# Generalised Rudin-Shapiro Constructions

Matthew G. Parker [1]

*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

*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*

**Abstract**

A Golay Complementary Sequence (CS) has Peak-to-Average-Power-Ratio (PAPR) $\leq 2.0$ 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 PAPR $\leq 2.0$ under <u>all</u> unitary transforms whose rows are unimodular linear (Linear Unimodular Unitary Transforms (LUUTs)), including one- and multi-dimensional generalised DFTs. We also propose tensor cosets of GDJ sequences arising from Rudin-Shapiro extensions of near-complementary pairs, thereby generating many infinite sequence families with tight low PAPR bounds under LUUTs.

*Key words:*
Complementary,Bent,PAPR,Golay,Fourier,Multidimensional,Quadratic,Rudin-Shapiro, Covering Radius,DFT,Transform,Unitary,Reed-Muller

Some preliminary definitions:
Length $N$ vectors **a**,**b**, where $\mathbf{a} \in Z_P^N$, $\mathbf{b} \in Z_Q^N$, and $a_j, b_j$ are sequence elements of **a** and **b**, respectively. We define,
**Correlation:** $\mathbf{a} \odot \mathbf{b} = \sum_{j=0}^{N-1} \epsilon^{\mu a_j - \lambda b_j}$, where $\epsilon = \exp(2\pi\sqrt{-1}/\mathrm{lcm}(P,Q))$, $\mu = \frac{\mathrm{lcm}(P,Q)}{P}$, $\lambda = \frac{\mathrm{lcm}(P,Q)}{Q}$, where lcm means 'least common multiple'.
**Orthogonal:** **a** and **b** are 'Orthogonal' to each other if $\mathbf{a} \odot \mathbf{b} = 0$.
**(Almost) Orthogonal:** **a** and **b** are '(Almost) Orthogonal' to each other if $0 \leq |\mathbf{a} \odot \mathbf{b}| \leq \sqrt{2N}$.
**Roughly Orthogonal:** **a** and **b** are 'Roughly Orthogonal' to each other if $0 \leq |\mathbf{a} \odot \mathbf{b}| \leq B$, for some pre-chosen $B$ significantly less than $N$.

[1] Supported by NFR Project Number 119390/431

**Tensor Permutation:** Tensor permutation of $m$ $r$-state variables, $x_i$, takes $x_i$ to $x_{\pi(i)}$, where permutation $\pi$ is any permutation of integers $Z_m$.
**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.

**Definition 1** $\mathbf{L_m}$ *is the infinite set of all linear functions in $m$ binary variables over* <u>*all*</u> *alphabets, $Z_n$, $1 \leq n \leq \infty$,*

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

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

**Definition 2** $\mathbf{F1_m} \subset \mathbf{L_m}$ *is the infinite set of all one-dimensional linear Fourier functions in $m$ binary variables over* <u>*all*</u> *alphabets, $Z_n$, $1 \leq n \leq \infty$,*

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

**Definition 3** $\mathbf{Fm_m} \subset \mathbf{L_m}$ *is the infinite set of all $m$-dimensional linear Fourier functions in $m$ binary variables over* <u>*all*</u> *alphabets, $Z_n$, $1 \leq n \leq \infty$,*

$$\begin{gathered}\mathbf{Fm_m} = \{(0, \delta + c_0) \oplus (0, \delta + c_1) \oplus (0, \delta + c_2) \oplus \ldots \oplus (0, \delta + c_{n-1}) \;\; mod\ n \\ 2 \leq n \leq \infty, n\ even, 0 \leq \delta < n/2, \qquad \gcd(\delta, n) = 1, c_i \in \{0, n/2\}\}\end{gathered} \tag{3}$$

**Definition 4** *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 $\mathbf{u} \odot (-\mathbf{v})$.*

## 1 Introduction

Length $N = 2^m$ Complementary Sequences (CS) are (Almost) Orthogonal to $\mathbf{F1_m}$ [4,3]. Length $2^m$ CS over $Z_{2^h}$, as formed using the Davis-Jedwab construction, $\mathbf{DJ_m}$, are also Roughly Orthogonal to each other [3,8]. This paper shows that $\mathbf{DJ_m}$ is (Almost) Orthogonal to $\mathbf{L_m}$, and therefore each member of $\mathbf{DJ_m}$ has a Peak-to-Average Power Ratio (PAPR) $\leq 2.0$ under all Linear Unimodular Unitary Transforms (LUUTs) of length $2^m$. The properties of $\mathbf{DJ_m}$ are shown to follow directly from a generalisation of the Rudin-Shapiro construction [10,9,4,5,1]. We then propose tensor cosets of $\mathbf{DJ_m}$, identifying near-complementary seed pairs whose power sum has PAPR $\leq \upsilon$ under certain LUUTs, where $\upsilon$ is small. We grow sequence sets from these pairs by repeated application of Rudin-Shapiro so that these sets also have PAPR $\leq \upsilon$ under certain LUUTs. In this way we extend [3,8] by proposing further infinite sequence families with tight one-dimensional Fourier PAPR bounds, and of degree higher than quadratic. We also confirm and extend recent results of [2] who construct families of Bent sequences using Bent sequences as seed pairs, although not in the context of Rudin-Shapiro.

## 2 Complementary Sequences (CS)

**Definition 5** *[4,3] Length $N$ sequences* $\mathbf{s0}$ *and* $\mathbf{s1}$ *are a CS pair if the sum of their one-dimensional Fourier power spectrums is flat and equal to $2N$.*

**Implication 1** *[4,3] A length $N$ CS,* $\mathbf{s}$*, has a Peak-to-Average-Power-Ratio (PAPR) for its one-dimensional Fourier power spectrum constrained by,*

$$1.0 \leq PAPR(\mathbf{s}) \leq \frac{2N}{N} = 2.0 \tag{4}$$

**Theorem 1** *[3]* $\mathbf{s}$ *is a Golay-Davis-Jedwab (GDJ) CS if of length $2^m$ and expressible as a function of $m$ variables over $Z_{2^h}$ as,*

$$\mathbf{s}(x_0, x_1, \ldots, x_{m-1}) = 2^{h-1} \sum_{k=0}^{m-2} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=0}^{m-1} c_k x_k + d \tag{5}$$

*where $\pi$ is a permutation of the symbols $\{0, 1, \ldots, m-1\}$, $c_k, d \in Z_{2^h}$, and the $x_k$ are linear functions 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* $\mathbf{DJ_m}$*.*

There are $(\frac{m!}{2})2^{h(m+1)}$ sequences in $\mathbf{DJ_{m,h}}$, and $\mathbf{DJ_{m,h}}$ has minimum Hamming Distance $\geq 2^{m-2}$. Thus, for distinct $\mathbf{s0}, \mathbf{s1} \in \mathbf{DJ_{m,1}}$, $\mathbf{s0} \odot \mathbf{s1} \leq 2^{m-1}$.

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

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

**Proof Overview:** We prove for $\mathbf{DJ_{m,1}}$ by using the Rudin-Shapiro construction [10,9] 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 $\mathbf{DJ_m}$. More specifically, let $\mathbf{s0_0}$, $\mathbf{s1_0}$ be the length 1 sequences, $\mathbf{s0_0} = (0)$, $\mathbf{s1_0} = (1)$, where $\mathbf{s0_0}, \mathbf{s1_0} \in \mathbf{DJ_{0,1}}$. The Rudin-Shapiro sequence construction is as follows:

$$\mathbf{s0_j} = \mathbf{s0_{j-1}} | \mathbf{s1_{j-1}}, \qquad \mathbf{s1_j} = \mathbf{s0_{j-1}} | \overline{\mathbf{s1_{j-1}}} \tag{6}$$

where $\mathbf{s0_j}, \mathbf{s1_j} \in \mathbf{DJ_{j,1}}$, $\overline{\mathbf{s}}$ means negation of $\mathbf{s}$, 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 RM$(1, m)$ 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,

$$\begin{array}{lll} A: & \mathbf{s0_j} = \mathbf{s0_{j-1}}|\mathbf{s1_{j-1}}, & \mathbf{s1_j} = \mathbf{s0_{j-1}}|\overline{\mathbf{s1_{j-1}}} \\ & \text{and} & \\ B: & \mathbf{s0_j} = \overline{\mathbf{s0_{j-1}}}|\mathbf{s1_{j-1}}, & \mathbf{s1_j} = \overline{\mathbf{s0_{j-1}}}|\overline{\mathbf{s1_{j-1}}} \end{array} \tag{7}$$

Algebraically, constructions (7) become,

$$\begin{array}{ll} A: & \begin{array}{l} \mathbf{s0_j}(x) = x_{j-1}(\mathbf{s0_{j-1}}(x') + \mathbf{s1_{j-1}}(x')) + \mathbf{s0_{j-1}}(x') \\ \mathbf{s1_j}(x) = \mathbf{s0_j}(x) + x_{j-1} \end{array} \\ & \text{and} \\ B: & \begin{array}{l} \mathbf{s0_j}(x) = x_{j-1}(\mathbf{s0_{j-1}}(x') + \mathbf{s1_{j-1}}(x') + 1) + \mathbf{s0_{j-1}}(x') + 1 \\ \mathbf{s1_j}(x) = \mathbf{s0_j}(x) + x_{j-1} \end{array} \\ & \text{where } x = (x_0, x_1, \dots, x_{j-1}), x' = (x_0, x_1, \dots, x_{j-2}) \end{array} \tag{8}$$

We generate $\mathbf{DJ_{m,1}}$ from this coset by permutation of the indices, $i$, of $x_i$ (tensor permutation). There are $\frac{m!}{2}$ such tensor permutations, (ignoring reversals).

Example 2: 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 prove Theorem 2 for construction (6). The proof for construction (7) 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 $\beta \in Z_n, 1 \le n \le \infty$. Let $p_j, q_j$ be complex numbers satisfying,

$$p_j = \mathbf{f_j} \odot \mathbf{s0_j}, \qquad q_j = \mathbf{f_j} \odot \mathbf{s1_j} \tag{9}$$

$$\text{Let} \qquad \mathbf{f_j} = \mathbf{f_{j-1}} \oplus (0, \alpha_{j-1}), \bmod n \tag{10}$$

$\alpha_{j-1} \in Z_n, 1 \le n \le \infty$, $\gcd(\alpha_{j-1}, n) = 1$. Using (10) $\forall \alpha_j$ we generate $\mathbf{L_j}$. Combining (9), (6) and (10),

$$p_j = \mathbf{f_{j-1}} \odot \mathbf{s0_{j-1}} + \epsilon^{\alpha_{j-1}} \mathbf{f_{j-1}} \odot \mathbf{s1_{j-1}} = p_{j-1} + \epsilon^{\alpha_{j-1}} q_{j-1} \tag{11}$$

$$q_j = \mathbf{f_{j-1}} \odot \mathbf{s0_{j-1}} - \epsilon^{\alpha_{j-1}} \mathbf{f_{j-1}} \odot \mathbf{s1_{j-1}} = p_{j-1} - \epsilon^{\alpha_{j-1}} q_{j-1} \tag{12}$$

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

$$|\phi p + \theta q|^2 + |\phi p - \theta q|^2 = 2(|\phi|^2|p|^2 + |\theta|^2|q|^2) \tag{13}$$

for the special case $|\phi|^2 = |\theta|^2 = 1$, to (11) and (12) we get,

$$|p_j|^2 + |q_j|^2 = 2(|p_{j-1}|^2 + |q_{j-1}|^2) = 2^j(|p_0|^2 + |q_0|^2) \tag{14}$$

Noting that $|p_0|^2 = |q_0|^2 = 1$, it follows that $|p_j|^2 \leq 2^{j+1}, |q_j|^2 \leq 2^{j+1}$. Theorem 2 follows directly for a subset of $\mathbf{DJ_{m,1}}$ comprising sequences generated by (6). The proof follows for the RM$(1,m)$ coset of $x_0x_1 + x_1x_2 + \ldots\ x_{m-2}x_{m-1}$ by replacing construction (6) with constructions (7). Further extension to $\mathbf{DJ_{m,1}}$ follows by observing that identical tensor-permuting of $\mathbf{f}$ and $\mathbf{s}$ leaves the argument of (11) - (12) unchanged. The proof for $\mathbf{DJ_m}$ follows. $\blacksquare$

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

From Theorem 2 sequences from $\mathbf{DJ_m}$ have (Almost) flat spectrum under all LUUTs (see Definition 4). By Parseval's theorem the PAPR of sequences from $\mathbf{DJ_m}$ under such transforms is $\leq 2.0$ 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). An $N \times N$ Consta-DFT (CDFT) matrix has rows from $\mathbf{F1_m}$ and is defined over $Z_n$ by,

$$\begin{pmatrix} 0 & d & 2d & \ldots & (N-1)d \\ 0 & d+k & 2(d+k) & \ldots & (N-1)(d+k) \\ . & . & . & . & . \\ 0 & d+(N-1)k & 2(d+(N-1)k) & \ldots & (N-1)(d+(N-1)k) \end{pmatrix} \qquad (15)$$

$1 \leq n \leq \infty$, $N|n$, $k = \frac{n}{N}$, $d \in Z_k$, $\gcd(d,k) = 1$, (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,

$$\begin{pmatrix} 0 & \delta_0 \\ 0 & \delta_0 + \frac{n}{2} \end{pmatrix} \oplus \begin{pmatrix} 0 & \delta_1 \\ 0 & \delta_1 + \frac{n}{2} \end{pmatrix} \oplus \ldots \oplus \begin{pmatrix} 0 & \delta_{m-1} \\ 0 & \delta_{m-1} + \frac{n}{2} \end{pmatrix} = \oplus_{i=0}^{m-1} \begin{pmatrix} 0 & \delta_i \\ 0 & \delta_i + \frac{n}{2} \end{pmatrix} \qquad (16)$$

$2 \leq n \leq \infty, n$ even, $0 \leq \delta_i < \frac{n}{2}$ $\gcd(\delta_i, \frac{n}{2}) = 1$, (including the case $\delta_i = 0$, $n = 2$). The 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 $Z_4$.

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

**Definition 6** *[6] A length $2^m$ sequence, $\mathbf{s}$, is Bent, Negabent, Constabent, if it has PAPR $= 1.0$ under HT, NHT, and CHT, respectively. It is (Almost) Bent, (Almost) Negabent, (Almost) Constabent, if it has PAPR $\leq 2.0$ under HT, NHT, and CHT, respectively.*

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

**Theorem 3** *[6]* $\mathbf{DJ_{m,1}}$ *is Bent for $m$ even, and (Almost) Bent, with PAPR $= 2.0$, for $m$ odd.*

**Theorem 4** *[6]* $\mathbf{DJ_{m,1}}$ *is Negabent for $m \neq 2$ mod 3, and (Almost) Negabent, with PAPR $= 2.0$, for $m = 2$ mod 3.*

**Corollary 5** *[6]* $\mathbf{DJ_{m,1}}$ *is Bent and Negabent for $m$ even, $m \neq 2$ mod 3.*

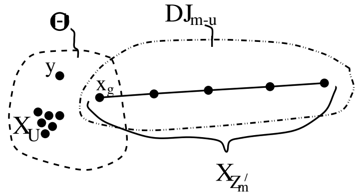
## 5 Seeded Extensions of $\mathbf{DJ_m}$

$\mathbf{DJ_m}$ 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 $|\mathbf{f} \odot \mathbf{s0_0}|^2 + |\mathbf{f} \odot \mathbf{s1_0}|^2 = 2.0$, $\forall \mathbf{f} \in \mathbf{L_0}$. 2.0 is the lowest possible value. We can, instead, take any pair of length-$t$ starting sequences $\mathbf{s0_0}$ and $\mathbf{s1_0}$, such that,

$$|\mathbf{f} \odot \mathbf{s0_0}|^2 + |\mathbf{f} \odot \mathbf{s1_0}|^2 \leq \upsilon t, \qquad \forall \mathbf{f} \in \mathbf{E_0} \tag{17}$$

where $\mathbf{E_0}$ is any desired set of length-$t$ sequences, and $\upsilon$ is a real value $\geq 2.0$. Let $t = w2^u$, $w$ odd. We define an ordered subset of $u$ integers, $\mathbf{U} = \{q_0, q_1, \ldots, q_{u-1}\}$ for integers $q_i$, $\mathbf{U} \subset \mathbf{Z_m}$, $q_i \neq q_k$, $i \neq k$. We also define $\mathbf{Z'_m} = \mathbf{Z_m} \not\cap \mathbf{U}$. $\mathbf{x_U}$ is the set of two-state variables $\{x_{q_0}, x_{q_1}, \ldots, x_{q_{u-1}}\}$ over which a starting seed is described, $\mathbf{x_{Z'_m}}$ is the set of two-state 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 length $2^{m-u}t$ linear functions 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 (17) for certain fixed (preferably small) $\upsilon$.

We illustrate the seed construction as follows, further developing the line graph representation of [8]. Each black dot symbolises a variable. The line between two dots (variables) indicates a quadratic component comprising the variables at either end of the line.




**Theorem 6** *The length $t2^{m-u}$ 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 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 $\upsilon$ is given by (17), and $g \in \mathbf{Z'_m}$.*

Theorem 6 allows us to construct favourable 'tensor cosets' of $\mathbf{DJ_m}$ by first identifying a starting pair of sequences with desirable correlation properties, i.e. a pair which satisfy (17) for small $\upsilon$, 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 $\in \mathbf{U}$. We identify tensor symmetries leaving PAPR invariant. The symmetry depends on $\mathbf{E_0}$.

**Lemma 7** *If $\mathbf{E_0} = \mathbf{Fu_u}$ 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 by $\mathbf{\Theta}$.*

We now give a few example constructions which all follow from Theorem 6, coupled with Theorems 3 and 4.

**Corollary 8** [2] *Let $\mathbf{s0_0}(\mathbf{x_U})$ and $\mathbf{s1_0}(\mathbf{x_U})$ be any two length $t = 2^u$ Bent Functions in $u$ variables 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 3: Let $\mathbf{s0_0}(\mathbf{x_U}) = x_0x_1 + x_1x_2 + x_2x_3$, $\mathbf{s1_0}(\mathbf{x_U}) = x_0x_1 + x_0x_2 + x_2x_3$ 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 (8) over $Z_{2^h}$ with tensor permutation we can use these two sequences to generate the (Almost) Bent family,

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

where $\mathbf{U} = \{q_0, q_1, \ldots, q_{u-1}\}$, $\mathbf{Z'_m} = \{r_0, r_1, \ldots, r_{m-u-1}\}$, $q_i \neq q_k$, $r_i \neq r_k$, $i \neq k$, $b_k \in Z_2$, $c_k, d \in Z_{2^h}$, $g \in \mathbf{Z'_m}$. By Lemma 7 PAPR invariance is 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 PAPR $= 2.0$ under HT for $j$ odd.

**Corollary 9** *Let $\mathbf{s0_0}(x)$ and $\mathbf{s1_0}(x)$ be any two length $t = 2^u$ Bent and Negabent Functions in $u$ variables 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 $m = u + j$ variables over $Z_{2^h}$ and, when $h = 1$, comprises Bent and Negabent functions for $j = 0$ mod 6.*

Example 3 is also an example for Corollary 9. Corollaries 2 and 9 and a similar one for Negabent sequences allows us to 'seed' many more Bent, Negabent and Bent/Negabent sequences with degree higher than quadratic.

### *5.1 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 (8), can be used to generate families of length

[2] This corollary has also recently been presented in Theorems 4 and 5 of [2], but not in the context of Rudin-Shapiro.

$N = t2^{m-u}$ sequences over $Z_{2^h}$ which have PAPR $\leq \upsilon$ under **all** length-$N$ CDFTs. In particular we find pairs of length $t = 2^u$, and present sets of length $2^m$ with PAPR $\leq \upsilon \leq 4.0$ in Table 1. In [3,8] 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 [3,8].

**Corollary 10** *Let* $\mathbf{s0_0}$ *and* $\mathbf{s1_0}$ *be length* $t = 2^u$ *binary sequences whose one-dimensional 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 one-dimensional Fourier PAPR* $\leq \upsilon$*. Table 1 shows such sets for* $u = 0, 1, 2$ *and* $\mathbf{U} \subset \{0, 1, 2, 3, 4\}$*, for cases* $\upsilon \leq 4.0$ [3]*.*

For the CHT examples previously discussed all choices and orderings of seed variables leave PAPR invariant (Lemma 7). In the case of CDFT PAPR, Lemma 7 does not hold. However 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 $q_i < q_{i+1}$.

**Lemma 11** *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* $q_i$*.*

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. Here is the complete set having PAPR $\leq 3.5396$,

$$
\begin{aligned}
{}_{\mathbf{3a}}\mathbf{\Gamma^1} &= {}_{\mathbf{3a}}\mathbf{\Theta}(\mathbf{x_U}, x_g) + \mathbf{DJ_{m-u,h}}(\mathbf{x_{Z'_m}}), \qquad \mathbf{U} = \{z, z+1\}, g \in \mathbf{Z'_m} \\
{}_{\mathbf{3a}}\mathbf{\Theta}(p, q, \tau) &= 2^{h-1}(pq + \tau(q + p) + b_1 q + b_0 p), \\
&\text{where} \quad b_0, b_1 \in \{0, 1\}, \qquad x_i \in Z_{2^h}, \forall i
\end{aligned} \tag{18}
$$

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, 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 ${}_{\mathbf{3a}}\mathbf{\Theta}$, e.g. the ANF form $x_2x_0 + x_3x_0 + x_2x_3 + x_2 + x_1x_5 + x_5x_4 + x_4x_0 + x_1 + 1$ has a PAPR $\leq 3.5396$, 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 term $x_1$. The following set has PAPR $\leq 3.8570$,

[3] further results for $u = 3$ can be found in [7]

$_{\mathbf{3a}}\mathbf{\Gamma^2} = {}_{\mathbf{3a}}\mathbf{\Theta}(\mathbf{x_U}, x_g) + \mathbf{DJ_{m-u,h}}(\mathbf{x_{Z'_m}}), \qquad \mathbf{U} = \{z, z+2\}, g \in \mathbf{Z'_m}$
$_{\mathbf{3a}}\mathbf{\Gamma^2}$ has exactly the same algebraic structure as $_{\mathbf{3a}}\mathbf{\Gamma^1}$, but $_{\mathbf{3a}}\mathbf{\Theta}$ is, instead, constructed over $x_0, x_2, x_g$. 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 $2^{m-2}$. Table 1 shows $\mathbf{\Gamma}$-sets using 1,2,3-variable seeds with PAPR $\leq 4.0$. We also use reversal symmetry to halve the number of inequivalent representatives for some $\mathbf{\Gamma}$ sets, (indicated by 'with R'). $_{\mathbf{1}}\mathbf{\Gamma}$ of Table 1 is an alternative derivation for a complementary set of size 4. The size of each $\mathbf{\Gamma}$-set is also shown in Table 1, relative to the size, $D$, of $\mathbf{DJ_{m,h}}$.

Table 1
Rudin-Shapiro Extensions Using $u + 1 = 1, 2, 3$-Variable Seeds

| $\mathbf{\Gamma}$ | $\frac{\mathbf{\Theta}(x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(\tau)}{2^{h-1}}$ | $\upsilon$ | $\lvert\mathbf{\Gamma}\rvert$ |
|---|---|---|---|
| $_{\mathbf{0}}\mathbf{\Gamma}$ | 0 | 2.0000 | $D$ |
| $\mathbf{\Gamma}$ | $\frac{\mathbf{\Theta}(x_z, x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,\tau)}{2^{h-1}}$ | $\upsilon$ | $\lvert\mathbf{\Gamma}\rvert$ |
| $_{\mathbf{1}}\mathbf{\Gamma}$ | $b_0 p$ | 4.0000 | $2^{1-h} D$ |
| $\mathbf{\Gamma}$ | $\frac{\mathbf{\Theta}(\mathbf{x_U}, x_g)}{2^{h-1}} = \frac{\mathbf{\Theta}(p,q,\tau)}{2^{h-1}}$ | $\upsilon$ | $\lvert\mathbf{\Gamma}\rvert$ |
| $_{\mathbf{2}}\mathbf{\Gamma^1}$ | $pq\tau +$ <br> $\{pq + q, q\} + b_0 p$ with R | 3.0000 | $\frac{2^{3-2h}}{m} D$ |
| $_{\mathbf{3}}\mathbf{\Gamma^1}$ | $pq + b_1 q + b_0 p$ | 3.5396 | $\frac{2^{2-2h}}{m} D$ |
| $_{\mathbf{3a}}\mathbf{\Gamma^1}$ | $pq + \tau(q+p) + b_1 q + b_0 p$ | 3.5396 | $\frac{2^{2-2h}}{m} D$ |
| $_{\mathbf{3}}\mathbf{\Gamma^2}$ | | 3.8570 | $\frac{2^{2-2h}(m-2)}{m(m-1)} D$ |
| $_{\mathbf{3a}}\mathbf{\Gamma^2}$ | | 3.8570 | $\frac{2^{2-2h}(m-2)}{m(m-1)} D$ |
| $_{\mathbf{3}}\mathbf{\Gamma^3}$ | | 3.9622 | $\frac{2^{2-2h}(m-3)}{m(m-1)} D$ |
| $_{\mathbf{3a}}\mathbf{\Gamma^3}$ | | 3.9622 | $\frac{2^{2-2h}(m-3)}{m(m-1)} D$ |
| $_{\mathbf{3}}\mathbf{\Gamma^4}$ | | 3.9904 | $\frac{2^{2-2h}(m-4)}{m(m-1)} D$ |
| $_{\mathbf{3a}}\mathbf{\Gamma^4}$ | | 3.9904 | $\frac{2^{2-2h}(m-4)}{m(m-1)} D$ |
| $_{\mathbf{3}}\mathbf{\Gamma^5}$ | | 3.9976 | $\frac{2^{2-2h}(m-5)}{m(m-1)} D$ |
| $_{\mathbf{3a}}\mathbf{\Gamma^5}$ | | 3.9976 | $\frac{2^{2-2h}(m-5)}{m(m-1)} D$ |
| $_{\mathbf{4}}\mathbf{\Gamma^1}$ | $\tau(p+q) + b_1 q + b_0 p$ | 4.0000 | $\frac{2^{2-2h}}{m} D$ |
| $_{\mathbf{4}}\mathbf{\Gamma^2}$ | | 4.0000 | $\frac{2^{2-2h}(m-2)}{m(m-1)} D$ |
| $_{\mathbf{4}}\mathbf{\Gamma^3}$ | | 4.0000 | $\frac{2^{2-2h}(m-3)}{m(m-1)} D$ |
| $_{\mathbf{4}}\mathbf{\Gamma^4}$ | | 4.0000 | $\frac{2^{2-2h}(m-4)}{m(m-1)} D$ |
| $_{\mathbf{4}}\mathbf{\Gamma^5}$ | | 4.0000 | $\frac{2^{2-2h}(m-5)}{m(m-1)} D$ |

$b_0, b_1 \in \{0, 1\}$, $\qquad D = \lvert\mathbf{DJ_{m,h}}\rvert = \left(\frac{m!}{2}\right) 2^{h(m+1)}$

## 6 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. We identified two sets of transforms, namely the one-dimensional Consta-Discrete Fourier Transforms, and $m$-dimensional Constahadamard Transforms, both of whose rows are from $\mathbf{L_m}$. 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 identified new low PAPR families not necessarily limited to quadratic degree.

## References


[1] 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

[2] 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

[3] 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

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

[5] 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

[6] M.G.Parker, "The Constabent Properties of Golay-Davis-Jedwab Sequences," *Int. Symp. Information Theory, Sorrento, Italy*, June 25-30, 2000

[7] M.G.Parker,C.Tellambura, "Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions," *To be Submitted, Preprint available on /∼matthew/MattWeb.html*, 2000

[8] 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

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

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