The Quantum Entanglement of Binary and Bipolar Sequences

Matthew G. Parker[1] and V. Rijmen[2]

[1] Inst. for Informatikk, University of Bergen, Norway,
matthew@ii.uib.no, http://www.ii.uib.no/~matthew/mattweb.html
[2] Cryptomathic, Lei 8A, B-3000 Leuven, Belgium

Summary. Classification of different forms of quantum entanglement is an active area of research, central to development of effective quantum computers, and similar to classification of error-correction codes, where code duality is broadened to equivalence under all 'local' unitary transforms. We explore links between entanglement, coding theory, and sequence design, by examining multi-spectra of quantum states under local unitary action, and show that optimal error-correcting codes and sequences represent states with high multiparticle entanglement.

1 Introduction

Classification of multiparticle entanglement of quantum particles is only beginning. How does one quantify entanglement? There is general agreement about the entanglement measure for two particles, namely the reduced state entropy of the density matrix for the pair [24], but for more than two particles the measurement criteria are unclear. Moreover, at the moment, a sufficiently refined measure (or measures) appears to be generally non-computable (using classical resources) for more than a few particles [31]. This paper highlights two partial entanglement measures, namely the 'Linear Entanglement' (LE) (Section 6, Definition 11), and 'Stubborness of Entanglement' (SE) (Section 7, Definition 16), which is a sequence of parameters. The paper is aimed at both coding theorists and sequence designers, and at quantum physicists, and argues that the best codes and/or sequences can be interpreted as describing multiparticle states with high entanglement. A binary linear error-correcting code (ECC), $\mathbf{C}$, is often partially described by its parameters $[n, k, d]$, where n is wordlength, k is code dimension, and d is minimum Hamming Distance [18], and more generally by its weight hierarchy. We show, by interpreting the length 2^n indicator for $\mathbf{C}$ as an n-particle quantum state that, for those states representing binary linear ECCs, the ECCs with optimal weight hierarchy also have optimal LE and optimal SE (Theorems 10 and 15). By action of local unitary transform on the indicator of $\mathbf{C}$, we can also view the quantum state as a bipolar sequence. In this context a sequence is often partially described by its nonlinear order, N, and correlation immunity order, CI (Definitions 21, 22). We show that N and CI give a lower bound on LE (Theorem 16). LE is the $n - \log_2$ of a spectral 'peak' measure of Peak-to-Average Power Ratio (PAR_l (Section 6, Definition 10)), which is also an

important measure in telecommunications [7,21,20]. This paper refers both to PAR_l and to LE, where the two parameters are trivially related (Definition 11). The quantum-mechanical rule of 'local unitary equivalence' is a generalisation of code duality.

We now state the most important results of this paper. We emphasise quantum states $\boldsymbol{s}$ from the set $\ell_{\mathbf{p}}$, where $\ell_{\mathbf{p}}$ is equivalent to the set of binary linear ECCs.

- LE and SE of $\boldsymbol{s}$ can be found from the HI multispectra (the multispectra resulting from a Local Unitary (LU) transform which is any tensor combination of 2×2 Hadamard and Identity transforms of $\boldsymbol{s}$) (Theorems 7 and 14).
- Quantum states from $\ell_{\mathbf{p}}$ which are equivalent under LU transform to binary linear ECCs with optimum or near-optimum Weight Hierarchy also have optimum or near-optimum LE and SE over the set $\ell_{\mathbf{p}}$ (Theorem 15, Corollary 3).
- LE($\boldsymbol{s}$) is lower-bounded by an additive combination of the Nonlinear Order and Correlation-Immunity of $\boldsymbol{s}$ (Theorem 16).

After an initial definition of Entanglement and Measurement (Section 2), we describe binary and bipolar quantum states (Sections 3, 4, 5), emphasising states from the set, $\ell_{\mathbf{p}}$. These are equivalent under LU transform to binary linear ECCs. We place this analysis in the context of HI multispectra (Section 5) leading to results for LE (Section 6) and SE (Section 7). After noting connections with cryptography (Section 8), we briefly investigate quadratic states outside $\ell_{\mathbf{p}}$ (Section 9), and discuss application of the work to measurement-driven Quantum Computation in Section 10.

2 Entanglement and Measurement

2.1 Definitions and Partial Quantification

A qubit is a two-state particle, (s_0, s_1), meaning it is in state 0 with complex probability s_0, and state 1 with complex probability s_1, such that $|s_0|^2 + |s_1|^2 = 1$.

Definition 1 *Let $\mathbf{l_n}$ be the infinite set of normalised linear vectors which can be written in the form $(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})$*

Entanglement exists between two or more particles if their joint probability state cannot be factorised using the tensor product. More formally,

Definition 2 *Let $\boldsymbol{s}$ be an n-qubit state. $\boldsymbol{s}$ is a pure entangled state if $\boldsymbol{s} \notin \mathbf{l_n}$. $\boldsymbol{s}$ is not entangled if $\boldsymbol{s} \in \mathbf{l_n}$.*

Example: Consider qubits, x_0 and x_1. Their joint probability state is given by $\boldsymbol{s} = (s_0, s_1, s_2, s_3)$, where s_i is complex and $\sum_{i=0}^{3} |s_i|^2 = 1$. If $\boldsymbol{s} \in \mathbf{l_2}$, then $\boldsymbol{s}$ is tensor-factorisable and the two qubits are not entangled. Conversely, if $\boldsymbol{s} \notin \mathbf{l_2}$ then the two qubits are entangled.

If $\boldsymbol{s}$ has more than one non-zero entry then the system exists in a 'superposition' of states. Conventional (classical) computers only use tensor-factorisable space of physical matter. Humans 'appear' to only experience this tensor product space, as the exponentially larger entangled space seems to decohere rapidly. However, perhaps nature also takes advantage of entanglement and superposition in some way, as entanglement allows us to manipulate exponentially larger data vectors than possible classically.

Partial Quantification of Entanglement

- Linear Entanglement: An obvious partial quantification of entanglement is to evaluate 'distance' of a state to the nearest tensor-product state, and Linear Entanglement (LE) is used in this paper to quantify this distance (Section 6, Definitions 10, 11).
- Stubborness of Entanglement: The second, more refined, partial entanglement quantification proposed in this paper is the Stubborness of Entanglement (SE), which is a series of k' parameters, β_j, specifying entanglement order after j most-destructive single-qubit measurements on $\mathbf{s}$ (Section 7, Definition 16), where the minimum number of measurements necessary to completely destroy entanglement is k'.

Measurement

Definition 3 *Let $\boldsymbol{s}$ be an n-qubit state. Then the vector $\boldsymbol{s} = (s_0, s_1, \ldots, s_{2^n-1})$ implies a measurement basis ($\boldsymbol{s}$-basis) such that qubit i is measured as η with probability $\sum_{\substack{k=0 \\ k_i=\eta}}^{2^n-1} |s_k|^2$, where k is decomposed as $k = \sum_{i=0}^{n-1} k_i 2^i$, and $\eta, k_i \in \{0, 1\}$. After measurement, $\boldsymbol{s}$ becomes $\boldsymbol{s}_{\boldsymbol{x_i}=\boldsymbol{\eta}}$.*

Example: For $\boldsymbol{s} = (s_0, s_1, s_2, s_3)$, there is a probability $|s_0|^2$,$|s_1|^2$,$|s_2|^2$,$|s_3|^2$ of measuring two qubits in states $00, 01, 10, 11$, respectively. As soon as we 'measure' (look at) one or more of the qubits in the $\boldsymbol{s}$-basis, then we destroy the entanglement and superposition of those qubits, effectively projecting $\boldsymbol{s}$ down to a subspace determined by the measurement basis.

For the rest of this paper normalisation of $\mathbf{s}$ is omitted for clarity. Normalisation will always ensure $\sum_{i=0}^{2^n-1} |s_i|^2 = 1$.

2.2 Entanglement and the Environment

Quantum physicists often envisage a more complicated scenario than that described above where one is trying to measure entanglement of an n-qubit

system which also has extraneous entanglements with the environment. It is inaccurate to measure entanglement between n qubits if the system is also entangled with the environment unless we also take into account the environment. This leads to the definition of 'mixed states' which are not described by vectors, but by density matrices. Let $\boldsymbol{s}$ be a two qubit pure quantum state (s_0, s_1, s_2, s_3). Then we represent this state by a 4×4 density matrix which is the outer product of $\boldsymbol{s}$ with $\boldsymbol{s}^*$. Thus, $\boldsymbol{\rho_s} = \begin{pmatrix} |s_0|^2 & s_0 s_1^* & s_0 s_2^* & s_0 s_3^* \\ s_1 s_0^* & |s_1|^2 & s_1 s_2^* & s_1 s_3^* \\ s_2 s_0^* & s_2 s_1^* & |s_2|^2 & s_2 s_3^* \\ s_3 s_0^* & s_3 s_1^* & s_2 s_3^* & |s_3|^2 \end{pmatrix}$. More generally, an n-qubit mixed state is then a statistically weighted sum of n-qubit pure states, and can be described by $\boldsymbol{\rho} = \sum_i p_i \boldsymbol{\rho_{s_i}}$ where $\sum_i p_i = 1$, and $0 \leq p_i \leq 1$ [13]. A local qubit basis is any basis vector from the set $\mathbf{l_n}$ (Definition 1). Although $\boldsymbol{\rho}$ may look different under a different local basis, any entanglement measure for the matrix should be local-basis-independent. The distance measure of entanglement for mixed states must now measure minimum distance of a mixed state to the n-qubit tensor product states which may also be entangled with the environment - these are called the 'separable' states. We visualise 'pure' and 'mixed' entanglement distance measures as in Fig 1. Mixed-state entanglement is often considered in the

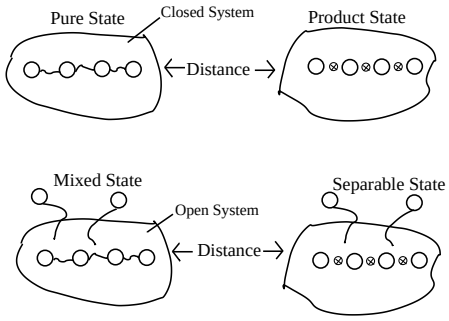

Fig. 1. Pure and Mixed-State Entanglement Measures

literature [13,15,1,33], although definitive entanglement measures have yet to be agreed upon for more than two particles. For two particles in a mixed state, Von Neumman entropy of the partial trace, (which is $\mathrm{Tr}(\boldsymbol{\rho_r} \log(\boldsymbol{\rho_r}))$, where $\boldsymbol{\rho_r}$ is the reduced state density matrix of $\boldsymbol{\rho}$ after 'tracing out' (fixing) one of the two particles) evaluates the distance to the separable states [24,30]. For mixed states of more than two particles, entanglement has been parameterised using polynomial invariant theory [1,14], and in many other ways [29,22,8,32,23,10,4], with an emphasis on asymptotic measures [15,30]. Moreover, some more general approaches to multiparticle pure state entanglement in an open system are given in [29,33,2,5,10]. A communications engineer could view entanglement of a mixed-state as the 'effectiveness' of a code in a

given channel. However, in this paper, we only consider pure state entanglement in a closed system - in other words we assume little or no entanglement with the environment. Thus we are examining the 'essence' of entanglement, but side-stepping the more practical issue of its context.

3 Entanglement and Error-Correction Codes

Proposition 1 *A binary linear* $[n, k]$ *error-correcting code (ECC),* $\mathbf{C}$*, can be represented by a length* 2^n *binary indicator,* $\mathbf{s}$*, where* $\mathbf{C} = \{(i_0, i_1, \ldots, i_{n-1}) | s_i \neq 0\}$*, where* $i = \sum_{j=0}^{n-1} i_j 2^j$, $i_j \in \{0, 1\}$*. More specifically, codeword* $(i_0, i_1, \ldots, i_{n-1})$ *in* $\mathbf{C}$ *occurs with probability* $|s_i|^2$*.*

In words, the state vector index is a codeword occurring with probability equal to the magnitude-squared of the complex value at that index. A qu**bit** state can be re-interpreted as a **binary** code, $\mathbf{C}$. If $\mathbf{s}$ is a binary vector then the state has binary probabilities, and each codeword is equally likely.

Proposition 2 *The n-qubit code represented by* $\boldsymbol{s}$ *satisfies* $\boldsymbol{s} \notin \boldsymbol{l_n}$ *if* $\boldsymbol{s}$ *has error-correction capability (Corollary 2).*

In words, $\boldsymbol{s}$ is entangled and cannot be written as a tensor-product of length 2 vectors if $\boldsymbol{s}$ has error-correction capability.

Examples Consider the two-qubit entangled vector, $\boldsymbol{s} = (1, 0, 0, 1)$. This state is known as the 'CAT' state in physics literature. Measurement of the two qubits in the $\boldsymbol{s}$-basis produces states 00 and 11 with equal likelihood. 01 and 10 are never measured. $\boldsymbol{s}$ is the 'indicator' for the parity-check $[2, 1, 2]$ code, $\mathbf{C} = \{00, 11\}$, with blocklength $n = 2$, dimension $k = 1$, and Hamming Distance $d = 2$. By Proposition 2, $\boldsymbol{s}$ is entangled because $\mathbf{C}$ has error-correction capability. In contrast, consider the two-qubit unentangled vector, $\boldsymbol{s} = (1, 0, 1, 0) = (1, 0) \otimes (1, 1)$. $\boldsymbol{s}$ defines a $[2, 1, 1]$ code, $\mathbf{C} = \{00, 10\}$, which has minimum Hamming Distance 1. This paper also shows that LE and SE are optimised over the set of binary linear ECCs when $\mathbf{C}$ is optimal (Corollary 3). Consider the three-qubit entangled vector, $\boldsymbol{s} = (1, 0, 0, 1, 0, 1, 1, 0)$. $\boldsymbol{s}$ defines a $[3, 2, 2]$ code, $\mathbf{C} = \{000, 011, 101, 110\}$ which can correct one error in any of the three bits. It also has optimal LE and SE over the set of length-3 binary linear ECCs. Of particular interest to physicists are generalised GHZ states which are indicators over n qubits for binary linear $[n, 1, n]$ ECCs. These are repetition codes, with two codewords, $00\ldots0$, and $11\ldots1$. By Corollary 2, the high distance, $d = n$, maximises the SE parameter, β_1, but the low dimension, $k = 1$, indicates that only one measurement is necessary to completely destroy entanglement.

4 Entanglement Equivalence Under Local Unitary Transformation

A unitary transform $\mathbf{U}$ satisfies $\mathbf{U}\mathbf{U}^{\dagger} = \mathbf{I}$ where $\dagger$ means conjugate transpose and $\mathbf{I}$ is identity. Quantum mechanics allows quantum states to be modified only by pre-multiplication by unitary matrices, or by 'destructive' measurement (however these destructive measurements could also be notionally described by large unitary matrices which cover both qubits and environment). By Parseval's theorem, the unity determinant of a unitary transform matrix preserves energy of the quantum state but, in general, can make or break entanglement. In this paper, we are particularly interested in the subclass of unitary matrices, $\mathbf{U}$, which are entanglement-invariant transformations. Let $\mathbf{U}$ be a $2^n \times 2^n$ unitary transform. Let $\boldsymbol{s}$ be the joint-state vector of n qubits.

Fact 1 *If* $\mathbf{U}$ *is tensor decomposable into* 2×2 *local unitary (LU) transforms, then the entanglement of* $\boldsymbol{s}$ *is the same as the entanglement of* $\mathbf{U}\boldsymbol{s}$.

Definition 4 *If* $\exists \mathbf{U}$, *where* $\mathbf{U}$ *is decomposable into* 2×2 *local unitaries, such that* $\boldsymbol{s}' = \mathbf{U}\mathbf{s}$, *then we write* $\boldsymbol{s}' \equiv_{LU} \boldsymbol{s}$ *(LU Equivalence).*

Fig 2 shows Local Unitary (LU) transformation. The left-hand (lh) diagram

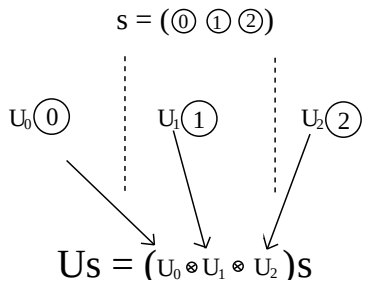

Fig. 2. Local Unitary (LU) Transformation

in Fig 3 shows invariance of entanglement under LU transformation, and the right-hand (rh) diagram shows that a tensor-unfactorisable matrix can break (or make) entanglement. LU equivalence allows us to develop large equivalence classes of states with identical entanglement, and view a quantum state from different angles. If we permit a description of a code such that codewords can occur with complex probabilities, then we can say,

Proposition 3 *If* $\boldsymbol{s} \equiv_{LU} \boldsymbol{s}'$ *then* $\boldsymbol{s}$ *and* $\boldsymbol{s}'$ *represent 'equivalent' codes.*

Proposition 4 *If* $\boldsymbol{s} \not\equiv_{LU} \boldsymbol{s}'$, *then* $\boldsymbol{s}$ *and* $\boldsymbol{s}'$ *represent 'inequivalent' codes.*

Fig. 3. Changing Entanglement

Code duality is a familiar example of entanglement equivalence. The $2^n \times 2^n$ Walsh-Hadamard Transform (WHT) is $\bigotimes_{i=0}^{n-1} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$:

Proposition 5 *Let* $\mathbf{C}$ *and* $\mathbf{C}^{\perp}$ *be binary linear ECCs described by the indicators* $\boldsymbol{s}$ *and* $\boldsymbol{s'}$*, respectively. Then* $\boldsymbol{s} \equiv_{LU} \boldsymbol{s'}$*, where the LU transform is the WHT.*

Example: The $[3, 1, 3]$ binary linear ECC, $\boldsymbol{s'} = (1, 0, 0, 0, 0, 0, 0, 1)$, is obtained from the $[3, 2, 2]$ binary linear ECC, $\boldsymbol{s} = (1, 0, 0, 1, 0, 1, 1, 0)$, by application of the 8×8 WHT [18,26].

5 *HI* Multispectra and the Set, $\ell_{\mathbf{p}}$

5.1 Theory

Entanglement of quantum states is invariant under any LU transform, but this paper emphasises the spectra of a subset of quantum states after transform by LU tensor products of $\mathbf{H}$ and $\mathbf{I}$, where $\mathbf{H} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and $\mathbf{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We call this set of transforms the '*HI* Transform', and the associated spectra the '*HI* multispectra'. In this section we identify a set of states, $\ell_{\mathbf{p}}$, which are LU equivalent to the set of binary linear ECCs, via *HI* transforms (Theorem 2). In later sections we show that, for states from $\ell_{\mathbf{p}}$, the LE and SE can be found from the *HI* multispectra (Theorems 7,8,14, 15). To describe these spectra we require the Algebraic Normal Form (ANF) for an associated function [18]. For instance, $\boldsymbol{s} = (1, 0, 0, 1, 0, 1, 1, 0)$ can alternatively be described by the boolean function, $s(x_0, x_1, x_2) = x_0 + x_1 + x_2 + 1$, where $s(x_0, x_1, x_2)$ can be interpreted as a sequence by concatenating the function evaluations at $x_2x_1x_0 = 000, 001, 010, \ldots, 111$ (a lexicographic ordering) to form the sequence 10010110. We further propose Algebraic Polar Form (APF) which separates magnitude (binary), and phase (bipolar) properties of $\boldsymbol{s}$,

$$\boldsymbol{s} = s(\mathbf{x}) = m(\mathbf{x})(-1)^{p(\mathbf{x})}$$

where $m(\mathbf{x})$ and $p(\mathbf{x})$ are both boolean Algebraic Normal Forms (ANFs) in n binary variables $\mathbf{x} = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$. The coefficients of $s(\mathbf{x})$ are in the set $\{-1, 0, 1\}$ (we consider more general alphabets in future papers). Normalisation is ignored so that it is always assumed that the magnitude-squareds of the coefficients of $s(\mathbf{x})$ sum to one. For example:

$$s(\mathbf{x}) = (x_0 + x_1 + x_2 + 1)(x_1 + x_3)(-1)^{(x_1x_2 + x_0 + 1)} = \\ 0, 0, 0, 1, 0, 0, 1, 0, -1, 0, 0, 0, 0, 1, 0, 0$$

where '+' and '−' are mod 2 operations. $m(\mathbf{x})$ is decomposed as $m(\mathbf{x}) = \prod_k h(\mathbf{x})_k$. For these preliminary investigations, we are interested in $m(\mathbf{x})$ comprising $h(\mathbf{x})_k$ of degree 1, and $p(\mathbf{x})$ of degree ≤ 2. APFs are useful because, for graphs with many qubits but relatively few $\overline{\text{XOR}}$ or AND connections (low-density) we do not wish to operate explicitly on a very large state vector. The APF allows us to implicitly act on this vector via the compact APF description [1]. Only main results are presented here. Appendix 12 provides proofs and further subsidiary theorems.

Definition 5 *"H acting on i" means the action of the 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* $H(i)[\boldsymbol{s}]$*.*

$\prod_{i \in \mathbf{T}} H(i)$ is the action of H on the subset of qubits i represented by the integers in $\mathbf{T}$. This action can happen in any order as each $H(i)$ acts **locally** only on qubit i.

Definition 6 *Let* $s(\mathbf{x}) = m(\mathbf{x})(-1)^{p(\mathbf{x})}$ *be a binary APF, where* $\deg(p(\mathbf{x})) \leq 2$*, and* $m(\mathbf{x})$ *is such that* $\deg(h(\mathbf{x})_k) = 1$*,* $\forall k$*. We refer to such an* $s(\mathbf{x})$ *as a 'binary spectra APF'. Let* $\boldsymbol{\Theta}$ *be the set of all binary spectra APF.*

Theorem 1 $\boldsymbol{\Theta}$ *is closed under the action of* $\prod_{i \in \mathbf{T}} H(i)$*,* $\forall$ $\mathbf{T}$*, where* $\mathbf{T} \subset \{0, 1, \ldots, n-1\}$*.*

Proof. Section 12. ∎

Theorem 1 implies that the HI multispectra (including WHT) of a binary spectra APF is at most three-valued. One subset of $\boldsymbol{\Theta}$ is $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$. Another subset of $\boldsymbol{\Theta}$ is $s(\mathbf{x}) = m(\mathbf{x})$, where $m(\mathbf{x})$ is a product of linear functions.

Definition 7 *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 8 $\ell_{\mathbf{p}}$ *is the subset of all* $s(\mathbf{x})$ *from* $\boldsymbol{\Theta}$ *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* $\deg(q_k(\mathbf{x_C})) = \deg(r_k(\mathbf{x_{C^\perp}})) = 1$ $\forall k$*, and where* $x_i \in p(\mathbf{x})$*,* $\forall$ $i \in \{0, 1, \ldots, n-1\}$*. We refer to* $\ell_{\mathbf{p}}$ *as the set of 'bipartite quadratic bipolar' states.*

Theorem 2 *If* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*, then the action of* $\prod_{i \in \mathbf{T}} H(i)$ *on* $\boldsymbol{s}$ *gives* $s'(\mathbf{x}) = m(\mathbf{x})$*, for* $\mathbf{T} = \mathbf{T_C}$*, or* $\mathbf{T} = \mathbf{T_{C^\perp}}$*.* $\boldsymbol{s'}$ *is the binary indicator for a binary linear* $[n, n-|\mathbf{T}|, d]$ *error correcting code,* $\mathbf{C}$*, (or* $\mathbf{C}^\perp$*), if* $\mathbf{T_C}$*, (or* $\mathbf{T_{C^\perp}}$*) is used.*

[1] LDPC and Turbo-Decoding strategies also exploit 'low-density' [19,12,3], and it is hoped that APF in conjunction with graph-based models will be useful for the construction and analysis of many-qubit entangled systems [27,9,34].

Proof. Section 12. ∎

Example: Let $\mathbf{T_C} = \{0, 2, 5, 7\}$ and $\mathbf{T_{C^\perp}} = \{1, 3, 4, 6\}$. Let, $s(\mathbf{x}) = (-1)^{x_0x_1+x_0x_3+x_0x_4+x_1x_2+x_1x_5+x_2x_3+x_2x_6+x_3x_7+x_4x_5+x_4x_7+x_5x_6+x_6x_7}$. Then, for $\mathbf{T} = \mathbf{T_C}$, $s'(\mathbf{x}) = (x_0 + x_1 + x_3 + x_4 + 1)(x_1 + x_2 + x_3 + x_6 + 1)(x_1 + x_4 + x_5 + x_6 + 1)(x_3 + x_4 + x_6 + x_7 + 1)$ is an indicator for the $[8, 4, 4]$ binary linear code. We now consider certain $p(\mathbf{x})$ of any degree.

Definition 9 *$\aleph$ is the set of $s(\mathbf{x})$ 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 $\deg(q_k(\mathbf{x_C})) = 1$ $\forall k$, $r_k(\mathbf{x_{C^\perp}})$ is of arbitrary degree $\forall k$, and where $x_i \in p(\mathbf{x})$, $\forall\ i \in \{0, 1, \ldots, n-1\}$.*

Conjecture 1 *If $\boldsymbol{s} \in \aleph$ then the action of $\prod_{i \in \mathbf{T_C}} H(i)$ on $\boldsymbol{s}$ gives $s'(\mathbf{x}) = m'(\mathbf{x})$, where $m'(\mathbf{x})$ is a binary polynomial. We can interpret $\boldsymbol{s'}$ as a binary error correcting code (linear or nonlinear, as appropriate).*

5.2 Examples

We now discuss a few examples of the LU equivalence via HI transforms between quadratic bipartite bipolar sequences (the set $\ell_{\mathbf{p}}$) and the binary indicators for binary linear ECCs, highlighting graphical representations.
Example 1: Let $\boldsymbol{s} = (+++-++-++++---+-)$, where '+' = 1, and '−' = −1. Then $\boldsymbol{s} = (-1)^{0001001000011101} \in \ell_{\mathbf{p}}$, In ANF this is, $s(x_0, x_1, x_2, x_3) = (-1)^{x_0x_1+x_1x_2+x_2x_3}$. This quadratic ANF satisfies a bipartite splitting where $\mathbf{T_C} = \{x_0, x_2\}$ and $\mathbf{T_{C^\perp}} = \{x_1, x_3\}$. We can apply $H(0)H(2)$ to $\boldsymbol{s}$ to get $\boldsymbol{s'} = (1000000100011000) = (x_0 + x_1 + 1)(x_1 + x_2 + x_3 + 1)$, which is the binary indicator for a $[4, 2, 2]$ binary linear block code, $\mathbf{C}$. Alternatively, we can apply $H(1)H(3)$ to $\boldsymbol{s}$ to get $\boldsymbol{s''} = (1001000000000110) = (x_0 + x_1 + x_2 + 1)(x_2 + x_3 + 1)$, which is the binary indicator for the $[4, 2, 2]$ binary linear block code, $\mathbf{C}^\perp$.

We can represent members of $\ell_{\mathbf{p}}$ graphically, as in Fig 4, where a circle is a qubit, and a line implies the existence of a quadratic term comprising the qubits at either end of the line. Applying $\mathbf{H}$ to all qubits on the left, or to all qubits on the right, converts the bipolar sequence to the binary indicator representing $\mathbf{C}$, or $\mathbf{C}^\perp$, respectively. The number of $\mathbf{H}$ operators applied determines the number of parity bits for the code (Theorem 2). Entanglement of a member of $\ell_{\mathbf{p}}$ is identical to the LU-equivalent indicators for $\mathbf{C}$ and $\mathbf{C}^\perp$ [2]. After appropriate Walsh-Hadamard rotations to the bipartite bipolar sequence, the resultant binary indicator can also be represented graphically, as shown in Fig 5, where squares with crosses represent $\overline{\text{XOR}}$. This ' Factor Graph' representation is currently the subject of much research in the context of Low Density Parity Check (LDPC) codes for iterative decoding [19,12], and

[2] A potential source of confusion is that a cryptographer often equates binary sequence *abcde* with bipolar sequence $(-1)^{abcde}$ via the operation $2\{0, 1\} - 1 = \{-1, 1\}$. This non-unitary equivalence is **forbidden** in quantum systems.

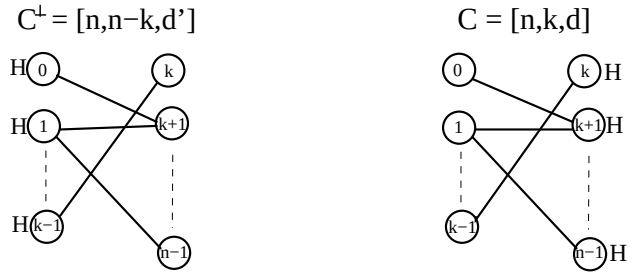

Fig. 4. Quadratic Bipolar Bipartite State from $\ell_{\mathbf{p}}$ Before/After Applying **H** Operators

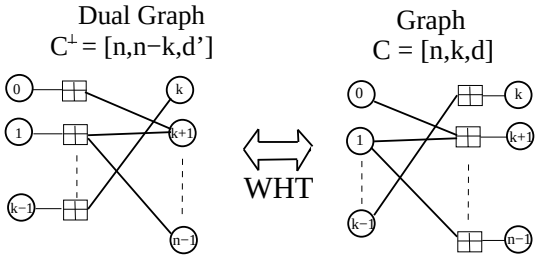

Fig. 5. Binary Indicator State (Factor Graph)

the Factor Graph form that arises from selective Walsh-Hadamard rotations of a quadratic bipartite bipolar sequence is the ' Normal Realisation', as recently described in [11].

Example 2: The sequence $+++-++-++-++-++++-++-++++++-++-+$ has ANF $s(x_0,x_1,x_2,x_3,x_4) = (-1)^{x_0x_1+x_0x_3+x_0x_4+x_1x_2+x_2x_3+x_2x_4}$ and is equivalent via action of $H(1)H(3)H(4)$ to the indicator, $s'(x_0,x_1,x_2,x_3,x_4) = (x_0+x_1+x_2+1)(x_0+x_2+x_3+1)(x_0+x_2+x_4+1)$, for a $[5,2,2]$ binary linear ECC, **C**. Alternatively $s(x_0,x_1,x_2,x_3,x_4)$ is equivalent via action of $H(0)H(2)$ to the indicator, $s''(x_0,x_1,x_2,x_3,x_4) = (x_0+x_1+x_3+x_4+1)(x_1+x_2+x_3+x_4+1)$, for a $[5,3,2]$ binary linear ECC, $\mathbf{C}^{\perp}$. We illustrate Example 2 in Fig 6 where the lh-side is a bipolar graph, and the rh-side is a binary graph for the associated binary code.

The LU equivalence between the set $\ell_{\mathbf{p}}$ and binary linear ECCs also extends to LU equivalence between **higher-degree** bipartite bipolar sequences and binary **nonlinear** ECCs. A bipolar bipartite sequence of any ANF degree is shown in Fig 7, where the black dot in a square represents AND, and the sequence is LU equivalent to a binary indicator for a binary ECC (linear if the bipolar degree ≤ 2, nonlinear otherwise), by application of **H** to all qubits on the rh-side (not the lh-side). The dimension of the associated binary code, k, is then given by the number of qubits on the lh-side. The general rule is that **H** is applied to one, and only one, variable in each product

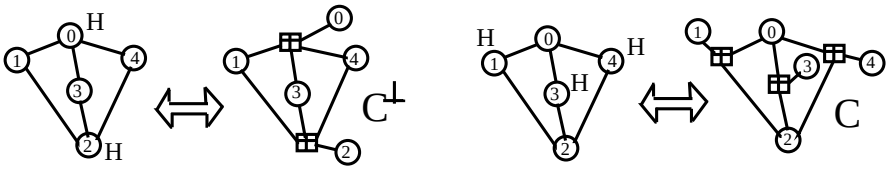

Fig. 6. Bipolar to Binary Equivalence (Example 2)

term of the bipolar ANF (Conjecture 1), and in Fig 7 no two qubits on the right occur in the same product term. Fig 7 shows, as an example, the ANF,

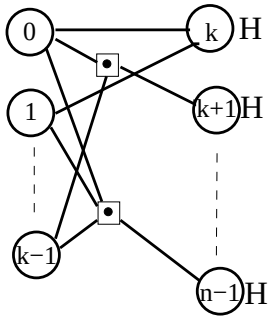

Fig. 7. Bipolar Bipartite Sequences of any ANF Degree

$(-1)^{x_0x_1x_{k-1}x_{n-1}+x_0x_{k-1}x_{k+1}+x_1x_k+x_0x_k+p'(\mathbf{x})}$, for some bipartite $p'(\mathbf{x})$.

Example 3: The nonlinear $[16,8,6]$ Nordstrom-Robinson binary ECC is LU-equivalent to a bipolar bipartite sequence (a member of $\aleph$, Conjecture 1) with an ANF which comprises 96 cubic terms and 40 quadratic terms, and where $|T_C| = |T_{C^\perp}| = 8$. The binary linear $[16,8,4]$ ECC, described by the 40 quadratic terms can be 'doped' with 96 cubic terms to increase Hamming Distance from 4 to 6. We have the following nonlinear subcodes with underlying linear subcodes, which are LU-equivalent under a combination of **H** and **I** operators to bipolar sequences with cubic + quadratic, or quadratic ANFs, respectively.

Nonlinear	$[16,8,6] \Leftarrow HI \Rightarrow$	96 cubics	40 quads
Linear	$[16,8,4] \Leftarrow HI \Rightarrow$	–	40 quads
Subcode:			
Nonlinear	$[12,4,6] \Leftarrow HI \Rightarrow$	16 cubics	20 quads
Linear	$[12,4,6] \Leftarrow HI \Rightarrow$	–	20 quads
Subcode:			
Linear	$[10,2,6] \Leftarrow HI \Rightarrow$	–	10 quads

6 PAR_l and Linear Entanglement (LE)

6.1 Definitions

Partial quantification of entanglement for $\boldsymbol{s}$ of length 2^n (n qubits) is achieved by measuring maximum possible correlation of $\boldsymbol{s}$ with **any** length 2^n 'linear' sequence, $\boldsymbol{l_n}$. This correlation maximum can be expressed as a 'Peak-to-Average-Power-Ratio' (PAR_l),

Definition 10

$$PAR_l(\boldsymbol{s}) = 2^n max_{\boldsymbol{l}}(|\boldsymbol{s} \cdot \boldsymbol{l}|^2)$$

where $\boldsymbol{l}$ is any normalised linear sequence from the set, $\boldsymbol{l_n} = \{(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})\}$, and $\cdot$ means 'inner product' [20].

Linear Entanglement (LE) is then defined as,

Definition 11

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

$\boldsymbol{s}$ is completely uncorrelated with all linear sequences and wholly correlated with a particular linear sequence (unentangled) when its PAR_l is 1 and 2^n, respectively. PAR_l is LU-invariant, and is a natural generalisation of well-known spectral measures, as it includes WHT spectra and, more generally, all one and multi-dimensional complex Discrete Fourier spectra, as subspectra. We can alternatively express PAR_l as,

Definition 12 *Let* $\boldsymbol{s'} = (s'_0, s'_1, \ldots, s'_{2^n-1}) = (\bigotimes_{j \in \mathbf{T}} \mathbf{U}(j))\boldsymbol{s}$, *where* $\mathbf{U}(j) = \begin{pmatrix} \cos\theta_j & \sin\theta_j e^{iw_j} \\ \sin\theta_j e^{-iw_j} & -\cos\theta_j \end{pmatrix}$, $i^2 = -1$, *and* θ_j *and* w_j *can take any real values,* $\forall j$. *Then,*

$$PAR_l(\boldsymbol{s}) = 2^n max_t(|s'_t|^2), \qquad \forall \mathbf{T} \subset \{0, 1, \ldots, n-1\}$$

We have written software to compute PAR_l for any $\boldsymbol{s}$. However the computation is too large for more than about 5 or 6 qubits.

6.2 PAR_l for States from $\ell_{\mathbf{p}}$

Definition 13

$$PAR(\boldsymbol{s}) = 2^n max_i(|s_i|^2)$$

Theorem 3 *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,*

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

Proof. Without loss of generality let $k \leq n-k$. The indicator for the $[n,k,d]$ code has 2^k equal magnitude non-zero coefficients. By Parseval's Theorem and normalisation, the PAR of such an indicator must be 2^{n-k}. ∎

Theorem 3 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 $\mathrm{PAR}_l \geq 2^{\lceil \frac{n}{2} \rceil}$. In this case LE coincides with the 'Schmidt Measure', $\mathbf{P}$ [10,5], defined as $\log_2$ of the minimal number of non-zero entries in any state, $\boldsymbol{s}'$, where $\boldsymbol{s}' \equiv_{\mathrm{LU}} \boldsymbol{s}$.

Theorem 4 *If $\boldsymbol{s} \in \ell_{\mathbf{p}}$ then $\boldsymbol{s}$ is LU equivalent to the indicator for an $[n,k,d]$ code, and the Schmidt Measure, P, satisfies, $P(\boldsymbol{s}) \leq min(k, n-k)$.*

Here is a stronger result.

Theorem 5 *Let $s(\mathbf{x}) = (-1)^{x_{\pi(0)}x_{\pi(1)} + x_{\pi(1)}x_{\pi(2)} + \cdots + x_{\pi(n-2)}x_{\pi(n-1)}}$, where π is any permutation of the indeces $\{0,1,\ldots,n-1\}$. Then $PAR_l = 2^{\lceil \frac{n}{2} \rceil}$.*

Proof. Corollary 6 of Section 7 of [20]. ∎

[5] also considers the "line graph" states of Theorem 5 (e.g. $|\Phi_4>$ of [5] is LU equivalent to $(-1)^{x_0x_1 + x_1x_2 + x_2x_3}$). In [5] Persistency of Entanglement (Section 7) of such states is proven to be $\lfloor \frac{n}{2} \rfloor$. This is the same as proof of PAR_l, because Persistency, LE, and Schmidt Measure all coincide for these states. These states also have PAR ≤ 2.0 under the one-dimension complex Discrete Fourier Transform [7,21,20]

We now show how to compute the PAR of any *HI* transform of a member of $\ell_{\mathbf{p}}$. Let $\mathbf{s} \in \ell_{\mathbf{p}}$. Recalling Definition 7, 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 $\mathbf{x}_* = \mathbf{x}_{\mathbf{t}^\perp} \cup \mathbf{x}_{\mathbf{t}}$. We 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 $p(\mathbf{x}) = \sum_{i \in \mathbf{T}_{\mathbf{C}^\perp}} x_i (\sum_{j \in \mathbf{T}_{\mathbf{C}}} M_{i,j-k} x_j)$. Then we define a submatrix, $\mathbf{M}_{\mathbf{t}}$, 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 $\mathbf{M}_{\mathbf{t}}$.

Theorem 6 *Let $\boldsymbol{s}'$ be the result of the action of $\prod_{i \in \mathbf{t}_{\mathbf{C}^\perp} \cup \mathbf{t}_{\mathbf{C}}} H(i)$ on $\boldsymbol{s} \in \ell_{\mathbf{p}}$. Then,*

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

Proof. We observe that $\mathrm{PAR}(\boldsymbol{s}') = \mathrm{PAR}(\mathrm{WHT}((-1)^{p_t(\mathbf{x}_*)}))$, where $p_t(\mathbf{x}_*) = \sum_{i \in \mathbf{t}_{\mathbf{C}^\perp}} x_i (\sum_{j \in \mathbf{t}_{\mathbf{C}}} M_{i,j-k} x_j)$. By affine transformation of the variables in $\mathbf{x}_*$ we can rewrite $p_t(\mathbf{x}_*)$ as,

$$p_t(\mathbf{x}_*) = \sum_{i=0}^{\chi_t - 1} f_i(\mathbf{x}_{\mathbf{t}^\perp}) g_i(\mathbf{x}_{\mathbf{t}})$$

where f_i and g_i are linearly independent linear combinations of the variables in $\mathbf{x}_{\mathbf{t}^\perp}$ and $\mathbf{x}_{\mathbf{t}}$, respectively, $\forall i$. For clarity we further rewrite p_t as,

$$p_t(\mathbf{x}_*) = p_t(\mathbf{y}, \mathbf{z}) = \sum_{i=0}^{\chi_t - 1} y_i z_i$$

where the y_i and z_i are linearly independent binary variables over the spaces $\mathbf{x}_{\mathbf{t}^\perp}$ and $\mathbf{x}_{\mathbf{t}}$, respectively. It is known that the WHT over the $2\chi_t$ binary variables $\mathbf{y} \cup \mathbf{z}$ of $(-1)^{p_t(\mathbf{y},\mathbf{z})}$ has PAR = 1, (i.e. p_t is bent, [18]). Therefore the WHT of $(-1)^{p_t(\mathbf{x}_*)}$ over the $h + h^\perp$ binary variables in $\mathbf{x}_*$ has PAR $= 2^{h+h^\perp-2\chi_t}$. ∎

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

Theorem 3 also follows trivially from Theorem 6.

Each $\mathbf{M_t}$ is associated with a different code, C_{M_t}, with dimension $n - \log_2(\mathrm{PAR}(\boldsymbol{s}'))$. In particular, when $\mathbf{t_{C^\perp}} = \mathbf{T_{C^\perp}}$ and $\mathbf{t_C} = \emptyset$ then $C_{M_t} = C$ with dimension k. Similarly, when $\mathbf{t_{C^\perp}} = \emptyset$ and $\mathbf{t_C} = \mathbf{T_C}$ then $C_{M_t} = C^\perp$ with dimension $k^\perp = n - k$. When $\mathbf{t_{C^\perp}} = \mathbf{t_C} = \emptyset$ then C_{M_t} has dimension n. Each code, C_{M_t}, is specified by the bit positions which are acted on by $H(i)$, i.e. the integers in $\mathbf{t_{C^\perp}} \cup \mathbf{t_C}$.

Lemma 1 *Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*, and let* $\boldsymbol{s}'$ *be a HI transform of* $\boldsymbol{s}$*. Let* $\boldsymbol{s}'' = H(i)[\boldsymbol{s}']$*. Then,*

$$\frac{PAR(\boldsymbol{s}'')}{PAR(\boldsymbol{s}')} \in \{\frac{1}{2}, 2\}$$

Proof. If an integer, e, is added or removed to or from either $\mathbf{t_{C^\perp}}$ or $\mathbf{t_C}$ then the associated qubit, x_e, is acted on by $H(e)$, and the associated row or column is added or removed to give $\mathbf{M_e}$, with associated rank, χ_e. From Theorem 6 we see that if $\chi_e = \chi_t$ or $\chi_t - 1$, respectively, then PAR doubles whereas, if $\chi_e = \chi_t$ or $\chi_t + 1$, respectively, then PAR halves. ∎

Theorem 7 PAR_l *of* $\boldsymbol{s} \in \ell_{\mathbf{p}}$ *is found in the HI multispectra of* $\boldsymbol{s}$*.*

Proof. Section 13. ∎

7 Weight Hierarchy and Stubborness of Entanglement (SE)

7.1 Weight Hierarchy

We prove that weight hierarchy of an $[n, k, d]$ linear code, $\mathbf{C}$, can be obtained from the HI multispectra.

Definition 14 *The Weight Hierarchy of* $\mathbf{C}$*, 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 8 *Let* $\boldsymbol{s_c}$ *be the indicator of an* $[n, k, d]$ *binary linear error-correcting code,* $\mathbf{C}$*. Let* $\mathbf{Q} \subset \{0, 1, \ldots, n-1\}$*. Let,*

$$m_{\mathbf{Q}} = \frac{|\mathbf{Q}| + \log_2(\mu) - n + k}{2}, \quad \textit{where } \mu = PAR(\boldsymbol{s'_c}) \tag{1}$$

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,*

$$d_j = min_{\mathbf{Q}|m_Q=j}(|\mathbf{Q}|)$$

Proof. Section 14 ∎

7.2 Stubborness of Entanglement

Theorem 9 *Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*. A single qubit measurement on* $\boldsymbol{s}$ *gives* $\boldsymbol{s'}$*, and has one of two results:*

- *Destructive Measurement, where* $|\{s'_i | s'_i \neq 0\}| = \frac{1}{2}|\{s_i | s_i \neq 0\}|$*, and* $PAR(\boldsymbol{s'}) = 2PAR(\boldsymbol{s})$*.*
- *Redundant Measurement, where* $|\{s'_i | s'_i \neq 0\}| = |\{s_i | s_i \neq 0\}|$*, and* $PAR(\boldsymbol{s'}) = PAR(\boldsymbol{s})$*.*

where $|s_i|, |s'_i| \in \{0, 1\}$*.*

Proof. Section 14. ∎

Let the entanglement order of a system be the size (in qubits) of the largest entangled subsystem of the system.

Definition 15 *A most-destructive series of* j *single-qubit measurement 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 *The Stubborness of Entanglement (SE) is a series of parameters,* β_j*,* $0 \leq j \leq k'$*, representing the smallest possible entanglement order,* β_j*, after* $k' - j$ *most-destructive measurements of an* n*-qubit system, where* $\beta_{k'} = n$*,* $\beta_0 = 0$*.*

Note that 'Persistency of Entanglement', as defined in [5], is k', as it is the minimum number of measurements necessary to reduce the state to entanglement order 0. This section shows that the similarity between Definitions 14 and 16 implies that the Weight Hierarchy upper bounds LE (Corollary

10) and becomes equivalence for optimal or near-optimal binary linear ECCs (Theorem 15). For a state from $\ell_{\mathbf{p}}$ which is LU-equivalent to an $[n,k,d]$ binary linear ECC, we show that the minimum number of single qubit measurements, **in any basis**, required to completely disentangle such a state is $\leq k$ (Theorem 11). We also show that, for such states, the series of 'most-destructive' measurements occurs in the HI multispectra (Theorem 14).

Definition 17 *The* $\mathbf{C}$*-basis for* $\boldsymbol{s}$ *is the basis in which the vector becomes an indicator for the code* $\mathbf{C}$*. This indicator has non-negative, multi-valued output and, for* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*, the indicator has binary values. Without loss of generality, we always assume* $|\mathbf{C}| \leq |\mathbf{C}^{\perp}|$*. There is not a* $\mathbf{C}$*-basis for every* $\boldsymbol{s}$ *but, for* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*, there exists a* $\mathbf{C}$*-basis and* $\mathbf{C}^{\perp}$*-basis.*

Example: By Theorem 18, the bipartite bipolar quadratic state $s(\mathbf{x}) = (-1)^{x_0x_1+x_1x_2+x_2x_3+x_3x_0}$ is LU equivalent to $s_c(\mathbf{x}) = (x_0+x_1+x_3+1)(x_1+x_2+x_3+1)$ which is the indicator for $\mathbf{C} = \{0000, 0111, 1010, 1101\}$. Measuring qubit 0 of $s(\mathbf{x})$ in the $\mathbf{C}$-basis gives the indicator for the subcode $\{000, 111\}$ if $x_0 = 0$, and the subcode $\{010, 101\}$ if $x_0 = 1$.

Lemma 2 *Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*. Let* $\boldsymbol{s'}$ *be a* HI *transform of* $\boldsymbol{s}$*. Then* $n - \log_2(PAR(\boldsymbol{s'}))$ *destructive measurements in the* $\boldsymbol{s'}$*-basis are sufficient to completely destroy entanglement in* $\boldsymbol{s}$*.*

Proof. Follows from Theorem 9. ∎

Theorem 10 *Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$*. Then* $LE(\boldsymbol{s})$ *measurements is the minimum number of measurements required to completely destroy the entanglement of* $\boldsymbol{s}$*.*

Proof. From Definition 11, Theorem 7, and Lemma 2. ∎

Theorem 11 *Let* k *and* k' *be as defined in Definitions 14 and 16. Then* $k' \leq k$*. In words,* k *destructive measurements in the* $\mathbf{C}$*-basis suffice to destroy all entanglement in* $\boldsymbol{s}$*, where* $\boldsymbol{s} \in \ell_{\mathbf{p}}$ *is equivalent to the binary linear* $[n,k,d]$ *error-correcting code,* $\mathbf{C}$*.*

Proof. From Theorem 3 and Lemma 2. ∎

Theorem 12 $k-j$ *destructive measurements in the* $\mathbf{C}$*-basis suffice to reduce the entanglement order of* $\boldsymbol{s}$ *to* d_j *qubits, where* $\boldsymbol{s} \in \ell_{\mathbf{p}}$ *is equivalent to the binary linear* $[n,k,d]$ *error-correcting code,* $\mathbf{C}$*.*

Proof. By recursive application of the proof for Theorem 11. ∎

Corollary 2 *For* $\mathbf{s} \in \ell_{\mathbf{p}}$*,*

$$k' < k \quad \text{or} \quad \beta_j \leq d_j \quad \text{if } k' = k$$

In words, for states from $\ell_{\mathbf{p}}$*, the Weight Hierarchy is an upper bound on Stubborness of Entanglement.*

Theorem 13 *The series of residual entanglement orders, β'_j, resulting from j most-destructive measurements of $\mathbf{s_c}$ in the $\mathbf{s_c}$-basis, satisfies $\beta'_j = d_j$. In words, the Stubborness of Entanglement confined to the $\mathbf{s_c}$-basis is equivalent to the weight hierarchy of $\mathbf{C}$.*

Proof. By recursive application of Theorems 9, 8, Lemma 2, and Theorem 10. ∎

Warning: Let $\mathbf{S^c}_j$ be a size d_j subset of $\{0, 1, \ldots, n-1\}$, such that the linear subcode of $\mathbf{C}$ defined by $\mathbf{S^c}_j$ has dimension j. Then it is <u>not</u> necessarily the case that $\mathbf{S^c}_j \subset \mathbf{S^c}_{j+1}$ for any j.

Definition 18 *If $\mathbf{s_c}$ is a binary indicator for $\mathbf{C}$ such that $\mathbf{S^c_j} \subset \mathbf{S^c_{j+1}}$ $\forall j$, then $\mathbf{s}$ satisfies the 'chain condition'. The weaker definition of 'greedy weights' identifies only weights d_j for which $\mathbf{S^c_j} \subset \mathbf{S^c_{j+1}}$.*

Similarly, let $\mathbf{S^q}_j$ be a size β_j subset of $\{x_0, x_1, \ldots, x_{n-1}\}$, comprising the subset of qubits with maximum entanglement order, β_j, after $k' - j$ most-destructive measurements. Then it is <u>not</u> necessarily the case that $\mathbf{S^q}_j \subset \mathbf{S^q}_{j+1}$ for any j.

Definition 19 *If $\mathbf{s}$ is such that $\mathbf{S^q_j} \subset \mathbf{S^q_{j+1}}$ $\forall j$, then $\mathbf{s}$ satisfies the 'quantum chain condition'. The weaker definition of 'quantum greedy weights' identifies only weights β_j for which $\mathbf{S^q_j} \subset \mathbf{S^q_{j+1}}$.*

We leave investigation of the quantum chain condition to future work.

Theorem 14 *Let $\mathbf{s} \in \ell_\mathbf{p}$. Then the Stubborness of Entanglement of $\mathbf{s}$ can be computed from a set of most-destructive measurements in the HI-basis of $\mathbf{s}$.*

Proof. A single-qubit measurement reduces (classical) entropy of the system by a maximum of 1 bit per measurement. This corresponds to measuring the qubit value as 0 or 1 with equal likelihood $(-(\frac{1}{2}\log_2(\frac{1}{2}) + \frac{1}{2}\log_2(\frac{1}{2})) = 1)$. Destructive measurements in the HI-basis of a state $\mathbf{s}$ from $\ell_\mathbf{p}$ are always of this form (Theorem 9). For states from $\ell_\mathbf{p}$, entropy is LE. The theorem follows from Theorem 10. ∎

Definition 20 *A binary linear $[n, k, d]$ code is here considered optimal for a given n if $d_1, d_2, \ldots, d_{k-1}$ are maximised for each k, $k \leq \lfloor \frac{n}{2} \rfloor$, with priority to the weights, d_i, with lowest i.*

Theorem 15 *Let $\mathbf{s} \in \ell_\mathbf{p}$ where $\mathbf{s}$ 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.*

Proof. We require the following Lemma.

Lemma 3 *Let $\boldsymbol{s}$ be LU equivalent to an optimal or near-optimal binary linear code, C. If C has dimension $k = \frac{n}{2}$, the HI multispectra of $\boldsymbol{s}$ only has PAR as high as 2^{n-k} for two HI transforms, one the WHT of the other. These two transform spectra, $\boldsymbol{s_c}$ and $\boldsymbol{s_{c^\perp}}$ are binary indicators for C and $C^\perp$, respectively. Similarly, when C has dimension $k < \frac{n}{2}$, the HI multispectra of $\boldsymbol{s}$ only has PAR as high as 2^{n-k} for one HI transform. This transform spectra, $\boldsymbol{s_c}$, is the binary indicator for C.*

Proof. (Lemma 3). By Theorem 8, an optimal or near-optimal binary linear code should have PAR as low as possible in the HI multispectra. It is easy to validate Lemma 3 for $1 \leq n \leq 4$ by exhaustive computation. Now consider a state, $\boldsymbol{s}$, that satisfies Lemma 3 for n even. Then we can identify (at least) one HI transform of $\boldsymbol{s}$ which gives a PAR of 2^{n-k}. Let us call this transform R. Let $\mathbf{s} = (-1)^{\mathbf{p}}$. Let $x_i x_j$ be an arbitrary term in $\boldsymbol{p}$ such that R contains $H(i)$. Let us increase n by one to $n' = n + 1$ by appending $x_l x_i$, to create $p^+(\mathbf{x}) = p(\mathbf{x}) + x_l x_i$, where x_l is a new qubit added to the system. Then $R \otimes I_l$ is the only HI transform of $\boldsymbol{s^+} = (-1)^{\boldsymbol{p^+}}$ which achieves a PAR as high as 2^{n-k+1} so Lemma 3 is satisfied for n odd, as long as it is satisfied for n even. Let us now increase n to $n'' = n + 2$ by appending $x_l x_i + x_m x_j + x_l x_m$, to create $p^{++}(\mathbf{x}) = p(\mathbf{x}) + x_l x_i + x_m x_j + x_l x_m$, where x_l and x_m are new qubits added to the system. Then $R \otimes I_l \otimes H_m$, $R \otimes H_l \otimes H_m$, and $R \otimes H_l \otimes I_m$ are HI transforms of $\boldsymbol{s^{++}} = (-1)^{\boldsymbol{p^{++}}}$ which achieve a PAR of 2^{n-k+1}, 2^{n-k}, and 2^{n-k-1}, respectively. Therefore Lemma 3 is satisfied for n even as no other HI transform can reach a PAR of 2^{n-k+1}. By induction on n it follows that we can construct states $\boldsymbol{s}$ which satisfy the conditions of Lemma 3 for all n and $k \leq \frac{n}{2}$. ∎

The most-destructive series of measurements on $\boldsymbol{s}$ must be performed in the basis which is the HI transform, $\boldsymbol{s'}$, of $\boldsymbol{s}$ that achieves highest PAR (Lemma 2, Theorem 10). But, from Lemma 3, $\boldsymbol{s'} = \boldsymbol{s_c}$ and, for $k = \frac{n}{2}$, $\boldsymbol{s'} = \boldsymbol{s_{c^\perp}}$ also. The Theorem follows from Theorem 13. ∎

Corollary 3 *Quantum states from $\ell_{\mathbf{p}}$ which have optimum Linear Entanglement and optimum Stubborness of Entanglement are LU equivalent to binary linear codes with optimum Weight Hierarchy.*

7.3 Examples

We abbreviate tensor product expressions such as $\mathbf{H} \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I}$ to $HIHI$. Let $\boldsymbol{s_c}$ be the indicator for the code, $\mathbf{C}$, and LU-equivalent to $\boldsymbol{s}$. Let $\boldsymbol{s'_c}$ be the spectrum of $\boldsymbol{s_c}$ after application of $\prod_{i \in \mathbf{Q}} H(i)$, where $\mathbf{Q} \subset \{0, 1, \ldots, n-1\}$. Let $\boldsymbol{s} \in \ell_{\mathbf{p}}$. Let $s(\mathbf{x}) = (-1)^{x_3 x_0 + x_0 x_2 + x_2 x_1 + x_1 x_4 + x_4 x_0}$, i.e. $\boldsymbol{s} \in \ell_{\mathbf{p}}$. Then under $IIHHH$ we get $s_c(\mathbf{x}) = (x_0 + x_3 + 1)(x_0 + x_1 + x_2 + 1)(x_0 + x_1 + x_4 + 1)$ (Theorem 18), which is the binary indicator for the $[5, 2, 3]$ code, $\mathbf{C} = \{00000, 11010, 01101, 10111\}$. The action of the HI transform on $\boldsymbol{s_c}$ can be

computed from Theorem 6 and gives the following PARs for the spectrum, $\boldsymbol{s}'_{\boldsymbol{c}}$:

$x_0x_1 : x_2x_3x_4$	III	HII	IHI	HHI	IIH	HIH	IHH	HHH
II	8	4	4	2	4	2	2	1
HI	4	2	2	1	2	1	1	2
IH	4	2	2	1	2	4	1	2
HH	2	1	4	2	1	2	2	4

For instance, the 3rd row, second column shows that the spectrum after application of $IHHII$ on $\boldsymbol{s_c}$ has a PAR of 2, where $\mathbf{Q} = \{1, 2\}$. Similarly, the 2nd row and 6th column shows that the spectrum after application of $HIHIH$ on $\boldsymbol{s_c}$ has a PAR of 1, where $\mathbf{Q} = \{0, 2, 4\}$. The entry for $\mathbf{Q} = \{-\}$ is $2^{n-k} = 8$, the entry for $\mathbf{Q} = \{0, 1, 2, 3, 4\}$ is $2^k = 4$, and the entry for $\mathbf{Q} = \{2, 3, 4\}$ is 1, as this is the bipolar form, $\boldsymbol{s}$. From the table and by Theorem 7 we see that $\mathrm{PAR}_l = 8$, where the maximum PAR occurs at $\boldsymbol{s_c}$. Therefore, by Theorem 15, we can equate SE with Weight Hierarchy. We now determine the weight hierarchy for this $[5, 2, 3]$ code from a most-destructive PAR trajectory in the HI multispectra, using Theorem 8. Before measurement of $\boldsymbol{s_c}$ we have $\mathbf{Q} = \{0, 1, 2, 3, 4\}$ and, after $k = 2$ destructive measurements in the $\mathbf{C}$-basis we have $\mathbf{Q} = \{-\}$. A series of most-destructive series of measurements achieves a system with smallest entanglement order after the smallest number of measurements. Here is a PAR trajectory corresponding to a most-destructive series of measurements in the $\mathbf{C}$-basis where, without loss of generality, the measurement result is always 0. A 'freed' qubit is the result of redundant measurement. (For states from $\ell_{\mathbf{p}}$ the optimal measurement strategy is independent of measurement outcome. This is not generally true for other quantum states):

action	WHT($s_c(\mathbf{x})$)	measure qubit 2	free qubit 4	measure qubit 3	free qubit 1	free qubit 0
$\mathbf{Q}$	$\{0, 1, 2, 3, 4\}$	$\{0, 1, 3, 4\}$	$\{0, 1, 3\}$	$\{0, 1\}$	$\{0\}$	$\{-\}$
HI	$HHHHH$	$\rightarrow HHIHH$	$\rightarrow HHIHI$	$\rightarrow HHIII$	$\rightarrow HIIII$	$\rightarrow IIIII$
PAR	4	2	4	2	4	8
$\mathbf{C}$	00000 11010 01101 10111	00_00 11_10	00_0_ 11_1_	00---	0---	----
$m_{\mathbf{Q}}$	2	1	1	0	0	0
d_j	$d_2 = 5$		$d_1 = 3$			$d_0 = 0$

The PAR trajectory shown above gives the weight hierarchy, $d_2 = 5$, $d_1 = 3$, $d_0 = 0$, where d_1 is the Hamming Distance of $\mathbf{C}$, which, in this case, is also SE, where $\beta_i = d_i$.

In contrast, here is a least destructive set of measurements in the **C**-basis for the same example state, $s(\mathbf{x}) = (-1)^{x_3x_0+x_0x_2+x_2x_1+x_1x_4+x_4x_0}$.

action	WHT($s_c(\mathbf{x})$)	measure qubit 2	measure qubit 4	free qubit 3	free qubit 1	free qubit 0
Q	$\{0,1,2,3,4\}$	$\{0,2,3,4\}$	$\{0,3,4\}$	$\{3,4\}$	$\{4\}$	$\{-\}$
HI	$HHHHH$	$\rightarrow HIHHH$	$\rightarrow HIIHH$	$\rightarrow IIIHH$	$\rightarrow IIIIH$	$\rightarrow IIIII$
PAR	4	2	1	2	4	8
C	00000 11010 01101 10111	0_000 1_111	00__00	__00	__0	____
$m_{\mathbf{Q}}$	2	1	0	0	0	0

Fig 8 shows the two measurement scenarios described above, and Fig 9 shows their corresponding PAR trajectories. The weight hierarchy corresponds to the highest possible PAR trajectory. For more general quantum states, states requiring most measurements to destroy entanglement will have flattest LU multispectra.

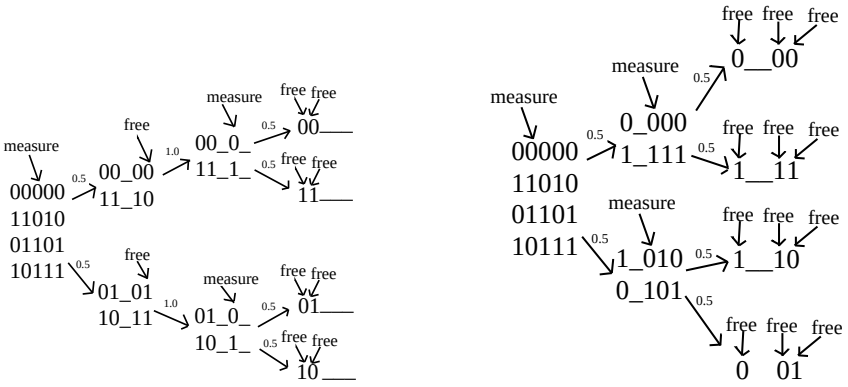

Fig. 8. Most-Destructive (lh) and Least-Destructive (rh) Measurement in the **C**-Basis

For quantum states outside $\ell_{\mathbf{P}}$ the most destructive set of measurements generally occurs outside the HI multispectra, but it is hoped that further research will lead to an identification of the spectral location of this most-destructive set of measurements. For more general states, the strategy becomes dependent on measurement outcomes. The entropy measure, $-p_0\log_2(p_0) - p_1\log_2(p_1)$, where $p_1 = (1-p_0)$, is then the natural generalisation of k measurements, as shown in Fig 10, giving rise to 'Entropic Weight Hierarchy'. (In this context, 'freed' qubits contribute zero to the entropy sum as $-p_0\log_2(p_0) - p_1\log_2(p_1)$ is zero if p_0 or $p_1 = 0$). Entropic Weight Hierarchies will be pursued in future papers.

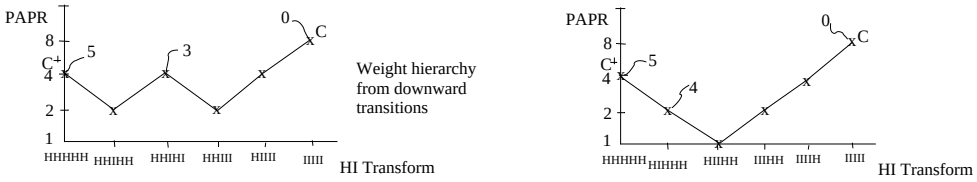

Fig. 9. PAR Trajectories for Most-Destructive (lh) and Least-Destructive (rh) **C**-Basis Measurements

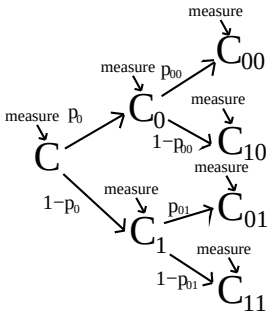

Fig. 10. A General Measurement Trajectory

8 Cryptographic Measures of Entanglement

8.1 An Upper Bound on PAR_l

We now consider properties of a bipolar sequence, $\boldsymbol{s}$, that are familiar to a cryptanalyst. Let $\boldsymbol{s_H}$ be the WHT of $\boldsymbol{s}$.

Definition 21 *The Nonlinear Order (N) of* $\boldsymbol{s}$ *is given by,*

$$N(\boldsymbol{s}) = n - \log_2(PAR(\boldsymbol{s_H}))$$

which, by Definition 11, is immediately a trivial upper bound on LE. For $\boldsymbol{s}$ linear, PAR $= 2^n$ and $N = 0$, and for $\boldsymbol{s}$ as nonlinear as possible, PAR $= 1$, and $N = n$. Nonlinear order is therefore a PAR measure in the WHT domain. A second measure commonly used is 'Correlation-Immunity Order' (CI$-t$) [35].

Definition 22 $\boldsymbol{s}$ *has Correlation-Immunity Order t (CI-t) if* $\boldsymbol{s_H}$ *is zero at all indeces with binary weight* > 0 *and* $\leq t$.

Note that, if $\boldsymbol{s_H}$ is an indicator for a code, $\mathbf{C_H}$, with minimum Hamming Distance $d = t+1$, then $\mathbf{s}$ has CI-t. [3]. The Nonlinear Order and Correlation-Immunity of a state from $\ell_{\mathbf{p}}$ provide an upper and lower bound on PAR_l.

Theorem 16 *Let* $s(\mathbf{x}) = (-1)^{p(\mathbf{x})} \in \ell_{\mathbf{p}}$ *and have nonlinear order,* N*. Then,*

$$n - N \leq \log_2(PAR_l(\boldsymbol{s})) \leq n - \frac{N}{2}$$

Furthermore, if the Correlation-Immunity of s *is CI-*t*,*

$$n - N \leq \log_2(PAR_l(\boldsymbol{s})) \leq max(n - t - 1 - \frac{N}{2}, n - N)$$

where $0 \leq t + 1 \leq n - N$*.*

Proof. The lower bound follows from Definitions 11 and 21. For the upper bound, the application of $H(i)$ on a member of $\ell_{\mathbf{p}}$ either decreases or increases PAR by a factor of 2 (Lemma 1). Therefore, $\mathrm{PAR}(\prod_{i\in\mathbf{T}} H(i)[\boldsymbol{s}])$ is maximised for some subset, $\mathbf{T}$, if $\exists\mathbf{T}'$ such that,

$$\mathrm{PAR}(\prod_{i\in\mathbf{T}'} H(i)[\boldsymbol{s}]) = 2^{|\mathbf{T}|-|\ |\mathbf{T}|-|\mathbf{T}'|\ |} \tag{2}$$

for at least one subset, $\mathbf{T}'$, of each size i, $0 \leq i \leq n$. But, for $|\mathbf{T}'| = n$, $\prod_{i\in\mathbf{T}'} H(i)[\boldsymbol{s}] = \boldsymbol{s_H}$, where $\boldsymbol{s_H} = \mathrm{WHT}(\boldsymbol{s})$. We have,

$$\mathrm{PAR}(\boldsymbol{s_H}) = 2^{n-N} \tag{3}$$

Combining (2) and (3) gives,

$$2^{2|\mathbf{T}|-n} = 2^{n-N} \Rightarrow \mathrm{PAR}_l(\boldsymbol{s}) \leq 2^{|\mathbf{T}|} = 2^{n-\frac{N}{2}}$$

thereby satisfying the first part of the Theorem. Now, if $\boldsymbol{s}$ is also known to be CI-t, then this is equivalent to saying that,

$$\mathrm{PAR}(\prod_{i\in\mathbf{T}'} H(i)[\boldsymbol{s}]) = 2^{n-N-t-1} \tag{4}$$

$\forall\mathbf{T}'$ where $|\mathbf{T}'| = n - t - 1$. Combining (2) and (4) gives,

$$\begin{array}{ll} \mathrm{PAR}_l(\boldsymbol{s}) \leq 2^{|\mathbf{T}|} = 2^{n-t-1-\frac{N}{2}}, & 0 \leq |\mathbf{T}| \leq n-t-1 \\ \mathrm{PAR}_l(\boldsymbol{s}) \leq 2^{n-N}, & n-t \leq |\mathbf{T}| \leq n \end{array}$$

The Theorem follows. ∎

[3] There is also an entropic version of CI-t, related to Fig 10, but we will investigate this more general parameter in future work. Entanglement measures discussed in this paper, such as spectral peak, spectral weight, and spectral entropy, can all be described by the 'Renyi Entropy' [36]

8.2 Example

$s(\mathbf{x}) = (-1)^{x_0x_1+x_0x_3+x_0x_5+x_1x_2+x_1x_4+x_2x_3+x_2x_5+x_3x_4+x_4x_5}$. Then $\boldsymbol{s} \in \ell_{\mathbf{p}}$ and is LU equivalent, via $IHIHIH$, to $\boldsymbol{s_c}$, which is the binary indicator for a $[6,3,2]$ binary linear ECC. As $k = 3$, no more than 3 measurements in the $\mathbf{C}$-basis are required to completely destroy the entanglement of $\boldsymbol{s}$ (Theorem 11). Moreover, $\mathrm{PAR}_l(\boldsymbol{s}) \geq 2^3$ (Theorem 3). Alternatively, we could examine $\boldsymbol{s}$ from a cryptographic angle. $\boldsymbol{s}$ is LU equivalent, via $HHHHHH$ (WHT) to $\boldsymbol{s_H}$, where $\boldsymbol{s_H} = (+000000000000000000 + 000000000000000000 + 000000000000000000-)$, where '+' means 1 and '−' means -1. $\boldsymbol{s_H}$ is an indicator for the $[6,2,3]$ ECC, $\mathbf{C_H} = \{000000, 010101, 101010, 111111\}$ (ignoring phase). So, in the 'WHT-basis', only 2 measurements are required to completely destroy the entanglement of $\boldsymbol{s}$, $\mathrm{PAR}_l(\boldsymbol{s}) \geq 2^4$ (nonlinear order is 2), and $\boldsymbol{s}$ is CI−1, (Hamming Distance is 2). We further examine PARs of all HI-multispectra of $\boldsymbol{s}$ to get the following table (**relative to $\boldsymbol{s_c}$**):

$x_0x_1x_2 : x_3x_4x_5$	III	HII	IHI	HHI	IIH	HIH	IHH	HHH
III	8	4	4	2	4	2	2	1
HII	4	2	8	4	2	1	4	2
IHI	4	2	2	1	2	1	1	2
HHI	2	1	4	2	1	2	2	4
IIH	4	2	8	4	2	1	4	2
HIH	8	4	16	8	4	2	8	4
IHH	2	1	4	2	1	2	2	4
HHH	4	2	8	4	2	4	4	8

There is only one PAR of 16 in the table, occuring at $HIHIHI$ relative to $\boldsymbol{s_c}$, which is $HHHHHH$ relative to $\boldsymbol{s}$. So, by Theorem 7, $\boldsymbol{s}$ has $\mathrm{PAR}_l = 16$ and, by Theorem 14, SE (measured in the WHT-basis) of $\beta_2 = 6, \beta_1 = 3, \beta_0 = 0$, as shown below.

action	$s(\mathbf{x})$	measure qubit 0	free qubit 2	free qubit 4	measure qubit 1	free qubit 3	free qubit 5
$\mathbf{Q}$	$\{0,1,2,3,4,5\}$	$\{1,2,3,4,5\}$	$\{1,3,4,5\}$	$\{1,3,5\}$	$\{3,5\}$	$\{5\}$	$\{-\}$
HI	$HHHHHH$	$\rightarrow$ $IHHHHH$	$\rightarrow$ $IHIHHH$	$\rightarrow$ $IHIHIH$	$\rightarrow$ $IIIHIH$	$\rightarrow$ $IIIIIH$	$\rightarrow$ $IIIIII$
PAR	1	2	4	8	4	8	16
$\mathbf{C}$	000000 010101 101010 111111	_00000 _10101	_0_000 _1_101	_0_0_0 _1_1_1	__0_0	___0	___
$m_{\mathbf{Q}}$	2	1	1	1	0	0	0
β_j	$\beta_2 = 6$			$\beta_1 = 3$			$\beta_0 = 0$

We find that $N = 2$ and $t = \beta_1 = 3$ so, by Theorem 16, it follows that

$$4 \leq \mathrm{PAR}_l \leq \max(1, 4)$$

which agrees exactly with computation, as $\mathrm{PAR}_l = 4$.

9 Non-Bipartite Quadratic Bipolar States

This paper has focussed on states from $\ell_{\mathbf{p}}$. In this section we take a preliminary look at quadratic bipolar states which do not have bipartite form. A 'Fully-Connected Quadratic' is a bipolar quantum state of the form,

$$s(\mathbf{x}) = (-1)^{\sum_{j=0}^{n-2} \sum_{i=j+1}^{n-1} x_j x_i}$$

Although these states appear to have a very low PAR of 2.0 under HI multi-spectra, their true PAR_l is 2^{n-1}. Fully-Connected States satisfy the following:

$$\mathbf{s}' = (10\ldots01) = \begin{pmatrix} w^7 & 0 \\ 0 & w \end{pmatrix}_f \prod_{j=0}^{n-1} \mathbf{NH}(j)\boldsymbol{s}$$

where $w = e^{\frac{2\pi i}{8}}$, $\mathbf{NH} = \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$ (the NegaHadamard Transform [20]), $i^2 = -1$, and $\mathbf{s}'$ is the binary indicator for the $[n, 1, n]$ Generalised GHZ state. $\left(\begin{smallmatrix} w^7 & 0 \\ 0 & w \end{smallmatrix}\right)_f$ acts on qubit f, where f is chosen arbitrarily from $\{0, 1, \ldots, n-1\}$. So Fully-Connected quadratic bipolar states are LU equivalent to $\ell_{\mathbf{p}}$. Moreover, as $k = 1$ for a Generalised GHZ state, only **one** measurement is necessary (of any qubit in the **NH**-basis) to completely disentangle the state. We illustrate the equivalence in Fig 11, where the rh-side shows the bipolar form of the GHZ state. [4] Next we present a quadratic bipolar state

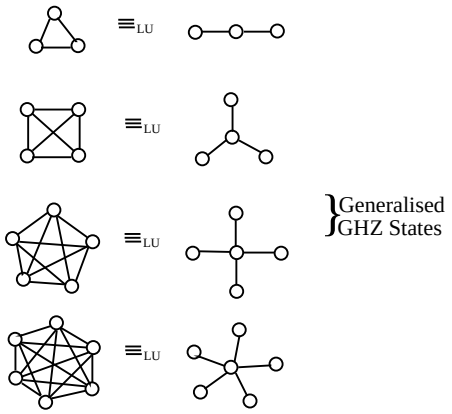

Fig. 11. Fully-Connected ↔ GHZ Equivalence

which is not LU equivalent to a code with binary probabilities. Let $s(\mathbf{x}) = (-1)^{x_0x_1+x_0x_2+x_0x_3+x_0x_4+x_1x_2+x_1x_4+x_2x_3+x_3x_4}$. By computation, $\mathrm{PAR}_l(\boldsymbol{s}) = 8.0$ (e.g. under the WHT), suggesting that only $\log_2(\frac{32}{8}) = 2$ measurements are necessary to completely disentangle the state, for instance, by measuring qubits 0 and 1 in the H-basis. The lh-side of Fig 12 is $s(\mathbf{x})$, and the rh-side is $s'(\mathbf{x}) = (-1)^{x_0x_1+x_0x_2+x_0x_4+x_1x_2+x_1x_3+x_1x_4}$, obtained from $s(\mathbf{x})$ by application of $H(0)H(1)$. Finally, our computations suggest that the quadratic bipolar state described by Fig 13 (or any of its 72 qubit permutations) has $\mathrm{PAR}_l = 4.486$, although at 6 qubits we are working at our computational limit). This PAR_l is very low - the lowest possible PAR_l for a 6-qubit state

[4] Fully-Connected quadratic bipolar states seem to be a generalisation of the 'maximal-connectedness' of [5] (see also [6])

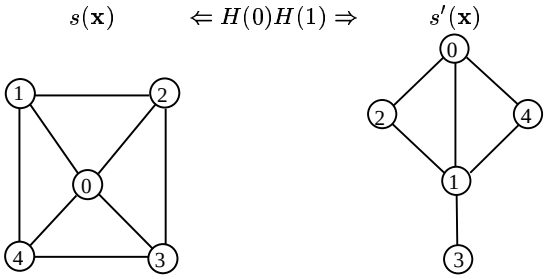

Fig. 12. LU-Equivalent Non-Bipartite Quadratic Bipolar States

from $\ell_{\mathbf{P}}$ is $2^3 = 8$. No other 6-qubit bipolar quadratics have PAR_l this low. No more than 4 measurements are required to completely destroy entanglement in the state. For instance, by measuring qubits 0,1,3,5 in the bipolar basis.

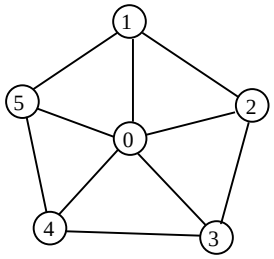

Fig. 13. Quadratic State with Conjectured $\mathrm{PAR}_l = 4.486$

10 Measurement-Driven Computation

Recent research [5,25] proposed entangled arrays of particles to perform Quantum Computation as in Fig 14, using the entangling primitive, $\frac{1}{2^{N/2}} \bigotimes_{a=0}^{N-1} (|0>_a \ \sigma_z^{(a+1)} + |1>_a)$, where $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The array holds a

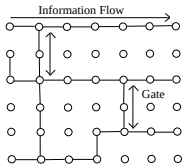

Fig. 14. Quadratically-Entangled Array

quadratic bipolar state. Moreover, this state is from $\ell_{\mathbf{p}}$ due to the bipartite form of a rectangular array. For such states, the Schmidt Measure of Entanglement, discussed in [25], corresponds to the LE discussed in this paper. The weight hierarchy of this paper further refines the 'Persistency of Entanglement' measure [5] to 'Stubborness of Entanglement'. Selective measurement drives computation on the array, exploiting inherent entanglement. We now give an example which was first described in [5], but we repeat it here. It is desired to teleport a quantum state from position i to position j. This can be achieved with certainty if we possess an entangled pair of qubits, x_i and x_j, which are in the state $x_i + x_j + 1$. By applying $H(i)$ we view this state as $(-1)^{x_i x_j}$. The problem is therefore to prepare the state $(-1)^{x_i x_j}$. In our array of qubits there is always a connective route from qubit i to qubit j for every i and j. We measure all extraneous variables to leave a quadratic line graph between x_i and x_j, ending in x_i and x_j. Therefore $s(\mathbf{x}) = (-1)^{x_i x_0 + x_0 x_1 + \ldots + x_{q-2} x_{q-1} + x_{q-1} x_j}$ and we wish to create $(-1)^{x_i x_j}$. Using Theorems 18 and 20, the application of $H(q-1)H(j)$ on $\boldsymbol{s}$ gives $s'(\mathbf{x}) = (-1)^{x_i x_0 + x_0 x_1 + \ldots + + x_{q-1} x_j + x_j x_{q-1}}$. So x_j and x_{q-1} swap in the expression, (although their physical position in the array remains unchanged). We now measure x_{q-1} to disentangle it. (This may produce the extra term x_j if x_{q-1} is measured as 1, but we can ignore this 'linear offset'). We repeat the above by applying $H(q-2)$ and $H(j)$, then measuring x_{q-2},...etc, until we are left with $(-1)^{x_i x_j}$. We can use our 'EPR pair', $(-1)^{x_i x_j}$, to teleport quantum information from position i to position j. This 'state preparation' is shown in Fig 15. This example is also useful in illustrating the 'danger' of entangle-

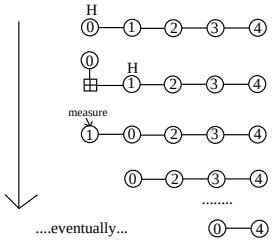

Fig. 15. Quantum State Preparation

ment with the environment. Consider the bipolar state $s(\mathbf{x}) = (-1)^{x_0 x_1 + x_1 x_e}$, where x_e is an environmental qubit. It may seem that qubits 0 and 1 are entangled independent of x_e but, as above, we can swap the positions of x_1 and x_e by applying IHH to get $s'(\mathbf{x}) = (-1)^{x_0 x_e + x_e x_1 = x_e(x_0 + x_1)}$. Thus $\rho_{\mathbf{e}}$, the mixed state of qubits 0 and 1, is separable, and there is no two-qubit entanglement between qubits 0 and 1.

11 Conclusion

This paper has approached Quantum Entanglement from a Coding and Sequence Theory perspective. We argue that optimum and near-optimum binary linear codes are quantum states with high entanglement. We show how to interpret coding and sequence parameters in a quantum context. In particular, we have identified sequence PAR, code dimension, weight hierarchy, nonlinear order, and correlation immunity, as having useful meanings in a quantum context. Most importantly, we have shown that, for quantum states which are equivalent under local unitary transform to indicators for binary linear error-correcting codes, the partial entanglement measures of Linear Entanglement and Stubbornness of Entanglement can be computed by only examining the multispectra arising from tensor products of 2×2 Walsh-Hadamard and Identity matrices. This allows us to consider entanglement of multiparticle states over many particles, in the same way that coding theorists consider properties of large blocklength codes. One implication of this is that current research into very long blocklength codes, using codes constructed on graphs, could be applied to the study of Quantum Entanglement [19], and vice versa. Local Unitary equivalence of quantum states allows us to look at classical coding and sequence design problems from new angles (literally) and, in future papers, we hope to use the idea of mixed-state entanglement to study the design and use of codes in certain channels. We also expect that Local Unitary equivalence will give us a new way of looking at cryptographic properties of certain sequences. This paper has concentrated on bipolar quadratic entanglement, in particular entanglement that can be described using binary linear block codes. Future work will consider higher-degree and higher-alphabet states, and we will need to search outside the HI multispectra to find the desired entanglement parameters.

12 Appendix: HI Multispectra and the Set, $\ell_{\mathbf{p}}$

12.1 The Action of $H(i)$

Lemma 4 *$A(-1)^B \Leftrightarrow A(-1)^{AB}$, where A and B are both binary functions.*

Lemma 5 *$\left(\prod_{i=0}^{F-1} a_i\right) + \left(\prod_{i=0}^{F-1}(a_i+1)\right) = \prod_{\substack{i=0 \\ i \neq j}}^{F-1}(a_j + a_i + 1)$, for some arbitrary $j \in \{0, 1, \ldots, F-1\}$.*

Definition 23 *We use the expression $x_k \in g(\mathbf{x})$ ($x_k \notin g(\mathbf{x})$) to indicate that $g(\mathbf{x})$ is (is not) a function of x_k.*

Definition 24 *For a certain x_i, let $\mathbf{R}$ be a subset of the integers such that $x_i \notin h(\mathbf{x})_k$, $\forall k \in \mathbf{R}$. Similarly, let $\mathbf{V}$ be a subset of the integers such that $x_i \in h(\mathbf{x})_k$, $\forall k \in \mathbf{V}$. Then $m(\mathbf{x}) = r(\mathbf{x})v(\mathbf{x})$, where $r(\mathbf{x}) = \prod_{k \in \mathbf{R}} h(\mathbf{x})_k$ and $v(\mathbf{x}) = \prod_{k \in \mathbf{V}} h(\mathbf{x})_k$, and where $r(\mathbf{x}) = 1$ if $\mathbf{R} = \emptyset$, and $v(\mathbf{x}) = 1$ if $\mathbf{V} = \emptyset$.*

Let $g(\mathbf{x})_{|x_i=t}$ mean the polynomial $g(\mathbf{x})$ evaluated at $x_i = t$. (In the quantum context this may be considered as the resultant state of g after a measurement of qubit i in the x_i basis which resulted in an observation of t for qubit i).

Definition 25 *$m_0 = m(\mathbf{x})_{|x_i=0}$, $m_1 = m(\mathbf{x})_{|x_i=1}$, where $i \in \{0, 1, \ldots, n-1\}$. We similarly define v_0, v_1, p_0, p_1 as being the evaluations of $v(\mathbf{x})$, $p(\mathbf{x})$, with x_i fixed to 0 and 1, respectively.*

Theorem 17 *Let $s = m(-1)^p$. Then the action of $H(i)$ on s is s', where,*

$$s' = m'(-1)^{p'} = r((v_0 + v_1) \oplus 2(v_0 v_1 (p_0 + p_1 + x_i + 1))) \times (-1)^{(v_0 v_1((p_0+1)(p_0+p_1+x_i)+p_0)+v_0 p_0+v_1(p_1+x_i))}$$

where $\oplus$ indicates conventional, non-modular addition.

Proof. $s = m(-1)^p = (1 + x_i)m_0(-1)^{p_0} + x_i m_1(-1)^{p_1}$, where m_0, m_1, p_0, p_1 are the result of fixing x_i. Applying $H(i)$ gives,

$$\begin{aligned} s' &= (1 + x_i)(m_0(-1)^{p_0} \oplus m_1(-1)^{p_1}) + x_i(m_0(-1)^{p_0} \ominus m_1(-1)^{p_1}) \\ &= (1 + x_i)(m_0(p_0 + 1) \oplus m_1(p_1 + 1) \ominus m_0 p_0 \ominus m_1 p_1) \\ &\quad + x_i(m_0(p_0 + 1) \ominus m_1(p_1 + 1) \ominus m_0 p_0 \oplus m_1 p_1) \end{aligned} \tag{5}$$

where $\oplus$ and $\ominus$ indicate non-modular addition and subtraction, respectively. We now use the identity,

$$A_0 \oplus A_1 \ominus B_0 \ominus B_1 = ((A_0 + A_1 + B_0 + B_1) \oplus 2(A_0 A_1 + B_0 B_1))(-1)^{B_0 B_1 + B_0 + B_1} \tag{6}$$

where $A_0, A_1, B_0, B_1 \in \{0, 1\}$. Applying (6) to (5) gives,

$$\begin{aligned} s' &= (1 + x_i)((m_0 + m_1) \oplus 2(m_0 m_1 (p_0 + p_1 + 1))(-1)^{m_0 m_1 p_0 p_1 + m_0 p_0 + m_1 p_1} \\ &\quad + x_i((m_0 + m_1) \oplus (m_0 m_1 (p_0 + p_1))(-1)^{m_0 m_1 p_0 (p_1+1) + m_0 p_0 + m_1 p_1 + m_1} \end{aligned} \tag{7}$$

Applying Lemma 4 to (7) enables us to factor out r from the exponent of (-1), and more generally reduce the exponent. Finally, we obtain Theorem 17 by observing that $p_0 p_1 = p_0(p_0 + p_1 + 1)$. ∎

We simplify Theorem 17 somewhat, as we are interested in binary APFs (i.e. where $m(\mathbf{x})$ and $p(\mathbf{x})$ are both binary).

Corollary 4 *$s'(\mathbf{x})$ of Theorem 17 is a binary APF iff either $v_0 + v_1 = 0$, or $v_0 v_1 = 0$. (Note that $(p_0 + p_1 + x_i + 1)$ can never be zero).*

Consider the case where $v_0 + v_1 = 0$.

Theorem 18 *If $v_0 + v_1 = 0$ then $x_i \notin m(\mathbf{x})$, and vice versa, and Theorem 17 reduces to,*

$$s' = m(c + x_i + 1)(-1)^{p_0}$$

where $c = p_0 + p_1$ is the sum of 'connection' terms, connected by multiplication to x_i in $p(\mathbf{x})$.

Proof. $v_0 + v_1 = 0$ iff $v_0 = v_1 = 1$. Theorem 18 follows by Lemma 4. ∎

Example: $H(2)$ acting on $s(\mathbf{x}) = (x_0 + x_3)(x_0 + x_1 + 1)(-1)^{x_0x_1x_3 + x_2x_3 + 1}$ gives $s'(\mathbf{x}) = (x_0 + x_3)(x_0 + x_1 + 1)(x_3 + x_2 + 1)(-1)^{x_0x_1x_3 + 1}$.
We now consider $v_0v_1 = 0$. Let $h_{0,k} = h(\mathbf{x})_{k_{|x_i=0}}$ and $h_{1,k} = h(\mathbf{x})_{k_{|x_i=1}}$.

Theorem 19 *$v_0v_1 = 0$ iff $m(\mathbf{x})$ contains at least one term $h(\mathbf{x})_k$ which has a linear dependence on x_i. In this case, Theorem 17 reduces to,*

$$s' = r(v_0 + v_1)(-1)^{p_0 + v_1(c + x_i)}$$

where $c = p_0 + p_1$.

Proof. If $h(\mathbf{x})_k$ is linear in x_i for some k, then $h_{1,k} = h_{0,k} + 1$, and $h_{1,k}h_{0,k} = 0$. $h_{0,k}$ is a factor of v_0, and $h_{1,k}$ is a factor of v_1, therefore $v_0v_1 = 0$. Theorem 17 initially reduces to $s' = r(v_0 + v_1)(-1)^{v_0p_0 + v_1(p_1 + x_i)}$. Therefore $s' = r(v_0 + v_1)(-1)^{(v_0 + v_1)p_0 + v_1(c + x_i)}$. Applying Lemma 4 gives Theorem 19. ∎

Example: $H(2)$ acting on $s(\mathbf{x}) = (x_2 + x_3 + 1)(x_0x_1 + 1)(x_0x_2)(-1)^{x_0x_3 + x_1x_2x_3}$ gives $s'(\mathbf{x}) = (x_0x_1 + 1)(x_0x_3)(-1)^{x_0x_1x_3 + x_0x_2x_3 + x_0x_3}$.

Theorem 20 *Let $m(\mathbf{x})$ be chosen so that $x_i \in m(\mathbf{x})$ and so that, if $x_i \in h(\mathbf{x})_k$, then $h(\mathbf{x})_k$ is linear in x_i. Then Theorem 17 reduces to a special case of Theorem 19, where,*

$$s' = r(v_0 + v_1)(-1)^{p_0 + h_{1,z}(c + x_i)}, \qquad z \in \mathbf{V}$$

where $c = p_0 + p_1$, z is chosen arbitrarily from $\mathbf{V}$, and,
$(v_0 + v_1) = \prod_{\substack{k \in \mathbf{V} \\ k \neq j}} (h_{0,j} + h_{0,k} + 1)$, $\quad j \in \mathbf{V}$ *, with j chosen arbitrarily from $\mathbf{V}$. We can make $j = z$ if we want to.*

Proof. $v_0 + v_1 = \left(\prod_{k \in \mathbf{V}} h_{0,k}\right) + \left(\prod_{k \in \mathbf{V}} h_{1,k}\right)$. But, for $h_k(\mathbf{x})$ linear in x_i, then $h_{1,k} = h_{0,k} + 1$. The expression for $v_0 + v_1$ in Theorem 20 follows by Lemma 5. $v_0 + v_1$ is only 1 when $h_{1,k} = 1\ \forall k$, or $h_{1,k} = 0\ \forall k$. Moreover, by definition, $v_1 = 1$ only when $h_{1,k} = 1\ \forall k$. We can therefore replace v_1 in the exponent of Theorem 20 by any function which is 1 for $h_{1,k} = 1\ \forall k$, and 0 for $h_{1,k} = 0\ \forall k$. We choose to replace v_1 with $h_{1,z}$, as described in Theorem 20, where v is arbitrarily chosen from $\mathbf{V}$. ∎

Example: $H(2)$ acting on $s(\mathbf{x}) = (x_1 + x_3)(x_0 + x_1 + x_2 + 1)(-1)^{x_0x_1x_2 + x_1x_3 + 1}$ gives $s'(\mathbf{x}) = (x_0 + x_2 + x_3)(-1)^{x_0x_2x_3 + x_0x_2 + x_1x_3 + x_1 + 1}$, where $h_{1,z}$ was chosen as $(x_3 + 1)$.

Proof. (**Theorem 1**) Let $s(\mathbf{x}) = m(\mathbf{x})(-1)^{p(\mathbf{x})}$ be a binary spectra APF. If $x_i \notin m(\mathbf{x})$, then Theorem 18 tells us that $\boldsymbol{s'}$ is a binary APF where $m(\mathbf{x})$ becomes $m'(\mathbf{x}) = m(\mathbf{x})(c + x_i + 1)$. Also $\deg(c) \leq 1$, so $m'(\mathbf{x})$ has a linear product decomposition and, from Theorem 18, $p(\mathbf{x})$ becomes p_0, where

$\deg(p_0) \leq 2$. Therefore, if $x_i \notin m(\mathbf{x})$ then $\boldsymbol{s}'$ has a binary spectra APF. Secondly, if $x_i \in m(\mathbf{x})$, then Theorem 19 tells us that $v_0 v_1 = 0$, as at least one $h(\mathbf{x})_k$ in $m(\mathbf{x})$ is linear in x_i. Theorem 20 tells us that, because all $h(\mathbf{x})_k$ are of degree one, then $\boldsymbol{s}'$ is a binary APF. This is because m' is still a product of degree one terms (i.e. $v_0 + v_1$ is a product of degree one terms). As both $h_{1,z}$ and $c + x_i$ are of degree one, then $\deg(p_0 + h_{1,z}(c + x_i)) \leq 2$. So, once again, $\boldsymbol{s}'$ has a binary spectra APF. ∎

Example: $H(0)$ acting on $s(\mathbf{x}) = (x_0 + x_1 + x_2 + x_3 + 1)(x_0 + x_1 + x_6)(x_0 + x_4 + 1)(-1)^{x_0 x_5}$ gives $s'(\mathbf{x}) = (x_2 + x_3 + x_6 + 1)(x_1 + x_2 + x_3 + x_4 + 1)(-1)^{(x_1+x_2+x_3)(x_0+x_5)}$, where we have chosen $h_{0,j} = (x_1 + x_2 + x_3 + 1)$ and $h_{1,z} = (x_1 + x_2 + x_3)$. We could alternatively choose, say, $h_{0,j} = (x_1 + x_2 + x_3 + 1)$ and $h_{1,z} = (x_4)$, in which case $s'(\mathbf{x}) = (x_2 + x_3 + x_6 + 1)(x_1 + x_2 + x_3 + x_4 + 1)(-1)^{(x_4)(x_0+x_5)}$. These two expressions for $\boldsymbol{s}'$ are equivalent.

Proof. (**Theorem 2**) Let $\boldsymbol{s} \in \ell_{\mathbf{P}}$. We wish to reduce the exponent of (-1) of $\boldsymbol{s}$ to zero by judicial applications of multiple $H(i)$. From Theorem 18, the action of $H(i)$ on $\boldsymbol{s}$ gives $s'(\mathbf{x})$, with exactly one linear term, $m'(\mathbf{x})$, namely $(c + x_i + 1)$. Let $x_j \in c$. From Theorem 20 the subsequent action of $H(j)$ on $s'(\mathbf{x})$ puts x_j back into the exponent of (-1), where it is 'reconnected' via multiplication to the term $h_{1,z}$. But in this case $h_{1,z}$ must be $(c + x_i + 1)_{|x_j=1}$, so the exponent must include the quadratic term $x_i x_j$. We have already used the actions $H(i)$ and $H(j)$, and no subsequent $H(k)$ actions, $k \neq j$, can remove this $x_i x_j$ term from the exponent. Thus, if x_i and x_j are connected via multiplication in $p(\mathbf{x})$, then i and j cannot both be part of the set $\mathbf{T_C}$ (or $\mathbf{T_C}^{\perp}$). Secondly, let the term $x_i x_0 + x_0 x_1 + \ldots + x_{q-1} x_j$ occur in $p(\mathbf{x})$ where, without loss of generality, we assume $i, j \notin \{0, 1, \ldots, q-1\}$. Let us apply $H(i)$ and $H(j)$ but not apply $H(0)$, $H(1)$, $\ldots$, $H(q-1)$. Then, from Theorem 18, $x_0 x_1 + \ldots + x_{q_2} x_{q-1}$ remains in the exponent of (-1). Elimination of these terms from the exponent is ensured if $q \leq 1$. The above two restrictions together imply that for each term of the form $x_i x_k + x_k x_j$ in $p(\mathbf{x})$, either $H(i)$ and $H(j)$ must be applied or $H(k)$ must be applied to ensure a final $s'(\mathbf{x}) = m'(\mathbf{x})$. This automatically implies a bipartite splitting, where $x_i, x_j \in \mathbf{T_C}$ and $x_k \in \mathbf{T_C}^{\perp}$. From Theorem 18 the application of $\prod_{i \in \mathbf{T_C}} H(i)$ to $\boldsymbol{s}$ must give a final p_0 equal to zero. To understand why these bipartite transformations reach all linear ECCs, we note that $s'(\mathbf{x}) = m'(\mathbf{x})$ must satisfy $s'(\mathbf{x}) = \prod_{i \in \mathbf{T_C}} (c_i + x_i + 1)$, where c_i is the linear sum of the variables connected by multiplication to x_i in $p(\mathbf{x})$. We could write each term $(c_i + x_i + 1)$ as a row of a parity check matrix, and in this way recover a conventional description for a linear ECC: Each $(c_i + x_i + 1)$ must be 1 for $s'(\mathbf{x})$ to be 1. This translates to each parity check row $(c_i + x_i)$ being equal to zero for a valid codeword. ∎

13 Appendix: PAR_l and Linear Entanglement (LE)

Proof. (**Theorem 7**) Let H_{e_i}, U_{e_i}, and I_{e_i} be the PARs of the resultant spectrum, $\boldsymbol{s}'$, after application of $H(e_i)$, $U(e_i)$, or $I(e_i)$, respectively, on $\boldsymbol{s}$, where $U(e_i)$ is any 2×2 unitary matrix acting on qubit x_{e_i}, and $I(e_i)$ is the 2×2 identity matrix acting on x_{e_i}. The maximum possible PAR scaling of $\boldsymbol{s}'$ relative to $\boldsymbol{s}$ after application of one 2×2 unitary matrix is by a factor of 2, either up or down. But from Lemma 1, when $\boldsymbol{s} \in \ell_{\mathbf{p}}$, the application of H_{e_i} on $\boldsymbol{s}'$ scales PAR by a factor of 2, upwards or downwards. We therefore conclude that,

$$\begin{array}{l} \text{either } U_{e_i} \geq H_{e_i} \quad \text{if } H_{e_i} = \frac{1}{2} I_{e_i} \\ \quad \text{or } U_{e_i} \leq H_{e_i} \quad \text{if } H_{e_i} = 2 I_{e_i} \end{array} \tag{8}$$

Moreover,

$$\frac{1}{2} I_{e_i} \leq U_{e_i} \leq 2 I_{e_i} \tag{9}$$

Combining (8) and (9) gives,

$$\begin{array}{l} \text{if } H_{e_i} = \frac{1}{2} I_{e_i} \text{ then } H_{e_i} \leq U_{e_i} \leq 2 I_{e_i} \\ \text{if } H_{e_i} = 2 I_{e_i} \text{ then } \frac{1}{2} I_{e_i} \leq U_{e_i} \leq H_{e_i} \end{array} \tag{10}$$

Let us write

$$U(e_i) = [U(e_i) H(e_i)]\, H(e_i) = V(e_i) H(e_i)$$

for some 2×2 unitary matrix, $V(e_i)$. Then,

$$\frac{1}{2} H_{e_i} \leq U_{e_i} \leq 2 H_{e_i} \tag{11}$$

Combining (10) and (11) gives,

$$\begin{array}{l} \text{if } H_{e_i} = \frac{1}{2} I_{e_i} \text{ then } H_{e_i} \leq U_{e_i} \leq I_{e_i} \\ \text{if } H_{e_i} = 2 I_{e_i} \text{ then } I_{e_i} \leq U_{e_i} \leq H_{e_i} \end{array} \tag{12}$$

Let any product of the H_{e_i}, U_{e_j}, and I_{e_k} define the resultant PAR after the application of the same tensor product of $H(e_i)$, $U(e_j)$, and $I(e_k)$. Then we can write,

$$\text{either } H_{e_j} U_{e_i} \leq U_{e_j} U_{e_i} \leq I_{e_j} U_{e_i}, \quad \text{or } I_{e_j} U_{e_i} \leq U_{e_j} U_{e_i} \leq H_{e_j} U_{e_i}, \quad i \neq j \tag{13}$$

Combining (12) and (13) guarantees that at least one of the four following conditions is satisfied:

$$\begin{array}{ll} \text{either} & H_{e_j} H_{e_i} \leq U_{e_j} U_{e_i} \leq I_{e_j} I_{e_i} \\ \text{or} & H_{e_j} I_{e_i} \leq U_{e_j} U_{e_i} \leq I_{e_j} H_{e_i} \\ \text{or} & I_{e_j} H_{e_i} \leq U_{e_j} U_{e_i} \leq H_{e_j} I_{e_i} \\ \text{or} & I_{e_j} I_{e_i} \leq U_{e_j} U_{e_i} \leq H_{e_j} H_{e_i} \end{array}$$

Continuing in this fashion, it follows that,

$$\prod_{i\in\mathbf{T}\backslash\mathbf{t}_*} H_{e_i} \prod_{j\in\mathbf{t}_*} I_{e_i} \leq \prod_{i\in\mathbf{T}} U_{e_i} \leq \prod_{i\in\mathbf{T}\backslash\mathbf{t}_*} I_{e_i} \prod_{j\in\mathbf{t}_*} H_{e_i}$$

for any integer set $\mathbf{T}$ where $\mathbf{t}_* \subset \mathbf{T}$. In words, for $\boldsymbol{s} \in \ell_{\mathbf{p}}$, the PAR of any LU transform of $\boldsymbol{s}$ is always upper and lower bounded by two points in the HI multispectra. ∎

14 Appendix: Weight Hierarchy and Stubborness of Entanglement (SE)

Proof. (**Theorem 8**) Decompose $\boldsymbol{s_c}$ as,

$$s_c(\mathbf{x}) = f_0(x_t = 0, g_0(\mathbf{x}\backslash x_t)) + f_1(x_t = 1, g_1(\mathbf{x}\backslash x_t))$$

for boolean functions f_i and g_i. From Lemma 1, let,

$$\gamma_t = \frac{\mathrm{PAR}(H(t)[\boldsymbol{s_c}])}{\mathrm{PAR}(\boldsymbol{s_c})} \in \{\frac{1}{2}, 2\}$$

Then $\gamma_t = 2$ iff $g_0 = g_1$, which is the same as saying that $\mathbf{C}$ has Hamming Distance $d = 1$. Otherwise $\gamma_t = \frac{1}{2}$. More generally we can find a subset, $\mathbf{x_w}$, of $\mathbf{x}$ such that, if $\mathbf{y_w} \subset \mathbf{x_w}$, then

$$\frac{\mathrm{PAR}(\prod_{t\in\mathbf{y_w}} H(t)[\boldsymbol{s_c}])}{\mathrm{PAR}(\boldsymbol{s_c})} = \begin{array}{ll} 2^{-|\mathbf{y_w}|}, & \mathbf{y_w} \neq \mathbf{x_w} \\ 2^{2-|\mathbf{y_w}|} = 2^{2-d_w}, & \mathbf{y_w} = \mathbf{x_w} \end{array}$$

where d_w is any member of the weight distribution of $\mathbf{C}$. Indeed, for a smallest-size non-empty subset, $\mathbf{x_w}$, we have $d_w = d_1 = d$, which is the Hamming Distance of $\mathbf{C}$. Similar arguments hold for the higher weights, $d_2, d_3, \ldots, d_k$ where, at each stage, a smallest unused non-empty subset, $\mathbf{x_{w_i}}$ is added. Let $\mathbf{Q} = \mathbf{y_{w_j}} \cup \bigcup_{i=0}^{j-1} \mathbf{x_{w_i}}$. After further manipulation we arrive at the Theorem. ∎

Proof. (**Theorem 9**) Let $\boldsymbol{s_c}$ be the binary indicator for a binary linear ECC. $\boldsymbol{s_c}$ takes one of two forms:

Form 1. $s_c(\mathbf{x}) = f_0(x_i = 0, g_0(\mathbf{x}\backslash x_i)) + f_1(x_i = 1, g_1(\mathbf{x}\backslash x_i))$
Form 2. $s_c(\mathbf{x}) = f_0(x_i = \gamma, g(\mathbf{x}\backslash x_i))$

where the f_i, g_i are boolean functions, and γ is fixed at 0 or 1. After measurement of x_i we obtain $s'_c(\mathbf{x}) = s_c(\mathbf{x})_{x_i=\gamma}$ which is,

- Destructive Measurement - when $\boldsymbol{s_c}$ is of Form 1.
- Redundant Measurement - when $\boldsymbol{s_c}$ is of Form 2.

The PAR relationships follow straightforwardly by Parseval's Theorem. Now, consider measuring $s'(\mathbf{x}) = H(i)[s_c(\mathbf{x})]$. If $\boldsymbol{s_c}$ is of Form 1. then $\boldsymbol{s'}$ is of Form 1. or 2. If $\boldsymbol{s_c}$ is of Form 2. then $\boldsymbol{s'}$ is of Form 1. In either case $\boldsymbol{s'}$ is still one of the same two forms and we have the same two measurement scenarios for $\boldsymbol{s'}$ as for $\boldsymbol{s_c}$. The proof follows recursively for the whole set, $\ell_{\mathbf{p}}$. ∎

References

1. Barnum H.,Linden N. (2001) Monotones and Invariants for Multi-Particle Quantum States. quant-ph/0103155 28 Mar
2. Bennett C.H.,Popescu S.,Rohrlich D.,Smolin J.A.,Thapliyal A.V. (1999) Exact and Asymptotic Measures of Multipartite Pure State Entanglement. quant-ph/9908073 24 Aug
3. Berrou C.,Glavieux A.,Thitimajshima P. (1993) Near Shannon-Limit Error-Correcting Coding and Decoding: Turbo-Codes. Proc. 1993 IEEE Int. Conf. on Communications (Geneva, Switzerland) 1064–1070,
4. Brassard G.,Mor T. (1999) Multi-Particle Entanglement via Two-Particle Entanglement. Lecture Notes in Computer Science QCQC'98,LNCS 1509, 1–9
5. Briegel H.J.,Raussendorf R. (2000) Persistent Entanglement in Arrays of Interacting Particles. quant-ph/0004051 v2 28 Aug
6. Brun T.A. (2001) A Quantum Web Page. quant-ph/0102046 8 Feb
7. Davis J.A.,Jedwab J. (1999) Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes. IEEE Trans. Inform. Theory **45.** No 7, 2397–2417, Nov
8. Dur W.,Cirac J.I. (1999) Classification of Multi-Qubit Mixed States: Separability and Distillability Properties. quant-ph/9911044 10 Nov
9. Dur W. (2000) Entanglement Molecules. quant-ph/0006105 22 Jun
10. Eisert J.,Briegel H.J. (2000) Quantification of Multi-Particle Entanglement. quant-ph/0007081 v2 29 Aug
11. Forney G.D. (2001) Codes on Graphs: Normal Realizations. IEEE Trans. Inform. Theory **47.** No 2, 520–548, Feb
12. Kschischang F.R.,Frey B.J.,Loeliger H-A. (2001) Factor Graphs and the Sum-Product Algorithm. IEEE Trans. Inform. Theory **47.** No 1, Jan
13. Fuchs C.A.,van de Graaf J. (1999) Cryptographic Distinguishability Measures for Quantum-Mechanical States. IEEE Trans. Inform. Theory **45.** No 4, 1216–1227, May
14. Grassl M.,Rotteler M.,Beth T. (1998) Computing Local Invariants of Quantum-Bit Systems. Physical Review A **58.** No 3, Sept
15. Horodecki M.,Horodecki P.,Horodecki R. (2000) Limits for Entanglement Measures. Physical Review Letters **84.** No 9, 28 Feb
16. Klove T.,Chen W. (1997) Bounds on the Weight Hierarchies of Linear Codes of Dimension 4 IEEE Trans. Inform. Theory **43.** No 6, 2047-2054
17. Linden N.,Popescu S. (1998) On Multi-Particle Entanglement Fortsch. Phys.. **46.** 567–578,
18. MacWilliams F.J.,Sloane N.J.A. (1977) **The Theory of Error-Correcting Codes** Amsterdam: North-Holland.
19. Parker M.G. (2000) Quantum Factor Graphs. 2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France Long version submitted to Annals of Telecom., available on /~matthew/mattweb.html or quant-ph/0010043, Sept 4–7
20. Parker M.G.,Tellambura C. (2000) Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions. Submitted to IEEE Trans. Inform. Theory, Preprint available on /~matthew/mattweb.html September
21. Paterson K.G.,Tarokh V. (2000) On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios. IEEE Trans. on Inform. Theory **46.** No 6, 1974–1987, Sept

22. Pittenger A.O.,Rubin M.H. (2001) Convexity and the Separability Problem of Quantum Mechanical Density Matrices. quant-ph/0103038 8 Mar
23. Plenio M.B.,Vedral V. (1998) Teleportation, Entanglement and Thermodynamics in the Quantum World. quant-ph/9804075 v2 22 May
24. Popescu S.,Rohrlich D. (1997) On the Measure of Entanglement for Pure States. Phys. Rev. A **56.** R3319
25. Raussendorf R.,Briegel H.J. (2000) Quantum Computing via Measurements Only. arXiv:quant-ph/0010033 7 Oct
26. Roychowdhury V.P.,Vatan F. (2001) Bounds for Weight Distribution of Weakly Self-Dual Codes. arXiv:math.CO/0104016 2 Apr
27. Schlingemann D.,Werner R.F. (2000) Quantum Error-Correcting Codes Associated with Graphs. quant-ph/0012111 20 Dec
28. Siegenthaler T. (1984) Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Alications. IEEE Trans. Inform. Theory **30.** No 5, 776–780
29. Thapliyal A.V. (1999) On Multipartite Pure-State Entanglement. quant-ph/9811091 v4 18 Feb
30. Vidal G. (1999) Entanglement Monotones. quant-ph/9807077 v2 25 Mar
31. Vidal G.,Werner R.F. (2001) A Computable Measure of Entanglement. quant-ph/0102117 22 Feb
32. Virmani S.,Plenio M.B. (2000) Ordering States with Entanglement Measures. quant-ph/9911119 v2 29 Feb
33. Wang X.,Sanders .C. (2001) Multipartite Entangled Coherent States. quant-ph/0104011 2 Apr
34. Wootters W.K. (2000) Entangled Chains. quant-ph/0001114 31 Jan
35. Xiao G.,Massey J.L. (1988) A Spectral Characterization of Correlation-Immune Combining Functions. IEEE Trans. Inform. Theory **34.** No 3, 569–571
36. Zyczkowski K.,Bengtsson I. (2001) Relativity of Pure States Entanglement. quant-ph/0103027 7 Mar