can further reduce ROM size. However, those $\mathbf{\Gamma}$-sets identified above, and comprising seeds over $T \leq 4$ variables do not provide disjoint sequence sets until $m = T+\chi+1$ which, worst-case, is $m = 7$ for $\chi = 2$, by which time quadratic codes have lost their rate and are not so practical. For about $5 \leq m \leq 7$ cubic codes comprising sequences with algebraic degree ≤ 3 are desirable as they maintain a good code rate whilst ensuring a Hamming Distance $\geq 2^{m-3}$. Similarly, quartic codes are desirable for $7 \leq m \leq 9$, and so on. To emphasise this point, [27] highlights that asymptotically good PAPR codes exist with constant rate, distance growing with $\sqrt{N}$, and PAPR growing with $\log N$ (it is an open problem to find code constructions satisfying these constraints). We observe that choosing a low PAPR subset of the sequences with algebraic degree $\leq \frac{m-1}{2}$ and length 2^m ensures we are selecting from a constant rate subspace of the whole space, and that the code distance remains upper bounded by $\sqrt{2}\sqrt{N}$. It remains to show that the low PAPR subset is a constant rate subset of this subspace with PAPR growing with $\log N$. The seed technique of this paper offers many infinite cubic families with low PAPR but cubic seeds can only be searched up to seeds of about 4 variables [6], so we cannot get enough cubics this way to justify a cubic-based low PAPR code. The full usefulness of the seed technique will only become apparent if a method can be found to construct seeds (as opposed to computational search). The authors currently know of no such method and it is left as an open problem. In general we note that a reasonable rate, low PAPR, Reed-Muller-based code of length 2^m, and with good distance, should comprise Algebraic Normal Forms of degree $\leq \lfloor \frac{m}{2} \rfloor$ (or thereabouts).

7 The Set, $\mathbf{G_m}$, of Linear Complex Modulated Sequences and its Distance From $\mathbf{DJ_m}$

Previous sections have focussed on unimodular binary linear functions which are (Almost) Orthogonal to $\mathbf{DJ_m}$. In this section we examine the distance of all binary linear functions in m variables with output over the complex plane from $\mathbf{DJ_m}$. The previous restriction to unimodular sequences allowed us to present our arguments using the integer field/ring Z_n. In this section we must use the complex-modulated form for sequences and basis functions, as we are now also dealing with sequence elements with non-unity magnitude. Thus $\mathbf{DJ_m}$ in this section refers to the complex-modulated form of $\mathbf{DJ_m}$.

Definition 11 *Let* $\mathbf{s}$, $\mathbf{f}$ *be length* N *vectors with complex elements* s_j, f_j, *respectively, such that* $\sum_{i=0}^{N-1} |s_i|^2 = \sum_{i=0}^{N-1} |f_i|^2 = N$. *Then the correlation of* $\mathbf{s}$ *and* $\mathbf{f}$ *is given by,*

$$\mathbf{s} \cdot \mathbf{f} = \sum_{j=0}^{N-1} s_j f_j^*$$

where * *means complex conjugate.*

This definition agrees with the definition of correlation for unimodular sequences at the beginning of this paper. The definitions of 'Orthogonality'...etc are equivalent to those at the beginning of the paper, where $\odot$ is replaced by $\cdot$. Remembering that complex-modulated $\mathbf{DJ_{m,h}}$ is the set of all length 2^m 'Phase-Shift-Keyed' (PSK) sequences with 2^h equally-spaced phases and unity magnitude, we state the following.

[6] Unlike quadratic seeds, PAPR equivalence classes for cubics do not conveniently fall into cosets of $\mathrm{RM}(1, m)$, so such symmetries cannot be used to reduce computational search time for cubic classes.

Theorem 6 *For* $\mathbf{s} \in \mathbf{DJ_m}$ *and* $\mathbf{g} \in \mathbf{G_m}$ [7], $|\mathbf{g} \cdot \mathbf{s}|^2 \leq 2^{2m-\lfloor \frac{m}{2} \rfloor}$.

Proof: Once again the proof hinges on the Rudin-Shapiro equality of (9), but this time $|\phi|^2$ is not necessarily equal to $|\theta|^2$. We only require, for normalisation, that $|\phi|^2 + |\theta|^2 = 2$. Let p_j, q_j be complex numbers satisfying,

$$p_j = \mathbf{g_j} \cdot \mathbf{s0_j}, \qquad q_j = \mathbf{g_j} \cdot \mathbf{s1_j} \tag{13}$$

where $\mathbf{g_j} \in \mathbf{G_j}$ and $\mathbf{s0_j}, \mathbf{s1_j}$ are a complementary pair in $\mathbf{DJ_j}$. Let,

$$\mathbf{g_j} = \mathbf{g_{j-1}} \otimes (\phi_j, \theta_j) \tag{14}$$

where $|\phi_j|^2 + |\theta_j|^2 = 2$. Then, using similar reasoning to that in (7) and (8),

$$p_j = \phi_{j-1}p_{j-1} + \theta_{j-1}q_{j-1}, \qquad q_j = \phi_{j-1}p_{j-1} - \theta_{j-1}q_{j-1} \tag{15}$$

Using (9) we get,

$$|p_j|^2 + |q_j|^2 = 2(|\phi_{j-1}|^2|p_{j-1}|^2 + |\theta_{j-1}|^2|q_{j-1}|^2) \tag{16}$$

Moreover, self-substitution in (15) gives,

$$\begin{array}{l} p_j = (\phi_{j-1} + \theta_{j-1})\phi_{j-2}p_{j-2} + (\phi_{j-1} - \theta_{j-1})\theta_{j-2}q_{j-2} \\ q_j = (\phi_{j-1} - \theta_{j-1})\phi_{j-2}p_{j-2} + (\phi_{j-1} + \theta_{j-1})\theta_{j-2}q_{j-2} \end{array} \tag{17}$$

We are interested in finding the largest possible values of $|p_j|$ or $|q_j|$, as j increases. We note the following,

$$\begin{array}{c} |\phi_{j-1} + \theta_{j-1}|^2 + |\phi_{j-1} - \theta_{j-1}|^2 = 4, \\ |\phi_{j-2}|^2 + |\theta_{j-2}|^2 = 2, \qquad |p_{j-2}|^2 + |q_{j-2}|^2 = k^2 \end{array}$$

for k some arbitrary real constant. It can be seen from (17) that $|p_j|^2 + |q_j|^2$ will be maximised if all energy is concentrated in just one of the four three-term products on the right-hand side of the two equations of (17). Without loss of generality we aim to maximise $|p_j|$ using Condition A:

$$\begin{array}{c} \text{Condition A:} \\ |\phi_{j-1} + \theta_{j-1}|^2 = 4, |\phi_{j-2}|^2 = 2, |p_j|^2 = k^2, \qquad j \text{ odd} \end{array}$$

From (17) this gives $|p_j| = 2\sqrt{2}$, $|q_j| = 0$ which conveniently concentrates all energy in p_j ready for the next application of (17) using Condition A.

[7] see Definition 6

We conclude that, given $|p_{j-i}| = k$, $|q_{j-1}| = 0$, i even, the largest possible value of $|p_j|$ (or $|q_j|$) is $(2\sqrt{2})^{\frac{i}{2}}k$. Secondly we note that $|p_0| = |q_0| = 1$. Consequently, from (15), $|p_1|^2 + |q_1|^2$ is maximised by choosing $|\phi_0| = |\theta_0| = 1$. We can also choose the phase angles of ϕ_0 and θ_0 so that $|p_1| = 2$, $|q_1| = 0$, which concentrate all energy in p_1, ready for subsequent iterations using (17) under Condition A. At all stages in the above arguments we have achieved maximisation of $|p_j|$. In this way we guarantee that maximum $|p_j| = (2\sqrt{2})^{\frac{j-1}{2}}2 = 2^{\frac{3j+1}{4}}$, j odd. Finally, for $|p_j| = 2^{\frac{3j+1}{4}}$, j odd, we know that $|q_j| = 0$. Therefore, from (15), $|p_{j+1}|$ is a maximum if $|p_{j+1}| = 2^{\frac{3j+3}{4}}$, j odd. Putting all the above arguments together,

$$|p_j|^2 \leq 2^{2j-\lfloor\frac{j}{2}\rfloor}, \qquad |q_j|^2 \leq 2^{2j-\lfloor\frac{j}{2}\rfloor} \tag{18}$$

whatever the choices for ϕ_i, θ_i, $0 \leq i < j$. ∎

The action of an LUT (Definition 7) on a sequence from $\mathbf{DJ_m}$ leaves the average power of the sequence invariant. A corollary of Theorem 6 is, therefore,

Corollary 6 *The action of an LUT on a sequence from* $\mathbf{DJ_m}$ *gives an output spectrum with PAPR* $\leq \frac{2^{2m-\lfloor\frac{m}{2}\rfloor}}{2^m} = 2^{m-\lfloor\frac{m}{2}\rfloor}$.

Example 6: An LUT, $\mathbf{G}$, which always achieves the worst-case PAPR of $2^{m-\lfloor\frac{m}{2}\rfloor}$ from at least one member of $\mathbf{DJ_m}$ is as follows,

$$\mathbf{G} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix} \otimes \ldots$$

For instance,
$\mathbf{G_3}(1,-1,1,1,-1,1,1,1)^T = (0,0,4\sqrt{2},0,0,4\sqrt{2},0,0)^T$, with PAPR $= \frac{32}{8} = 4$.

7.1 A Lower Bound on the Correlation Between Any Length 2^m Unimodular Sequence and $\mathbf{G_m}$

Consider the length 2^m sequence, $\mathbf{s}$, over Z_P, which represents a function in m binary variables. Then we can write $\mathbf{s}$ in Algebraic Normal Form as,

$$\mathbf{s}(x_0, x_1, \ldots, x_{m-1}) = \sum_{v \in Z_2^m} c_v \prod_{i=0}^{m-1} x_i^{v_i}, \quad \text{where } c_v \in Z_P$$

Theorem 7 *The sequence* $\mathbf{s}$ *has a correlation of at least* $(2^{\frac{t}{2}})2^{m-t}$ *with at least one member of* $\mathbf{G_m}$*, where* t *is the minimum number of variables,* x_i*, that one must fix to a constant value from* Z_P *so as to reduce* $\mathbf{s}$ *to a linear function with output over* Z_P *in* $m-t$ *variables.*

Proof: We illustrate the proof by example. Consider a sequence from $\mathbf{DJ_m}$. For instance, consider a binary sequence, $\mathbf{s}$, with quadratic part, say, $x_0x_2+x_2x_3+x_3x_5+x_5x_1+x_1x_4$. We only need to fix x_0, x_3, x_1, or x_2, x_3, x_1, or x_2, x_5, x_1, or x_2, x_5, x_4, to some constants from Z_∞ to ensure that $\mathbf{s}$ reduced in this way is a linear function, $\mathbf{s_r}$, of 3 variables with output over Z_∞. In this case $t = 3$, and performing a $2^t = 8$-point HT on any of the $2^{m-t} = 8$ length-8 linear subsequences, $\mathbf{s_r}$, results in a maximum spectral value of $2^{m-t} = 8$. The HT is implicitly expanded to cover m variables by tensor multiplication with the $2^t \times 2^t$ identity matrix, which must be scaled by $\sqrt{2}^t$ to normalise so that each row of the resultant matrix is in $\mathbf{G_m}$. ∎
Example 6 is also a specific instance of Theorem 7 for $\mathbf{DJ_m}$. Theorem 7 applies to any function, not just members of $\mathbf{DJ_m}$. However, for sequences from $\mathbf{DJ_m}$ we have the following corollary.

Corollary 7 *For* $\mathbf{s} \in \mathbf{DJ_m}$*,* $\exists \mathbf{g} \in \mathbf{G_m}$ *such that* $|\mathbf{g} \cdot \mathbf{s}|^2 \geq 2^{2m-\lfloor \frac{m}{2} \rfloor}$.

Proof: As evident from the proof of Theorem 7, when m is even (odd) we need to fix $\frac{m}{2}$ ($\lfloor \frac{m}{2} \rfloor$) variables to reduce $\mathbf{s}$ to a linear function, respectively. This linear function has a maximum correlation with a row of the HT of $\lfloor 2^{\frac{m}{2}} \rfloor$). After scaling by $\sqrt{2}^{\lceil \frac{m}{2} \rceil}$ and taking squares we arrive at Corollary 7. ∎
The lower bound of Corollary 7 is identical to the upper bound of Theorem 6.

Corollary 8 *For* $\mathbf{s} \in \mathbf{DJ_m}$*, only 1 out of the* $\binom{m}{\lfloor \frac{m}{2} \rfloor}$ *possible choices of variables to fix reduces* $\mathbf{s}$ *to a linear function when* m *is odd, and only* $\frac{m}{2}+1$ *out of the* $\binom{m}{\frac{m}{2}}$ *possible choices of variables to fix reduces* $\mathbf{s}$ *to a linear function when* m *is even.*

In the context of unitary matrices we also have the following corollary of Theorem 7.

Corollary 9 $\exists$ *an LUT such that any member of* $\mathbf{DJ_m}$ *has PAPR* $\geq 2^{m-\lfloor \frac{m}{2} \rfloor}$ *under this LUT. linear function.*

The upper bound of Corollary 9 is identical to the lower bound of Corollary 6.

The conclusion from this section is that unimodular sequences are open to correlation attack from LUTs if fixing a small number of variables projects the sequence to a linear function. However, finding LUTs which exploit this weakness becomes more costly as the number of variables to fix rises. In particular, from Corollary 8, $\mathbf{DJ_m}$ seems relatively secure from LUT attack. We can also use the 'weakness' of $\mathbf{DJ_m}$ to develop an efficient decoder for $\mathbf{DJ_m}$-based OFDM (an alternative to the schemes of [18, 22]) where a correlation peak identifies the codeword sent. Another way of looking at the properties of $\mathbf{DJ_m}$ is to consider the Quantum Entangling properties of the Rudin-Shapiro recursion. The (Almost) Orthogonality of $\mathbf{DJ_m}$ to $\mathbf{L_m}$ can be interpreted as strong quantum entanglement in a certain quantum axis and suggests that Rudin-Shapiro recursion is a good Quantum Entangling primitive, but the weaker (Rough) Orthogonality of $\mathbf{DJ_m}$ to $\mathbf{G_m}$ indicates a moderation in the entanglement strength of $\mathbf{DJ_m}$ in another quantum axis. These connections are discussed in [24] where it is shown how Rudin-Shapiro recursion can be used to construct good error-correcting codes which, in turn, represent highly entangled quantum states.

8 A Representation For All $2^m \times 2^m$ Unitary Matrices with Linear Rows

Whereas multidimensional CHTs can be described as tensor products of 2×2 matrices, the one-dimensional CDFTs also require the inclusion of 'twiddle factors' [7, 1]. This section outlines a tensor decomposition for **all** LUTs. Radix-2 CHTs and CDFTs are then seen as instances of this decomposition. Consider the length 2^m binary sequence $\mathbf{s}(x_0, x_1, \ldots, x_{m-1})$. Then a $2^m \times 2^m$ LUT matrix, $\mathbf{Q}$, which only acts on variable i of the complex-modulated form of $\mathbf{s}$ can be represented as,

$$\mathbf{Q} = \mathbf{I_i} \otimes \mathbf{Q(i)} \otimes \mathbf{I_{m-i-1}}$$

where $\mathbf{I_k}$ is the $2^k \times 2^k$ identity matrix, and $\mathbf{Q(i)}$ is a 2×2 LUT matrix. We refer to the action of $\mathbf{Q}$ on variable i by $\mathbf{Q(i)}$, where the context of m variables is implicit. In a similar way we refer to LUUT diagonal matrices $\mathbf{\Delta(i, k)}$ which only act on variables i and k out of m variables.

Theorem 8 *(Based on the 'Quantum FFT Algorithm' of [8, 32]). All LUTs, $\mathbf{G}$, can be represented by the following decomposition.*

$$\mathbf{G} = \mathbf{P}\mathbf{Q_0}(\mathbf{0})\mathbf{\Delta_1}\mathbf{Q_1}(\mathbf{1})\mathbf{\Delta_2}\mathbf{Q_2}(\mathbf{2})\ldots\mathbf{\Delta_{m-1}}\mathbf{Q_{m-1}}(\mathbf{m-1})$$

where $\mathbf{\Delta_k}$ is a diagonal matrix whose diagonal entries are all unimodular and $\mathbf{P}$ is any permutation matrix which permutes the rows of $\mathbf{G}$.

The radix-2 linearity of the rows of $\mathbf{G}$ (Definitions 6 and 7) is ensured because each $\mathbf{Q_k}$ acts on only one variable at a time, and because the only other matrices in the decomposition of $\mathbf{G}$ are row permutations or diagonal. Consider the following sub-cases:

- For CHTs we have,

  $$\mathbf{\Delta_k} = \mathbf{I_m}, \qquad \mathbf{Q_k} = \begin{pmatrix} 1 & \epsilon^{\delta_k} \\ 1 & -\epsilon^{\delta_k} \end{pmatrix}, \qquad \forall k$$

  where ϵ is a non-degenerate n^{th}complex root of 1, $0 \leq \delta_k < \frac{n}{2}$, $1 \leq n \leq \infty$, $\gcd(\delta_k, \frac{n}{2}) = 1$, n even. $\mathbf{P}$ is the identity matrix.
  Example 7. The 4×4 HT is decomposed as,

  $$\mathbf{Q}(\mathbf{0})\mathbf{Q}(\mathbf{1}) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

- For CDFTs we have,

  $$\mathbf{\Delta_i} = \prod_{k=0}^{i-1} \mathbf{\Delta}(\mathbf{i}, \mathbf{k})$$

  where $\mathbf{\Delta}(\mathbf{i}, \mathbf{k})$ acts on variables i and k [8], and is of the form,

  $$\mathbf{\Delta}(\mathbf{i}, \mathbf{k}) = \mathrm{Diag}(1, 1, 1, \epsilon^{2^{m-1-(i-k)}})$$

  $$\text{and,} \qquad \mathbf{Q_k} = \begin{pmatrix} 1 & \epsilon^{2^k\delta} \\ 1 & -\epsilon^{2^k\delta} \end{pmatrix}$$

  where ϵ is a non-degenerate nth complex root of 1, $0 \leq \delta < \frac{n}{2}$, $1 \leq n \leq \infty$, $\gcd(\delta, \frac{n}{2}) = 1$. $\mathbf{P}$ is the 'bit-reversal' permutation reversing the roles of x_0 and x_{m-1}, x_1 and x_{m-2},...etc.

[8]This specific decomposition of Δ is due to [8] and allows implementation of the FFT as a series of unitary matrices acting on only one or two variables per matrix.

Example 8. The 8×8 one-dimensional DFT is decomposed as,

$$\mathbf{PQ}(\mathbf{0})\mathrm{Diag}(1,1,1,\epsilon^2,1,1,1,\epsilon^2)\mathbf{Q}(\mathbf{1})\times$$
$$\mathrm{Diag}(1,1,1,1,1,\epsilon,1,\epsilon)\mathrm{Diag}(1,1,1,1,1,1,\epsilon^2,\epsilon^2)\mathbf{Q}(\mathbf{2})$$

where $\mathbf{Q} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, and $\epsilon = e^{\frac{\pi i}{4}}$, $i^2 = -1$.

9 Discussion and Conclusions

We have shown that Golay-Davis-Jedwab Complementary Sequences, $\mathbf{DJ_m}$, are (Almost) Orthogonal to the set $\mathbf{L_m}$ of all linear functions in m binary variables, and therefore have PAPR $\leq$ 2.0 under all Linear Unimodular Unitary Transforms (LUUTs). We identified two transform subsets of LUUTs, namely one-dimensional Consta-Discrete Fourier Transforms, and m-dimensional Constahadamard Transforms (CHTs), both of whose rows are from $\mathbf{L_m}$. We further showed that rows of all CHTs partition $\mathbf{L_m}$, and therefore that CHTs provide efficient transforms for testing Z_n-linearity. Using the Rudin-Shapiro construction we identified many seeds from which to construct infinite sequence families with (Almost) Constabent properties, and other seeds with low PAPR under one-dimensional Consta-DFTs. In this way we have identified new low PAPR families not necessarily limited to quadratic degree. These families are of particular importance with relation to the requirement for large families of sequences with low PAPR and good Hamming Distance for Orthogonal Frequency Division Multiplexing transmission [9, 26]. One of the contributions of this paper in this context is to provide more infinite families with low PAPR and good distance in addition to $\mathbf{DJ_m}$. Their union provides codes with improved rate and smaller hardware implementation. The low degree (e.g. quadratic, cubic) ensures good Hamming distance for the combined families. We also determined the distance of $\mathbf{DJ_m}$ from the set, $\mathbf{G_m}$, of complex linear functions in m variables, where $\mathbf{G_m}$ contains $\mathbf{L_m}$. In transform terminology these results imply a PAPR $\leq 2^{m-\lfloor\frac{m}{2}\rfloor}$ under all Linear Unitary Transforms (LUTs) constructed from members of $\mathbf{G_m}$. Consequently ciphers which incorporate the set $\mathbf{DJ_m}$ are highly resistant to correlation attack from transforms with unimodular rows (LUUTs), but there exist rare unitary transforms with non-unimodular rows (LUTs) which can yield a PAPR as high as $2^{m-\lfloor\frac{m}{2}\rfloor}$ from members of the set, $\mathbf{DJ_m}$. However, this is not so high. The linear nature of the LUT rows implies that they possess a radix-2 tensor decomposition into tensor products of 2×2 LUT matrices together with optional inter-product twiddle factors, as discussed in the last section. This tensor decomposition translates to an efficient software or hardware implementation to compute correlations with members of $\mathbf{G_m}$. These LUTs therefore have $\mathrm{O}(N \log N)$ complexity algorithms, which simultaneously imply cryptographic weakness and efficient decoding algorithms for any codeset which has a pronounced spectral peak under one or more LUTs. We should emphasise that the combined size of the new infinite sequence families provided by this paper cannot maintain overall code rate without substantial computational search to find suitable low PAPR pairs. This computational overhead (and consequent ROM storage overhead) soon becomes prohibitive for increasing sequence length. We therefore need some way to efficiently construct seeds. Finally, we reiterate the open problem, posed by [27], namely to discover an infinite construction for an asymptotically good error-correcting code with low PAPR.

References

[1] R.E.Blahut, **Fast Algorithms for Digital Signal Processing,** Reading, Addison-Wesley, 1985

[2] S.Boyd, "Multitone Signals with Low Crest Factor," *IEEE Trans Circuits Syst*, Vol 33,No 10,pp 1018-1022, Oct 1986

[3] J.Brillhart,P.Morton, "A Case Study in Mathematical Research: The Golay-Rudin-Shapiro Sequence," *American Mathematical Monthly*, Vol 103, Part 10, pp 854-869, 1996

[4] S.Z.Budisin, "New Complementary Pairs of Sequences," *Electron. Lett.*, Vol 26, pp. 881-883, 1990

[5] A.Canteaut,C.Carlet,P.Charpin,C.Fontaine, "Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions," *EUROCRYPT 2000, Lecture Notes in Comp. Sci.*, Vol 1807, pp. 507-522, 2000

[6] G.D.Cohen,M.G.Karpovsky,H.F.Mattson Jr., "Covering Radius-Survey and Recent Results," *IEEE Trans. Inform. Theory*, Vol IT-31, pp. 328-343, May 1985

[7] J.W.Cooley,J.W.Tukey, "An Algorithm for the Machine Calculation of Complex Fourier Series", *Math. Comput.*, Vol 19, No 2, pp 297-301, 1965

[8] D.Coppersmith, "An Approximate Fourier Transform Useful in Quantum Factoring", *IBM Research Rep.* No. 19642, 1994

[9] J.A.Davis,J.Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *IEEE Trans. Inform. Theory*, Vol 45, No 7, pp 2397-2417, Nov 1999

[10] R.L.Frank, "Polyphase Complementary Codes," *IEEE Trans on Information Theory*, Vol 26, No 6, pp 641-647, Nov 1980

[11] M.J.E.Golay, "Multislit Spectroscopy", *J. Opt. Soc. Amer.*, Vol 39, pp. 437-444, 1949

[12] M.J.E.Golay, "Static Multislit Spectrometry and its applications to the Panoramic Display of Infrared Spectra", *J. Opt. Soc. Amer.*, Vol 41, pp. 468-472, 1961

[13] M.J.E.Golay, "Complementary Series", *IRE Trans. Inform. Theory*, Vol IT-7, pp 82-87, Apr 1961

[14] J.Granata,M.Conner,R.Tolimieri, "Tensor Products", *IEEE Signal Processing Magazine*, pp 41-48, Jan 1992

[15] T.Helleseth,T.Kløve,J.Mykkeltveit, "On the Covering Radius of Binary Codes", *IEEE Trans. Inform. Theory*, Vol IT-24, No 5, pp. 627-628, 1978

[16] T.Høholdt,H.E.Jensen,J.Justesen, "Aperiodic Correlations and the Merit Factor of a Class of Binary Sequences," *IEEE Trans on Information Theory*, Vol 31, No 4, pp 549-552, July 1985

[17] T.Høholdt,H.E.Jensen,J.Justesen, "Autocorrelation Properties of a Class of Infinite Binary Sequences," *IEEE Trans on Information Theory*, Vol 32, No 3, pp 430-431, May 1986

[18] A.E.Jones,T.A.Wilkinson, "Performance of Reed-Muller Codes and a Maximum-Likelihood Decoding Algorithm for OFDM", *IEEE Trans. Comm.*, Vol 47, No 7, pp 949-952, July 1999

[19] F.J.MacWilliams,N.J.A.Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, 1977

[20] J.Mykkeltveit, "The Covering Radius of the $(128, 8)$ Reed-Muller Code is 56", *IEEE Trans. Inform. Theory*, Vol IT-24, pp. 259-262, 1980

[21] H.Ochiai,H.Imai, "Block Coding Scheme Based on Complementary Sequences for Multicarrier Signals", *IEICE Trans. Fundamentals*, Vol E80-A, pp. 2136-2143, 1997

[22] K.G.Paterson,A.E.Jones, "Efficient Decoding Algorithms for Generalised Reed-Muller Codes," *HP Technical Report*, HPL-98-195, Nov, 1998

[23] M.G.Parker, "The Constabent Properties of Golay-Davis-Jedwab Sequences," *Int. Symp. Information Theory, Sorrento, Italy*, June 25-30, 2000 Available at: *http://www.ii.uib.no/ matthew/mattweb.html*

[24] M.G.Parker,V.Rijmen, "The Quantum Entanglement of Bipolar Sequences," *To be presented at SETA01, Bergen, Norway*, May 13-17, 2001 Available at: *http://www.ii.uib.no/ matthew/mattweb.html*

[25] M.G.Parker,C.Tellambura, "Generalised Rudin-Shapiro Constructions," *WCC2001, Workshop on Coding and Cryptography, Paris(France)*, Jan 8-12, 2001 Available at: *http://www.ii.uib.no/ matthew/mattweb.html*

[26] K.G.Paterson, "Generalized Reed-Muller Codes and Power Control in OFDM Modulation," *IEEE Trans. Inform. Theory*, Vol 46, No 1, pp. 104-120, Jan. 2000

[27] K.G.Paterson,V.Tarokh, "On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios," *IEEE Trans. on Inform. Theory*, Vol 46, No 6, pp 1974-1987, Sept. 2000

[28] W.Rudin, "Some Theorems on Fourier Coefficients", *Proc. Amer. Math. Soc.*, No 10, pp. 855-859, 1959

[29] H.S.Shapiro, "Extremal Problems for Polynomials", *M.S. Thesis, M.I.T.*, 1951

[30] S.J.Shepherd,P.W.J.Van Eetvelt,C.W.Wyatt-Millington,S.K.Barton, "Simple Coding Scheme to Reduce Peak Factor in QPSK Multicarrier

Modulation", *Electronics Letters*, Vol 31, No 14, pp 1131-1132, 6th July, '95

[31] R.Sivaswamy, "Multiphase Complementary Codes," *IEEE Trans. Inform. Theory*, Vol IT-24, pp. 546-552, 1978

[32] R.R.Tucci, "A Rudimentary Quantum Compiler", *LANL: quant-ph/9902062*, 18 Feb, 1999

[33] R.D.J.Van Nee, "OFDM Codes for Peak-to-Average Power Reduction and Error Correction", *IEEE Globecom 1996, (London, U.K.)*, pp. 740-744, Nov. 1996

[34] K.Yang,Y-K.Kim,P.V.Kumar, "Quasi-Orthogonal Sequences for Code-Division Multiple-Access Systems", *IEEE Trans. Inform. Theory*, Vol 46, No 3, pp 982-993, May 2000

Table 7: Rudin-Shapiro Extensions Using $u+1 = 4$-Variable Seeds, All Cosets of RM$(1,1)$ in p

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U},x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
$_5\mathbf{\Gamma}^{1,1}$	$\tau pqr + \{\tau(pr+qr+q+r)+pq+pr+q+r,$ $\tau(pr+qr+p+q)+pq+q,$ $\tau(pr+qr)+pqr+pq+pr+qr,$ $\tau(pr+qr)+pq+pr,$ $\tau(pr+qr+q+r)+pqr+pq+qr,$ $\tau(pr+qr)+pqr+pq+qr,$ $\tau(pq+p+q+r)+pq,$ $\tau(pr+qr)+pq\}$ with R	2.5000	0
$_6\mathbf{\Gamma}^{1,1}$	$\tau pqr + \{\tau(p+r)+pqr+pq+pr+r,$ $\tau(q+r)+pqr+pq+pr+r,$ $pqr+pq+pr+r,$ $\tau(pq+pr+qr+r)+pq+pr,$ $\tau(pq+pr+qr+p+q+r)+pqr+qr+r,$ $\tau(pq+pr+qr+p)+pqr+qr+r,$ $\tau(pq+pr+qr+q)+pqr+qr+r,$ $\tau(pq+pr+qr+r)+pqr+qr+r\}$ with R	2.6578	0
$_7\mathbf{\Gamma}^{1,1}$	$\tau pqr + \{\tau(p+r)+pq+q,$ $\tau(pq+pr+qr+p)+pq+q,$ $\tau(pq+pr+qr+q)+pq,$ $\tau(q+r)+pq,$ $\tau(q+r)+pr+r,$ $\tau(pq+pr+qr+r)+pr+r,$ $\tau(p+q)+pr,$ $\tau(pq+pr+qr+p)+pr\}$ with R	2.7199	0
$_8\mathbf{\Gamma}^{1,1}$	$\tau pqr + \{\tau(pq+q)+pq+pr+q+r,$ $\tau(pq+r)+pq+pr,$ $\tau(pq+q)+pqr+pr+r,$ $\tau(pq+r)+pqr+pr+r,$ $\tau(pq+p)+pr+r,$ $\tau(pr+qr)+pr+r,$ $\tau(pr+qr+p+r)+pr,$ $\tau(pq+r)+pr\}$ with R	2.7500	0
$_9\mathbf{\Gamma}^{1,1}$	$\tau pq + \{\tau(q+r)+pq+pr+qr+q+r,$ $\tau(q+r)+pr+r,$ $\tau(q+r)+pr+qr,$ $\tau(p+r)+pr\}$ with R	2.7698	0

Table 8: Rudin-Shapiro Extensions Using $u+1=4$-Variable Seeds (continued), All Cosets of $\mathrm{RM}(1,1)$ in p

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U},x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
${}_{\mathbf{9a}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau pq + \{pr + r,$ $\tau(p+q) + pr\}$ with R	2.7698	1
${}_{\mathbf{10}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau pqr + \{\tau(qr+q+r) + pq + pr + q + r,$ $\tau qr + pqr + pq + pr + qr,$ $\tau(pq+pr+p+q+r) + pq + pr,$ $\tau qr + pq + pr,$ $\tau(qr+q+r) + pr + r,$ $\tau(pq+pr+q) + pr + r,$ $\tau(pq+pr+p+q+r) + pr,$ $\tau(qr+p+q) + pr\}$ with R	2.9282	0
${}_{\mathbf{11}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau(pq+pr) + \{\tau q + pq + qr + q + r,$ $\tau q + pq + pr + qr + q + r,$ $\tau(p+q+r) + pq + qr + q,$ $\tau q + qr + r,$ $\tau(p+q+r) + pr + qr + r,$ $\tau q + pr + qr + r\}$ with R	2.9285	0
${}_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau pqr + \{\tau(pr+p+r) + pq + pr + q + r,$ $\tau(pr+p+q) + pqr + pq + q,$ $\tau(pr+p+r) + pqr + pq + pr + r,$ $\tau(pr+p+q) + pq + pr,$ $\tau(pq+qr+p+q+r) + pq + pr,$ $\tau(pq+qr+r) + pq,$ $\tau(pq+qr+p+q+r) + pqr + qr + r,$ $\tau(pq+qr+r) + pqr + qr + r,$ $\tau(pq+qr+p) + pr + r,$ $\tau(pr+q+r) + pr + r,$ $\tau(pr+p+q) + pr,$ $\tau(pq+qr+r) + pr\}$ with R	2.9425	0
${}_{\mathbf{13}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau(pq+pr) + \{pq + qr + r,$ $\tau(p+r) + pq + qr,$ $\tau(p+r) + pr + qr + r,$ $pr + qr + r\}$ with R	2.9514	0
${}_{\mathbf{14}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau pqr + \{\tau(pq+q+r) + pq + q,$ $\tau(pq+p+r) + pq,$ $\tau(pq+p+r) + pqr + r,$ $\tau(pq+q+r) + pqr + r\}$ with R	2.9575	0

Table 9: Rudin-Shapiro Extensions Using $u+1=4$-Variable Seeds (continued), All Cosets of RM$(1,1)$ in p

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U},x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
$_{\mathbf{15}}\mathbf{\Gamma^{1,1}}$	$\tau(pq+pr+qr)+pqr+\{pq+q,$	3.0000	0
$_{\mathbf{15}}\mathbf{\Gamma^{1,2}}$	$pr+qr+q,$		
$_{\mathbf{15}}\mathbf{\Gamma^{1,3}}$	$\tau(p+q)+q,$		
$_{\mathbf{15}}\mathbf{\Gamma^{1,4}}$	$\tau(p+q)+pq+pr+qr\}$ with R		
$_{\mathbf{16}}\mathbf{\Gamma^{2,1}}$	$\tau(pq+pr+qr)+pqr+\{qr+r,$	3.0000	0
$_{\mathbf{16}}\mathbf{\Gamma^{3,1}}$	$qr+q+r,$		
$_{\mathbf{16}}\mathbf{\Gamma^{4,1}}$	$pq+pr+r,$		
	$pq+pr+q+r,$		
	$\tau(q+r)+q+r,$		
	$\tau(q+r)+pq+pr+qr+q,$		
	$\tau(q+r)+pq+pr+qr,$		
	$\tau(q+r)+r\}$		
$_{\mathbf{17}}\mathbf{\Gamma^{1,1}}$	$pqr+\{\tau(p+q+r)+pr+r,$	3.0000	0
	$\tau(p+q+r)+pq+qr+q+r,$		
	$\tau(pq+q+r)+pq+pr+qr,$		
	$\tau(pq+q+r)+pr+qr+q+r,$		
	$\tau(pr+qr+q)+pq+q,$		
	$\tau(pr+qr+q)+pq+pr+qr,$		
	$\tau(pr+qr+r)+pq+pr+r,$		
	$\tau(pq+p+r)+qr+r,$		
	$\tau(pq+p+r)+pq+qr,$		
	$\tau(pr+qr+p+q+r)+qr+r,$		
	$\tau(pq+pr+qr+p+r)+pr+r,$		
	$\tau(pq+pr+qr+p+r)+pq+qr\}$ with R		

Table 10: Rudin-Shapiro Extensions Using $u+1 = 4$-Variable Seeds, Quadratic Seeds Only, $3.0 < \upsilon \leq 4.0$, All Cosets of RM$(1,3)$ in p,q,r

$\boldsymbol{\Gamma}$	$\frac{\boldsymbol{\Theta}(\mathbf{x_U},x_g)}{2^{h-1}} = \frac{\boldsymbol{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau p + \{\tau q + qr,$ $\tau r + qr\}$	3.3746	2
$_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau p + \{\tau q + pq + pr,$ $\tau r + pq + pr\}$	3.3746	1
$_{\mathbf{19}}\boldsymbol{\Gamma}^{\mathbf{1,2}}$	$\tau r + \{\tau p + pq,$ $\tau q + pq\}$	3.4243	2
$_{\mathbf{19a}}\boldsymbol{\Gamma}^{\mathbf{1,2}}$	$\tau r + \{\tau p + pr + qr,$ $\tau q + pr + qr\}$	3.4243	1
$_{\mathbf{19}}\boldsymbol{\Gamma}^{\mathbf{1,1}}, {_{\mathbf{19a}}\boldsymbol{\Gamma}^{\mathbf{1,1}}}$		3.4467	
$_{\mathbf{20}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau q + \{\tau p + pr,$ $\tau r + pr\}$	3.4702	2
$_{\mathbf{20a}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau q + \{\tau p + pq + qr,$ $\tau r + pq + qr\}$	3.4702	1
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{2,1}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{2,1}}}$		3.4964	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{1,3}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{1,3}}}$		3.5168	
$_{\mathbf{20}}\boldsymbol{\Gamma}^{\mathbf{2,1}}, {_{\mathbf{20a}}\boldsymbol{\Gamma}^{\mathbf{2,1}}}$		3.5216	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{3,1}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{3,1}}}$		3.5287	
$_{\mathbf{20}}\boldsymbol{\Gamma}^{\mathbf{3,1}}, {_{\mathbf{20a}}\boldsymbol{\Gamma}^{\mathbf{3,1}}}$		3.5351	
$_{\mathbf{19}}\boldsymbol{\Gamma}^{\mathbf{1,3}}, {_{\mathbf{19a}}\boldsymbol{\Gamma}^{\mathbf{1,3}}}$		3.5364	
$_{\mathbf{19}}\boldsymbol{\Gamma}^{\mathbf{1,4}}, {_{\mathbf{19a}}\boldsymbol{\Gamma}^{\mathbf{1,4}}}$		3.5364	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{1,2}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{1,2}}}$		3.5366	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{4,1}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{4,1}}}$		3.5369	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{1,4}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{1,4}}}$		3.5373	
$_{\mathbf{20}}\boldsymbol{\Gamma}^{\mathbf{4,1}}, {_{\mathbf{20a}}\boldsymbol{\Gamma}^{\mathbf{4,1}}}$		3.5385	
$_{\mathbf{21}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau(p+q+r) + pq$	3.5396	1
$_{\mathbf{22}}\boldsymbol{\Gamma}^{\mathbf{1,1}}$	$\tau(p+q+r) + qr$	3.5396	1
$_{\mathbf{21}}\boldsymbol{\Gamma}^{\mathbf{1,2}}$		3.5396	
$_{\mathbf{21}}\boldsymbol{\Gamma}^{\mathbf{1,3}}$		3.5396	
$_{\mathbf{21}}\boldsymbol{\Gamma}^{\mathbf{1,4}}$		3.5396	
$_{\mathbf{22}}\boldsymbol{\Gamma}^{\mathbf{2,1}}$		3.5396	
$_{\mathbf{22}}\boldsymbol{\Gamma}^{\mathbf{3,1}}$		3.5396	
$_{\mathbf{22}}\boldsymbol{\Gamma}^{\mathbf{4,1}}$		3.5396	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{2,2}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{2,2}}}$		3.7741	
$_{\mathbf{20}}\boldsymbol{\Gamma}^{\mathbf{1,2}}, {_{\mathbf{20a}}\boldsymbol{\Gamma}^{\mathbf{1,2}}}$		3.8260	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{3,2}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{3,2}}}$		3.8361	
$_{\mathbf{18}}\boldsymbol{\Gamma}^{\mathbf{2,3}}, {_{\mathbf{18a}}\boldsymbol{\Gamma}^{\mathbf{2,3}}}$		3.8470	

Table 11: Rudin-Shapiro Extensions Using $u + 1 = 4$-Variable Seeds, Quadratic Seeds Only, $3.0 < \upsilon \leq 4.0$, All Cosets of RM$(1, 3)$ in p, q, r

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U}, x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,3}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,3}}$		3.8480	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,2}}$		3.8483	
$_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{2,2}}$		3.8492	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,1}}$		3.8497	
$_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{3,2}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{3,2}}$		3.8550	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\tau(p+q+r)+pr$	3.8570	1
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{1,2}}$		3.8570	
$_{\mathbf{21}}\mathbf{\Gamma}^{\mathbf{2,1}}$		3.8570	
$_{\mathbf{21}}\mathbf{\Gamma}^{\mathbf{2,2}}$		3.8570	
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{2,2}}$		3.8570	
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{3,2}}$		3.8570	
$_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{1,3}}$		3.9530	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,3}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,3}}$		3.9599	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{3,2}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{3,2}}$		3.9616	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{3,1}}$		3.9617	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{1,2}}$		3.9622	
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{1,3}}$		3.9622	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{2,1}}$		3.9622	
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{2,3}}$		3.9622	
$_{\mathbf{21}}\mathbf{\Gamma}^{\mathbf{3,1}}$		3.9622	
$_{\mathbf{21}}\mathbf{\Gamma}^{\mathbf{3,2}}$		3.9622	
$_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{1,4}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{1,4}}$		3.9880	
$_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{4,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{4,1}}$		3.99038	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{1,3}}$		3.9904	
$_{\mathbf{22}}\mathbf{\Gamma}^{\mathbf{1,4}}$		3.9904	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{2,2}}$		3.9904	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{3,1}}$		3.9904	
$_{\mathbf{21}}\mathbf{\Gamma}^{\mathbf{4,1}}$		3.9904	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{1,4}}$		3.9976	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{2,3}}$		3.9976	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{3,2}}$		3.9976	
$_{\mathbf{23}}\mathbf{\Gamma}^{\mathbf{4,1}}$		3.9976	

Table 12: Rudin-Shapiro Extensions Using $u+1 = 4$-Variable Seeds, Quadratic Seeds Only, $3.0 < \upsilon \leq 4.0$, All Cosets of RM$(1,3)$ in p, q, r

$\mathbf{\Gamma}$	$\frac{\mathbf{\Theta}(\mathbf{x_U}, x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,r,\tau)}{2^{h-1}}$	υ	χ
$_{\mathbf{24}}\mathbf{\Gamma}^{\mathbf{1,1}}$ $_{\mathbf{24}}\mathbf{\Gamma}^{\mathbf{1,4}}$ $_{\mathbf{24}}\mathbf{\Gamma}^{\mathbf{2,1}}$ $_{\mathbf{24}}\mathbf{\Gamma}^{\mathbf{3,1}}$ $_{\mathbf{24}}\mathbf{\Gamma}^{\mathbf{4,1}}$	$\{\tau(p+q+r)+pq+qr,$ $\tau(p+q+r)+pr+qr,$ $\tau(q+r)+pq+pr+qr,$ $\tau(p+q)+pq+pr+qr,$ $\tau(p+r)+pq+pr+qr,$ $\tau(p+q+r)+pq+pr,$ $\tau(q+r)+pq+pr,$ $\tau(p+q)+pr+qr,$ $\tau(p+r)+pq+qr\}$	4.0000	0
$_{\mathbf{25}}\mathbf{\Gamma}^{\mathbf{1,1}}$ $_{\mathbf{25}}\mathbf{\Gamma}^{\mathbf{1,4}}$ $_{\mathbf{25}}\mathbf{\Gamma}^{\mathbf{2,1}}$ $_{\mathbf{25}}\mathbf{\Gamma}^{\mathbf{3,1}}$ $_{\mathbf{25}}\mathbf{\Gamma}^{\mathbf{4,1}}$	$\{pq+pr,$ $pq+qr,$ $pr+qr\}$	4.0000	2

Table 13: The Size of $\mathbf{\Gamma}$-Sets

$\mathbf{\Gamma}$	$\lvert\mathbf{\Gamma}\rvert$
$_{\mathbf{0}}\mathbf{\Gamma}$	D
$_{\mathbf{1}}\mathbf{\Gamma}$	$2^{1-h}D$
$_{\mathbf{2}}\mathbf{\Gamma}^{\mathbf{1}}$	$\frac{2^{3-2h}}{m}D$
$_{\mathbf{3}}\mathbf{\Gamma}^{\mathbf{1}}, {}_{\mathbf{3a}}\mathbf{\Gamma}^{\mathbf{1}}$	$\frac{2^{2-2h}}{m}D$
$_{\mathbf{3}}\mathbf{\Gamma}^{\mathbf{2}}, {}_{\mathbf{3a}}\mathbf{\Gamma}^{\mathbf{2}}$	$\frac{2^{2-2h}(m-2)}{m(m-1)}D$
$_{\mathbf{3}}\mathbf{\Gamma}^{\mathbf{3}}, {}_{\mathbf{3a}}\mathbf{\Gamma}^{\mathbf{3}}$	$\frac{2^{2-2h}(m-3)}{m(m-1)}D$
$_{\mathbf{3}}\mathbf{\Gamma}^{\mathbf{4}}, {}_{\mathbf{3a}}\mathbf{\Gamma}^{\mathbf{4}}$	$\frac{2^{2-2h}(m-4)}{m(m-1)}D$
$_{\mathbf{3}}\mathbf{\Gamma}^{\mathbf{5}}, {}_{\mathbf{3a}}\mathbf{\Gamma}^{\mathbf{5}}$	$\frac{2^{2-2h}(m-5)}{m(m-1)}D$
$_{\mathbf{4}}\mathbf{\Gamma}^{\mathbf{1}}$	$\frac{2^{2-2h}}{m}D$
$_{\mathbf{4}}\mathbf{\Gamma}^{\mathbf{2}}$	$\frac{2^{2-2h}(m-2)}{m(m-1)}D$
$_{\mathbf{4}}\mathbf{\Gamma}^{\mathbf{3}}$	$\frac{2^{2-2h}(m-3)}{m(m-1)}D$
$_{\mathbf{4}}\mathbf{\Gamma}^{\mathbf{4}}$	$\frac{2^{2-2h}(m-4)}{m(m-1)}D$
$_{\mathbf{4}}\mathbf{\Gamma}^{\mathbf{5}}$	$\frac{2^{2-2h}(m-5)}{m(m-1)}D$
$_{\mathbf{5}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{6}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{7}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{8}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{10}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{5-3h}}{m(m-1)}D$
$_{\mathbf{9a}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{3-3h}}{m(m-1)}D$
$_{\mathbf{11}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{3-3h}3}{m(m-1)}D$
$_{\mathbf{12}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{4-3h}3}{m(m-1)}D$
$_{\mathbf{9}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{13}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{14}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{15}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{4-3h}}{m(m-1)}D$
$_{\mathbf{15}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{16}}\mathbf{\Gamma}^{\mathbf{2,1}}$	$\frac{2^{4-3h}(m-3)}{m(m-1)(m-2)}D$
$_{\mathbf{15}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{16}}\mathbf{\Gamma}^{\mathbf{3,1}}$	$\frac{2^{4-3h}(m-4)}{m(m-1)(m-2)}D$
$_{\mathbf{15}}\mathbf{\Gamma}^{\mathbf{1,4}}, {}_{\mathbf{16}}\mathbf{\Gamma}^{\mathbf{4,1}}$	$\frac{2^{4-3h}(m-5)}{m(m-1)(m-2)}D$
$_{\mathbf{17}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{4-3h}3}{m(m-1)}D$
$_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{1,1}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{1,1}}$	$\frac{2^{4-3h}}{m(m-1)}D$
$_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{2,1}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,1}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{2,1}}$ $_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{1,2}}, {}_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{2,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,1}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{2,1}}$	$\frac{2^{4-3h}(m-3)}{m(m-1)(m-2)}D$
$_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{2,2}}$ $_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{1,3}}, {}_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{2,2}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{2,2}}$ $_{\mathbf{18}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{19}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{20}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{18a}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma}^{\mathbf{3,1}}, {}_{\mathbf{20a}}\mathbf{\Gamma}^{\mathbf{3,1}}$	$\frac{2^{4-3h}(m-4)}{m(m-1)(m-2)}D$

where $D = \lvert\mathbf{DJ_{m,h}}\rvert = \left(\frac{m!}{2}\right)2^{h(m+1)}$

Table 14: The Size of $\mathbf{\Gamma}$-Sets (continued)

$\mathbf{\Gamma}$	$\lvert\mathbf{\Gamma}\rvert$
${}_{\mathbf{18}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{19}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{20}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{18}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{19}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{20}}\mathbf{\Gamma^{2,3}}$ ${}_{\mathbf{18a}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{19a}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{20a}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{18a}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{19a}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{20a}}\mathbf{\Gamma^{2,3}}$ ${}_{\mathbf{18}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{19}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{20}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{18}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{19}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{20}}\mathbf{\Gamma^{4,1}}$ ${}_{\mathbf{18a}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{19a}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{20a}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{18a}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{19a}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{20a}}\mathbf{\Gamma^{4,1}}$	$\frac{2^{4-3h}(m-5)}{m(m-1)(m-2)}D$
${}_{\mathbf{21}}\mathbf{\Gamma^{1,1}}, {}_{\mathbf{22}}\mathbf{\Gamma^{1,1}}, {}_{\mathbf{23}}\mathbf{\Gamma^{1,1}}$	$\frac{2^{3-3h}}{m(m-1)}D$
${}_{\mathbf{21}}\mathbf{\Gamma^{1,2}}, {}_{\mathbf{22}}\mathbf{\Gamma^{1,2}}, {}_{\mathbf{23}}\mathbf{\Gamma^{1,2}}, {}_{\mathbf{21}}\mathbf{\Gamma^{2,1}}, {}_{\mathbf{22}}\mathbf{\Gamma^{2,1}}, {}_{\mathbf{23}}\mathbf{\Gamma^{2,1}}$	$\frac{2^{3-3h}(m-3)}{m(m-1)(m-2)}D$
${}_{\mathbf{21}}\mathbf{\Gamma^{1,3}}, {}_{\mathbf{22}}\mathbf{\Gamma^{1,3}}, {}_{\mathbf{23}}\mathbf{\Gamma^{1,3}}, {}_{\mathbf{21}}\mathbf{\Gamma^{2,2}}, {}_{\mathbf{22}}\mathbf{\Gamma^{2,2}}, {}_{\mathbf{23}}\mathbf{\Gamma^{2,2}}$ ${}_{\mathbf{21}}\mathbf{\Gamma^{3,1}}, {}_{\mathbf{22}}\mathbf{\Gamma^{3,1}}, {}_{\mathbf{23}}\mathbf{\Gamma^{3,1}}$	$\frac{2^{3-3h}(m-4)}{m(m-1)(m-2)}D$
${}_{\mathbf{21}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{22}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{23}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{21}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{22}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{23}}\mathbf{\Gamma^{2,3}}$ ${}_{\mathbf{21}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{22}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{23}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{21}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{22}}\mathbf{\Gamma^{4,1}}, {}_{\mathbf{23}}\mathbf{\Gamma^{4,1}}$	$\frac{2^{3-3h}(m-5)}{m(m-1)(m-2)}D$
${}_{\mathbf{24}}\mathbf{\Gamma^{1,1}}$	$\frac{2^{3-3h}9}{m(m-1)}D$
${}_{\mathbf{24}}\mathbf{\Gamma^{1,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,1}}$	$\frac{2^{3-3h}9(m-3)}{m(m-1)(m-2)}D$
${}_{\mathbf{24}}\mathbf{\Gamma^{1,3}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{3,1}}$	$\frac{2^{3-3h}9(m-4)}{m(m-1)(m-2)}D$
${}_{\mathbf{24}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{24}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{4,1}}$	$\frac{2^{3-3h}9(m-5)}{m(m-1)(m-2)}D$
${}_{\mathbf{25}}\mathbf{\Gamma^{1,1}}$	$\frac{2^{3-3h}3}{m(m-1)}D$
${}_{\mathbf{25}}\mathbf{\Gamma^{1,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,1}}$	$\frac{2^{3-3h}3(m-3)}{m(m-1)(m-2)}D$
${}_{\mathbf{25}}\mathbf{\Gamma^{1,3}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{3,1}}$	$\frac{2^{3-3h}3(m-4)}{m(m-1)(m-2)}D$
${}_{\mathbf{25}}\mathbf{\Gamma^{1,4}}, {}_{\mathbf{24}}\mathbf{\Gamma^{2,3}}, {}_{\mathbf{24}}\mathbf{\Gamma^{3,2}}, {}_{\mathbf{24}}\mathbf{\Gamma^{4,1}}$	$\frac{2^{3-3h}3(m-5)}{m(m-1)(m-2)}D$

where $D = \lvert\mathbf{DJ_{m,h}}\rvert = \left(\frac{m!}{2}\right)2^{h(m+1)}$