Spectrally Bounded Sequences, Codes and States: Graph Constructions and Entanglement

Matthew G. Parker

Code Theory Group, Inst. for Informatikk, HIB,
University of Bergen, Norway
E-mail: matthew@ii.uib.no,
Web: http://www.ii.uib.no/∼matthew/MattWeb.html

Abstract. A recursive construction is provided for sequence sets which possess good Hamming Distance and low Peak-to-Average Power Ratio (PAR) under any Local Unitary Unimodular Transform. We identify a subset of these sequences that map to binary indicators for linear and nonlinear Factor Graphs, after application of subspace Walsh-Hadamard Transforms. Finally we investigate the quantum PAR_l measure of 'Linear Entanglement' (LE) under any Local Unitary Transform, where optimum LE implies optimum weight hierarchy of an associated linear code.

1 Introduction

Golay Complementary sequences of length 2^n form sequences with Peak-to-Average Power Ratio (PAR) ≤ 2 under the one-dimensional continuous Discrete Fourier Transform (DFT_1^∞) [9]. The upper PAR bound of 2 follows by forming these Complementary Sequences using Rudin-Shapiro construction [25, 26]. This set is the union of certain quadratic cosets of Reed-Muller (RM) $(1, n)$ [5]. Moreover the quadratic coset representatives can be viewed as 'line graphs' in Algebraic Normal Form (ANF) [21]. As these sequences are a subset of $\mathrm{RM}(2, n)$, the Hamming Distance, D, between sequences in the set satisfies $D \geq 2^{n-2}$. The problem of finding error-correcting codes where each codeword also has low PAR has application to Orthogonal Frequency Division Multiplexing (OFDM) communications systems [11]. However the fundamental codeset identified by Davis and Jedwab [5] (DJ sequences) suffers from vanishing rate as n increases, and much higher rates are possible and desirable, where PAR $\leq O(n)$ [27, 22]. A generalisation of Rudin-Shapiro 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...etc can also be added, increasing code rate at price of distance, D, which decreases. However these rate improvements are marginal. In this paper we present a construction for much larger codesets of sequences with PAR $\leq 2^t$, comprising ANFs up to degree u, where $u \leq t$ for $t > 1$, and $u = 2$ for $t = 1$ [19]. These codesets have PAR $\leq 2^t$ under **all** Linear Unimodular Unitary Transforms (LUUTs), including one and multi-dimensional continuous DFTs. As LUUTs include the Walsh-Hadamard

Transform (WHT) then our construction gives large codesets of Almost-Bent functions [3, 23]. The functions are cryptographically even stronger, as the binary sequences are distant from linear sequences over all alphabets, not just over Z_2. We then describe a mapping of a subset of the bipolar sequences, generated using our construction, to Factor Graphs [12]. By applying tensor products of Hadamard and Identity kernels to our bipolar sequence we transform to a Factor Graph in a Normal Realisation [7] representing a linear or nonlinear error-correcting code. This transformation provides spectral characterisation for Factor Graphs (and Quantum Factor Graphs [15]). Finally we present PAR_l, which is a partial measure of quantum entanglement and measures PAR under **all** Linear Unitary Transforms (LUTs) [17, 18]. We also define 'Linear Entanglement' (LE), and 'Stubborness of Entanglement' (SE), which is a series of parameters related to PAR_l over all sequence subspaces. At least in the bipartite quadratic case, a length 2^n bipolar sequence with optimal LE and SE represents a $[n, k, d]$ binary linear code with optimal weight hierarchy. We conjecture that optimally entangled subsystems represent optimal linear and nonlinear codes - and vice versa. A similar relationship between secrecy and entanglement has recently been highlighted by [4].

2 A Construction For Low PAR Error-Correcting Codes

Joint work with C.Tellambura [19]

PAR is a spectral measure. We must therefore define the transforms over which the spectrum is computed:

2.1 Definitions

Definition 1 *$\boldsymbol{L_n}$ is the infinite set of length 2^n complex linear unimodular sequences, $\boldsymbol{l} = (l_0, l_1, \ldots, l_{2^n-1})$, where $|l_i| = |l_j|$, $\forall i, j$, $\sum_{i=0}^{2^n-1} |l_i|^2 = 1$, and,*

$$\boldsymbol{l} = \{2^{\frac{-n}{2}}(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})\}$$

where $\otimes$ means 'tensor product'.

Definition 2 *A $2^n \times 2^n$ Linear Unimodular Unitary Transform (LUUT) matrix $\mathbf{L}$ has rows taken from $\boldsymbol{L_n}$ such that $\mathbf{L}\mathbf{L}^\dagger = \mathbf{I_{2^n}}$, where $\dagger$ means conjugate transpose, and $\mathbf{I_{2^n}}$ is the $2^n \times 2^n$ identity matrix.*

Definition 3 *$\boldsymbol{G_n}$ is the infinite set of length 2^n complex linear sequences, $\boldsymbol{l} = (l_0, l_1, \ldots, l_{2^n-1})$, where $\sum_{i=0}^{2^n-1} |l_i|^2 = 1$ and,*

$$\boldsymbol{l} = \{2^{\frac{-n}{2}}(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})\}$$

Note that $\boldsymbol{G_n} \supset \boldsymbol{L_n}$.

Definition 4 *A $2^n \times 2^n$ Linear Unitary Transform (LUT) matrix $\mathbf{G}$ has rows taken from $\boldsymbol{G_n}$ such that $\mathbf{G}\mathbf{G}^\dagger = \mathbf{I_{2^n}}$. LUUTs are a special case of LUT.*

Let s_i be an element of a length 2^n vector, $\boldsymbol{s}$. PAR($\boldsymbol{s}$) is computed by measuring maximum possible correlation of $\boldsymbol{s}$ with **any** length 2^n 'linear' unimodular sequence, $\boldsymbol{l} \in \boldsymbol{L_n}$:

Definition 5 $$PAR(\boldsymbol{s}) = 2^n max_{\boldsymbol{l}}(|\boldsymbol{s} \cdot \boldsymbol{l}|^2)$$
where $\boldsymbol{l} \in \boldsymbol{L_n}$ and $\cdot$ means 'inner product' [17].

Let $\boldsymbol{x} = \{x_0, x_1, \ldots, x_{n-1}\}$. Then $p(\boldsymbol{x})$: $Z_2^n \rightarrow Z_2$ has a bipolar representation, $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})} = (s_0, s_1, \ldots, s_{2^n-1})$, where $s_i = (-1)^{p(x_0=i_0, x_1=i_1, \ldots, x_{n-1}=i_{n-1})}$, and $i = \sum_{k=0}^{n-1} i_k 2^k$ is a radix-2 decomposition of i.

2.2 Construction

This paper focuses on a special case of a more general construction. Here, all x_i are two-state binary variables, and the fundamental recursion is based on Walsh-Hadamard Transform (WHT) kernels. The more general construction is presented in [19]. We now present the construction:

$$\begin{array}{l} p(\boldsymbol{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} f_{l,j}(x_{\pi(t(j+1))}, x_{\pi(t(j+1)+1)}, \ldots, x_{\pi(t(j+2)-1)}) \\ + \sum_{j=0}^{L-1} g_j(x_{\pi(tj)}, x_{\pi(tj+1)}, \ldots, x_{\pi(tj+t-1)}) \end{array} \tag{1}$$

where $n = Lt$, π permutes Z_n, and where $f_{l,j} : Z_2^t \rightarrow Z_2$ is such that $f_{\gamma_j} = (f_{0,j}, f_{1,j}, \ldots, f_{t-1,j})$ is an invertible boolean function (permutation polynomial) from $Z_2^t \rightarrow Z_2^t$, governed by the permutation, $i' = \gamma_j(i)$, where $i' = \sum_{l=0}^{t-1} i'_l 2^l$ is a radix-2 decomposition, $i'_l = f_{l,j}(i_0, i_1, \ldots, i_{t-1})$, and each γ_j permutes Z_t. To avoid unnecessary duplications, we exclude the f_{γ_j} where one or more $f_{l,j}$ has a '+1' constant offset, and also the cases where all $f_{l,j}$ are monomials, except when f_{γ_j} is the identity function.

Theorem 1 *[19] The length $N = 2^n$ bipolar sequence $\boldsymbol{s} = (-1)^{\boldsymbol{p}}$ satisfies $PAR(s) \leq 2^t$ under all LUUTs, where $\boldsymbol{p}$ is generated using construction (1).*

Proof. (sketch) Let m factor fully as $m = \prod_{i=0}^{F-1} p_i$, p_i not necessarily distinct. A length m vector, $\boldsymbol{l}$, is defined linear if it satisfies $\boldsymbol{l} = \bigotimes_{i=0}^{F-1} \boldsymbol{v_i}$ where length($\boldsymbol{v_i}$) $= p_i$, and $\sum_{j=0}^{m-1} |l_j|^2 = 1$. Let $\boldsymbol{E_j}$ and $\boldsymbol{A_j}$, $1 \leq j \leq L$, be a series of $N \times N$ and $N \times N^j$ complex matrices, respectively, where $\boldsymbol{A_1} = \boldsymbol{E_1}$ is unitary. Let the rows of $\boldsymbol{A_{j-1}}$, $(\boldsymbol{a_{0,j-1}}, \boldsymbol{a_{1,j-1}}, \ldots, \boldsymbol{a_{N-1,j-1}})$, form a complementary set of N sequences under any $N^{j-1} \times N^{j-1}$ unitary transform with linear unimodular rows. Let $\boldsymbol{l}$ and $\boldsymbol{l_j}$ be normalised linear rows of length N^{j-1} and N, respectively. Let $\boldsymbol{r} = \boldsymbol{A_{j-1}}\boldsymbol{l}$. Let γ permute Z_N. Construct the $N \times N^j$ matrix, $\boldsymbol{A_j}$, such that $\boldsymbol{a_{i,j}} = ((\boldsymbol{a_{\gamma(0),j-1}}|\boldsymbol{a_{\gamma(1),j-1}}| \ldots, |\boldsymbol{a_{\gamma(N-1),j-1}}) \odot (\boldsymbol{e_{i,j}} \otimes \boldsymbol{1}))$ where $\boldsymbol{x} \odot \boldsymbol{y} = (x_0 y_0, x_1 y_1, \ldots, x_{N^j-1} y_{N^j-1})$, $\boldsymbol{1}$ is the length N^{j-1} all-ones vector, $\boldsymbol{e_{i,j}}$ is the ith row of $\boldsymbol{E_j}$, and '$|$' means concatenation. The rows of $\boldsymbol{A_j}$ form a complementary N-set under any unitary transform if $\boldsymbol{r'} = \boldsymbol{A_j}(\boldsymbol{l_j} \otimes \boldsymbol{l})$ satisfies, $\sum_{k=0}^{N-1} |r'_i|^2 = 1$. This follows if $\sum_{i=0}^{N-1} | \sum_{k=0}^{N-1} (r_{\gamma(k)} e_{i,k} l_k)|^2 = 1$, for $r_k, e_{i,k}$ and l_k elements of

$\boldsymbol{r}$,$\boldsymbol{e_{i,j}}$ and $\boldsymbol{l_j}$, respectively. This is true if $\boldsymbol{E_j}$ is unitary, and if $\boldsymbol{e_{i,j}} \odot \boldsymbol{l_j}$ is unimodular, which follows if $\boldsymbol{e_{i,j}}$ and $\boldsymbol{l_j}$ are unimodular. Construction (1) occurs when successive $\boldsymbol{A_j}$ are recursively generated, where all $\boldsymbol{E_i}$ are $2^t \times 2^t$ WHTs. The γ permutation essentially maps to f_γ, and concatenation is widened to a more general permutation, π, over all linear variables. ∎

Theorem 2 *For a fixed t, let $\boldsymbol{P}$ be the codeset of length 2^n binary sequences of degree μ or less, generated using (1). Then,*

$$\begin{aligned} \frac{|\boldsymbol{P}|}{2^{n+1}} &\leq \frac{(\frac{\Gamma}{t!})^{\frac{n}{t}-1} n!(2^{2^t-t-1})^{\frac{n}{t}}}{2t!}, \qquad \mu = 2 \\ &\leq \frac{((2^t-1)!)^{\frac{n}{t}-1} n!(2^{2^t-t-1})^{\frac{n}{t}}}{2t!}, \qquad \mu \geq 2 \end{aligned} \tag{2}$$

where $\Gamma = \prod_{i=0}^{t-1}(2^t - 2^i) = |GL(t,2)|$. (GL is the General Linear Group). (Only for $t = 1$ is the upper bound exact).

Proof. By counting arguments we can show that, for $\mu = 2$,

$$\frac{|\boldsymbol{P}|}{2^{n+1}} \leq \frac{\prod_{l=1}^{t} \binom{\frac{ln}{t}}{\frac{n}{t}}}{t!} \times \frac{(\frac{n}{t})!^t}{2} \times (\frac{\Gamma}{t!})^{\frac{n}{t}-1} \times (2^{\binom{t}{2}})^{\frac{n}{t}}$$

For $\mu \geq 2$, we replace $\frac{\Gamma}{t'}$ with $\frac{(2^t)!}{2^t}$, which is the number of permutations excluding those with a constant offset, '+1'. The Theorem follows. ∎

In Section 2.4 we show how to generate all degree-one permutation polynomials, via an isomorphism to the General Linear Group, where the number of degree-one permutation polynomials is Γ.

2.3 Examples

The $2^n \times 2^n$ Walsh-Hadamard (WHT) and Negahadamard (NHT) Transform matrices are $\bigotimes_{i=0}^{n-1} \boldsymbol{H}$, and $\bigotimes_{i=0}^{n-1} \boldsymbol{N}$, respectively, where $\boldsymbol{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\boldsymbol{N} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. DFT$_1^\infty$ is the set of $2^n \times 2^n$ matrices, the union of whose rows form a subset of $\boldsymbol{L_n}$ such that each row satisfies $a_i = 1$, $b_i = \omega^{ik}$ for some fixed k, and ω is a complex root of unity (see Definition 1). These three transforms are used as 'spot-checks' in the examples to validate the PAR upper-bound.

Example 1 Let γ_j be the identity permutation $\forall j$. Then,
$f_{l,j}(x_{\pi(t(j+1))}, x_{\pi(t(j+1)+1)}, \ldots, x_{\pi(t(j+2)-1)}) = x_{\pi(t(j+1)+l)}$, and (1) becomes,

$$p(\boldsymbol{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} x_{\pi(t(j+1)+l)} + \sum_{j=0}^{L-1} g_j(x_{\pi(tj}, x_{\pi(tj+1)}, \ldots, x_{\pi(tj+t-1)}) \tag{3}$$

When $\deg(g_j) < 2$, $\forall j$, it is well-known that $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ is Bent (PAR = 1 under the WHT) for L even [14] and (perhaps not known) that $\boldsymbol{s}$ has PAR = 2^t

under the WHT for L odd. In general, for any g_j, s has PAR $\leq 2^t$ under all LUUTs. For example, if $L = 4$ and,

$$p(\boldsymbol{x}) = x_0x_3 + x_1x_4 + x_2x_5 + x_3x_6 + x_4x_7 + x_5x_8 + x_6x_9 + x_7x_{10} + x_8x_{11}$$

then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR $= 1.0$ under the WHT, PAR $= 1.0$ under the NHT, and PAR $= 7.09$ under DFT_1^∞. 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 $\boldsymbol{s'} = (-1)^{p(\boldsymbol{x})+g_0+g_1+g_2}$ has PAR $= 4.0$ under the WHT, PAR $= 2.0$ under the NHT, and PAR $= 7.54$ under DFT_1^∞. In all cases, PAR ≤ 8.0 under any LUUT.

Example 2, PAR $\leq$ 2.0 Let $t = 1$. Then we have one possible permutation polynomial, namely, $f_\gamma = x$, (we exclude $f_\gamma = x + 1$). From (1) we obtain,

$$p(\boldsymbol{x}) = \textstyle\sum_{j=0}^{L-2} x_{\pi(j)}x_{\pi(j+1)} + c_jx_j + d, \qquad c_j, d \in Z_2 \tag{4}$$

This is exactly the DJ set of binary quadratic cosets of RM$(1, n)$, where $n = L$ [5]. This set has PAR ≤ 2.0 under DFT_1^∞ [5]. Such sequences are Bent for n even [14, 23] and, in [16, 17] it was shown that such a set has PAR $= 2.0$ under the WHT for n odd, and also, under the NHT, has PAR $= 1.0$ for $n \neq 2 \bmod 3$ (NegaBent), and PAR $= 2.0$ for $n = 2 \bmod 3$. More generally the DJ set has PAR ≤ 2.0 under any LUUT [17], and this agrees with Theorem 1. For example, let $p(\boldsymbol{x}) = x_0x_4 + x_4x_1 + x_1x_2 + x_2x_3 + x_1 + 1$. Then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR $= 2.0$ under the WHT, PAR $= 2.0$ under the NHT, and PAR $= 2.0$ under DFT_1^∞. The DJ set, being cosets of $R(2, n)$, forms a codeset with Hamming Distance, $D >= 2^{n-2}$. The rate of the DJ codeset follows $\frac{(\frac{n!}{2})2^{n+1}}{2^{2^n}}$ as n increases. This is their primary drawback as the code rate vanishes rapidly as n increases.

Example 3, PAR $\leq$ 4.0 [5, 22, 17, 23] have all proposed 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 code (although still vanishing), where PAR ≤ 4.0. To achieve this we set $t = 2$ in (1). There are $\frac{(2^t)!}{2^t t!} = 3$ valid permutation polynomials, $f_\gamma = (f_0, f_1)$. These polynomials map from $Z_2^2 \rightarrow Z_2^2$, and are taken from the set,

$$f_\gamma(x_0, x_1) \in \{(x_0, x_1), (x_0 + x_1, x_1), (x_0, x_0 + x_1)\}$$

Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR≤ 4.0 under all LUUTs. We now list, for this construction, the $p(\boldsymbol{x})$ arising from the the 3 invertible polynomial functions, f_γ, for one 'section' of the polynomial, i.e. for $L = 2$, where we fix π to the identity permutation.

$$\begin{aligned}
p(\boldsymbol{x}) &= x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4) \\
p(\boldsymbol{x}) &= x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4) \\
p(\boldsymbol{x}) &= x_0x_2 + x_1(x_2 + x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4)
\end{aligned}$$

where $c_0, c_1 \in Z_2$. The quadratic part of each of these 3 functions is isomorphic to a distinct invertible boolean $t \times t$ matrix, where $t = 2$ (Section 2.4), as the permutation polynomials form a group which is isomorphic to the General Linear Group, GL$(t,2)$, where $|\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$ [13]. Two of the 3 quadratic functions are inequivalent under permutation of the four variable indices, e.g.,

$$p(\boldsymbol{x}) = x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$$
$$p(\boldsymbol{x}) = x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$$

An upper bound on $|\boldsymbol{P}|$ is given by Theorem 2, (2). Substituting $t = 2$ into (2),

$$\frac{|\boldsymbol{P}|}{2^{n+1}} < n! 2^{\frac{n-4}{2}} 3^{\frac{n}{2}-1} \tag{5}$$

An exact enumeration and construction for this set remains open, due to extra 'hidden' symmetries. Computationally we are able to calculate the exact number of quadratic coset leaders for $n = 4, 6, 8, 10$, and these are compared to the upper bound of (5) in Table 1. They are also compared to the number of quadratic coset leaders, $(= \frac{n!}{2})$ in the binary DJ codeset (Example 2). By assigning $t = 2$

Table 1. The Number of Quadratic Coset Leaders for Construction (1) when $t = 2$

n	4	6	8	10
Theorem 2, (5),(2), $\lvert\boldsymbol{P}\rvert/2^{n+1}$	72	12960	4354560	2351462400
Exact Computation	36	9240	4086096	2317593600
$\frac{\text{DJ Code}}{2^{n+1}}$	12	360	20160	1814400
$\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	6.2	13.7	22.1	31.1
$\log_2$(Number of quadratics)	6	15	28	45

we have a construction for a much larger codeset than the DJ codeset and with the same Hamming Distance, $D = 2^{n-2}$, but the price paid is that the PAR is now upper-bounded by 4.0 instead of 2.0. For example, let,
$p(\boldsymbol{x}) = x_0x_2 + x_1x_2 + x_1x_6 + x_2x_5 + x_6x_3 + x_6x_5 + x_5x_4 + x_3x_7 + x_0x_1 + x_5x_3 + x_7 + x_1$
Then $\boldsymbol{s} = (-1)^{\boldsymbol{p}}$ has PAR $= 1.0$ under the WHT, PAR $= 2.0$ under the NHT, and PAR $= 3.43$ under DFT_1^∞.

Example 4, PAR $\leq$ 8.0 Set $t = 3$ in (1). There are now $\frac{(2^t)!}{2^t t!} = 840$ valid permutation polynomials, $f_\gamma = (f_0, f_1, f_2)$. These polynomials map from $Z_2^3 \rightarrow Z_2^3$. Moreover, $(2^3-1)(2^3-2)(2^3-2^2)/t! = \frac{168}{6} = 28$ of the polynomials are degree-one permutations leading to quadratic forms, $p(\boldsymbol{x})$, and can be represented by the following 7 permutation polynomials.

$f_\gamma(x_0, x_1, x_2) \in \{$
$(x_0, x_1, x_2), (x_0 + x_2, x_1, x_2), (x_0 + x_2, x_1 + x_2, x_2), (x_0 + x_1 + x_2, x_1, x_2),$
$(x_0 + x_1, x_1 + x_2, x_2), (x_0 + x_1 + x_2, x_1 + x_2, x_2), (x_0 + x_2, x_1 + x_0, x_2 + x_0 + x_1)\}$

Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR$\leq$ 8.0 under all LUUTs. We now list, for this construction, all quadratic $p(\boldsymbol{x})$ arising from the 7 inequivalent degree-one permutation polynomials, f_γ, for one 'section' of the polynomial, i.e. for $L = 2$, where π is fixed as the identity permutation.

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

where $g(\boldsymbol{x}) = c_0x_0x_1 + c_1x_0x_2 + c_2x_1x_2 + c_3x_0x_1x_2 + c_4x_3x_4 + c_5x_3x_5 + c_6x_4x_5 + c_7x_3x_4x_5 + \mathrm{RM}(1,6)$, and $c_0, c_1, \ldots, c_7 \in Z_2$. An upper bound to $|\boldsymbol{P}|$ can be computed from Theorem 2, (2), and the upper bound is compared to the total number of quadratics in n binary variables in Table 2. As with $t = 2$, an

Table 2. The Number of Quadratic Coset Leaders for Construction (1) when $t = 3$

n	6	9	12	15
Theorem 2, (2), $\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	16.7	33.5	51.7	70.9
$\log_2$(Number of quadratics)	15	36	66	105

exact enumeration and construction for this set remains open, due to extra 'hidden' symmetries. By assigning $t = 3$ we have a construction for a codeset with Hamming Distance, $D \geq 2^{n-2}$ and PAR ≤ 8.0 under all LUUTs.

For $t = 3$ we can also include cubic forms in Construction (1). There are $\frac{5040-168}{6} = 812$ degree 2 permutation polynomials, $f_\gamma = (f_0, f_1, f_2)$, that map from $Z_2^3 \rightarrow Z_2^3$, and lead to cubic forms, $p(\boldsymbol{x})$. This set can be represented by 147 degree 2 permutation polynomials which are inequivalent under variable permutation, and these are listed at [20]. (Along with the 7 inequivalent degree 1 permutation polynomials, this makes a total of 154 inequivalent permutation polynomials for $t = 3$ [10, 28]). Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR$\leq$ 8.0 under all LUUTs, and Hamming Distance, $D \geq 2^{n-3}$. An upper bound to $|\boldsymbol{P}|$ can be computed from Theorem 2, (2), and the upper bound is compared to the total number of quadratics and cubics in n binary variables in Table 3. Here is an example from this codeset, where ijk, uv

Table 3. The Number of Cubic and Quadratic Coset Leaders for Construction (1) when $t = 3$

n	6	9	12	15
Theorem 2, (2), $\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	23.6	46.3	70.4	95.5
$\log_2$(Number of quadratics and cubics)	35	120	286	560

is short for $x_i x_j x_k + x_u x_v$. Let,

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

then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR $= 4.0$ under the WHT, PAR $= 6.625$ under the NHT, and PAR $= 7.66$ under DFT_1^∞. In all cases, PAR ≤ 8.0.

2.4 A Matrix Construction for all Quadratic Codes from (1)

Each degree-one permutation polynomial, f_γ from $Z_2^t \rightarrow Z_2^t$ can be viewed as a $t \times t$ binary adjacency matrix. Let $x = \{x_0, x_1, \ldots, x_{t-1}\}$. We can write,

$$\begin{array}{llll} M \Leftrightarrow f_\gamma(x) = (f_0(x), f_1(x), \ldots, f_{t-1}(x)), & & M = \{m_{i,l}\}, \deg(f_l(\boldsymbol{x})) = 1, & \text{and} \\ m_{i,l} = 1 \quad \text{if } x_i \in f_l(x) & m_{i,l} = 0 & \text{otherwise} & \end{array}$$

The mapping is an isomorphism from the degree-one permutation polynomials to the General Linear Group, $G = \text{GL}(t, 2)$, of all binary $t \times t$ invertible matrices [13]. To construct all quadratic sequences, $p(\boldsymbol{x})$, for a given n and t we need to construct all degree one permutation polynomials, f_γ. These can, in turn be constructed by generating all members of $G = \text{GL}(t, 2)$, and this is accomplished as follows [1, 2].

Definition 6 *A binary $t \times t$ 'transvection' matrix, X_{ab}, satisfies,*

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

Definition 7 *The Borel subgroup of G over Z_2 is the $t \times t$ upper-triangular binary matrices, B.*

Definition 8 *The Weyl subgroup of G is the $t \times t$ permutation matrices, W.*

Assign a fixed ordering, O, to the $\frac{\binom{t}{2}}{2}$ matrices, X_{ab}, $a < b$. Let $w \in W$ be a permutation of Z_t and its associated $t \times t$ permutation matrix. 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 are ordered according to O.

Theorem 3 *[1, 2]*

$$G = X'_w W B \tag{6}$$

where X'_w is any sub-product of X_w that maintains the ordering of the X_{ab} matrices in X_w. This is the 'Bruhat' decomposition.

All quadratic constructions using (1) can be constructed using Theorem 3., where $|\boldsymbol{G}| = \Gamma = \prod_{i=0}^{t-1}(2^t - 2^i)$.

3 Graphical Representations

Joint work with V.Rijmen [18]

We now identify a subset of the length 2^n sequence constructions of (1), where $(-1)^{p(\boldsymbol{x})}$ exhibits a bipolar $\leftrightarrow$ binary equivalence under transform by a tensor product of combinations of $\boldsymbol{H}$ and $\boldsymbol{I}$ 2×2 matrices. The resultant length 2^n binary sequences can be interpreted as indicators for binary linear or nonlinear $[n, k, d]$ error-correcting codes. In such cases, $p(\boldsymbol{x})$ is closely related to a Normal Realisation for the Factor Graph of the associated $[n, k, d]$ code [7]. Let $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$.

Definition 9 *"H acting on i" means the action of the $2^n \times 2^n$ transform, $\mathbf{I} \otimes \ldots \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I}$ on $\boldsymbol{s}$, where $\mathbf{H}$ is preceded by i $\mathbf{I}$ matrices, and followed by $n - i - 1$ $\mathbf{I}$ matrices. We write this as $H(i)$, or $H(i)[\boldsymbol{s}]$.*

Definition 10 *Let $\mathbf{T_C}$, $\mathbf{T_{C^\perp}}$ be integer sets chosen so that $\mathbf{T_C} \cap \mathbf{T_{C^\perp}} = \emptyset$, and $\mathbf{T_C} \cup \mathbf{T_{C^\perp}} = \{0, 1, \ldots, n-1\}$. This is a bipartite splitting of $\{0, 1, \ldots, n-1\}$. Let us also partition the variable set $\mathbf{x}$ as $\mathbf{x} = \mathbf{x_C} \cup \mathbf{x_{C^\perp}}$, where $\mathbf{x_C} = \{x_i | i \in \mathbf{T_C}\}$, and $\mathbf{x_{C^\perp}} = \{x_i | i \in \mathbf{T_{C^\perp}}\}$.*

Definition 11 *$\kappa_{\mathbf{p}}$ is the set of all $s(\mathbf{x})$ of the form $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$, where $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, where $\deg(q_k(\mathbf{x_C})) = 1$ $\forall k$, and where $x_i \in p(\mathbf{x})$, $\forall$ $i \in \{0, 1, \ldots, n-1\}$. We refer to $\kappa_{\mathbf{p}}$ as the set of 'half-linear bipartite bipolar' states. $\ell_{\mathbf{p}}$ is the subset of $\kappa_{\mathbf{p}}$ where $\deg(r_k(\mathbf{x_C})) = 1$ $\forall k$.*

Theorem 4 *[18] Let $m(\mathbf{x})$ be a binary ANF. If $s(\mathbf{x}) \in \kappa_{\mathbf{p}}$, then the action of $\prod_{i \in \mathbf{T_C}} H(i)$ on $s(\mathbf{x})$ gives $s'(\mathbf{x}) = m(\mathbf{x})$. If $s(\mathbf{x}) \in \ell_{\mathbf{p}}$, then the action of $\prod_{i \in \mathbf{T_{C^\perp}}} H(i)$ on $s(\mathbf{x})$ gives $s''(\mathbf{x}) = m(\mathbf{x})$. $s'(\mathbf{x})$ ($s''(\mathbf{x})$) is the binary indicator for a binary linear or nonlinear $[n, n - |\mathbf{T}|, d]$ error correcting code, $\mathbf{C}$.*

Theorem 4 is particularly relevant when $p(\boldsymbol{x})$ is constructed using (1), as the 'strongest' members of $\kappa_{\mathbf{p}}$ are generated as a subclass of the construction if $\deg(g_j) < 2$, $\forall j$. (By considering matrices other than $\boldsymbol{H}$ it is conjectured that it is always possible to convert a bipolar sequence, $\boldsymbol{s} = (-1)^{\boldsymbol{p}}$, constructed using (1) to a binary form, even when $\deg(g_j) \geq 2$). If $\boldsymbol{s}$ can be transformed to a binary linear indicator, $\boldsymbol{s'}$, using only tensor products of $\boldsymbol{H}$ and $\boldsymbol{I}$, then we say that $\boldsymbol{s}$ is 'HI-equivalent to' $\boldsymbol{s'}$.

Theorem 5 *[18] The set $\ell_{\mathbf{p}}$ is HI-equivalent to the set of $[n, k, d]$ binary linear codes.*

3.1 Examples

Example A Let $t = 2$, $L = 3$. Then (1) can generate,

$$p(\boldsymbol{x}) = x_0x_2 + x_1x_3 + x_2x_4 + x_3x_5 + x_2x_5$$

Let $\mathbf{T_C} = \{0, 1, 4, 5\}$ and $\mathbf{T_{C^\perp}} = \{2, 3\}$. Applying $H(0)H(1)H(4)H(5)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ gives the binary sequence, $\boldsymbol{s'} = m(x) = (x_0 + x_2 + 1)(x_1 +$

$x_3+1)(x_2+x_4+1)(x_2+x_3+x_5+1)$, which is the indicator for a $[6,2,2]$ binary linear code, $\mathbf{C}$. Graphical representations for $\boldsymbol{s}$ and $\boldsymbol{s'}$ are shown in Fig 1, where the graph for $\boldsymbol{s'}$ is a Normal Realisation of a Factor Graph [7]. If, instead, we apply $H(2)H(3)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$, we get the binary sequence, $\boldsymbol{s''} = m(x) = (x_0+x_2+x_4+x_5+1)(x_1+x_3+x_5+1)$, which is the indicator for a $[6,4,2]$ binary linear code, $\mathbf{C}^\perp$, the dual of $\mathbf{C}$. Applying $H(0)H(1)H(4)H(5)$ to $\boldsymbol{s'}$, followed by $H(2)H(3)$, gives $\boldsymbol{s''}$. This is the same as applying the WHT to $\boldsymbol{s'}$, and it is known that binary indicators of a linear code code, $\mathbf{C}$, and its dual, $\mathbf{C}^\perp$, are related by the WHT [14].

Example B Let $t=3$, $L=3$. Then (1) can generate,

$$p(\boldsymbol{x}) = 034, 035, 045, 134, 135, 145, 234, 235, 245, 03, 05, 14, 15, 36, 47, 58$$

Let $\mathbf{T_C} = \{0,1,2,6,7,8\}$ and $\mathbf{T_{C^\perp}} = \{3,4,5\}$. Applying $H(0), H(1), H(2), H(6), H(7), H(8)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ gives,

$$\begin{aligned}
&\boldsymbol{s'} = m(x) = \\
&(x_0 + x_3x_4 + x_3x_5 + x_4x_5 + x_3 + x_5 + 1)(x_1 + x_3x_4 + x_3x_5 + x_4x_5 + x_4 + x_5 + 1) \\
&\times(x_2 + x_3x_4 + x_3x_5 + x_4x_5 + 1)(x_3 + x_6 + 1)(x_4 + x_7 + 1)(x_5 + x_7 + 1)
\end{aligned}$$

which is the indicator for a $[9,3,3]$ binary nonlinear code, $\mathbf{C}$. Graphical representations for $\boldsymbol{s}$ and $\boldsymbol{s'}$ are shown in Fig 1, where the graph for $\boldsymbol{s'}$ is a Normal Realisation of a **nonlinear** Factor Graph. In this case application of $H(3)H(4)H(5)$ does not produce the dual code, $\mathbf{C}^\perp$, but the nonlinear dual could be obtained by nonlocal transform over x_3, x_4, x_5.

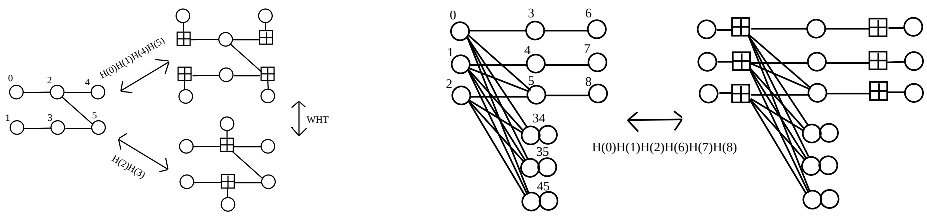

Fig. 1. Bipolar $\leftrightarrow$ Factor Graph HI-Equivalence for Examples A and B

Example C The nonlinear $[16,8,6]$ Nordstrom-Robinson binary code is HI-equivalent to a half-linear bipolar bipartite sequence, $(-1)^{p(\boldsymbol{x})}$, where $p(\boldsymbol{x})$ can be constructed using (1), and has ANF comprising 96 cubic and 40 quadratic terms, and where $|T_C| = |T_{C^\perp}| = 8$. The quadratic part of $p(\boldsymbol{x})$ is HI-equivalent to a binary linear $[16,8,4]$ code, so we can view the 96 cubic terms of $p(\boldsymbol{x})$ as further 'doping' to increase Hamming Distance, d, from 4 to 6.

3.2 Comments

This section has identified an important subset of $\kappa_{\mathbf{p}}$ as a subset of the construction of (1), where a member of $\kappa_{\mathbf{p}}$ can be transformed to a binary sequence under selective action of $\boldsymbol{H}$. Conversely, this gives us a way of analysing a Factor Graph, by transforming it back into bipolar sequence form. A natural question to ask is which length 2^n bipolar sequences are transform-equivalent to the best $[n, k, d]$ linear and nonlinear codes? We offer offer the following conjecture,

Conjecture 1 *Optimal linear or nonlinear codes can be constructed from (1) if $L = 2$, and $(-1)^{g_j}$ is, itself, HI-equivalent to an optimal linear or nonlinear code, $\forall j$. But what f_{γ_j} should be chosen?*

In the next section we pose the related question: Which quantum n-qubit states have optimal Linear Entanglement?

4 PAR$_l$ and Quantum 'Linear' Entanglement (LE)

Joint work with V.Rijmen [18]

In previous sections our PAR metric has been measured relative to all LUUTs. Quantum systems require that we compute our PAR metric (now called PAR$_l$) relative to all LUTs, of which LUUTs are a subset. It is argued in [18] that PAR$_l$ and Linear Entanglement (LE) are good partial measures of quantum entanglement. [1] Let $\boldsymbol{s}$ be a length 2^n bipolar sequence. In the context of quantum systems we interpret (after appropriate normalisation) this sequence as a probability density function of an n-qubit quantum state. Let s_i be an element of $\boldsymbol{s}$. Then $|s_i|^2$ is the probability of measuring the quantum system in state i. We must normalise so that $\sum_{i=0}^{2^n-1} |s_i|^2 = 1$, although normalisation constants are usually omitted in this paper. An n-qubit state, $\boldsymbol{s}$, contains entanglement if $\boldsymbol{s}$ is not a member of $\boldsymbol{G_n}$. The definition of PAR$_l$ is then identical to Definition 5 except that, now, $|l_i|$ does not have to equal $|l_j|$, i.e. $\boldsymbol{l}$ is not necessarily unimodular.

Definition 12 $\quad PAR_l(\boldsymbol{s}) = 2^n max_{\boldsymbol{l}}(|\boldsymbol{s} \cdot \boldsymbol{l}|^2))$
where $\boldsymbol{l}$ is any normalised linear sequence from the set, $\boldsymbol{G_n}$, and $\cdot$ means 'inner product' [17, 18].

Linear Entanglement (LE) is then defined as,

Definition 13 $\quad LE(\boldsymbol{s}) = n - \log_2(PAR_l(\boldsymbol{s}))$

Entanglement and LE are invariant under transformation of $\boldsymbol{s}$ by any LUT. Therefore PAR$_l$ is Local Unitary (LU)-invariant, and two states, $\boldsymbol{s}$ and $\boldsymbol{s'}$, related by a transform from LUT, are LU-equivalent. Code duality under the WHT and the HI-equivalence between $\boldsymbol{s}$ and $\boldsymbol{s'}$, as discussed in Section 3, are special cases of LU-equivalence. One can also view entanglement invariance as a generalisation of code duality.

[1] Quantum information theorists often consider 'mixed-state' entanglement, where entanglement with the environment is unavoidable [24, 8]. This is similar to the analysis of classical communications codes in the context of a corrupting channel. In this paper we only consider a closed (pure) quantum system with no environmental entanglements [6].

4.1 PAR$_l$ for States from $\ell_\mathbf{p}$

Theorem 6 *[18] If $\boldsymbol{s} \in \ell_\mathbf{p}$, then $\boldsymbol{s}$ is LU equivalent to the indicator for an $[n,k,d]$ binary linear code, and,*

$$PAR_l(\boldsymbol{s}) \geq 2^r, \quad \textit{where } r = max(k, n-k)$$

Theorem 6 implies that states, $\boldsymbol{s}$, from $\ell_\mathbf{p}$ have a minimum lower bound on PAR$_l$ (upper bound on LE) when the associated $[n,k,d]$ code, $\mathbf{C}$, satisfies $k = \lfloor \frac{n}{2} \rfloor$, with PAR$_l \geq 2^{\lceil \frac{n}{2} \rceil}$. Here is a stronger result.

Theorem 7 *[18] In (1), let $t = 1$ and $f_{\gamma j}$ be the identity permutation $\forall j$. Using (1), we can generate $s(\mathbf{x}) = (-1)^{p(\boldsymbol{x})}$ for $p(\boldsymbol{x})$ constructed using (4). Then $PAR_l(\boldsymbol{s}) = 2^{\lceil \frac{n}{2} \rceil}$.*

Definition 14 $\quad PA(\boldsymbol{s}) = 2^n max_i(|s_i|^2)$

We now compute PA for any HI transform of a member of $\ell_\mathbf{p}$. Let $\mathbf{s} \in \ell_\mathbf{p}$. Recalling Definition 10, let $k = |\mathbf{T}_{\mathbf{C}^\perp}|$, $k^\perp = |\mathbf{T}_\mathbf{C}|$, and $k + k^\perp = n$. Without loss of generality we renumber integer sets $\mathbf{T}_{\mathbf{C}^\perp}$ and $\mathbf{T}_\mathbf{C}$ so that $\mathbf{T}_{\mathbf{C}^\perp} = \{0, 1, \ldots, k-1\}$ and $\mathbf{T}_\mathbf{C} = \{k, k+1, \ldots, n-1\}$. Let $\mathbf{t}_{\mathbf{C}^\perp} \subset \mathbf{T}_{\mathbf{C}^\perp}$ and $\mathbf{t}_\mathbf{C} \subset \mathbf{T}_\mathbf{C}$, where $h = |\mathbf{t}_{\mathbf{C}^\perp}|$ and $h^\perp = |\mathbf{t}_\mathbf{C}|$. Let $\mathbf{x}_{\mathbf{t}^\perp} = \{x_i | i \in \mathbf{t}_{\mathbf{C}^\perp}\}$, $\mathbf{x}_\mathbf{t} = \{x_i | i \in \mathbf{t}_\mathbf{C}\}$, and $\mathbf{x}_* = \mathbf{x}_{\mathbf{t}^\perp} \cup \mathbf{x}_\mathbf{t}$. Define $\mathbf{M}$ to be a $k \times k^\perp$ binary matrix where $M_{i,j-k} = 1$ iff $x_i x_j \in p(\mathbf{x})$, and $M_{i,j-k} = 0$ otherwise. Thus $p(\mathbf{x}) = \sum_{i \in \mathbf{T}_{\mathbf{C}^\perp}} x_i (\sum_{j \in \mathbf{T}_\mathbf{C}} M_{i,j-k} x_j)$. Let $\mathbf{M_t}$ be a submatrix of $\mathbf{M}$, which comprises only the rows and columns of $\mathbf{M}$ specified by $\mathbf{t}_{\mathbf{C}^\perp}$ and $\mathbf{t}_\mathbf{C}$. Let χ_t be the rank of $\mathbf{M_t}$.

Theorem 8 *[18] Let $\boldsymbol{s'}$ be the result of $\prod_{i \in \mathbf{t}_{\mathbf{C}^\perp} \cup \mathbf{t}_\mathbf{C}} H(i)$ on $\boldsymbol{s} \in \ell_\mathbf{p}$. Then,*

$$PA(\boldsymbol{s'}) = 2^{h + h^\perp - 2\chi_t}$$

Corollary 1 *As $0 \leq \chi_t \leq min(h, h^\perp)$, it follows that, for $\boldsymbol{s} \in \ell_\mathbf{p}$, $PA(\boldsymbol{s'}) \geq 2^{|h - h^\perp|}$*

In general, PAR$_l$ must consider PA($\boldsymbol{s}$) under all LUTs. PA($\boldsymbol{s}$) for $\boldsymbol{s} \in \ell_\mathbf{p}$ is easily computed. Let the 'HI multispectra' be the union of the power spectra of $\boldsymbol{s}$ under the action of $\prod_{i \in \boldsymbol{T}} H(i)$, for all possible subsets, $\boldsymbol{T}$, of $\{0, 1, \ldots, n-1\}$.

Theorem 9 *[18] PAR$_l$ of $\boldsymbol{s} \in \ell_\mathbf{p}$ is found in the HI multispectra of $\boldsymbol{s}$.*

Theorem 9 means that, for $\boldsymbol{s} \in \boldsymbol{\ell_p}$, we only need compute the 2^n HI transforms to compute PAR$_l$. If PA($\boldsymbol{s}$) is optimally low over the HI multispectra, then $\boldsymbol{s'} = m(\boldsymbol{x})$ is an optimal binary linear code when $\boldsymbol{T} = \boldsymbol{T_C}$ or $\boldsymbol{T} = \boldsymbol{T_{C^\perp}}$.

Definition 15 *The Weight Hierarchy of a linear code* $\mathbf{C}$*, is a series of parameters,* d_j*,* $0 \leq j \leq k$*, representing the smallest blocklength of a linear sub-code of* $\mathbf{C}$ *of dimension* j*, where* $d_k = n$*,* $d_1 = d$*, and* $d_0 = 0$*.*

Theorem 10 *[18] Let* $\boldsymbol{s_c}$ *be the indicator of an* $[n, k, d]$ *binary linear code,* $\mathbf{C}$*. Let* $\mathbf{Q} \subset \{0, 1, \ldots, n-1\}$*. Let,*

$$m_{\mathbf{Q}} = \frac{|\mathbf{Q}| + \log_2(\mu) - n + k}{2}, \qquad \text{where } \mu = PA(\boldsymbol{s'_c}) \tag{7}$$

and $\boldsymbol{s'_c} = \prod_{t \in \mathbf{Q}} H(t)[\boldsymbol{s_c}]$*. Then the Weight Hierarchy of* $\mathbf{C}$ *is found from the HI multispectra of* $\boldsymbol{s_c}$*, where* $d_j = min_{\mathbf{Q}|m_Q=j}(|\mathbf{Q}|)$

Quantum measurement projects a system to a subsystem. This allows us to equate a series of quantum measurements with a series of subcodes of $\boldsymbol{C}$. Let the entanglement order of a system be the size (in qubits) of the largest entangled subsystem of the system. A most-destructive series of j single-qubit measurements over some set of possible measurements on $\boldsymbol{s}$ produces a final state $\boldsymbol{s'}$ such that entanglement order($\boldsymbol{s}$) − entanglement order($\boldsymbol{s'}$) is maximised.

Definition 16 *Stubborness of Entanglement (SE) is a series of parameters,* β_j*,* $0 \leq j \leq k'$*, representing smallest possible entanglement order,* β_j*, after* $k' - j$ *most-destructive measurements of an* n*-qubit system, where* $\beta_{k'} = n$*,* $\beta_0 = 0$*.*

Theorem 11 *[18] Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$ *where* $\boldsymbol{s}$ *is LU equivalent to an optimal or near-optimal binary linear code of dimension* $\leq \frac{n}{2}$*. Then Stubborness of Entanglement is equal to the Weight Hierarchy of the code.*

Corollary 2 *Quantum states from* $\ell_{\mathbf{p}}$ *which have optimum LE and optimum SE are LU-equivalent to binary linear codes with optimum Weight Hierarchy.*

The results of this section suggests the following modification of Conjecture 1.

Conjecture 2 *States with optimal LE can be constructed from (1) if* $L = 2$*, and* $(-1)^{g_j}$ *also has optimal LE,* $\forall j$*. But what* f_{γ_j} *should be chosen?*

5 Discussion and Open Problems

We have highlighted the importance PAR plays (explicitly or implicitly) in current research. We emphasis four areas:
a) Low PAR error-correcting codes for OFDM and CDMA.
b) Highly nonlinear, distinguishable sequence sets for cryptography.
c) Graphical construction primitives for Factor Graphs which represent good error-correcting codes.
d) Classification and quantification of quantum entanglement.
We finish with a list of a few open problems.

- Construction (1) only provides an exact, implementable encoder if the two following sub-problems can be solved:

- Provide algorithms to generate all permutation polynomials, f_γ, of degree $\mu - 1$. $\mu = 0$ is trivial. Section 2.4 provides an answer for $\mu = 1$. But, for $\mu > 1$ the situation is unclear.
- Given an algorithm to generate all permutation polynomials, then construction (1) only generates distinct $p(\boldsymbol{x})$ for $t = 1$. For $t > 1$, the permutation, π, induces extra symmetries which cause many $p(\boldsymbol{x})$ to be generated more than once. This situation is reflected in (2), which is a strict upper bound for $t > 1$. It remains an open problem to provide an algorithm for $t > 1$ which ensures the generated $p(\boldsymbol{x})$ are distinct and form the whole code. Such an algorithm would replace of (2) with an exact expression.

– Construct decoders for the above codes.
– It is considered that successful iteration on a Factor Graph requires few short graph cycles. This is ensured if the graph has a large girth. How does one construct Factor Graphs with low PAR_l and large girth?
– Provide a construction for optimally large sets, $\boldsymbol{P}$, of pure quantum states such that each state satisfies a low upper bound on PAR_l, and where any two members of $\boldsymbol{P}$ are optimally distinguishable. This problem is 'simply' the LUT extension of the problem of low PAR error-correcting codes for OFDM and cryptography.

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**, 507–522, (2000)
4. Collins, D.,Popescu, S.: A Classical Analogue of Entanglement *http://xxx.soton.ac.uk/ps/quant-ph/0107082* 16 Jul. 2001
5. 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, 2397–2417, Nov (1999)
6. Eisert, J.,Briegel, H.J.: Quantification of Multi-Particle Entanglement. *http://xxx.soton.ac.uk/ps/quant-ph/0007081 v2* 29 Aug (2000)
7. Forney, G.D.: Codes on Graphs: Normal Realizations. IEEE Trans. Inform. Theory **47.** No 2, 520–548, Feb, (2001)
8. Fuchs, C.A.,van de Graaf, J.: Cryptographic Distinguishability Measures for Quantum-Mechanical States. IEEE Trans. Inform. Theory **45.** No 4, 1216–1227, May (1999)
9. Golay, M.J.E.: Complementary Series. IRE Trans. Inform. Theory, **IT-7**, pp 82–87, Apr (1961)
10. Harrison, M.A.: The Number of Classes of Invertible Boolean Functions. J. ACM, **10**, 25–28, (1963)

11. 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**, 2098–2099, (1994)
12. Kschischang, F.R.,Frey, B.J.,Loeliger, H-A.: Factor Graphs and the Sum-Product Algorithm. IEEE Trans. Inform. Theory **47.** No 1, Jan, (2001)
13. Lidl, L.,Niederreiter, H.: **Introduction to Finite Fields and their Applications** Cambridge Univ Press, pp 361–362, (1986)
14. MacWilliams, F.J.,Sloane, N.J.A.: **The Theory of Error-Correcting Codes** Amsterdam: North-Holland. (1977)
15. Parker, M.G.: Quantum Factor Graphs. Annals of Telecom., July-Aug, pp 472-483, (2001), originally 2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France Sept 4–7, (2000), *http://xxx.soton.ac.uk/ps/quant-ph/0010043*, (2000) *http://www.ii.uib.no/∼matthew/mattweb.html*
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/mattweb.html*
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/mattweb.html* March (2001)
18. Parker, M.G., Rijmen, V.: The Quantum Entanglement of Binary and Bipolar Sequences. Short version accepted for Discrete Mathematics, Long version at *http://xxx.soton.ac.uk/ps/quant-ph/0107106* or *http://www.ii.uib.no/∼matthew/mattweb.html* Jun. (2001)
19. Parker, M.G.,Tellambura, C.: A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio. *Submitted to Int. Symp. Inform. Theory, Laussane, Switzerland, (2002)*, *http://www.ii.uib.no/∼matthew/mattweb.html* October (2001)
20. Inequivalent Invertible Boolean Functions for $t = 3$, *http://www.ii.uib.no/∼matthew/mattweb.html*, (2001)
21. 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)
22. 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, 1974–1987, Sept (2000)
23. Paterson, K.G., Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebriac Coding Theory. Hewlett-Packard Technical Report, HPL-2001-146, (2001)
24. Popescu, S.,Rohrlich, D.: On the Measure of Entanglement for Pure States. Phys. Rev. A **56.** R3319, (1997)
25. Rudin, W.,: Some Theorems on Fourier Coefficients. Proc. Amer. Math. Soc., No 10, pp. 855–859, (1959)
26. Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T., (1951)
27. 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, 5–10, Jan (1998)
28. Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences. $(1, 2, 154, \ldots)$, *http://www.research.att.com/∼njas/sequences/index.html*