REPORTS
IN
INFORMATICS

ISSN 0333-3590

A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio

Matthew G. Parker and Chintha Tellambura

REPORT NO 242 **February 2003**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL
http://www.ii.uib.no/publikasjoner/texrap/ps/2003-242.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio

Matthew G. Parker* and Chintha Tellambura†

20th February 2003

Abstract

A recursive construction is provided for sequence sets which possess good Hamming Distance and low Peak-to-Average Power Ratio (PAR) with respect to **any** Local Unitary Unimodular Transform (including all one and multi-dimensional Discrete Fourier Transforms).

1 Introduction

Pairs of Golay Complementary Sequences (CS) have the property that the sidelobes of the Aperiodic Autocorrelation of each sequence in the pair sum to zero [7]. Consequently they have found application in the areas of Telecommunications and Physics for such tasks as channel-sounding, spread-spectrum, and synchronization. It follows that the Peak-to-Average Power Ratio (PAR) with respect to the one-dimensional continuous Discrete Fourier Transform (DFT_1^∞) of each sequence in the pair satisfies PAR ≤ 2. For lengths 2^n one can generate CS pairs using Golay-Rudin-Shapiro (RuS) construction [28, 29]. However it has not yet been proved that all length 2^n CS can be constructed using RuS as $n \rightarrow \infty$. Davis and Jedwab have shown that the RuS set comprise a union of certain binary quadratic cosets of Reed-Muller (RM) $(1,n)$ when expressed in Algebraic Normal Form (ANF)[4]. Moreover, as these sequences are a subset of $\mathrm{RM}(2,n)$, then the Hamming Distance, D, between sequences in the set satisfies $D \geq 2^{n-2}$. Although the properties of RuS and CS pairs have been known for many years, the description of [4] brought together and formalised much of this work in the context of Reed-Muller codes. This was in response to the pressing demand of Orthogonal Frequency Division Multiplexing (OFDM) communications systems for error-correcting codes where each codeword also has low PAR with respect to (wrt) DFT_1^∞. The low PAR is required to alleviate the linearity requirements of the amplifier at the transmitter. The question of error-correcting codes with low PAR wrt DFT_1^∞ was highlighted by [10], prompting a great deal of research culminating in the fundamental codeset of Davis and Jedwab (DJ set), as outlined in the papers of [4, 23] (equation (6) of this paper), which exploit the properties of RuS. However, a communications engineer will probably point out that the major weakness of the DJ set for OFDM is that its code rate only remains acceptably high for up to about 32 frequency carriers, the

*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/, Author funded by NFR Project Number 119390/431

†C. Tellambura is with the Department of Electrical and Computer Engineering, Electrical and Computer Engineering Research Facility, University of Alberta, Edmonton, Alberta, Canada, T6G 2V4. E-mail: chintha@ee.ualberta.ca. Phone/Fax: +780-492-7228(1811)

rate vanishing as $n \to \infty$, and most current OFDM systems require anywhere from 256 to 8192 frequency carriers. Therefore, in practise, most engineers will implement some form of clipping or Selected-Mapping in order to reduce spectral peaks (PAR) at the OFDM transmitter. In other words, instead of constructing and sending a sequence, the transmitter will generate an arbitrary sequence or sequences, test their PARs, then either clip their peaks before transmission or choose to send the sequence with lowest PAR. Constructive techniques can avoid all this testing, but a major requirement for any constructive coding technique is that its rate remains acceptably high for large numbers of carriers. Higher rates are certainly possible and desirable for PAR $\leq O(n)$ and D large [24]. A generalisation of RuS construction to other starting seeds [16, 17] allows inclusion of more low PAR quadratic cosets of $\mathrm{RM}(1, n)$ in the code, thereby improving code rate somewhat. Higher degree cosets can also be added, marginally increasing code rate at price of distance, D, which decreases. However the rate remains unacceptably low for more than about 32 carriers.

This paper provides new answers to this problem by defining constructive techniques for low PAR error-correcting codes of blocklength > 32 with acceptable rate. For instance, we can (almost) construct a rate $\frac{1}{3}$ code of length 64 with distance 16 and PAR ≤ 4.0, a rate $\frac{2}{3}$ code of length 64, distance 4, and PAR ≤ 8.0, and a rate $\frac{1}{2}$ code of length 256, distance 4, and PAR ≤ 16.0. We emphasise 'almost' because, although we most certainly identify and algebraically describe very large codesets with low PAR, our constructions are not strictly implementable yet, due to certain edge symmetries (coding collisions) which compromise invertibility of the encoding. It remains an open challenge to eliminate these coding collisions, and part of the aim of this paper is to present and motivate this challenge in a clear way.

It turns out that our construction also requires the ability to generate all distinct permutation polynomials from $Z_2^t \to Z_2^t$ of algebraic degree $\leq d$ for some d, $1 \leq d < t$. To the best knowledge of the authors, such an algorithm only exists in the literature for the case $d = 1$ (namely "Bruhat Decomposition", or as encountered when generating all possible binary linear error-correcting codes of maximum rank and length) and, for $d = 1$, there are $\prod_{i=0}^{t-1}(2^t - 2^i)$ such polynomials. This paper provides strong motivation to develop further algorithms for the cases $1 < d < t$, along with the enumeration of the size of such sets as t varies.

Another aim of this paper is to advertise the fact that RuS sequences, and their generalisation as described in this paper, have a much stronger property than just a low PAR upper bound wrt the DFT_1^∞. [13, 16, 17, 25] have all pointed out the Bent/Almost Bent properties of the RuS set, and [16, 17] and this paper proves that the RuS set, and their generalisations satisfy PAR $\leq 2^t$ wrt <u>all</u> possible Linear Unitary Unimodular Transforms (LUUTs), including DFT_1^∞ and Walsh-Hadamard Transform (WHT). We will define LUUTs in the sequel. Consequently, the RuS construction and its generalisation have relevance also to Multi-Code CDMA [16, 17, 25], Weight Hierarchy and Quantum Entanglement [18, 19], and Cryptography [27].

To summarise, the main new contributions of this paper are as follows:

- A proposal to measure PAR wrt the infinite set of Linear Unimodular Unitary Transforms (LUUTs), whose rows comprise all possible linear unimodular sequences. This set includes DFT_1^∞, the Walsh-Hadamard Transform (WHT), and many other transforms.
- A construction (Constructions 1 - 3) for large sets of sequences with tight constant upper bound on PAR and good distance properties, where PAR is computed wrt the

infinite set of LUUTs.

Although we acknowledge that our constructions are implicitly covered in the literature by Golay [6, 7], Turyn [34], and others [33, 5], wrt DFT_1^∞, no mention in the literature is given of low PAR constructions wrt to the much larger set of LUUTs and, apart from the special case considered by Davis and Jedwab [4] wrt DFT_1^∞, and the case of low PAR wrt the WHT [3, 25], no attempt has been made to express these constructions in concise Algebraic Normal Form (ANF) or to consider the construction of such sequences, or to consider the Hamming Distance between members of the sequence set.

Our Construction as a Generalisation of Golay-Rudin-Shapiro Construction:
Golay-Rudin-Shapiro (RuS) sequences are a special case of Golay Complementary Pairs as first introduced by Marcel Golay [6, 22]. RuS sequence construction [7, 28, 29] exploits the recursion,

$$\begin{aligned} \mathbf{a}' &= \mathbf{a}|\mathbf{b} \\ \mathbf{b}' &= \mathbf{a}|\overline{\mathbf{b}} \end{aligned} \tag{1}$$

where $\mathbf{a}$ and $\mathbf{b}$ are both bipolar sequences of length N, $\mathbf{a}'$ and $\mathbf{b}'$ are both sequences of length $2N$, '$|$' means concatenation, and $\overline{\mathbf{b}}$ means the multiplication of elements of $\mathbf{b}$ by -1. The key observation that motivates the constructions of this paper is that we can write (1) as,

$$(\mathbf{a}', \mathbf{b}')^T = \mathbf{E} \odot \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{a} & \mathbf{b} \end{pmatrix}$$

where $\mathbf{E} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and '$\odot$' means point-multiplication of matrix elements. For instance, if $a = (1, 1)$ and $b = (1, -1)$, then $a' = (1, 1, 1, -1)$ and $b' = (1, 1, -1, 1)$.

This paper shows that RuS sequences satisfy PAR ≤ 2.0 wrt all LUUTs <u>precisely</u> because $\mathbf{E}$ is an orthogonal 2×2 matrix. The RuS generalisation of this paper uses sequence recursion where successive $\mathbf{E}$ matrices are arbitrary $R \times R$ Hadamard matrices, such that the generated sequences have PAR $\leq R$. For a given canonical representation of a Hadamard matrix, $\mathbf{E}$, an arbitrary row/column permutation of $\mathbf{E}$ is specified by γ, for row permutation, and θ, for column permutation. In this paper we emphasise the case where $\mathbf{E}$ is the Walsh-Hadamard Transform (WHT) matrix, although the basic construction still works when $\mathbf{E}$ is a more general Hadamard matrix. Given that $\mathbf{E}$ is a WHT, the sequence construction is then primarily specified by the permutations γ_j and θ_j, at each stage of the recursion. As stated earlier, much of the difficulty relating to the construction of this paper arises from an attempt to classify, enumerate, and generate these permutations according to their algebraic degree, as these degrees determine the overall ANF degree of the constructed sequence, which in turn determines the (Reed-Muller) Hamming Distance of the code. This paper therefore gives a strong justification for future research into classification and enumeration of permutation polynomials according to maximum polynomial degree.

Construction 1 provides a way of generating low PAR error-correcting codes of any length, r^n, and over any alphabet. As a special case, Construction 2 generates binary codesets of length 2^n and PAR $\leq 2^t$, comprising ANFs up to degree μ, where $\mu \leq 2t - 2$ for $t > 1$, and $\mu = 2$ for $t = 1$. These codesets have PAR $\leq 2^t$ wrt **all** LUUTs, including one and multi-dimensional continuous DFTs [16, 17]. As LUUTs include WHTs, then our construction gives large codesets of (Near)-Bent functions [15, 3, 26]. These binary sequences are not just (Near)-Bent but are also distant from linear sequences over <u>all</u> (unimodular) alphabets, not just over Z_2 - a particularly strong cryptographic attribute. Construction 2 of this paper can be viewed as a recursive generalisation of a **two-sided** Maiorana-McFarland construction where our sequence set has low PAR wrt **all** LUUTs, not just WHT. We also provide an explicit generation method for the complete quadratic subset of Construction 2 using Bruhat decomposition [2, 1]. In [25], Paterson increases code rate, at the price of increased PAR wrt the WHT, by replacing the inherent one-to-one permutation of Maiorana-McFarland construction with a many-to-one map. Construction 3 of this paper similarly generalises Construction 2 by replacing the constituent permutations with many-to-one and/or one-to-many maps. Throughout this paper, we assume our sequences are of length r^n for some integers, r, n, although we emphasise the case where $r = 2$.

2 Linear Sequences, Linear Unimodular Unitary Transforms (LUUTs) and Peak-to-Average Power Ratio (PAR)

PAR is a spectral measure. We must therefore first define the transforms over which the spectrum is to be computed. We call these transforms *LUUTs* (defined below), and LUUTs have linear rows, so we first define linearity:

Definition 1. *Let $\mathbf{l} = (l_0, l_1, \ldots, l_{r^n-1})$ be a length r^n complex sequence. $\mathbf{l}$ is defined to be* unimodular *if $|l_i| = |l_j|$, $\forall i, j$,* unitary *if $\sum_{i=0}^{r^n-1} |l_i|^2 = 1$, and r*-linear *if,*

$$\begin{aligned} \mathbf{l} = &\quad (a_{0,0}, a_{0,1}, \ldots, a_{0,r-1}) \otimes (a_{1,0}, a_{1,1}, \ldots, a_{1,r-1}) \otimes \ldots \otimes (a_{n-1,0}, a_{n-1,1}, \ldots, a_{n-1,r-1}) \\ = &\quad \bigotimes_{i=0}^{n-1} (a_{i,0}, a_{i,1}, \ldots, a_{i,r-1}) \end{aligned}$$

where $\otimes$ is the 'left tensor product', such that $\mathbf{A} \otimes (B_0, B_1, \ldots) = (B_0\mathbf{A}, B_1\mathbf{A}, \ldots)$. For length r^n sequences where r is prime, r-linear is called linear.

For example,

$l = \frac{1}{\sqrt{2}}(1, 0, 0, 1)$ is a unitary sequence,
$l = \frac{1}{2}(1, 1, 1, -1)$ is a unimodular unitary sequence,
$l = \frac{1}{2}(1, -1, 1, -1) = \frac{1}{\sqrt{2}}(1, -1) \otimes \frac{1}{\sqrt{2}}(1, 1)$ is a linear, unimodular, unitary sequence

Definition 2. $\mathbf{L_{r,n}}$ *is the infinite set of length r^n complex r-linear, unitary, unimodular sequences.*

Definition 3. *A $r^n \times r^n$ matrix, $\mathbf{U}$, is* unitary *if $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I_{r^n}}$, where $\dagger$ means conjugate transpose, and $\mathbf{I_{r^n}}$ is the $r^n \times r^n$ identity matrix.*

Definition 4. *A $r^n \times r^n$ r-*Linear Unimodular Unitary Transform *(r-LUUT) matrix $\mathbf{L}$ has rows taken from $\mathbf{L_{r,n}}$ such that $\mathbf{L}\mathbf{L}^\dagger = \mathbf{I_{r^n}}$. When r is prime, $r^n \times r^n$ r-LUUTs are called* LUUTs. *Note that the set of $r^n \times r^n$ q-LUUTs is a subset of the set of $r^n \times r^n$ r-LUUTs iff $q|r$.*

Example LUUTs for $r = 2$: The $2^n \times 2^n$ Walsh-Hadamard (WHT) and Negahadamard (NHT) matrices are LUUTs defined by $\bigotimes_{i=0}^{n-1} \mathbf{H}$, and $\bigotimes_{i=0}^{n-1} \mathbf{N}$, respectively, where $\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\mathbf{N} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. For instance, for $n = 2$, the WHT is the LUUT whose rows have the following tensor decomposition:

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

Similarly, for $n = 2$, the NHT is the LUUT whose rows have the following tensor decomposition:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & i & i & -1 \\ 1 & -i & i & 1 \\ 1 & i & -i & 1 \\ 1 & -i & -i & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,i) & \otimes & (1,i) \\ (1,-i) & \otimes & (1,i) \\ (1,i) & \otimes & (1,-i) \\ (1,-i) & \otimes & (1,-i) \end{pmatrix}$$

where $i^4 = 1$.

Definition 5. *We define* DFT_1^∞ *for length* 2^n *vectors to be an infinite subset of* $2^n \times 2^n$ *LUUTs, the union of whose rows form a subset of* $\mathbf{L_{2,n}}$ *such that each row factors, as in Definition 1, into a tensor product of length-two vectors* $(a_{i,0}, a_{i,1})$ *which, in turn, must satisfy* $a_{i,0} = \frac{1}{\sqrt{2}}$, $a_{i,1} = \frac{\omega^{ik}}{\sqrt{2}}$ *for some fixed integer* k*, where* ω *is any complex root of unity.*

For instance, for $n = 2$, DFT_1^∞ includes the LUUT which is the 4-point one-dimensional Cyclic DFT whose rows have a tensor decomposition as follows:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,1) & \otimes & (1,1) \\ (1,i) & \otimes & (1,-1) \\ (1,-1) & \otimes & (1,1) \\ (1,-i) & \otimes & (1,-1) \end{pmatrix}$$

where $i^2 = -1$.

DFT_1^∞ also includes the LUUT which is the 4-point one-dimensional NegaCyclic DFT whose rows have a tensor decomposition as follows:

$$\frac{1}{2}\begin{pmatrix} 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^3 & \omega^6 & \omega \\ 1 & \omega^5 & \omega^2 & \omega^7 \\ 1 & \omega^7 & \omega^6 & \omega^5 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,\omega) & \otimes & (1,\omega^2) \\ (1,\omega^3) & \otimes & (1,\omega^6) \\ (1,\omega^5) & \otimes & (1,\omega^2) \\ (1,\omega^7) & \otimes & (1,\omega^6) \end{pmatrix}$$

where $\omega^4 = -1$.

By taking more and more 4×4 LUUTs of this form, we more closely approximate DFT_1^∞ for the case $r = 2, n = 2$. It is also helpful to notice that <u>all</u> rows of DFT_1^∞ occur as a subset of the rows of certain LUUTs formed from tensor products of 2×2 LUUTs. For instance, for $n = 2$, the rows of the 4×4 Cyclic DFT are contained in two rows of each of $\mathbf{H} \otimes \mathbf{H}$ and $\mathbf{N} \otimes \mathbf{H}$. Similarly, the rows of the 4×4 NegaCyclic DFT are contained in two rows of each of $\mathbf{W_1} \otimes \mathbf{N}$ and $\mathbf{W_3} \otimes \mathbf{N}$, where $\mathbf{W_1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \omega \\ 1 & -\omega \end{pmatrix}$, $\mathbf{W_3} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \omega^3 \\ 1 & -\omega^3 \end{pmatrix}$.

Having defined linear unimodular sequences, we are in a position to define PAR with respect to $\mathbf{L_{r,n}}$:

Definition 6. *Let* s_i *be the* i*th element of a length* r^n *vector,* $\mathbf{s}$*. Then* r*-PAR*$(\mathbf{s})$ *is computed by measuring the maximum possible correlation squared of* $\mathbf{s}$ *with* **any** *length* r^n r*-linear unimodular sequence,* $\mathbf{l} \in \mathbf{L_{r,n}}$*:*

$$r\text{-}PAR(\mathbf{s}) = r^n max_{\mathbf{l}\in\mathbf{L_{r,n}}}(|\mathbf{s}\cdot\mathbf{l}|^2) = r^n max_{\mathbf{l}\in\mathbf{L_{r,n}}}(|\sum_{i=0}^{r^n-1} s_i l_i^*|^2)$$

where $\cdot$ *means 'inner product', and* * *means complex conjugate. Similarly,*

$$PA(\mathbf{s}) = r^n max_{\mathbf{l}}(|\mathbf{s}\cdot\mathbf{l}|^2)$$

$\mathbf{l}$ *taken over all rows of a* **fixed, specified** *subset of* $r^n \times r^n$ *unitary transforms,* $\mathbf{U}$

For a length r^n *sequence, the values of* r*-PAR and PA range from* 1.0 *(for an ideal spectrally flat sequence) to* r^n *(for a spectral* δ*-function). When* r *is prime,* r*-PAR is termed PAR.*

We can compute r-PAR of $\mathbf{s}$ by examining the transform spectra of $\mathbf{s}$ wrt **all** r-LUUTs (more practically we can approximate this continuous spectrum by applying a large enough subset of well-chosen r-LUUTs).

Example: Let $\mathbf{s} = 2^{\frac{-3}{2}}(1,1,1,-1,1,-1,1,-1)$. Then PA$(\mathbf{s})$ wrt the LUUT, $\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N}$, is obtained by first computing the matrix-vector product:

$$\begin{aligned}
\mathbf{S} = (\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N})\mathbf{s} &= 2^{\frac{-3}{2}} \begin{pmatrix} 1 & 1 & 1 & 1 & i & i & i & i \\ 1 & -1 & 1 & -1 & i & -i & i & -i \\ 1 & 1 & -1 & -1 & i & i & -i & -i \\ 1 & -1 & -1 & 1 & i & -i & -i & i \\ 1 & 1 & 1 & 1 & -i & -i & -i & -i \\ 1 & -1 & 1 & -1 & -i & i & -i & i \\ 1 & 1 & -1 & -1 & -i & -i & i & i \\ 1 & -1 & -1 & 1 & -i & i & i & -i \end{pmatrix} 2^{\frac{-3}{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \\
&= 2^{-3} \begin{pmatrix} 2 \\ 2+4i \\ 2 \\ -2 \\ 2 \\ 2-4i \\ 2 \\ -2 \end{pmatrix}
\end{aligned}$$

The largest magnitude value in $\mathbf{S}$ is $2^{-3}(2 \pm 4i)$. It follows that PA$(\mathbf{s}) = 2^3(2^{-6}(2^2 + 4^2)) = 2.5$ wrt $\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N}$. This also means that PAR$(\mathbf{s})$ is lower bounded by 2.5.

2.1 Complementary Sequence Sets (CS Sets)

A Complementary Sequence Set (*CS set*) of R unitary sequences of length R' conventionally has the complementary property that the sum of the one-dimensional Aperiodic Autocorrelations of each sequence in the set results in the δ function of magnitude R (zero sidelobe energy) [7, 33]. Equivalently this means that the sum of the R DFT$_1^\infty$ power spectra of the sequences at each spectral index is $\frac{R}{R'}$, i.e. the DFT$_1^\infty$ power spectral sum of the sequences is completely flat at all spectral indices. This implies that each of the R sequences has PA$\leq R$ wrt the DFT$_1^\infty$. We now modify the CS definition as follows,

Definition 7. *We define the* Complementary Set *(*CS Set*) to mean a set of sequences which is complementary wrt any specified set of unitary transforms, $\{\mathcal{T}\}$, such that the sum of the power spectra of the set of R sequences of length R', wrt any member of the set, $\mathcal{T}$, sum to $\frac{R}{R'}$ at each spectral index [16, 21]. Therefore, for $\mathbf{s}$ a member of the CS set, PAR$(\mathbf{s}) \leq R$.*

We formalise this as follows:

Definition 8. *The rows of an $R \times R'$ matrix, $\mathbf{A}$, form a complementary set of R sequences wrt the set of $R' \times R'$ unitary transform matrices, $\mathcal{T}$, iff, for every $\mathcal{U} \in \mathcal{T}$, $\mathbf{b_i} = \frac{R'}{R}\mathbf{A}\mathbf{u_i^T}$ is unitary, where $\mathbf{u_i}$ is the ith row of $\mathcal{U}$, and the rows of $\mathbf{A}$ are unitary.*

Lemma 1 provides an initial starting CS set for the example of the next section and the subsequent constructions:

Lemma 1. *Let $\mathbf{A}$ be a $R \times R$ unitary matrix. Then the rows of $\mathbf{A}$ form a* CS set *of R sequences wrt all $R \times R$ unitary matrices.*

Proof. Let $\mathbf{B}$ be an $R \times R$ matrix with rows, $\mathbf{b_i}$, where the $\mathbf{b_i}$ are constructed as in Definition 8. Then $\mathbf{B} = \mathbf{A}\mathcal{U}^\mathbf{T}$. Similarly $\mathbf{B}^\dagger = \mathcal{U}^*\mathbf{A}^\dagger$, where $*$ means conjugate. Then $\mathbf{B}\mathbf{B}^\dagger = \mathbf{A}\mathcal{U}^\mathbf{T}\mathcal{U}^*\mathbf{A}^\dagger = \mathbf{I_R}$, where $\mathbf{I_R}$ is the $R \times R$ identity matrix. Therefore $\mathbf{B}$ is unitary which means all $\mathbf{b_i}$ are unitary, and Lemma 1 follows from Definition 8. $\square$

3 Construction Example

Before presenting the formal constructions of this paper, we first provide an example which highlights the main points of the constructions. For clarity of exposition we usually omit the normalisation constant for each matrix or sequence which would ensure the unitarity of the matrix or sequence. For instance, $\mathbf{A}$ below should be multiplied by $\frac{1}{2}$. We also provide and utilise ANFs, $p(x_0, x_1, \ldots, x_{n-1})$, for the binary sequence exponent of the bipolar sequences constructed, where the ith element, p_i of the length 2^n binary sequence, p, is given by $p(x_0 = i_0, x_1 = i_1, \ldots, x_{n-1} = i_{n-1})$, where $(i_0, i_1, \ldots, i_{n-1})$ is the 2-adic expansion of i. For instance, the function $p = x_0 + x_1$ has a truth table $\begin{array}{cc|c} x_0 & x_1 & p \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{array}$ which can be used to represent the sequence $(-1)^p = (-1)^{0110} = 1, -1, -1, 1$.

The construction strategy is as follows:

3.0.1 Choose Unitary Matrix

Choose, for example, the unitary matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} (-1)^0 \\ (-1)^{x_0} \\ (-1)^{x_1} \\ (-1)^{x_0+x_1} \end{pmatrix}$$

By Lemma 1 the four rows of $\mathbf{A}$ form a CS set wrt any 4×4 unitary matrix, i.e. any 4×4 4-LUUT. We can perform a number of operations on $\mathbf{A}$ to generate a length 16 bipolar sequence with 4-PAR ≤ 4.00 wrt any 4-LUUT (which includes any 2-LUUT).

3.0.2 Concatenate Rows:

Concatenating rows of $\mathbf{A}$ gives the length 16 sequence,

$$\mathbf{s} = 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad = (-1)^{x_0x_2+x_1x_3}$$

This sequence has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs including all 2-LUUTs. As will be shown, the upper bound is 4.0 because $\mathbf{A}$ is a 4×4 unitary matrix whose four rows form a CS set wrt all 4-LUUTs, which includes all 2-LUUTs. The transform set includes all 2-LUUTs because 2 divides 4. For example, $\mathbf{s}$ has PAs of 3.12, 1.00, and 4.00 wrt DFT$_1^\infty$, WHT, and NHT, respectively. (Note that PA wrt DFT$_1^\infty$ is computed approximately by taking the PA wrt enough 16×16 LUUTs of the form discussed in Definition 5. In other words we 'oversample' the one-dimensional DFT to sufficient precision).

3.0.3 Permute Rows and/or Columns Prior to Concatenation:

Choose any row/column permutation of $\mathbf{A}$ prior to concatenation. For example, choose the concatenation: Row 1 | Row 3 | Row 2 | Row 0, giving,

$$\begin{aligned} \mathbf{s} &= 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \\ &= (-1)^{x_0x_3+x_1x_2+x_1x_3+x_0} \end{aligned}$$

This sequence also has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 1.95, 1.00, and 1.00 under DFT$_1^\infty$, WHT, and NHT, respectively.

As another example, consider the column permutation: Col 3,Col 0,Col 2,Col 1, followed by the row permutation and concatenation: Row 2 | Row 3 | Row 0 | Row 1, giving,

$$\begin{aligned}\mathbf{s} &= -1\ \ 1\ \ -1\ \ 1\ \ 1\ \ 1\ \ -1\ \ -1\ \ 1\ \ 1\ \ 1\ \ 1\ \ -1\ \ 1\ \ 1\ \ -1 \\ &= (-1)^{x_0x_2+x_0x_3+x_1x_2+x_0+x_2+x_3+1}\end{aligned}$$

This sequence also has $\mathrm{PAR}(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 1.999, 1.00, and 1.00 wrt DFT_1^∞, WHT, and NHT, respectively. (Note that for 4×4 matrices, a combined row and column permutation is equivalent to a row (or column) permutation. This is not generally the case for square matrix dimension > 4).

3.0.4 Generate Cosets

Let $\mathbf{g}$ be any length-4 bipolar vector. Let us express $\mathbf{A}$ as

$$\mathbf{A} = \begin{pmatrix} \mathbf{a_0} \\ \mathbf{a_1} \\ \mathbf{a_2} \\ \mathbf{a_3} \end{pmatrix}$$

where the a_i are length-4 bipolar vectors.

Let $\mathbf{A^g}$ be any matrix of the form,

$$\mathbf{A^g} = \begin{pmatrix} \mathbf{a_0} \odot \mathbf{g} \\ \mathbf{a_1} \odot \mathbf{g} \\ \mathbf{a_2} \odot \mathbf{g} \\ \mathbf{a_3} \odot \mathbf{g} \end{pmatrix}$$

where $\mathbf{a} \odot \mathbf{g} = (a_0g_0, a_1g_1, \ldots, a_3g_3)$, For instance, let $\mathbf{g} = (1, 1, 1, -1)$. Then,

$$\mathbf{A^g} = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$$

Then concatenation of any row/column permutation of $\mathbf{A^g}$ also has 4-PAR ≤ 4.0 wrt all 4-LUUTs, which includes all 2-LUUTs. As an example, consider the column permutation of $\mathbf{A^g}$: Col 0,Col 3,Col 2,Col 1, followed by the row permutation and concatenation: Row 1 | Row 3 | Row 0 | Row 2, giving,

$$\begin{aligned}\mathbf{s} &= 1\ \ 1\ \ 1\ \ -1\ \ 1\ \ -1\ \ -1\ \ -1\ \ 1\ \ -1\ \ 1\ \ 1\ \ 1\ \ 1\ \ -1\ \ 1 \\ &= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_1x_2}\end{aligned}$$

This sequence has 4-$\mathrm{PAR}(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including 2-LUUTs. For example, $\mathbf{s}$ has PAs of 2.97, 1.00, and 2.00 wrt DFT_1^∞, WHT, and NHT, respectively.

3.0.5 Symmetric Permutation:

Definition 9. *Let π be any permutation of Z_n. Then π_r is defined to be any* r-symmetric permutation *of Z_{r^n}, where $\pi_r(i) = \sum_{k=0}^{n-1} i_{\pi(k)} r^k$, and i has a radix-r decomposition as $\sum_{k=0}^{n-1} i_k r^k$, $i_k \in Z_r$, $\forall k$. We can then write the r-symmetric permutation of $\mathbf{s}$ as,*

$$\pi_r(\mathbf{s}) = (s_{\pi_r(0)}, s_{\pi_r(1)}, \ldots, s_{\pi_r(r^n-1)})$$

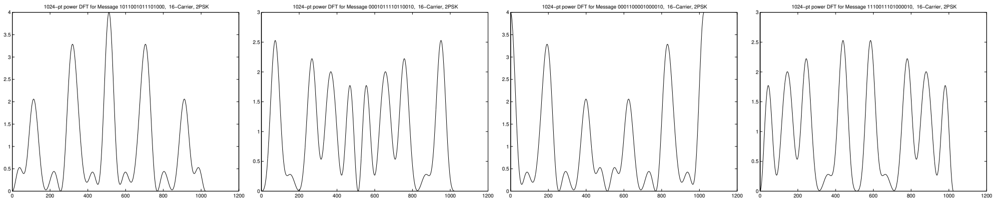

Figure 1: Power Spectrums for Size-4 Complementary Set, $\{\mathbf{s_0}, \mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}\}$, wrt DFT_1^∞ (x-axis is spectral index, y-axis is power value)

If $\mathbf{s}$ has 4-PAR ≤ 4.0 wrt all 4-LUUTs, then $\pi_2(\mathbf{s})$ has PAR ≤ 4.0 wrt all 2-LUUTs. (Note that because π_2 is a radix-2 permutation, the PAR upper bound no longer covers all 4-LUUTs). For instance, we have just stated that
$\mathbf{s} = 1,1,1,-1,1,-1,-1,-1,1,-1,1,1,1,-1,1$ has 4-PAR ≤ 4.0 wrt all 4-LUUTs. Let $\pi = (0)(1,2,3)$ be a permutation of Z_4. Then π_2 permutes the indices of $\mathbf{s}$ according to $(0)(1)(2,4,8)(3,5,9)(6,12,10)(7,13,11)(14)(15)$ to give,

$$\begin{aligned} \mathbf{s} &= 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \\ &= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_2x_3} \end{aligned}$$

This sequence has $\mathrm{PAR}(\mathbf{s}) \leq 4.0$ wrt all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 2.56, 1.00, and 2.00 wrt DFT_1^∞, WHT, and NHT, respectively.

3.0.6 Form Complementary Sequence (CS) Set:

Let $\mathbf{E}$ be another 4×4 unitary matrix (it could be the same as $\mathbf{A}$). For example,

$$\mathbf{E} = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

where the element at row i and column j is $e_{i,j}$. For any row and/or column permutation of $\mathbf{A}$ (or $\mathbf{A^g}$) we can form four length-16 CS. For instance, from subsection 3.0.4, let our constructed sequence be,
$\mathbf{s} = \mathbf{a_0^g}|\mathbf{a_1^g}|\mathbf{a_2^g}|\mathbf{a_3^g} = 1,1,1,-1,1,-1,-1,-1,1,-1,1,1,1,1,-1,1$, where
$\mathbf{a_0^g} = 1,1,1,-1$, $\mathbf{a_1^g} = 1,-1,-1,-1$, $\mathbf{a_2^g} = 1,-1,1,1$, $\mathbf{a_3^g} = 1,1,-1,1$. Then our size-4 CS set is:

$$\begin{array}{l} \mathbf{s_0} = e_{0,0}\mathbf{a_0^g}|e_{0,1}\mathbf{a_1^g}|e_{0,2}\mathbf{a_2^g}|e_{0,3}\mathbf{a_3^g} = \quad + \; + \; + \; - \; + \; - \; - \; - \; + \; - \; + \; + \; - \; - \; + \; - \\ \mathbf{s_1} = e_{1,0}\mathbf{a_0^g}|e_{1,1}\mathbf{a_1^g}|e_{1,2}\mathbf{a_2^g}|e_{1,3}\mathbf{a_3^g} = \quad + \; + \; + \; - \; + \; - \; - \; - \; - \; + \; - \; - \; + \; + \; - \; + \\ \mathbf{s_2} = e_{2,0}\mathbf{a_0^g}|e_{2,1}\mathbf{a_1^g}|e_{2,2}\mathbf{a_2^g}|e_{2,3}\mathbf{a_3^g} = \quad + \; + \; + \; - \; - \; + \; + \; + \; + \; - \; + \; + \; + \; + \; - \; + \\ \mathbf{s_3} = e_{3,0}\mathbf{a_0^g}|e_{3,1}\mathbf{a_1^g}|e_{3,2}\mathbf{a_2^g}|e_{3,3}\mathbf{a_3^g} = \quad - \; - \; - \; + \; + \; - \; - \; - \; + \; - \; + \; + \; + \; + \; - \; + \end{array}$$

where '$+$' is 1 and '$-$' is -1.

Then $|\mathbf{s_0} \cdot \mathbf{l}|^2 + |\mathbf{s_1} \cdot \mathbf{l}|^2 + |\mathbf{s_2} \cdot \mathbf{l}|^2 + |\mathbf{s_3} \cdot \mathbf{l}|^2 = 4.0$ for $\mathbf{l}$ 4-linear. In other words, the four sequences, $\mathbf{s_i}$, form a size-4 CS set wrt any 4-LUUT, which includes any 2-LUUT, as the sum of their power spectrums wrt any 4-LUUT is a constant at every point. Therefore each sequence satisfies 4-PAR$(\mathbf{s_i}) \leq 4.0$ wrt any 4-LUUT, which includes any 2-LUUT. The power spectrums wrt DFT_1^∞ for each sequence of the above CS set are shown in Fig 1, and the spectrums sum to 4.0 at each spectral index. The power spectrums wrt the 16-point

WHT for each of the four sequences are as follows:

Sequence	Power Spectrum															
$\mathbf{s_0}$	0	4	0	0	4	0	0	0	0	0	4	0	0	0	0	4
$\mathbf{s_1}$	0	0	4	0	0	0	0	4	0	4	0	0	4	0	0	0
$\mathbf{s_2}$	4	0	0	0	0	4	0	0	0	0	0	4	0	0	4	0
$\mathbf{s_3}$	0	0	0	4	0	0	4	0	4	0	0	0	0	4	0	0

The power spectrums wrt the 16-point NHT for each of the four sequences are as follows:

Sequence	Power Spectrum															
$\mathbf{s_0}$	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
$\mathbf{s_1}$	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
$\mathbf{s_2}$	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
$\mathbf{s_3}$	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0

In all cases the power spectrums sum to 4.0 at each point. Furthermore, the sequences, $\pi_2(\mathbf{s_i})$ also form a size-4 CS set wrt any 2-LUUT, for any π_2.

3.0.7 Iterate Construction:

Let us now assign

$$\mathbf{A}' = \begin{pmatrix} \mathbf{s_0} \\ \mathbf{s_1} \\ \mathbf{s_2} \\ \mathbf{s_3} \end{pmatrix} = \begin{pmatrix} e_{0,0}\mathbf{a_0^g} & e_{0,1}\mathbf{a_1^g} & e_{0,2}\mathbf{a_2^g} & e_{0,3}\mathbf{a_3^g} \\ e_{1,0}\mathbf{a_0^g} & e_{1,1}\mathbf{a_1^g} & e_{1,2}\mathbf{a_2^g} & e_{1,3}\mathbf{a_3^g} \\ e_{2,0}\mathbf{a_0^g} & e_{2,1}\mathbf{a_1^g} & e_{2,2}\mathbf{a_2^g} & e_{2,3}\mathbf{a_3^g} \\ e_{3,0}\mathbf{a_0^g} & e_{3,1}\mathbf{a_1^g} & e_{3,2}\mathbf{a_2^g} & e_{3,3}\mathbf{a_3^g} \end{pmatrix}$$

for any size-4 CS set of length 16 sequences, $\mathbf{s_i}$, as constructed using the previous subsections. Let $\mathbf{E}'$ be any 4×4 unitary matrix. For instance,

$$\mathbf{E}' = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\mathbf{A}'$ takes the place of the $\mathbf{A}$ matrix discussed previously. We again perform row permutation or column-segment permutation of $\mathbf{A}'$, with optional coset offset and symmetric permutation to construct sequences of length 64 with 4-PAR ≤ 4.0 wrt any 4-LUUT. (Note that we refer to column-segment permutation because we only permute the 4 segments of each row of $\mathbf{A}'$). $\mathbf{E}'$ now takes the place of the $\mathbf{E}$ matrix discussed previously, allowing us to construct size-4 CS sets of length 64 whose power spectrums sum to a constant wrt any 4-LUUT. For example, we can concatenate the sequences $\mathbf{s_i}$, constructed in subsection 3.0.6, to get the length 64 sequence,

+++−+−−−+−++−−+−+++−+−−−−+−−++−++++−−++++−++++−+−−−++−−−+−++++−+

$$= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_2x_3+x_2x_5+x_3x_4+x_4x_5}$$

where '$+$' and '$-$' are short for 1 and -1, respectively. This sequence has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 3.01, 1.00, and 1.00 wrt DFT$_1^\infty$, WHT, and NHT, respectively. Using $\mathbf{E}'$ we can construct the size-4 CS set,

+++−+−−−+−++−−+−+++−+−−−−+−−++−+−−−++−−−−+−−−−+−+++−−+++−+−−−−+−
+++−+−−−+−++−−+−−−−+−++++−++−−+−+++−−++++−++++−++++−−+++−+−−−−+−
+++−+−−−+−++−−+−+++−+−−−−+−−++−++++−−++++−++++−+−−−++−−−+−++++−+
+++−+−−−+−++−−+−−−−+−++++−++−−+−−−−++−−−−+−−−−+−−−−++−−−+−++++−+

which is a set of 4 length-64 sequences whose power spectrums sum to a constant wrt any 4-LUUT, which includes any 2-LUUT.

We can iterate the contruction as many times as we like to produce sequences of length 2^{2L} for some positive integer L, where each sequence has 4-PAR ≤ 4.0 wrt any 4-LUUT. (If there is symmetric permutation by π_2 then each sequence generally only has PAR ≤ 4.0 wrt any 2-LUUT, not any 4-LUUT).

3.0.8 Summary of Example Construction

We summarise the construction operations as follows:

- 1. Choose a 4×4 unitary matrix, $\mathbf{A}$.
- 2. Permute rows and/or columns of $\mathbf{A}$.
- 3. Select length-4 sequence, $\mathbf{g}$, to act as coset offset for $\mathbf{A}$.
- 4. Choose 4×4 unitary matrix, $\mathbf{E}$.
- 5. Concatenate the rows of (permuted coset of) $\mathbf{A}$ and multiply each row-segment by the appropriate entry in $\mathbf{E}$, for each row of $\mathbf{E}$, to form a size-4 CS set of length 16 sequences with 4-PAR ≤ 4.0 wrt any 4-LUUT. Define this 4-set as a 4×16 matrix, $\mathbf{A}'$.
- 6. Iterate the construction L times by looping back to step 2, where $\mathbf{A}$, $\mathbf{E}$ and $\mathbf{g}$ are replaced by $\mathbf{A}'$, a new 4×4 unitary matrix, $\mathbf{E}'$, and a new length-4 unitary vector, $\mathbf{g}'$, respectively.
- 7. Finally, symmetrically permute each sequence in the size-4 CS set, using the same permutation, π_2, for each sequence, and define this set as a 4×4^L matrix, each row of which has PAR ≤ 4.0 wrt any 2-LUUT, and such that the four rows form a size-4 CS set.

Our construction can be fully specified by the sequence of 4×4 unitary matrices, $\mathbf{E_j}$, where $\mathbf{A} = \mathbf{A_0} = \mathbf{E_0}$, by the row/column permutations over Z_4 at each iteration, the coset offset at each iteration, the number of iterations of the construction, and the final symmetric permutation over $Z_{2^{2L}}$. Using this construction we can generate a vast number of sequences with low PAR wrt any 2-LUUT. However, the difficulty with the construction arises because the above constructive operations are not disjoint (orthogonal), so it is problematic to count the complete sequence set, and to design hardware/software to implement the construction without gneerating a (small) fraction of the sequences more than once. We tackle the quadratic case in subsection 4.4.

In subsection 4 we formalise the construction and generalise to r-PAR $\leq R$, for any R by using $R \times R$ matrices, $\mathbf{E_j}$, to recursively construct matrices, $\mathbf{A_j}$. Instead of applying the row/column permutations and coset offset to the $\mathbf{A_j}$ matrices, we shall, equivalently, apply these operations to the $\mathbf{E_j}$ matrices.

4 Constructions

4.1 Construction 1

Let $N = r^n$, $R = r^t$. Let $\mathbf{E_j}$ and $\mathbf{A_j}$, $0 \leq j < L$, be a sequence of $R \times R$ and $R \times R^{j+1}$ complex matrices, respectively, $\mathbf{E_j}$ a unitary, unimodular matrix with rows $\mathbf{e_{i,j}}$, $\mathbf{A_j}$ with unitary, unimodular rows, $\mathbf{a_{i,j}}$. Let γ_j and θ_j permute Z_R, and $\mathbf{E'_j}$, with rows $\mathbf{e'_{i,j}}$, be the row/column permutation of $\mathbf{E_j}$, specified by γ_j and θ_j, respectively. Let $\mathbf{A_0} = \mathbf{E'_0}$. Then $\mathbf{A_j}$ is formed as,

$$\mathbf{a_{i,j}} = (\mathbf{a_{0,j-1}}|\mathbf{a_{1,j-1}}|\ldots|\mathbf{a_{R-1,j-1}}) \odot (\mathbf{1} \otimes \mathbf{e'_{i,j}}) \tag{2}$$

where $\mathbf{x} \odot \mathbf{y} = (x_0y_0, x_1y_1, \ldots, x_{R^j-1}y_{R^j-1})$, $\mathbf{1}$ is the length R^j all-ones vector, $'|'$ means concatenation, and $\mathbf{e'_{i,j}}$ is the ith row of $\mathbf{E'_j}$.

Theorem 1. *Let $\mathbf{s}$ be a length $N = R^L$ row of $\mathbf{A_{L-1}}$. Then $\pi_r(\mathbf{s})$ satisfies r-PAR$(\pi_r(\mathbf{s})) \leq R$ wrt all $N \times N$ r-LUUTs, where π_r is any r-symmetric permutation of $\mathbf{s}$.*

Proof. Assume the rows of $\mathbf{A_{j-1}}$ form a size-R CS set wrt any r-LUUT. Let $\mathbf{l_j}$ and $\mathbf{l}$ be unitary unimodular r-linear rows of length R^{j+1} and R, respectively. Let $\mathbf{b} = R^{j-1}\mathbf{A_{j-1}}\mathbf{l^T_{j-1}}$. Then, by Definition 8, $\mathbf{b}$ is unitary. By Definitions 2,4,8, the rows of $\mathbf{A_j}$ must form a size-R CS set wrt any r-LUUT if $\mathbf{b'} = R^j\mathbf{A_j}(\mathbf{l_{j-1}} \otimes \mathbf{l})^T$ is unitary $\forall \mathbf{l_{j-1}}, \mathbf{l}$. This follows because $b'_i = \sum_{k=0}^{R-1}(\mathbf{a_{k,j-1}}\mathbf{l^T_{j-1}})(e'_{i,j,k}l_k) = \sum_{k=0}^{R-1} b_k e'_{i,j,k} l_k$ for $b'_k, b_k, e'_{i,j,k}$ and l_k the kth elements of $\mathbf{b'}$, $\mathbf{b}$,$\mathbf{e'_{i,j}}$ and $\mathbf{l}$, respectively. To make $\mathbf{b'}$ unitary, we require $P = R\sum_{i=0}^{R-1}|b'_i|^2 = R\sum_{i=0}^{R-1}|\sum_{k=0}^{R-1}(b_k e'_{i,k} l_k)|^2 = 1$. Let $\mathbf{z} = \sqrt{R}(b_0l_0, b_1l_1, \ldots, b_{R-1}l_{R-1})^T$, and $\mathbf{Z} = \mathbf{E'_j}\mathbf{z}$. Then $P = 1$ if $\mathbf{Z}$ is unitary, which follows by Parseval's Theorem if $\mathbf{E'_j}$ is a unitary matrix, and if $\mathbf{z}$ is unitary. $\mathbf{E'_j}\mathbf{z}$ is a unitary matrix and $\mathbf{z}$ is unitary because $\mathbf{b}$ is unitary and $\mathbf{l}$ is unitary <u>unimodular</u>. It follows that the rows of $\mathbf{A_j}$ form a size-R CS set if the rows of $\mathbf{A_{j-1}}$ form a size-R CS set. The induction is completed by noting that the rows of $\mathbf{A_0} = \mathbf{E'_0}$ form a size-R CS set. Finally, any r-symmetric permutation of $\mathbf{s}$ is allowed because $\mathbf{l}$ and $\mathbf{l_j}$ are both r-linear. $\square$

Note that, if $\mathbf{l_j}$ is not unimodular then Theorem 1 does not, in general, hold.

It is interesting to observe that the Hadamard matrix construction of [14] is related to the constructions of this paper. Using the terminology of [14], their construction is,

$$\mathbf{H} = \begin{pmatrix} c_{11} + \mathbf{B_1} & c_{12} + \mathbf{B_2} & \ldots & c_{1m} + \mathbf{B_m} \\ c_{21} + \mathbf{B_1} & c_{22} + \mathbf{B_2} & \ldots & c_{2m} + \mathbf{B_m} \\ \ldots & \ldots & \ldots & \ldots \\ c_{m1} + \mathbf{B_1} & c_{m2} + \mathbf{B_2} & \ldots & c_{mm} + \mathbf{B_m} \end{pmatrix}$$

where $\mathbf{C} = [c_{ij}]$, the $\mathbf{B_i}$ are $T \times T$ Hadamard matrices, and their alphabet comprises $\{0, 1\}$ instead of $\{1, -1\}$, and they use '$+$', mod 2, instead of $\times$. One can relate this construction to the first iteration of Construction 1 of our paper by equating our $\mathbf{E}$ matrix with their $\mathbf{C}$ matrix, assigning $T = m = R$, and by assigning $\mathbf{B_{i+1}}$ to be derived from $\mathbf{B_i}$ where every column of $\mathbf{B_i}$ is cyclically shifted round by one position. Then we pick out every Rth row of $\mathbf{H}$ to form a CS set of R sequences of length R^2, where every sequence has PAR $\leq R$ wrt all LUUTs. There are R such sets. It would be interesting to develop a classification of Hadamard matrices according to the worst-case PAR of the rows of the matrix.

PAR ≤ 8.0

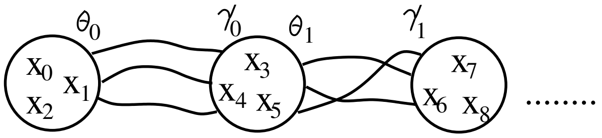

Figure 2: Construction 2 for $t = 3$

4.2 Construction 2 (special case of Construction 1)

Consider Construction 1. Let $r = 2$ *and all* $\mathbf{E_j}$ *be* $2^t \times 2^t$ *WHTs. Let* $\mathbf{x} = \{x_0, x_1, \ldots, x_{n-1}\}$ *be* n *binary variables. Then* $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{\mathbf{p(x)}}$*, where,*

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \theta_j(\mathbf{x_j})\gamma_j(\mathbf{x_{j+1}}) + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{3}$$

where θ_j *and* γ_j *are any permutations:* $Z_2^t \rightarrow Z_2^t$*,*
$\mathbf{x_j} = \{x_{\pi(tj)}, x_{\pi(tj+1)}, \ldots, x_{\pi(t(j+1)-1)}\}$*,* $n = Lt$*,* π *permutes* Z_n*, and* g_j *is any function from* $Z_2^t \rightarrow Z_2$*.*

To clarify (3) note that, $\forall j$, we can define $\rho(\mathbf{x_j}, \mathbf{x_{j+1}}) = \theta_j(\mathbf{x_j})\gamma_j(\mathbf{x_{j+1}})$ such that ρ can be expanded as the function $\rho : Z_2^{2t} \rightarrow Z_2$, $\rho(\mathbf{x_j}, \mathbf{x_{j+1}}) = \theta_{0,j}(\mathbf{x_j})\gamma_{0,j}(\mathbf{x_{j+1}}) + \theta_{1,j}(\mathbf{x_j})\gamma_{1,j}(\mathbf{x_{j+1}}) + \ldots + \theta_{t-1,j}(\mathbf{x_j})\gamma_{t-1,j}(\mathbf{x_{j+1}})$ where $\theta_j = (\theta_{0,j}, \theta_{1,j}, \ldots, \theta_{t-1,j})$, $\gamma_j = (\gamma_{0,j}, \gamma_{1,j}, \ldots, \gamma_{t-1,j})$ and all $\theta_{i,j}, \gamma_{i,j}$ are balanced functions : $Z_2^t \rightarrow Z_2$, chosen so that θ_j and γ_j are permutations.

Corollary 1. *The length* $N = 2^n$ *sequences,* $\mathbf{s}$*, of Construction 2, satisfy PAR*$(\mathbf{s}) \leq 2^t$ *wrt all* $N \times N$ *LUUTs.*

Proof. Construction 2 is a special case of Construction 1 where all $\mathbf{E_j}$ are $2^t \times 2^t$ WHTs. The Corollary therefore follows from Theorem 1. □

When $L = 2$ and when θ or γ is the identity permutation, then Construction 2 reduces to the Maiorana McFarland construction over $2t$ variables. [1] It is helpful to illustrate Construction 2 graphically, and Fig 2 illustrates the construction for $t = 3$, where we are also free to permute the indices, i, of x_i using π. An example for Fig 2 could be,

$$\begin{aligned} p(\mathbf{x}) = \quad & (x_0)(x_3 + x_5) + (x_1)(x_5) + (x_1 + x_2)(x_4) + (x_3 + x_4)(x_6 + x_7 + x_8) \\ & +(x_3)(x_6) + (x_5)(x_7) + g_0(x_0, x_1, x_2) + g_1(x_3, x_4, x_5) + g_2(x_6, x_7, x_8) \end{aligned}$$

where g_0, g_1, g_2 are any functions: $Z_2^3 \rightarrow Z_2$. This example has guaranteed 8-PAR ≤ 8.0 wrt all 8-LUUTs, which includes all 2-LUUTs, but with index permutation of the x_i, PAR ≤ 8.0 is only guaranteed wrt all 2-LUUTs.

Theorem 2. *For fixed* t*, let* $\mathbf{P}$ *be the subset of* $p(\mathbf{x})$ *of degree* μ *or less, generated using Construction 2. Then* $D \geq 2^{n-\mu}$*, where* D *is the Hamming Distance between members of*

[1]Thanks to V.Rijmen for pointing out the Maiorana-McFarland connection.

$\mathbf{P}$*, and,*

$$
\begin{array}{lll}
|\mathbf{P}| & \leq B = \frac{n!}{\Gamma}(\frac{2^{t+\binom{t}{2}}\Gamma}{t!})^{\frac{n}{t}} & \mu = 2 \\
& \leq B = \frac{n!}{V}(\frac{2^{2^t-1}V}{t!})^{\frac{n}{t}} & \mu = 2t-2, t > 1
\end{array} \quad (4)
$$

where $\Gamma = \prod_{i=0}^{t-1}(2^t - 2^i) = |GL(t,2)|$*, (GL is the General Linear Group), and* $V = ((2^t-1)!)^2 - (\Gamma^2 - \Gamma)$*. (For* $t = 1$ *the bound is exact). (Note that this paper does not give upper bounds on the size of* $\mathbf{P}$ *for the intermediate cases where* $2 < \mu < 2t-2$*.)*

Proof. The result on Hamming Distance, D, is a well-known propery of Reed-Muller codes [13]. Let us now prove (4). When $\mu = 2$ then θ and γ are linear permutations. In this case the two-way permutation, $\mathbf{x_j}\gamma(\mathbf{x_{j+1}})$, covers the same set of permutations as $\theta(\mathbf{x_j})\gamma(\mathbf{x_{j+1}})$. So we can set θ to the identity permutation. Each term, $\mathbf{x_j}\gamma_j(\mathbf{x_{j+1}})$, for γ_j linear, is isomorphic to GL$(t,2)$, where GL is the General Linear Group. Therefore we can represent the linear permutations at each iteration by the set, GL$(t,2)$ of binary invertible $t \times t$ matrices, where $\Gamma = |\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$. For $L = \frac{n}{t}$ and $L-1$ iterations we have Γ^{L-1} possible combinations of permutations. There are $\frac{1}{2}\prod_{i=1}^{L}\binom{it}{t}$ ways of ordering a linked line of subsets of t disjoint variables out of n variables. At each iteration we can choose g_j from one of $2^{t+\binom{t}{2}}$ quadratic functions of t variables. Over L iterations we therefore have a choice of $(2^{t+\binom{t}{2}})^L$ combinations of functions, g_j. The first part of (4) follows by noting that $\prod_{i=1}^{L}\binom{it}{t} = \frac{n!}{(t!)^L}$.
The case $\mu = 2t-2$ occurs when θ and γ are permutation polynomials each up to degree $t-1$ ($t-1$ is the maximum possible degree of a permutation polynomial from $Z_2^t \rightarrow Z_2^t$). Therefore each of θ and γ can be chosen from $\frac{(2^t)!}{2^t}$ different polynomials to make a total of $\left(\frac{(2^t)!}{2^t}\right)^2$ polynomial configurations for one iteration. [2] However remember that the case of $\theta\gamma$ quadratic corresponds to θ and γ both linear in which case we can, without loss of generality, make θ the identity. Therefore instead of contributing Γ^2 configurations, the case of $\theta\gamma$ quadratic contributes only Γ configurations, so the total number of polynomial configurations after one iteration is $V = \frac{(2^t)!}{2^t} - (\Gamma^2 - \Gamma)$. Therefore, after $L-1$ iterations we have V^{L-1} possible combinations of permutations. We therefore replace Γ in the first line of equation (4) with V. At each iteration we can now choose g from one of 2^{2^t-1} functions of t variables of degree $\leq t$ (ignoring constant offset). The second part of (4) follows. □

Definition 10. *A* $[2^n, k, D, W]$ *nonlinear error-correcting code has length* 2^n*, dimension* k *(*$\log_2$ *of the number of codewords), Hamming Distance* D*, and each codeword has PAR* $\leq W$ *wrt all LUUTs.*

Corollary 2. *Application of Construction 2 and reference to Theorem 2 allows us to construct and parameterise* $[2^n, \log_2(|\mathbf{P}|), 2^{n-\mu}, 2^t]$ *nonlinear error-correcting codes.*

4.3 Examples for Construction 2

The WHT, NHT, and DFT$_1^\infty$ are used as 'spot-checks' in the following examples to validate the PAR upper-bound. Furthermore, the PAR is lower-bounded by the maximum PAR resulting from these three spot-checks.

[2] Note that we divide by 2^t so as not to include all offsets of the permutation θ (or γ) by the constant '1', i.e. we ignore permutations which have one or more constituent elements of the form $\theta_{i,j}(\mathbf{x_j}) + 1$ (or $\gamma_{i,j}(\mathbf{x_j}) + 1$). These constant offsets to the permutations are implicitly included by suitable assignments to the g_j polynomials in (5).

There are, of course, an infinite number of LUUTs, all of which validate the PAR upper-bound for the constructed set.

4.3.1 Example 1, Identity Permutations

Let θ_j and γ_j be identity permutations $\forall j$. Then, $\theta(\mathbf{x_j}) = \gamma(\mathbf{x_j}) = \mathbf{x_j}$ and Construction 2 becomes,

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} x_{\pi(t(j+1)+l)} + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{5}$$

When $\deg(g_j) < 2, \forall j$, it is well-known that $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})}$ is Bent (PA $= 1$ wrt the WHT) for L even [13] and (perhaps not known) that $\mathbf{s}$ has PA $= 2^t$ wrt the WHT for L odd. In general, for any g_j, $\mathbf{s}$ has PAR $\leq 2^t$ wrt all LUUTs. For example, if $L = 4$, $t = 3$, and $p(\mathbf{x}) = x_0x_3 + x_1x_4 + x_2x_5 + x_3x_6 + x_4x_7 + x_5x_8 + x_6x_9 + x_7x_{10} + x_8x_{11}$, then $\mathbf{s}$ has PA $= 1.0$ wrt WHT and NHT, and PA $= 7.09$ wrt DFT$_1^\infty$. Similarly, let $g_0(x_0, x_1, x_2) = x_1x_2$, $g_1(x_3, x_4, x_5) = x_3x_4x_5$, and $g_2(x_6, x_7, x_8) = 0$. Then $\mathbf{s}' = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})+g_0+g_1+g_2}$ has PAs 4.0, 2.0, and 7.54 wrt WHT, NHT, and DFT$_1^\infty$, respectively. In all cases, PAR $\leq 2^t = 8.0$.

4.3.2 Example 2, PAR ≤ 2.0, ($t = 1$)

Let $t = 1$. We need only consider the identity permutations, $\theta_j(x_{\pi(j)}) = \gamma_j(x_{\pi(j)}) = x_{\pi(j)}$, as $\theta_j(x_{\pi(j)}) = \gamma_j(x_{\pi(j)}) = x_{\pi(j)} + 1$ is implicitly covered by $g_j(\mathbf{x_j})$. From Construction 2,

$$p(\mathbf{x}) \quad = \textstyle\sum_{j=0}^{L-2} x_{\pi(j)}x_{\pi(j+1)} + c_jx_j + k, \qquad c_j, k \in Z_2 \tag{6}$$

This is exactly the DJ set of binary quadratic cosets of RM$(1, n)$, where $n = L$, as described by Davis and Jedwab [4]. This set has PA ≤ 2.0 wrt DFT$_1^\infty$ [4]. Such sequences are Bent for n even [13, 26] and, in [16, 17] it is shown that such a set has PA $= 2.0$ wrt WHT for n odd, and also, wrt NHT, has PA $= 1.0$ for $n \neq 2 \bmod 3$ (NegaBent), and PA $= 2.0$ for $n = 2 \bmod 3$. More generally the DJ set has PAR ≤ 2.0 wrt any LUUT [17], and this agrees with Theorem 1. For example, let $p(\mathbf{x}) = x_0x_4 + x_4x_1 + x_1x_2 + x_2x_3 + x_1 + 1$. Then $\mathbf{s}$ has PAR $= 2.0$ wrt the WHT, NHT, and DFT$_1^\infty$. The DJ set, being cosets of $R(2, n)$, forms a codeset with Hamming Distance, $D \geq 2^{n-2}$. The rate of the DJ codeset is $\frac{(\frac{n!}{2})2^{n+1}}{2^{2^n}}$. Therefore we can construct a $[2^n, \log_2(n!) + n, 2^{n-2}, 2.0]$ error-correcting code. The primary drawback of this code is that its rate vanishes rapidly as n increases.

4.3.3 Example 3, PAR ≤ 4.0, ($t = 2$)

[4, 24, 16, 17, 26] all propose techniques for the inclusion of further quadratic cosets, so as to improve rate at the price of increased PAR. We here propose an improved rate quadratic code (although still vanishing, asymptotically), where PAR ≤ 4.0. To achieve this we set $t = 2$ in Construction 2. For $t = 2$ then the algebraic degree of all sequences is $\mu = 2$. Therefore, as stated in the proof of Theorem 2, we can set θ to the identity permutation. There are $\Gamma = \frac{(2^t)!}{2^t} = 6$ non-trivial linear permutation polynomials, γ_j, (ignoring constant offset). These polynomials map from $Z_2^2 \rightarrow Z_2^2$, and comprise the set, $\gamma(x_r, x_s) \in \{(x_r, x_s), (x_r + x_s, x_s), (x_r, x_r + x_s), (x_s, x_r), (x_r + x_s, x_r), (x_s, x_r + x_s)\}$. Substituting for γ_j and g_j in Construction 2 gives a large set of polynomials with PAR≤ 4.0 wrt all LUUTs. We now list, for this construction, the $p(\mathbf{x})$ arising from the 6 invertible polynomials, γ, for one 'iteration' of Construction 2, i.e. for $L = 2$, where $n = Lt = 4$, and where we fix π to the identity.

$$
\begin{array}{l}
p(\mathbf{x}) = x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4) \\
p(\mathbf{x}) = x_0(x_2+x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4) \\
p(\mathbf{x}) = x_0x_2 + x_1(x_2+x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4) \\
p(\mathbf{x}) = x_0x_3 + x_1x_2 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4) \\
p(\mathbf{x}) = x_0(x_2+x_3) + x_1x_2 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4) \\
p(\mathbf{x}) = x_0x_3 + x_1(x_2+x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)
\end{array}
\tag{7}
$$

where $c_0, c_1 \in Z_2$. The permutations, γ_j, above are isomorphic to a distinct invertible boolean $t \times t$ matrix, where $t = 2$ (Section 4.4), as the permutation polynomials form a group isomorphic to the binary General Linear Group, $\mathrm{GL}(t, 2)$, where $|\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$ [11]. Explicitly,

$$
\mathrm{GL}(2,2) = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \}
$$

Note that, by inspection, any two of the quadratics in (7) are inequivalent under permutation, π, of the indices of the four variables, e.g., $p(\mathbf{x}) = x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$ and $p(\mathbf{x}) = x_0(x_2+x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$. An upper bound, B, on $|\mathbf{P}|$ is given by Theorem 2. Substituting $t = 2$ into (4),

$$
|\mathbf{P}| < B = \frac{n!}{6} 24^{\frac{n}{2}} \tag{8}
$$

Therefore we can construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-2}, 4.0]$ error-correcting code. Exact enumeration and unique generation for this set remains open, due to extra symmetries, induced by π, which occur for $t > 1$. As an example of this π-induced symmetry, consider the two coset leaders, $x_0x_2 + x_1x_3 + g_0(x_0,x_1) + g_1(x_2,x_3)$ and $x_0x_1 + x_2x_3 + g_0'(x_0,x_2) + g_1'(x_1,x_3)$ which both contribute to the count in the above enumeration, but are equal when $g_0(x_0,x_1) = x_0x_1$, $g_1(x_2,x_3) = x_2x_3$, $g_0'(x_0,x_2) = x_0x_2$, $g_1'(x_1,x_3) = x_1x_3$. This equality leads to an overcount and such symmetries render B a strict upper bound for all cases but $t = 1$. We computed the exact number of quadratic coset leaders for $n = 4, 6, 8, 10$, by simply counting the number of distinct coset leaders, and these are compared to the upper bound, B, of (8) in Table 1. They are also compared to the $\frac{n!}{2}$ quadratic coset leaders in the binary DJ set (Example 2). Thus, for instance, Table 1 shows the existence of a $[64, 20.2, 16, 4.0]$ low PAR error-correcting code, i.e. of length 64, dimension $k = 20.2$, distance $D = 16$, and PAR ≤ 4.0, which can be compared with the fundamental DJ binary codeset for $n = 6$, which is a $[64, 15.5, 16, 2.0]$ low PAR error-correcting code. We see that rate has been improved over the DJ codeset at the price of PAR, which also increases. Thus, by assigning $t = 2$ we have a construction for a much larger codeset than

Table 1: The Number of Quadratic Coset Leaders for Construction 2 when $t = 2$

n	4	6	8	10
Theorem 2, (8),(4), $B/2^{n+1}$	72	12960	4354560	2351462400
Exact Computation(3), $\lvert\mathbf{P}\rvert/2^{n+1}$	36	9240	4086096	2317593600
$\lvert$DJ Code $\rvert/2^{n+1}$	12	360	20160	1814400
$\log_2(B/2^{n+1})$	6.2	13.7	22.1	31.1
$\log_2(\lvert\mathbf{P}\rvert/2^{n+1})$	5.2	13.2	22.0	31.1
$\log_2$(Number of homogeneous quadratics)	6	15	28	45

the DJ codeset and with the same Hamming Distance, $D = 2^{n-2}$, but now PAR is upper-bounded by 4.0 instead of 2.0. Table 1 also shows the $\log_2$ of the size of the complete set of homogeneous quadratic functions, and it is evident from Table 1 that $\mathbf{P}$ contains a significant proportion of these homogeneous quadratic functions for $n \leq 10$. Note that, as n increases, the discrepancy between the upper bound, B, and $|\mathbf{P}|$ becomes negligible as a fraction of $|\mathbf{P}|$. Therefore, in practice, for $n \geq 10$, it may be acceptable, from the viewpoint of an engineer who wishes to use this codeset in an OFDM system, to incorporate the coding collision errors induced by π into the overall error-rate without significant detriment to performance. In which case we can already claim to have constructed an *implementable* low PAR error-correcting code for OFDM systems using 1024 or more carriers which is significantly larger than any previously proposed that uses construction techniques. However Table 1 also indicates that the rate of this code is still unacceptably small for $n \geq 10$. For instance, from Table 1, when $n = 10$, we see that the code rate of $\mathbf{P}$ is $\frac{42.1}{1024}$, which is very small.

As an example of a codeword from this set, let $p(\mathbf{x}) = x_0x_2 + x_1x_2 + x_1x_6 + x_2x_5 + x_6x_3 + x_6x_5 + x_5x_4 + x_3x_7 + x_0x_1 + x_5x_3 + x_7 + x_1$. Then $\mathbf{s}$ has PAs $=$ 1.0, 2.0, and 3.43 wrt WHT, NHT, and DFT_1^{∞}, respectively.

Table 2: The Number of Quadratic Coset Leaders for Construction 2 when $t = 3$

n	6	9	12	15
$\log_2(B/2^{n+1})$	16.7	33.5	51.7	70.9
$\log_2$(Number of homogeneous quadratics)	15	36	66	105

4.3.4 Example 4, PAR ≤ 8.0, ($t = 3$)

There are now $\frac{(2^t)!}{2^t} = 5040$ non-trivial permutation polynomials from $Z_2^3 \rightarrow Z_2^3$, and of linear or quadratic degree for each of θ, and γ (ignoring constant-offset). Thus, $\theta\gamma$ can be quadratic, cubic or quartic according to the subset of permutations used. In this paper we only explicitly enumerate upper bounds for the quadratic and quartic cases, leaving the cubic case to future work.

Quadratic Construction ($\mu = 2$):
When $\mu = 2$ we have a quadratic construction, and θ and γ are linear permutations. For this case, as discussed previously, we can, without loss of generalisation, set θ to the identity permutation. There are $\Gamma = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$ linear permutation polynomials. By inspection, these 168 polynomials can be represented by the following 7 linear permutations which are inequivalent under input and output variable index permutation.

$$\begin{aligned}\gamma(x_q, x_r, x_s) \in \quad & \{(x_q, x_r, x_s), (x_q + x_s, x_r, x_s), (x_q + x_s, x_r + x_s, x_s), (x_q + x_r + x_s, x_r, x_s), \\ & (x_q + x_r, x_r + x_s, x_s), (x_q + x_r + x_s, x_r + x_s, x_s), (x_q + x_s, x_r + x_q, x_s + x_q + x_r)\}\end{aligned}$$

Substituting for γ and g in Construction 2, with θ fixed as the identity, gives a large set of polynomials with PAR$\leq$ 8.0 wrt all LUUTs. We now list, for this construction, all quadratic $p(\mathbf{x})$ arising from the 7 inequivalent degree-one permutations, γ, for one 'iteration' of Construction 2, i.e. for $L = 2$, where π is fixed as the identity:

$$p(\mathbf{x}) = x_0x_3 + x_1x_4 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_5 + x_1x_4 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_4 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x})$$
$$p(\mathbf{x}) = x_0x_3 + x_0x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_2x_5 + g(\mathbf{x})$$

where $g(\mathbf{x}) = c_0x_0x_1 + c_1x_0x_2 + c_2x_1x_2 + c_3x_0x_1x_2 + c_4x_3x_4 + c_5x_3x_5 + c_6x_4x_5 + c_7x_3x_4x_5 + \text{RM}(1,6)$, $c_0, c_1, \ldots, c_7 \in Z_2$, with $c_3 = c_7 = 0$. An upper bound, B, to $|\mathbf{P}|$ can be computed from Theorem 2, (4), with $\mu = 2$, and the upper bound is compared to the total number of homogeneous quadratics in n binary variables in Table 2. Once again, a substantial proportion of the possible homogeneous quadratics appear to be contained in $\mathbf{P}$ for $n \leq 15$. As with $t = 2$, exact enumeration and unique generation for this set remains open, due to extra symmetries induced by π. This codeset has Hamming Distance, $D \geq 2^{n-2}$ and PAR ≤ 8.0 wrt all LUUTs. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-2}, 8.0]$ error-correcting code. For instance, Table 2 shows the existence of a $[64, \simeq 23.7, 16, 8.0]$ low PAR error-correcting code.

Cubic Construction ($\mu = 3$):
For $t = 3$ we can also include cubic forms in Construction 2, where θ and γ are each quadratic or linear. There are 168 linear and $5040 - 168 = 4872$ quadratic permutations for each of θ and μ and, by inspection, this set can be represented by 7 linear and 147 quadratic permutation polynomials which are inequivalent under input and output variable permutation. This makes a total of 154 inequivalent permutation polynomials for $t = 3$ [8, 31]. Substituting for θ, γ and g in Construction 2 gives a large set of polynomials with PAR≤ 8.0 wrt all LUUTs, and Hamming Distance, $D \geq 2^{n-3}$. However, we leave to further work the challenge of upper bounding, enumerating and uniquely generating this set. Here is an example from this codeset, where ijk, uv is short for $x_ix_jx_k + x_ux_v$, π is the identity, θ_j is linear and γ_j is quadratic $\forall j$. Let,

$$\begin{aligned} p(\mathbf{x}) = \;& 034, 035, 045, 135, 145, 234, 235, 245, 367, 368, 378, 567, 568, 69A, 79A, 7AB, \\ & 89A, 345, 9AB, 03, 05, 14, 24, 25, 36, 38, 47, 58, 69, 6A, 6B, 7A, 7B, 89, 8B, 67, 78, AB \end{aligned}$$

Then $\mathbf{s}$ has PAs 4.0, 6.625, and 7.66 wrt the WHT, NHT, and DFT$_1^\infty$, respectively. Moreover, PAR ≤ 8.0. Here is another example from this codeset, where π is the identity, θ_0 is linear, γ_0 is quadratic, θ_1 and γ_1 are both linear, and θ_2 is quadratic, γ_2 is linear. Let,

$$\begin{aligned} p(\mathbf{x}) = \;& 034, 035, 045, 134, 135, 145, 234, 235, 245, 789, 67A, 68A, 67B, 68B, \\ & 03, 05, 14, 15, 36, 38, 46, 47, 56, 57, 58, 69, 79, 89, 8A, 7B \end{aligned}$$

Then $\mathbf{s}$ has PAs 1.0, 2.5, and 5.44 wrt the WHT, NHT, and DFT$_1^\infty$, respectively. Moreover, PAR ≤ 8.0. Successful enumeration would allow us to construct a $[2^n, k, 2^{n-3}, 8.0]$ error-correcting code.

Quartic Construction ($\mu = 4$):
Finally, for $t = 3$, we can also include quartic forms, $p(\mathbf{x})$, which occur for the subset of cases where both θ and γ are quadratic permutations. This gives a large set of polynomials of degree ≤ 4 with PAR ≤ 8.0 wrt all LUUTs, and Hamming Distance, $D \geq 2^{n-4}$. Table 3 uses (4) to compute an upper bound on the quartic code size for $t = 3$ as n varies. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-4}, 8.0]$ error-correcting code. For instance, Table 3 shows the existence of a $[64, \simeq 42.9, 4, 8.0]$ error-correcting code.

Table 3: Upper Bound on Size of the Quartic Codeset Using Construction 2 for $t = 3$

n	6	9	12
$\log_2(B)$	42.92	80.91	120.29

We leave the exact enumeration and unique generation of this set to future work. Here is an example from this codeset. Let,

$$p(\mathbf{x}) = \begin{array}{l} 0235, 0245, 023, 025, 1235, 1245, 0234, 0235, 0245, 1234, 1235, 1245, \\ 123, 125, 035, 045, 134, 145, 134, 135, 145, 234, 235, 245, 03, 05, 14, 15 \end{array}$$

Then $\mathbf{s}$ has PAs 6.25, 3.25, and 3.74 wrt the WHT, NHT, and DFT_1^∞, respectively. In all cases, PAR ≤ 8.0.

4.3.5 Example 5, PAR ≤ 16.0, ($t = 4$)

Table 4 uses (4) to compute an upper bound on the sextic ($\mu = 6$) code size for $t = 4$ as n varies. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-6}, 16.0]$ error-correcting code. For instance, Table 4 shows the existence of a $[256, \simeq 116.6, 4, 16.0]$ error-correcting code.

Table 4: Upper Bound on Size of the Sextic Codeset Using Construction 2 for $t = 4$

n	8	12	16
$\log_2(B)$	116.63	221.08	312.00

We leave the exact enumeration and unique generation of this set to future work.

4.4 A Matrix Construction for all Quadratic Codes from Construction 2

For the case $\mu = 2$ we can, without loss of generality, fix θ to the identity permutation, and then aim to construct all possible linear permutations for γ. Each degree-one permutation, γ: $Z_2^t \rightarrow Z_2^t$ can be viewed as a $t \times t$ binary adjacency matrix under the mapping,

$$\begin{array}{ll} M = \{m_{i,l}\} \Leftrightarrow \gamma_j(\mathbf{x_j}) = (\gamma_{0,j}(\mathbf{x_j}), \gamma_{1,j}(\mathbf{x_j}), \ldots, \gamma_{t-1,j}(\mathbf{x_j})), & \gamma_{l,j} : Z_2^t \rightarrow Z_2, \deg(\gamma_{l,j}) = 1, \quad \forall l \\ m_{i,l} = 1 \qquad \text{if } \gamma_{l,j}(\mathbf{x_j}) \text{ contains the linear term, } x_i & \\ m_{i,l} = 0 \text{ otherwise} & \end{array}$$

The above mapping is an isomorphism from degree-one permutations to the General Linear Group, $\mathbf{G} = \text{GL}(t, 2)$, of all binary $t \times t$ invertible matrices, mod 2 [11]. Therefore, to construct all quadratics, $p(\mathbf{x})$, for a given n and t we need to generate all degree one permutations, γ, which can, in turn, be constructed by generating all of $\mathbf{G} = \text{GL}(t, 2)$, as follows [1, 2]:

Definition 11. *A binary $t \times t$* transvection *matrix, X_{ab}, satisfies,*

$$X_{ab} = \{u_{i,j}\}, \quad \begin{array}{ll} \textit{where } u_{i,j} = 1, & i = j, \textit{ and } i = a, j = b \\ u_{i,j} = 0, & \textit{otherwise} \end{array}$$

Definition 12. *The Borel subgroup of* $\mathbf{G}$ *over* Z_2 *is the set of* $t \times t$ *upper-triangular binary matrices,* $\mathbf{B}$.

Definition 13. *The Weyl subgroup of* $\mathbf{G}$ *is the set of* $t \times t$ *permutation matrices,* $\mathbf{W}$.

Arbitrarily assign a fixed ordering, O, to the $\binom{t}{2}$ matrices, X_{ab}, $a < b$. Let $w \in \mathbf{W}$ be a $t \times t$ permutation matrix where w also represents a permutation of Z_t such that $w \begin{pmatrix} a_0 \\ a_1 \\ \cdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} a_{w(0)} \\ a_{w(1)} \\ \cdots \\ a_{w(t-1)} \end{pmatrix}$ For each w, form the matrix product, X_w, comprising all X_{ab} which satisfy $a < b = w(a) > w(b)$, where the X_{ab} in X_w are ordered according to O.

Theorem 3. *[1, 2] ('Bruhat Decomposition')*

$$\mathbf{G} = \mathbf{X'_w}\mathbf{W}\mathbf{B} \tag{9}$$

where $\mathbf{X'_w}$ *is the set of sub-products of* X_w *that maintain the ordering of the* X_{ab} *matrices in* X_w*, including the identity matrix.*

All linear permutations, γ, can be uniquely constructed using Theorem 3, where $|\mathbf{G}| = \Gamma = \prod_{i=0}^{t-1}(2^t - 2^i)$. This means that we can generate all quadratics, $p(\mathbf{x})$, for Construction 2 for any t and L. However, as indicated previously, the $p(\mathbf{x})$ are not guaranteed to be unique due to the extra symmetries induced by π. We leave to further work the challenge of modifying the Bruhat decomposition to eliminate these residual symmetries.

4.5 Examples of Bruhat Decomposition

$t = 2$**:**
For $t = 2$, $X_{01} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\}$, $\mathbf{W} = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\}$. Assign the trivial ordering X_{01} to the one matrix, X_{ab}. Now $w = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ defines the identity permutation $(0)(1)$ and makes $X_w = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Moreover $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ defines the permutation $(0, 1)$ and makes $X_w = X_{01}$. Therefore, when w defines $(0)(1)$ we generate 2 matrices of $\mathbf{G}$, and when w defines $(0, 1)$ we generate 4 matrices of $\mathbf{G}$, bringing the total to 6, which is correct.
$t = 3$**:**
For $t = 3$, $X_{01} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $X_{02} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $X_{12} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $|\mathbf{B}| = 8$, $|\mathbf{W}| = 6$. We can arbitrarily choose to assign the ordering $X_{01}X_{02}X_{12}$ to the 3 matrices, X_{ab}. The partitioning of matrices in $\mathbf{G}$ is then as follows:

w	X_w	$\lvert$subset of $\mathbf{G}\rvert$
$(0)(1)(2)$	I	8
$(0)(1, 2)$	X_{12}	16
$(0, 1)(2)$	X_{01}	16
$(0, 2)(1)$	$X_{01}X_{02}X_{12}$	64
$(0, 2, 1)$	$X_{01}X_{02}$	32
$(0, 1, 2)$	$X_{02}X_{12}$	32
		Total $= \lvert\mathbf{G}\rvert = 168$

5 A Further Generalisation

Lemma 20 of [25] extends the Maiorana-McFarland construction to a large codeset with near-Bent properties, where a 1-1 map is replaced by a 2^δ-1 map. In this section we apply similar ideas to Construction 2 to obtain Construction 3 below, (proofs omitted). Construction 3 is quite complicated and so far we have not found a better way to express the construction. We advise readers to skip this section on first reading. We do, however, provide some examples in the appendix which will help to clarify the construction.

Construction 3 tackles the case when the number of variables in each of the L iterations is allowed to vary. Using the terminology of Construction 1, this implies more than one $\mathbf{E}$ matrix for some iterations, where each $\mathbf{E}$ matrix is unitary and is associated with an independently chosen row/column permutation. Before describing the construction we must first specify some new terminology.

Let permutation $\theta : Z_2^t \rightarrow Z_2^t$ have as domain the t binary variables, $\mathbf{x}$. Let $f : Z_2^u \rightarrow Z_2$ have as domain the set of u binary variables, $\mathbf{z}$. Let us now assume that the form of θ depends on the output of $f(\mathbf{z})$. We write this as $\theta(\mathbf{x})\{f(\mathbf{z})\}$ and this expression can be partly evaluated as,

$$\theta(\mathbf{x})\{f(\mathbf{z})\} = (f(\mathbf{z}) + 1)\theta^0(\mathbf{x}) + f(\mathbf{z})\theta^1(\mathbf{x})$$

where we must define 2 permutations, θ^0 and θ^1, from $Z_2^t \rightarrow Z_2^t$. For brevity we can write this as $\theta\{f\}$. We can generalise this definition to make θ dependent on v associated functions, f_i, from $Z_2^{u_i} \rightarrow Z_2$, $0 \leq i < v$. We write this as $\theta(\mathbf{x})\{f_0(\mathbf{z_0}), f_1(\mathbf{z_1}), \ldots, f_{v-1}(\mathbf{z_{v-1}})\}$, and we must now define 2^v permutations, $\theta^0, \theta^1, \ldots, \theta^{2^v-1}$, from $Z_2^t \rightarrow Z_2^t$, one of which is 'selected' according to the combined outputs of the f_i. For brevity we can write this as $\theta\{f_0, f_1, \ldots, f_{v-1}\}$. We can further abbreviate the notation by labeling $\{F\} = \{f_0, f_1, \ldots, f_{v-1}\}$. We can then *NEST* dependencies $F_0, F_1, F_2, \ldots$. This is written as $\theta = \theta\{F_0\{F_1\{F_2\{\ldots\}\}\}\}$, and means that the form of the functions in F_{i-1} depend on the outputs of the functions F_i. We express the *NEST* operation as,

$$NEST(\theta\{F\}, \{F'\}) \rightarrow \theta\{F\{F'\}\}$$

Let $|F|$ mean the number of functions labeled by F. Let $v = \sum_{i=0}^{Q-1} |F_i|$. Then, if we *NEST* to a depth of Q using the function sets, F_i, $0 \leq i < Q$, then we must define 2^v permutations, $\theta^0, \theta^1, \ldots, \theta^{2^v-1}$, from $Z_2^t \rightarrow Z_2^t$, one of which is 'selected' according to the combined outputs of the F_i. As an example, let $F_0 = \{f_0(\mathbf{z_0}), f_1(\mathbf{z_1}))\}$, and $F_1 = \{f_2(\mathbf{z_2})\}$. Then, with f_0, f_1, f_2 outputting $\rightarrow Z_2$,

$$\theta(\mathbf{x})\{F_0\{F_1\}\} = \theta(\mathbf{x})\{f_0(\mathbf{z_0}), f_1(\mathbf{z_1})\{f_2(\mathbf{z_2})\}\}$$

which, for brevity, can be written as,

$$\theta\{F_0, F_1\} = \theta\{f_0, f_1\{f_2\}\}$$

and can be partially evaluated as,

$$\begin{aligned}&(f_2(\mathbf{z_2})+1)((f_1(\mathbf{z_1})+1)(f_0(\mathbf{z_0})+1)\theta^0(\mathbf{x}) + (f_1(\mathbf{z_1})+1)f_0(\mathbf{z_0})\theta^1(\mathbf{x}) + f_1(\mathbf{z_1})(f_0(\mathbf{z_0})+1)\theta^2(\mathbf{x})\\ &+f_1(\mathbf{z_1})f_0(\mathbf{z_0})\theta^3(\mathbf{x})) + f_2(\mathbf{z_2})((f'_1(\mathbf{z_1})+1)(f'_0(\mathbf{z_0})+1)\theta^4(\mathbf{x}) + (f'_1(\mathbf{z_1})+1)f'_0(\mathbf{z_0})\theta^5(\mathbf{x})\\ &+f'_1(\mathbf{z_1})(f'_0(\mathbf{z_0})+1)\theta^6(\mathbf{x}) + f'_1(\mathbf{z_1})f'_0(\mathbf{z_0})\theta^7(\mathbf{x}))\end{aligned}$$

where f'_i is not necessarily the same as f_i, and where 8 permutations, $\theta^i : Z_2^t \rightarrow Z_2^t$, $0 \leq i < 8$, must be defined with domain $\mathbf{x}$.

We will also decompose the permutation $\theta_j : Z_2^t \rightarrow Z_2^t$ as $\theta_j = (\theta_{0,j}, \theta_{1,j}, \ldots, \theta_{t-1,j})$, where $\theta_{i,j} : Z_2^t \rightarrow Z_2$. Similarly, $\gamma_j : Z_2^t \rightarrow Z_2^t$ is decomposed as
$\gamma_j = (\gamma_{0,j}, \gamma_{1,j}, \ldots, \gamma_{t-1,j})$, where $\gamma_{i,j} : Z_2^t \rightarrow Z_2$.

We now define the *EXTEND* operation. Let F be a length $t' - t$ vector of functions of arbitrary domain each of which outputs $\rightarrow Z_2$ (where it is assumed that $t' \geq t$). Then,

$$EXTEND(\theta_j, F) \rightarrow (\theta_{j,0}, \theta_{j,1}, \ldots, \theta_{j,t-1}, F)$$

is a mapping $\rightarrow Z_2^{t'}$. In other words, θ_j has been extended by means of the vector F from a permutation of Z_2^t to a mapping which outputs to $Z_2^{t'}$. Construction 3 uses combinations of *NEST* and *EXTEND* to construct θ'_j and γ'_j, which output (after *NESTING* and *EXTENSION*) to $Z_2^{t\text{max}}$, where t_{max} is defined below. θ'_j and γ'_j can then be 'multiplied', in the same way as $\theta_j\gamma_j$ in (3), and the resulting expressions added to form the final polynomial, p.

We are now ready to describe Construction 3.

Construction 3: *To construct a function of n boolean variables with PAR $\leq 2^{t_{max}}$ wrt all LUUTs, we pursue the following strategy (the y_i are auxilliary boolean variables which can be used at the end to select between different sequences):*

- *Choose t_{max} so that $1 \leq t_{max} \leq n$.*
- *Partition the n binary variable indices, $\{0, 1, \ldots, n-1\}$, into L disjoint variable subsets, $\mathbf{S_j}$, such that $t_j = |\mathbf{S_j}| \leq t_{max}$, $\forall j$, $0 \leq j < L$.*
- *For each j, $0 \leq j < L-1$, define θ_j comprising $2^{t_{max}-t_j}$ permutations, $\theta_j^0, \theta_j^1, \ldots, \theta_j^{2^{t_{max}-t_j}-1}$, from $Z_2^{t_j} \rightarrow Z_2^{t_j}$ with domain the set of t_j binary variables $\mathbf{x_j} = \{x_i\}$, $i \in \mathbf{S_j}$.*
  Similarly, for each j, $0 \leq j < L-1$, define γ_j comprising $2^{t_{max}-t_{j+1}}$ permutations, $\gamma_j^0, \gamma_j^1, \ldots, \gamma_j^{2^{t_{max}-t_{j+1}}-1}$, from $Z_2^{t_{j+1}} \rightarrow Z_2^{t_{j+1}}$ with domain the set of t_{j+1} binary variables $\mathbf{x_{j+1}} = \{x_i\}$, $i \in \mathbf{S_{j+1}}$.
- *For $j = 0$, $j < L-1$, j++ do:*

```
{
.     t = t_j.
.     Assign F as the zero vector of length t_max − t_j.
.     For i = j + 1, i ≤ L − 1, i++ do:
.     {
.          if t < t_i
.          {
.               assign θ_j = NEST(θ_j, {γ_{i−1,t}, γ_{i−1,t+1}, ..., γ_{i−1,t_i−1}}).
.               set t = t_i.
.          }
.     }
.     if t < t_max
.          assign θ_j = NEST(θ_j, {y_t, y_{t+1}, ..., y_{t_max−1}}).
.     θ'_j = EXTEND(θ_j, F).
.     t = t_{j+1}.
.     F = ().
.     For i = j + 1, i < L − 1, i++ do:
.     {
.          if t < t_{i+1}
.          {
.               assign F = {γ_{i,t}, γ_{i,t+1}, ..., γ_{i,t_{i+1}−1}}.
.               assign γ_j = NEST(γ_j, F).
.               assign γ_j = EXTEND(γ_j, F).
.               set t = t_{i+1}.
```

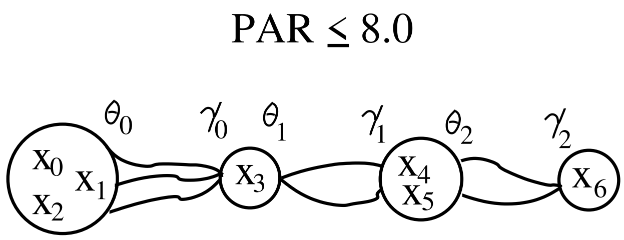

Figure 3: Example of Construction 3 where $t_{\max} = 4$

.   }
.   }
.   *if* $t < t_{max}$
.   {
.   *assign* $F = \{y_t, y_{t+1}, \ldots, y_{t_{max}-1}\}$.
.   *assign* $\gamma_j = NEST(\gamma_j, F)$.
.   *assign* $\gamma_j = EXTEND(\gamma_j, F)$.
.   }
. $\gamma'_j = \gamma_j$.
}

- *Then* $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})}$, *where* p *is given by,*

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \theta'_j \gamma'_j + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{10}$$

where $2^{t_{max}-t_{L-1}}$ *different sequences are generated according to the assignments given to the* $t_{max} - t_{L-1}$ *auxilliary variables,* y_i*, which are present in the* θ'_j *or* γ'_j*, and where the* g_j *are arbitrary functions of* $\mathbf{x_j}$*, outputting* $\rightarrow Z_2$*. (Note that, for this generalisation, the permutation,* π*, of the indices* $\{0, 1, \ldots, n-1\}$ *is implicitly included in the initial index partition operation).*

Corollary 3. *The length* $N = 2^n$ *sequences,* $\mathbf{s}$*, of Construction 3, satisfy PAR*$(\mathbf{s}) \leq 2^{t_{\max}}$ *wrt all* $N \times N$ *LUUTs.*

Fig 3 illustrates Construction 3 for the case of Example 1 in the Appendix, where we are also free to permute indices, i, of x_i.

Corollary 4. *Each of the* $2^{t_{max}-t_{L-1}}$ *sequences,* $\mathbf{s}$*, of Construction 3 is a coset leader for a coset of* $2^{t_{L-1}}$ *sequences formed from any linear offset of* $\mathbf{s}$ *by linear combinations of members of* $\mathbf{x_{L-1}}$*. The union of these* $2^{t_{max}-t_{L-1}}$ *cosets forms a CS set of* $2^{t_{max}}$ *sequences of length* 2^n*.*

The Appendix provides examples for Construction 3.

In Construction 3, if $t_j = t_{\max}, \forall j$, then there is no *NESTING* or *EXTENSION* and the construction simplifies to Construction 2. It remains open to exactly enumerate and uniquely generate the sequences in Construction 3. Note that, just as Construction 2 is a special case of Construction 1, so Construction 3 is a special case of a more general construction where the $\mathbf{E}$ matrices are not necessarily WHT matrices. This further generalisation is conceptually straightforward once Construction 3 is understood. Note also that Construction 3 allows us to add yet more sequences to our low PAR codesets without degrading distance, and these improvements in code rate will be discussed in future papers.

6 Discussion and Open Problems

This paper presented a construction for low PAR error-correcting codes which significantly generalises the fundamental codeset of Davis and Jedwab, and concisely summarises the complementary set constructions of Golay, Turyn, and Tseng and Liu. An important subcase, Construction 2, can be viewed either as recursion or specialisation of a two-sided Maiorana-McFarland construction. The paper highlights the central importance for PAR constructions of generating permutation polynomials of prescribed maximum degree, and provides motivation for further research work in this area, and also motivates the search for solutions to a number of open problems which we will now discuss.

Open Problems:

- The constructions of this paper only provide a unique, implementable encoder if we can provide algorithms to generate all permutations and/or many-to-one/one-to-many mappings of specified maximum algebraic degree. Symmetric permutations are straightforward. Section 4.4 provides a (previously-known) generation scheme for linear permutations (producing 'quadratic' sequences). But the problem of unique generation of permutations of degree greater than one is, as far as the authors know, unsolved. Solutions to this problem would have far-reaching application in cryptography, and this paper shows that such algorithms are central to the development of constructions for low PAR error-correcting codes.

- Given an algorithm to generate all permutation polynomials, then Construction 2 only generates distinct $p(\mathbf{x})$ for $t = 1$. For $t > 1$, π, the permutation of variable indices induces extra symmetries causing a few $p(\mathbf{x})$ to be generated more than once. In other words, for $t > 1$ it is possible that the action of two (or more) distinct permutations, π and π', may result in the same polynomial, $p(\mathbf{x})$. This situation is reflected in (4), which is a strict upper bound for $t > 1$. It remains open to provide an algorithm to generate all <u>distinct</u> $p(\mathbf{x})$. Such an algorithm would replace (4) with an exact expression and provide a 'black-box' encoding solution for OFDM systems. The problem is closest to solution for the case of linear permutations, where Section 4.4 solves the permutation generation part, and it remains to eliminate the coding collisions caused by distinct permutations π. We have not yet tackled the problem of unique generation of codewords for Construction 3, but this is clearly an even harder task.

- It would also be interesting to choose the $\mathbf{E_j}$ other than WHTs for Constructions 1 and 3. In particular, note that the case of $t = 1, 2, 3$ refers to Hadamard matrices of size $2, 4, 8$, respectively (PAR $\leq 2, 4, 8$, respectively). It is known that, for $t \leq 3$, all Hadamard matrices are row/column permutation equivalent to WHT matrices, so Construction 2 covers all cases. However, for $t = 4$, (PAR ≤ 16) we know that there are 5 row/column permutation inequivalent 16×16 Hadamard matrices, one of which is the WHT [32]. Therefore, for $t = 4$, there are essentially 5 different versions of Construction 1, one of which is Construction 2. As t increases we have yet more inequivalent classes of Hadamard matrices. This paper therefore establishes a direct link between the classification of Hadamard matrices, and the classification of PAR classes, and provides a strong motivation to discover manageable ANF descriptions for each of these classes.

- One important way to improve code rate whilst keeping PAR low is to choose rectangular $\mathbf{E_j}$, with more rows than columns, where the rows form a set of near-orthogonal sequences. Application of Construction 1 would then result in a slowly rising PAR bound as L increases, but the rate of the code would also improve compared to the cases where $\mathbf{E_j}$ is a square matrix. This raises the possibility of even higher rate low PAR error-correcting codes. For instance, in CDMA, the WHT rows can be used as a sequence set, due to their orthogonality. But larger near-orthogonal sequence sets are highly desirable, and the set of Gold sequences is such a set. The set of Kerdock sequences is an even larger set [9]. One could therefore use one of these larger sequence sets to form our $\mathbf{E}$ matrices, one sequence per row. Our row permutation, γ, would then operate over a larger space, resulting in an improved code rate. And the near-orthogonality of the sequence set would ensure the upper-bound on PAR only rose slowly after each iteration of the construction, although computing the precise upper-bound in such cases remains an open challenge.

- In this paper we have proposed the study of PAR wrt all LUUTs. One can completely generalise the set of LUUTs to the set of *Linear Unitary Transforms* (LUTs) by including unitary matrices which are the tensor product of $r \times r$ unitary matrices such that each matrix entry is no longer constrained to have a magnitude of $\frac{1}{\sqrt{r}}$. For instance, linear unitary matrices which have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\frac{1}{2}\begin{pmatrix} \sqrt{3} & 1 \\ 1 & -\sqrt{3} \end{pmatrix}$ as tensor factors are in the set of LUTs but not the smaller subset represented by LUUTs. It is of interest to study the PAR of sequences wrt all LUTs. This study has been initiated in [18, 19] where it was shown that the length 2^n sequences which represent indicator functions for linear error-correcting codes of blocklength n have PAR wrt all LUTs <u>lower</u> bounded by $2^{\frac{n}{2}}$. Moreover, it is proved in [18] that, for indicator functions which represent linear error-correcting codes (functions outputting to 0 or 1), the worst-case spectral peak wrt all LUTs, (and hence the peak which defines the PAR wrt all LUTs), occurs in one or more of the spectra generated by action of the set of transforms formed from all possible tensor products of the matrices $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The nice thing about this result is that we don't have to search the complete infinite space of LUTs to find the worst-case spectral peak. However, little more is known about the PAR wrt all LUTs for more general functions. The study has direct relevance to Quantum Entanglement and it has recently been shown that the spectral index of the worst-case spectral peak wrt all LUTs identifies a generalised linear weakness for classical cryptosystems [27], where a large PAR means a large linear bias.

- One celebrated area of study is the unresolved quest to find flat polynomials on the unit circle [12]. This translates, in the terminology of this paper, into the search for a sequence construction of length 2^n (restricted, say, to the alphabet $\{1, -1\}$), such that the sequence has PAR wrt DFT_1^{∞} of $1.0 + \epsilon_0$ and a lowest spectral power trough of $1.0 - \epsilon_1$ such that the ϵ terms vanish as length, 2^n, increases. No construction with these properties is known for the bipolar case. We can pose a more general problem. Do flat polynomials exist wrt all LUUTs (not just DFT_1^{∞})? And an even more general problem would be: Do flat polynomials exist wrt all LUTs? More realistically, how well can we do for these transform sets?

7 Acknowledgements

We would like to thank Kenneth G. Paterson for giving helpful and encouraging advice regarding this paper.

8 Appendix

We provide some examples for Construction 3.

8.1 Example 1

Let $n = 7$. Consider the partition, $\mathbf{S_0} = \{0,1,2\}$, $\mathbf{S_1} = \{3\}$, $\mathbf{S_2} = \{4,5\}$, $\mathbf{S_3} = \{6\}$, as shown in Fig 3. Then $t_0 = 3$, $t_1 = 1$, $t_2 = 2$, $t_3 = 1$, $t_{\max} = t_0 = 3$, and $L = 4$.

Applying Construction 3, we must initially define the following permutations:

$$
\begin{array}{ll}
\theta_0^0 & \text{with domain } (x_0, x_1, x_2) \\
\gamma_0^0, \gamma_0^1, \gamma_0^2, \gamma_0^3, \text{ and } \theta_1^0, \theta_1^1, \theta_1^2, \theta_1^3 & \text{with domain } (x_3) \\
\gamma_1^0, \gamma_1^1, \text{ and } \theta_2^0, \theta_2^1 & \text{with domain } (x_4, x_5) \\
\gamma_2^0, \gamma_2^1, \gamma_2^2, \gamma_2^3 & \text{with domain } (x_6)
\end{array}
$$

It then follows, from Construction 3, that,

$$
\begin{array}{ll}
\theta'_0 \leftarrow \theta_0(x_0, x_1, x_2) & \gamma'_0 \leftarrow (\gamma_0(x_3)\{\gamma_{1,1}\{y_2\}\}, \gamma_{1,1}\{y_2\}, y_2) \\
\theta'_1 \leftarrow (\theta_1(x_3)\{\gamma_{1,1}\{y_2\}\}, 0, 0) & \gamma'_1 \leftarrow (\gamma_1(x_4, x_5)\{y_2\}, y_2) \\
\theta'_2 \leftarrow (\theta_2(x_4, x_5)\{y_2\}, 0) & \gamma'_2 \leftarrow (\gamma_2(x_6)\{y_1, y_2\}, y_1, y_2)
\end{array}
$$

Let us now assign, as examples, specific (arbitrary) permutation polynomials to each of the θ_j and γ_j. Let,

$$
\begin{array}{ll}
\theta_0 = (x_0, x_1, x_2) & \gamma_0^0 = (x_3), \gamma_0^1 = (x_3), \gamma_0^2 = (x_3), \gamma_0^3 = (x_3 + 1) \\
\theta_1^0 = (x_3 + 1), \theta_1^1 = (x_3), \theta_1^2 = (x_3), \theta_1^3 = (x_3) & \gamma_1^0 = (x_4, x_5), \gamma_1^1 = (x_4 + x_5, x_5) \\
\theta_2^0 = (x_4 + x_5, x_5), \theta_2^1 = (x_4, x_5) & \gamma_2^0 = (x_6), \gamma_2^1 = (x_6), \gamma_2^2 = (x_6), \gamma_2^3 = (x_6 + 1)
\end{array}
\tag{11}
$$

Given these permutation assignments we can evaluate:

$$
\begin{array}{l}
\gamma_0(x_3)\{\gamma_{1,1}\{y_2\}\} = (y_2 + 1)((x_5 + 1)x_3 + x_5x_3) + y_2((x_5 + 1)x_3 + x_5(x_3 + 1)) = x_3 + x_5y_2 \\
\theta_1(x_3)\{\gamma_{1,1}\{y_2\}\} = (y_2 + 1)((x_5 + 1)(x_3 + 1) + x_5x_3) + y_2((x_5 + 1)x_3 + x_5x_3) = x_3 + x_5 + 1 + (x_5 + 1)y_2 \\
\gamma_1(x_4, x_5)\{y_2\} = (y_2 + 1)(x_4, x_5) + y_2(x_4 + x_5, x_5) = (x_4 + x_5y_2, x_5) \\
\theta_2(x_4, x_5)\{y_2\} = (y_2 + 1)(x_4 + x_5, x_5) + y_2(x_4, x_5) = (x_4 + x_5 + x_5y_2, x_5) \\
\gamma_2(x_6)\{y_1, y_2\} = (y_1 + 1)(y_2 + 1)x_6 + y_1(y_2 + 1)x_6 + (y_1 + 1)y_2x_6 + y_1y_2(x_6 + 1) = x_6 + y_1y_2
\end{array}
$$

Therefore,

$$
\begin{aligned}
\theta'_0\gamma'_0 &= x_0x_3 + x_1x_5 + y_2(x_0x_5 + x_2) \\
\theta'_1\gamma'_1 &= x_3x_4 + x_4x_5 + x_4 + y_2(x_0x_5 + x_2) \\
\theta'_2\gamma'_2 &= x_4x_6 + x_5x_6 + y_1x_5 + y_2x_5x_6 + y_1y_2x_4
\end{aligned}
$$

Therefore,

$$
\sum_{j=0}^{2} \theta'_j\gamma'_j = x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4 + y_1x_5 + y_2(x_0x_5 + x_3x_5 + x_4x_5 + x_5x_6 + x_2 + x_4) + y_1y_2x_4
$$

Let us arbitrarily first consider that all g functions in (10) are zero (for ease of exposition). Then, $p = \sum_{j=0}^{2} \theta'_j\gamma'_j$. Moreover we have 4 different choices of sequence, $\mathbf{s}$, depending on the values of y_1 and y_2. Table 5 shows the PARs wrt WHT, NHT, and DFT_1^∞, for each of these 4 sequences.

In all cases the PAR is upper-bounded by $2^{t_{\max}} = 8.0$, as predicted by Corollary 3. Note that, as stated by Corollary 4, the final optional addition of '$+x_6$' onto each of the 4 sequences in Table 5 produces a CS set of 8 sequences (of length 128) wrt all LUUTs.

Table 5: PAs of Example 1 wrt WHT, NHT, and DFT_1^∞

y_1y_2	p	PA: WHT	NHT	DFT_1^∞
00	$x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4$	2.0	1.0	4.18
10	$x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4 + x_5$	2.0	1.0	4.25
01	$x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_6 + x_2$	2.0	1.0	5.79
11	$x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_6 + x_2 + x_4 + x_5$	2.0	1.0	6.02

It is helpful to alternatively construct these sequences visually, by using a generalised version of the strategy outlined in Section 3, which is also the foundation for Construction 1. Although we have not formally proved Construction 3 in this paper, the following construction technique essentially provides the proof for Construction 3. We use unitary WHT matrices, $\mathbf{E_j^k}$, $0 \le k < 2^{t_{\max} - t_j}$. Specifically, for Example 1, we have one 8×8 matrix, $\mathbf{E_0}$, four 2×2 matrices, $\mathbf{E_1^0}, \mathbf{E_1^1}, \mathbf{E_1^2}, \mathbf{E_1^3}$, and two 4×4 matrices, $\mathbf{E_2^0}, \mathbf{E_2^1}$. The rows and columns of $\mathbf{E_j^k}$ are permuted by γ_{j-1}^k and θ_j^k, respectively. Specifically,

θ_0 permutes columns of $\mathbf{E_0}$,	γ_0^r permutes consecutive row pairs of $\mathbf{E_0}$, $0 \le r < 4$
θ_1^k permutes columns of $\mathbf{E_1^k}$, $0 \le k < 4$,	γ_1^r permutes consecutive sets of four rows of column-concatenated $\mathbf{E_1^k}$, $0 \le r < 2$
θ_2^k permutes columns of $\mathbf{E_2^k}$, $0 \le k < 2$,	γ_2^r permutes consecutive row pairs of column-concatenated $\mathbf{E_2^k}$, $0 \le r < 4$

Let us choose the permutations for $\theta$and γ as shown in (11) of Example 1. Then these permutations act in conjunction with the $\mathbf{E}$ matrices as follows (where '$\overline{a}$' means multiply a by -1). Note that, after each γ permutation, the appropriate rows are concatenated before point-multiplying by elements of the appropriate E matrix:

θ_0 WHT	γ_0 Last 2 rows swapped	θ_1 2-col segment swap on first 2 rows	γ_1 Last 2 rows swapped
+ + + + + + + +	+ + + + + + + +	+ + + + + + + + + − + − + − + −	+ + + + + + + + + − + − + − + − $= a$
+ − + − + − + −	+ − + − + − + −	+ + + + + + + + + − + − + − + −	− − − − − − − − + − + − + − + − $= b$
+ + − − + + − −	+ + − − + + − −	+ + − − + + − − + − − + + − − +	+ + − − + + − − + − − + + − − + $= c$
+ − − + + − − +	+ − − + + − − +	+ + − − + + − − + − − + + − − +	+ + − − + + − − − + + − − + + − $= d$
+ + + + − − − −	+ + + + − − − −	+ + + + − − − − + − + − − + − +	+ + + + − − − − + − + − − + − + $= e$
+ − + − − + − +	+ − + − − + − +	+ + + + − − − − + − + − − + − +	+ + + + − − − − − + − + + − + − $= f$
+ + − − − − + +	+ − − + − + + −	+ − − + − + + − + + − − − − + +	+ − − + − + + − − − + + + + − − $= g$
+ − − + − + + −	+ + − − − − + +	+ − − + − + + − + + − − − − + +	+ − − + − + + − + + − − − − + + $= h$

θ_2 Last 2-col segment swap on first 4 rows	γ_2 Last 2 rows swapped	$\mathbf{s}$ Consecutive row pairs concatenated
$abcd$	$abcd$	$abcda\overline{bc}d$
$a\overline{bc}d$	$a\overline{bc}d$	
$ab\overline{cd}$	$ab\overline{cd}$	$ab\overline{cd}a\overline{b}c\overline{d}$
$a\overline{b}c\overline{d}$	$a\overline{b}c\overline{d}$	
$efgh$	$efgh$	$efghe\overline{f}g\overline{h}$
$e\overline{f}g\overline{h}$	$e\overline{f}g\overline{h}$	
$ef\overline{gh}$	$e\overline{fg}h$	$e\overline{fg}hef\overline{gh}$
$e\overline{fg}h$	$ef\overline{gh}$	

It is straightforward to check that the above 4 sequences, $\mathbf{s}$, correspond exactly to the 4 sequences, $\mathbf{s}$, in Table 5, as represented by p. This example also illustrates that if the $\mathbf{E_j^k}$ are chosen to be row/column inequivalent to WHT matrices, then we can further generalise Construction 3.

Finally, for Example 1, let us now make the g functions non-zero. Arbitrarily, let $g_0(x_0, x_1, x_2) = x_0x_1x_2 + x_2$, $g_1(x_3) = x_3$, $g_2(x_4, x_5) = x_4x_5 + x_5$, and $g_3(x_6) = 0$. Table 6 shows the PAs after addition of $g_0 + g_1 + g_2 + g_3$ onto each of the four sequences of Table 5.

Once again, in all cases the PAR is upper-bounded by $2^{t_{\max}} = 8.0$, as predictedby Corollary 3. Note that, as stated by Corollary 4, the final optional addition of '$+x_6$' onto each of the 4 sequences in Table 6 forms a CS set of 8 sequences wrt all LUUTs.

Table 6: PAs of Example 1 wrt WHT, NHT, and DFT_1^∞ after Addition of $g_0 + g_1 + g_2 + g_3$

$y_1 y_2$	p	PA: WHT	NHT	DFT_1^∞
00	$x_0x_1x_2 + x_0x_3 + x_1x_5 + x_3x_4 + x_4x_6 + x_5x_6 + x_4 + x_2 + x_3 + x_5$	4.5	2.5	4.04
10	$x_0x_1x_2 + x_0x_3 + x_1x_5 + x_3x_4 + x_4x_6 + x_5x_6 + x_4 + x_2 + x_3$	4.5	2.5	4.83
01	$x_0x_1x_2 + x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4x_6 + x_3 + x_5$	4.5	2.0	3.59
11	$x_0x_1x_2 + x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4x_6 + x_4 + x_3$	4.5	2.0	3.51

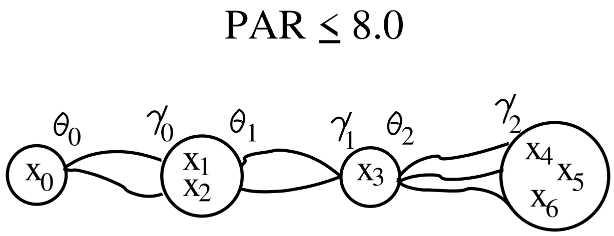

Figure 4: Example of Construction 3 where $t_{\max} = 4$ (Reverse of Figure 3)

8.2 Example 2

Except for the special case of Construction 2, Construction 3 does not give the same set of sequences when starting from the rightmost variable set (as shown), instead of the leftmost variable set. Example 2 emphasises this point by describing the construction for the partition of Figure 4, which is clearly the reverse of Figure 3.

The partition is, $\mathbf{S_0} = \{0\}$, $\mathbf{S_1} = \{1, 2\}$, $\mathbf{S_2} = \{3\}$, $\mathbf{S_3} = \{4, 5, 6\}$, as shown in Fig 4. Then $t_0 = 1$, $t_1 = 2$, $t_2 = 1$, $t_3 = 3$, $t_{\max} = t_3 = 3$, and $L = 4$.

Applying Construction 3, we must initially define the following permutations:

$\theta_0^0, \theta_0^1, \theta_0^2, \theta_0^3$	with domain (x_0)
γ_0^0, γ_0^1 and θ_1^0, θ_1^1	with domain (x_1, x_2)
$\gamma_1^0, \gamma_1^1, \gamma_1^2, \gamma_1^3$, and $\theta_2^0, \theta_2^1, \theta_2^2, \theta_2^3$	with domain (x_3)
γ_2^0	with domain (x_4, x_5, x_6)

It then follows, from Construction 3, that,

$$
\begin{array}{ll}
\theta'_0 \leftarrow (\theta_0(x_0)\{\gamma_{0,1}\{\gamma_{2,2}\}\}, 0, 0) & \gamma'_0 \leftarrow (\gamma_0(x_1, x_2)\{\gamma_{2,2}\}, \gamma_{2,2}) \\
\theta'_1 \leftarrow (\theta_1(x_1, x_2)\{\gamma_{2,2}\}, 0) & \gamma'_1 \leftarrow (\gamma_1(x_3)\{\gamma_{2,1}, \gamma_{2,2}\}, \gamma_{2,1}, \gamma_{2,2}) \\
\theta'_2 \leftarrow (\theta_2(x_3)\{\gamma_{2,1}, \gamma_{2,2}\}, 0, 0) & \gamma'_2 \leftarrow \gamma_2(x_4, x_5, x_6)
\end{array}
$$

Let us now assign the same permutations as Example 1, but in reverse, to each of the θ_j and γ_j. Let,

$$
\begin{array}{ll}
\theta_0^0 = (x_0), \theta_0^1 = (x_0), \theta_0^2 = (x_0), \theta_0^3 = (x_0 + 1) & \gamma_0^0 = (x_1 + x_2, x_2), \gamma_0^1 = (x_1, x_2) \\
\theta_1^0 = (x_1, x_2), \theta_1^1 = (x_1 + x_2, x_2) & \gamma_1^0 = (x_3 + 1), \gamma_1^1 = (x_3), \gamma_1^2 = (x_3), \gamma_1^3 = (x_3) \\
\theta_2^0 = (x_3), \theta_2^1 = (x_3), \theta_2^2 = (x_3), \theta_2^3 = (x_3 + 1) & \gamma_2 = (x_4, x_5, x_6)
\end{array}
$$

Given these permutation assignments we can evaluate:

$$
\begin{array}{l}
\theta_0(x_0)\{\gamma_{0,1}\{\gamma_{2,2}\}\} = x_2x_6 + x_0 \\
\gamma_0(x_1, x_2)\{\gamma_{2,2}\} = (x_2x_6 + x_1 + x_2, x_2) \\
\theta_1(x_1, x_2)\{\gamma_{2,2}\}, 0) = (x_2x_6 + x_1, x_2) \\
\gamma_1(x_3)\{\gamma_{2,1}, \gamma_{2,2}\} = x_5x_6 + x_3 + x_5 + x_6 + 1 \\
\theta_2(x_3)\{\gamma_{2,1}, \gamma_{2,2}\} = x_5x_6 + x_3
\end{array}
$$

Therefore,

$$\begin{aligned}
\theta_0'\gamma_0' &= x_0x_2x_6 + x_1x_2x_6 + x_0x_1 + x_0x_2 \\
\theta_1'\gamma_1' &= x_1x_5x_6 + x_2x_3x_6 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_5 + x_1 \\
\theta_2'\gamma_2' &= x_4x_5x_6 + x_3x_4
\end{aligned}$$

Therefore,

$$\sum_{j=0}^{2} \theta_j'\gamma_j' = x_0x_2x_6+x_1x_2x_6+x_1x_5x_6+x_2x_3x_6+x_4x_5x_6+x_0x_1+x_0x_2+x_1x_3+x_1x_5+x_1x_6+x_2x_5+x_3x_4+x_1 \tag{12}$$

Let us, arbitrarily, consider that all g functions in (10) are zero (for ease of exposition). Then, $p = \sum_{j=0}^{2} \theta_j'\gamma_j'$. Unlike Example 3, we now only have 1 choice of sequence, $\mathbf{s}$. This sequence has a PA of 8.0, 2.5, and 4.93 wrt the WHT, NHT, and DFT_1^∞, respectively. In all cases the PAR is upper-bounded by $2^{t_{\max}} = 8.0$, as predicted by Corollary 3. Note that, as stated by Corollary 4, a CS set of 8 sequences (of length 128) wrt all LUUTs is formed by $\mathbf{s}$ and all linear offsets of $\mathbf{s}$ over the variables $\{x_4, x_5, x_6\}$.

We can, alternatively, construct this sequence using a generalised version of the strategy outlined in Section 3. We obtain the following construction steps:

θ_0 Cols swapped on last 2 rows	γ_0 Second pair of rows swapped	θ_1 Last 2 col segments swapped on last 4 rows	γ_1 First 2 rows swapped	θ_2 Col segments swapped on last 2 rows	
++	++	+ + + − + − ++	+ + − + + − − −	+ + − + + − − − + + + − + − ++	$= a$
+−	+−	+ + +− + −++	+ + + − + − ++	+ + − + + − − − + + + − + − ++	$= b$
++	+−	+ + + − + − ++	+ + + − − + − −	+ + + − − + − − + + − + − + ++	$= c$
+−	++	+ + + − + − ++	+ + − + − + ++	+ + + − − + − − + + − + − + ++	$= d$
++	++	+ + + − + + − +	+ + + − + + − +	+ + + − + + − + + + − + − − − +	$= e$
+−	+−	+ + + − ++ − +	+ + − + − − − +	+ + + − + + − + + + − + − − − +	$= f$
++	++	+ + + − + + −+	+ + + − − − +−	+ + + − − − + − + + − + + + +−	$= g$
−+	−+	+ + +− + +−+	+ + − + + + +−	+ + + − − − +− + + − + + + + −	$= h$

Finally, γ_2 generates $\mathbf{s} = a\,b\,c\,d\,e\,f\,g$

It is straightforward to check that the above sequence, $\mathbf{s}$, corresponds exactly to the $\mathbf{s}$, as represented by p in (12).

References

[1] Alperin, J.L.,Bell, R.B.: **Groups and Representations,** Graduate Texts in Mathematics, Springer, **162**, pp. 39–48, (1995)

[2] Brundan, J.: Web Lecture Notes: Math 607, Polynomial representations of GL_n, *http://darkwing.uoregon.edu/∼brundan/teaching.html* pp. 29–31, Spring (1999)

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

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

[5] Feng, K.,Shiue P.J-S.,Xiang Q., On aperiodic and periodic complementary binary sequences, IEEE Trans. Inf. Theory, **45**, 1, pp. 296–303, Jan. (1999)

[6] Golay, M.J.E.: Multislit spectroscopy. J. Opt. Soc. Amer., **39**, pp. 437–444, (1949)

[7] Golay, M.J.E.: Complementary Series. IRE Trans. Inform. Theory, **IT-7**, pp. 82–87, Apr. (1961)

[8] Harrison, M.A.: The Number of Classes of Invertible Boolean Functions. J. ACM, **10**, pp. 25–28, (1963)

[9] Helleseth, T.,Kumar, P.V.: Sequences with Low Correlation. in *Handbook of Coding Theory*, R.Brualdi,C.Huffman,V.Pless, Eds.

[10] Jones, A.E.,Wilkinson, T.A.,Barton, S.K.: Block Coding Scheme for Reduction of Peak to Mean Envelope Power Ratio of Multicarrier Transmission Schemes. Elec. Lett. **30**, pp. 2098–2099, (1994)

[11] Lidl, L.,Niederreiter, H.: **Introduction to Finite Fields and their Applications** Cambridge Univ Press, pp. 361–362, (1986)

[12] Littlewood, J.E.: On polynomials $\sum \pm z^m$, $\sum \exp(\alpha_m) z^m$,$z = e^{i\theta}$, *J. London Math. Soc.*, **41**, pp. 367–376, (1966)

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

[14] J-S.No, H-Y.Song; "Generalized Sylvester-Type Hadamard Matrices", *Int. Symp. Inf. Theory, Sorrento, Italy*, June 25-30, 2000

[15] Nyberg, K.: Construction of Bent Functions and Difference Sets. *Proc. EuroCrypt90, Lecture Notes in Computer Science (LNCS), Springer, Berlin*, Vol 473, pp. 151–160, (1991)

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

[17] Parker, M.G.,Tellambura, C.: Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions. Submitted to IEEE Trans. Inform. Theory, *http://www.ii.uib.no/∼matthew/* March (2001)

[18] Parker, M.G., Rijmen, V.: The Quantum Entanglement of Binary and Bipolar Sequences. Short version in **Sequences and Their Applications**, Discrete Mathematics and Theoretical Computer Science Series, Springer, 2001 Long version at *http://xxx.soton.ac.uk/ps/quant-ph/0107106* or *http://www.ii.uib.no/∼matthew/* Jun (2001)

[19] Parker, M.G.: Spectrally Bounded Sequences, Codes and States: Graph Constructions and Entanglement., *Invited Talk at Eighth IMA International Conference on Cryptography and Coding, Cirencester, UK, 2001, To be published in Lecture Notes in Computer Science, 2001, also http://www.ii.uib.no/∼matthew/*, 17-19 December, 2001

[20] Inequivalent Invertible Boolean Functions for $t = 3$, *http://www.ii.uib.no/∼matthew/mattweb.html*, (2001)

[21] Parker, M.G.,Tellambura, C.: A construction for binary sequence sets with low peak-to-average power ratio. Int. Symp. Inform. Theory, Lausanne, Switzerland, June 30-July 5, (2002)

[22] Parker, M.G.,Paterson, K.G.,Tellambura, C.: Golay Complementary Sequences. Wiley Encyclopedia of Telecommunications, Editor: J.G.Proakis, Wiley Interscience, (2002)

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

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

[25] Paterson, K.G.,: On Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA. **Sequences and Their Applications***, Discrete Mathematics and Theoretical Computer Science Series, Springer*, (2001)

[26] Paterson, K.G.: Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebraic Coding Theory. Hewlett-Packard Technical Report, HPL-2001-146, (2001)

[27] Raddum, H.,Parker M.G. Z_4-Linear Cryptanalysis. Technical Report for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), (2002)

[28] Rudin, W.: Some Theorems on Fourier Coefficients. Proc. Amer. Math. Soc., No 10, pp. 855–859, (1959)

[29] Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T., (1951)

[30] Shepherd, S.J.,Orriss, J.,Barton, S.K.: Asymptotic Limits in Peak Envelope Power Reduction by Redundant Coding in QPSK Multi-Carrier Modulation. IEEE Trans. Comm., **46**, No 1, pp. 5–10, Jan. (1998)

[31] Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences. $(1, 2, 154, \ldots)$, *http://www.research.att.com/∼njas/sequences/index.html*

[32] Sloane, N.J.A.: A Library of Hadamard Matrices $(1, 2, 154, \ldots)$, *http://www.research.att.com/ njas/hadamard/index.html*

[33] Tseng, C.-C. Liu, C.L.: Complementary sets of sequences, IEEE Trans. Inform. Theory, **IT-18**, no. 5, pp. 644–651, Sept. (1972)

[34] Turyn, R.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings J. Comb. Theory Ser. A, **16**, pp. 313–333, (1974)