Generalised Bent Criteria for Boolean Functions (I)

Constanza Riera and Matthew G. Parker, *Member, IEEE,*

***Abstract*— Generalisations of the bent property of a Boolean function are presented, by proposing spectral analysis with respect to a well-chosen set of local unitary transforms. Quadratic Boolean functions are related to simple graphs and it is shown that the orbit generated by successive local complementations on a graph can be found within the transform spectra under investigation. The flat spectra of a quadratic Boolean function are related to modified versions of its associated adjacency matrix.**

***Index Terms*— additive codes, bent functions, Boolean functions, Clifford group, cryptography, graph states, graph theory, local complementation, Pauli group, quantum codes.**

I. Introduction

It is often desirable that a Boolean function, p, used for cryptographic applications, is highly *nonlinear*, where nonlinearity is determined by examining the spectrum of p with respect to (w.r.t.) the *Walsh Hadamard transform* (WHT), and where the nonlinearity is maximised for those functions that minimise the magnitude of the spectral coefficients. Define the Boolean function of n variables $p : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Define $\deg(p)$ to be the algebraic degree of p when expressed using algebraic normal form (ANF). Let the WHT be the $2^n \times 2^n$ unitary matrix $U = H \otimes H \ldots \otimes H = \prod_{i=0}^{n-1} H_i$, where the Walsh-Hadamard kernel is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

'$\otimes$' indicates the tensor product of matrices, and unitary means that $UU^\dagger = I$, where '$\dagger$' means transpose-conjugate and I is the $2^n \times 2^n$ identity matrix. We further define a vector $s \in (\mathbb{C}^2)^{\otimes n}$, $s = (s_{0\ldots00}, s_{0\ldots01}, s_{0\ldots11}, \ldots, s_{1\ldots11})^T$, such that $s_{\mathbf{i}} = (-1)^{p(\mathbf{i})}$, where $\mathbf{i} \in \mathbb{F}_2^n$. Then the Walsh-Hadamard spectrum of p is given by the matrix-vector product $P = Us$, where P is a vector of 2^n real spectral coefficients, $P_{\mathbf{k}}$, where $\mathbf{k} \in \mathbb{F}_2^n$.

The spectral coefficient, $P_{\mathbf{k}}$, with maximum magnitude tells us the minimum (Hamming) distance, d, of p to the set of affine Boolean functions, where $d = 2^{n-1} - 2^{\frac{n-2}{2}}|P_{\mathbf{k}}|$. By Parseval's theorem, the extremal case occurs when all $P_{\mathbf{k}}$ have equal magnitude, in which case p is said to have a *flat* WHT spectra, and is referred to as *bent*. If p is bent, then it is at maximum distance from the affine functions [33], which is a desirable cryptographic design goal. It is an open problem to classify all bent Boolean functions, although many results are known [20], [32], [13], [21], [31].

In this paper, we extend the concept of a bent Boolean function to some *generalised bent criteria* for a Boolean function, where we now require that p has flat spectra w.r.t. one or more transforms from a specified set of unitary transforms. The set of transforms we choose is not arbitrary but is motivated by a choice of local unitary transforms that are central to the structural analysis of pure n-qubit *stabilizer* quantum states. We here apply such transforms to a n-variable Boolean function, and examine the resultant spectra accordingly. In particular we apply all possible transforms formed from n-fold tensor products of the identity

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

the Walsh-Hadamard kernel, H, and the negahadamard kernel [35],

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

where $i^2 = -1$.

Definition 1: The $\{I, H, N\}^n$ *transform set* is the set of 3^n transforms of the form

$$\{I, H, N\}^n = \prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j,$$

where the sets $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ partition $\{0, \ldots, n-1\}$, and H_j, say, is short for $I \otimes I \otimes \ldots \otimes I \otimes H \otimes I \otimes \ldots \otimes I$, with H in the j^{th} position.

Each one of the 3^n transforms in $\{I, H, N\}^n$ acts on a Boolean function of n variables to produce a spectrum of 2^n spectral elements (complex numbers). By contrast, the WHT can be described as $\{H\}^n$, which is a transform set of size one, where the single resultant output spectrum comprises 2^n spectral elements.

Definition 2: Let $\mathcal{X}$ be an arbitrary set of $2^n \times 2^n$ unitary transform matrices. For each transform, $U \in \mathcal{X}$, we can, for a given vector, s, compute the set of spectral values $P = Us$. We will call the set $\{|P_{\mathbf{k}}|^2, \mathbf{k} \in \mathbb{F}_2^n\}_U$ the *multi-set of power spectral values* of the vector s w.r.t. U. Then $\{\{|P_{\mathbf{k}}|^2, \mathbf{k} \in \mathbb{F}_2^n\}_U, \quad \forall U \in \mathcal{X}\}$ is the set of multi-sets of power spectral values w.r.t. the transform set, $\mathcal{X}$.
In this paper we focus on such multi-sets and, in particular, the set of multi-sets w.r.t. the transform set $\{I, H, N\}^n$.

We note that there are other ways to generalise the concept of a bent function. For instance, in [59], Wolfmann identifies that the special subgroups of the Galois ring $\mathrm{GR}(4^n)$ are difference sets w.r.t. the additive subgroup of $\mathrm{GR}(4^n)$, and also constructs bent functions of a Maiorana-McFarland type over $\mathbb{Z}_4$, mapping these constructions back to bent binary functions via the Gray map. Alternatively, in [42], Poinsot

C. Riera was with the Depto. de Álgebra, Facultad de Matemáticas, Universidad Complutense de Madrid, Avda. Complutense s/n, 28040 Madrid, Spain. E-mail: criera@mat.ucm.es. Supported by the Spanish Government Grant AP2000-1365, and a Marie Curie Scholarship from the European Union.

C.Riera and M.G.Parker are with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: constanza,matthew@ii.uib.no. Supported by the University of Bergen and the Norwegian Research Council. Web: http://www.ii.uib.no/~matthew/

and Harari generalise, to any Abelian group of involutions, the translations associated with the autocorrelation dual of the Fourier transform and, in this way, generalise the notion of a bent Boolean function.

A. The Quantum Context

In this paper, $s = (-1)^p$ will be taken to represent both a complex vector $\in (\mathbb{C}^2)^n$, and a *pure* [1] quantum state of n qubits $\in (\mathbb{C}^2)^n$. More precisely, let $2^{\frac{-n}{2}} s \in (\mathbb{C}^2)^{\otimes n}$ represent the pure quantum state of n qubits such that a joint measurement of $2^{\frac{-n}{2}} s$ in the computational basis (i.e. the basis over which the state is defined) evaluates to $\mathbf{i}$ with probability $2^{-n}|(-1)^{p(\mathbf{i})}|^2 = 2^{-n}$. For brevity, for the rest of this paper, we often refer to the quantum state as s, although strict normalisation would require that we refer to that state as $2^{\frac{-n}{2}} s$.

Definition 3: A *product state*, s, of n qubits can be represented by a vector $s \in (\mathbb{C}^2)^{\otimes n}$, where $s = \bigotimes_{j=0}^{n-1}(a_j, b_j)$, $a_j, b_j \in \mathbb{C}$, i.e. s is wholly tensor factorisable.

Definition 4: The *Pauli group* is generated by the *Pauli matrices*, which are $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\sigma_y = i\sigma_x\sigma_z$, and is of size 16. The identity matrix, $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, is also classed as a Pauli matrix.

The Pauli matrices form a basis for the set of 2×2 unitary matrices, and therefore a basis for the set of local errors that could act on a qubit.

Definition 5: The *local Clifford group*, $\mathbf{C}_1$, with respect to the Pauli group, is defined to be the set of matrices that *normalise* [2] , to within a multiplicative factor of ± 1, the Pauli group. H and N are generators for $\mathbf{C}_1$, [11], [30], [55], where $|\mathbf{C}_1| = 192$.

The focus on I, H, and N, in this paper is motivated by their role as normalisers for the Pauli matrices.

The n-qubit local Clifford group, $\mathbf{C}_n$, can, similarly, be represented by the set of $2^n \times 2^n$ matrices that decompose into a tensor product of 2×2 unitary matrices from the local Clifford group, $\mathbf{C}_1$, where $|\mathbf{C}_n| = 192^n$. These matrices normalise tensor products of the Pauli matrices, and can be generated by the 2^n generators, $\{H, N\}^n$. Fortunately we are primarily interested in the multi-set of power spectral values w.r.t. each of the 192^n transforms. As is shown in section III, this allows us to focus on a subgroup, $\mathbf{T}_1$, of $\mathbf{C}_1$, where $\mathbf{T}_1 = \{I, \lambda, \lambda^2\}$,

$$\lambda = \frac{\omega^5}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix},$$

$\lambda^2 = \frac{\omega^3}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ -i & i \end{smallmatrix}\right)$, $\omega = e^{2\pi i/8}$, $|\mathbf{T}| = 3$, and λ is a generator for $\mathbf{T}_1$. One can obtain $\mathbf{T}_1$ by dividing $\mathbf{C}_1$ by another of its subgroups, namely the *diagonal group*, $\mathbf{D}_1$, where $|\mathbf{D}_1| = 64$. $\mathbf{D}_1$ comprises all members of $\mathbf{C}_1$ whose action on an arbitrary vector leaves its multi-set of power spectra values invariant. Any member of $\mathbf{C}_1$ can be expressed uniquely as $\Delta\lambda^j$, $0 \leq j < 3$, where $\Delta \in \mathbf{D}_1$. It follows that, for a given vector s and a given j, the two multi-sets of power spectral values of $\Delta\lambda^j s$ and $\Delta'\lambda^j s$ are identical, $\forall \Delta, \Delta' \in \mathbf{D}_1$. This allows us to choose to examine spectra w.r.t. $\{I, H, N\}^n$ instead of w.r.t. $\{I, \lambda, \lambda^2\}^n$, as they share the same set of 3^n multi-sets of power spectral values, where $N = \Delta\lambda$ and $H = \Delta'\lambda^2$, $\Delta, \Delta' \in \mathbf{D}_1$.

A *quantum error-correcting code (QECC)* of the stabilizer type is derived from the structure of the Pauli matrices. Let $\hat{s} = Es$, where $E \in \{I, \sigma_x, \sigma_z, \sigma_y\}^n$ is an error operator acting on s and formed from a tensor product of Pauli matrices [3]. Let $w(E)$ be the number of non-identity positions in the tensor product expansion of E. (For instance $w(I \otimes \sigma_x \otimes \sigma_y \otimes I) = 2$). Then we can think of s as an n-qubit QECC of dimension zero and distance d, i.e. an $[[n, 0, d]]$ QECC, if $s \cdot \hat{s} = 0$, $\forall E$ satisfying $w(E) < d$, where '$\cdot$' indicates the inner product of vectors. This is because, in such a case, the vectors s and $\hat{s}$ are mutually orthogonal and therefore perfectly distinguishable. For a fixed s, let $\mathcal{P}(s) = \{P \quad | \quad P = Us, \forall U \in \{I, H, N\}^n\}$. It can be shown that, if s is a $[[n, 0, d]]$ QECC w.r.t. the error set, E, then all pure states in the set $\mathcal{P}(s)$ are also $[[n, 0, d]]$ QECCs w.r.t. E [17]. In other words, the action of a transform from the set $\{I, H, N\}^n$ on the pure state, s, keeps invariant the distance properties of the state s, when viewed as a zero-dimensional QECC. Above, we refer to a single complex vector and its spectra wrt $\{I, H, N\}^n$ as instances of a specific zero-dimensional QECC w.r.t. E. More generally, the largest eigensubspace of all operators belonging to a specific abelian subgroup of the Pauli group is defined to be a *stabilizer QECC*. In this paper we are concerned only with the spectra of single complex vectors of length 2^n, i.e. where the stabilizer QECC is a one-dimensional eigensubspace.

One reason why we choose, in this paper, to use the transform set, $\{I, H, N\}^n$, instead of the set, $\{I, \lambda, \lambda^2\}^n$, is to highlight that the local Clifford group contains *multivariate discrete Fourier transforms*, as represented by $\{H, N\}^n$. This Fourier interpretation then helps us to establish a link with a generalised form of linear approximation in the context of classical cryptanalysis [40].

Recently, certain pure quantum states have created significant interest due to their suitability as components in a potentially robust, distributed quantum computer. Such configurations are referred to as *cluster states* [43], [6], [44] or *graph states* [51], [55], [28]. Graph states are locally equivalent to the subclass of stabilizer QECCs which have dimension zero [51], [24], [26], and are defined to be the unique eigenvectors (to within global phase) of a particular subclass of abelian subgroups of the Pauli group that can be characterised using a graph (see (23) of appendix I). Proposition 2.14 of [55] further shows that all graph states are equivalent under local unitaries to quadratic forms expressed as $(-1)^p$, where p is a quadratic Boolean function. We further show (Appendix I,

[1] A *pure state* can be written as a normalised complex vector, s. A *mixed state* is a statistical sum of normalised complex vectors.

[2] For two groups, G and H, G *normalises* H iff $ghg^{-1} \in H$, $\forall g \in G$, $\forall h \in H$.

[3] As the Pauli matrices form a basis for the set of 2×2 unitary matrices, general quantum errors can always be represented by the error operator $\mathcal{E} = \sum_j \rho_j E_j$, where each E_j is some tensor product of Pauli matrices, and $\sum_j |\rho_j|^2 = 1$. The first stage of the error-correction process projects (e.g. via suitable measurement of an ancillary system) the error $\mathcal{E}$ onto an error E_j with probability $|\rho_j|^2$. The second stage of the error-correction then only needs to deal with an error of the form E_j [53].

theorem 11) that no graph state is equivalent to a state $(-1)^p$ if the algebraic degree of p is other than 2. Thus the study of zero-dimensional stabilizer QECCs, or graph states, can be cast as a study of quadratic Boolean functions, as is done in this paper. A preliminary study of the class of pure quantum states that can be represented by quadratic Boolean functions in this way was undertaken in [38].

In this paper we examine the spectra of graph states, s, w.r.t. $\{I,H,N\}^n$, characterise those transforms $U \in \{I,H,N\}^n$ that yield flat spectra, and present preliminary results on those states represented by Boolean functions of degree greater than two. In part II [45] we count the number of spectra which are flat, taken over all 3^n transforms of s w.r.t. $\{I,H,N\}^n$. As is shown in [45], the number of flat spectra w.r.t. $\{I,H,N\}^n$ for pure states of the form $s=(-1)^p$ is strongly dependent on the algebraic degree of p, with the enumeration typically maximised if $\deg(p)=2$. [45] also shows experimentally that those graph states which represent $[[n,0,d]]$ QECCs with highest distance, d, also have the most flat spectra w.r.t. $\{I,H,N\}^n$.

B. The Graphical Context

Quantum graph arrays, called *cluster states*, were proposed in [43], [6]. These clusters form the 'substrate' for *measurement-driven* quantum computation [44]. A type of measurement-driven quantum computation on a *quantum factor graph* was also proposed in [37], where the graphs under consideration are locally-equivalent to bipartite cluster states. The graphical description of certain pure quantum states was also investigated in [38], where observations were made about a *local unitary (LU) equivalence* between their graphs. These graphs were interpreted as quadratic Boolean functions and it was noted that bipartite graphs are LU-equivalent to indicators for binary linear error-correcting codes. [51] identified a graphical description for *stabilizer* quantum error-correcting codes (QECCs), and such descriptions were also developed in [24], [25], and in [26]. For QECCs of dimension zero, the associated graphs are *graph states* [28].

LU-equivalence for graph states can be characterised, graphically, via *local complementation* (LC) on graphs, which was proven, in the context of QECCs, in [24], where LC was called *vertex-neighbour-complement* (VNC), and also, independently, by [28], and by [56]. Local complementation was defined by Fraysseix [23] and used by Bouchet [7], [8], [9] in the context of *isotropic systems*, and also used by Fon-der-Flaas [22]. By applying LC to a graph G we obtain a graph G', in which case we say that G and G' are *LC-equivalent*. Moreover, the set of all LC-equivalent graphs form an *LC-orbit*. LC-equivalence translates into the natural equivalence between $\mathbb{F}_4$ additive codes that keeps the weight distribution of the code invariant [11], [15], [16], [19]. There has been recent renewed interest in Bouchet's work motivated, in part, by the application of *interlace graphs* to the reconstruction of DNA strings [3], [2]. In particular, various *interlace polynomials* have been defined [2], [1], [4], [5] which mirror some of the quadratic results of part II of this paper [45]. We investigate these links further in [46], [50].

C. The Boolean Context

For γ a r^{th} complex root of 1, we can approximate, by appropriate normalisation, any vector $s \in (\mathbb{C}^2)^{\otimes n}$, by

$$s(\mathbf{x}) \simeq m(\mathbf{x})\gamma^{p(\mathbf{x})}, \tag{1}$$

for some sufficiently large choice of integer, r, where $m : \mathbb{F}_2^n \to \mathbb{Z}$, $p : \mathbb{F}_2^n \to \mathbb{Z}_r$, and $\mathbf{x} \in \mathbb{F}_2^n$, such that the $\mathbf{j}^{th}$ element of s, $s_{\mathbf{j}} = m(\mathbf{j})\gamma^{p(\mathbf{j})}$, where $\mathbf{j} \in \mathbb{F}_2^n$. Once again we omit normalisation - when viewed as a pure quantum state of n qubits, the reader should remember that s should actually satisfy $\sum_{\mathbf{i}} |m(\mathbf{i})\gamma^{p(\mathbf{i})}|^2 = 1$.

Definition 6: For γ a r^{th} complex root of 1, a *generalised affine function* of n Boolean variables, $u(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{C}$, is a product state given by

$$u(\mathbf{x}) = m(\mathbf{x})\gamma^{p(\mathbf{x})},$$

where $m : \mathbb{F}_2^n \to \mathbb{Z}$ is a generalised Boolean function of the form $m = \prod_{j\in K}(e_j x_j + c_j)$, $e_j, c_j \in \mathbb{Z}, K \subset \mathbb{Z}_n$, and $p : \mathbb{F}_2^n \to \mathbb{Z}_r$ is an affine generalised Boolean function.

Remark: In this paper we consider that m is a generalised Boolean function of the form $m : \mathbb{F}_2^n \to \mathbb{Z}_t$, for some positive integer, t, but by abuse of notation, interpret its outputs, elements $0,1,\ldots,t-1$, as the integers $0,1,\ldots,t-1$, respectively.

Observation: A row of $\bigotimes_{j=0}^{n-1} U_j$, where the U_j are 2×2 unitary matrices, can always be written as a product state, and a subset of generalised affine functions are described by the rows of $\{I,H,N\}^n$, where $m(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{F}_2$ is a minterm, and $p(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{Z}_4$ is an affine function.

In this paper our aim is to introduce new generalised bent criteria which try to answer the question:

which Boolean functions are as far away as possible from the subset of generalised affine functions as defined by the rows of $\{I,H,N\}^n$?

Spectral analysis w.r.t. $\{I,H,N\}^n$ also has application to the cryptanalysis of classical cryptographic systems. In particular, for a block cipher it models attack scenarios where one has full read/write access to a subset of plaintext bits and access to all ciphertext bits [17]. The analysis of spectra w.r.t. $\{I,H,N\}^n$ tells us more about p than is provided by the spectrum w.r.t. the WHT; for instance, identifying relatively high generalised linear biases for p [40]. For example, [40] tells us that the component functions of the S-box used in the Advanced Encryption Standard (AES) have a nonlinearity of 112 w.r.t $\{H\}^n$, but this is reduced to an *effective nonlinearity* [4] of 97.93 w.r.t. $\{H,N\}^n$ and 94.06 w.r.t. both $\{I,H\}^n$ and $\{I,H,N\}^n$. By extension, if significantly increased biases can be found over 'well-designed' S-boxes, then they should also exist across any 'well-designed' block cipher (such as AES). However the application of standard linear and differential cryptanalysis to a block cipher w.r.t. any tensor transform

[4][40]. The effective nonlinearity of $p(\mathbf{x})$ satisfies $\gamma(p) = 2^{\frac{n}{2}-1}(2^{\frac{n}{2}} - \sqrt{\mathrm{PAR}_{\mathcal{U}}(p)})$, where the *peak-to-average power ratio* $\mathrm{PAR}_{\mathcal{U}}(p) = 2^{-n}\max(|P_k|^2 \mid P = U(-1)^p, \forall U \in \{\mathcal{U}\})$, where the PAR is taken w.r.t. a specified finite or infinite set, $\mathcal{U}$, of unitary transforms.

containing N will result in characteristics which are key-dependent in their location if the round key is XOR'ed into the cipher, as is typically done, and this will make high-bias characteristics hard to find. Such key-dependency does not occur if we restrict ourselves to biases w.r.t. $\{I, H\}^n$ and, as observed above, the effective nonlinearity of the S-box used in AES is already reduced to 94.06 w.r.t. $\{I, H\}^n$.

The classification of bent quadratic (degree-two) Boolean functions is well-known [32], and is facilitated because the bent criteria is an invariant of affine transformation of the input variables. However, the classification of generalised bent criteria for a quadratic Boolean function w.r.t. the $\{I, H, N\}^n$ transform set is new, and the generalised bent criteria are not, in general, invariant to affine transformation of the inputs. This paper characterises these generalised bent criteria for both quadratic and more general Boolean functions. We associate a quadratic Boolean function with an undirected graph, which allows us to interpret spectral flatness with respect to $\{I, H, N\}^n$ as a *maximum rank* property of suitably modified adjacency matrices. We interpret LC as an operation on quadratic Boolean functions, and as an operation on the associated adjacency matrix, and we also identify the LC-orbit with a subset of the flat spectra w.r.t. $\{I, H, N\}^n$. The spectra w.r.t. $\{I, H, N\}^n$ motivate us to examine the properties of the WHT of all $\mathbb{Z}_4$-linear offsets of Boolean functions, the WHT of all subspaces of Boolean functions that can be obtained by fixing a subset of the variables, the WHT of all $\mathbb{Z}_4$-linear offsets of all of the above subspace Boolean functions, the WHT of each member of the LC-orbit, and the distance of Boolean functions to all $\mathbb{Z}_4$-linear functions. We are able to characterise and analyse the criteria for quadratic Boolean functions by considering properties of the adjacency matrix for the associated graph.

D. Paper Overview

For the interested reader, Appendix I reviews the graph state and its intepretations in the literature. In Section II we review LC as an operation on an undirected graph [24], [25], and provide an algorithm for LC in terms of the adjacency matrix of the graph. In Section III we show that the LC-orbit of a quadratic Boolean function lies within the set of transform spectra w.r.t. tensor products of the 2×2 matrices, I, $\sqrt{-i\sigma_x}$, and $\sqrt{\sigma_x\sigma_z}$, where σ_x and σ_z are Pauli matrices, i.e. w.r.t. $\{I, \sqrt{-i\sigma_x}, \sqrt{\sigma_x\sigma_z}\}^n$. We also show, equivalently, that the orbit lies within the spectra w.r.t. $\{I, \lambda, \lambda^2\}^n$, and also lies within the spectra w.r.t. $\{I, H, N\}^n$. We show that doing LC to vertex x_v can be realised, to within affine offset, by the application of the negahadamard kernel, N, to position v (and the identity matrix to all other positions) of the bipolar vector $(-1)^{p(\mathbf{x})}$, i.e.

$$\begin{aligned}\omega^{4p'(\mathbf{x})+a(\mathbf{x})} &= \omega^{a(\mathbf{x})}(-1)^{p'(\mathbf{x})} = U_v(-1)^{p(\mathbf{x})} \\ &= I \otimes \cdots \otimes I \otimes N \otimes I \otimes \cdots \otimes I \ (-1)^{p(\mathbf{x})} \ ,\end{aligned}$$

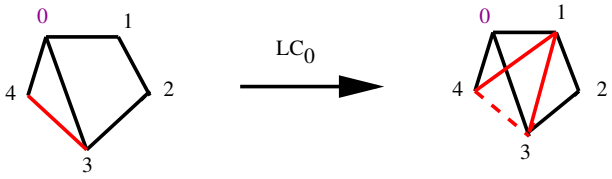
where $p(\mathbf{x})$ and $p'(\mathbf{x})$ are quadratic Boolean functions, $p'(\mathbf{x})$ is obtained by applying LC to variable x_v of $p(\mathbf{x})$, $\omega = e^{2\pi i/8}$, and $a(\mathbf{x})$ is an affine offset over $\mathbb{Z}_8$. In Appendix II we identify spectral symmetries that hold for $p(\mathbf{x})$ of any degree w.r.t. $\{I, H, N\}^n$. In Section IV, we introduce the concepts of *bent*$_4$, *I-bent*, *I-bent*$_4$, and *LC-bent* Boolean functions, and show how, for quadratic Boolean functions, these properties can be evaluated by examining the ranks of suitably modified versions of the adjacency matrix.

II. Local Complementation (LC)

Given an undirected graph G with adjacency matrix Γ, define its *complement* to be the graph with adjacency matrix $\Gamma + I + \mathbf{1}$ (mod 2), where I is the identity matrix and $\mathbf{1}$ is the all-ones matrix. Let $\mathcal{N}(v)$ be the set of neighbours of vertex, v, in the graph, G, i.e. the set of vertices connected to v in G.

Definition 7: [7] The action of *local complementation* (LC) on a graph G at vertex v is the graph transformation obtained by replacing the subgraph $G[\mathcal{N}(v)]$ by its complement.

Example: For LC with $v = 0$,



By Glynn (see [24]), a self-dual quantum code $[[n, 0, d]]$ corresponds to a graph on n vertices, which may be assumed to be connected if the code is indecomposable. It is shown there that two graphs G and G' give equivalent self-dual quantum codes iff G and G' are LC-equivalent.

[7], [8], [9], [14] describe the relation between local complementation and *isotropic systems*. A suitably-specified isotropic system has graph presentations G and G' iff G and G' are LC-equivalent.

A. LC in terms of the adjacency matrix

Let $p(\mathbf{x}) : F_2^n \to F_2$ be a (homogeneous) quadratic Boolean function, defined by,

$$p(\mathbf{x}) = \sum_{0 \le i < j \le n-1} a_{ij} x^i x^j \ .$$

Express $p(\mathbf{x})$ by the adjacency matrix, Γ, of its associated graph, G, Γ, such that $\Gamma(i,j) = \Gamma(j,i) = a_{ij}$, $i < j$, $\Gamma(i,i) = 0$. W.l.o.g. the LC operation on vertex 0 of G changes Γ to Γ_0, where

$$\Gamma_0 = \begin{pmatrix} 0 & a_{01} & \dots & a_{0n} \\ a_{01} & 0 & \dots & a_{1n} + a_{01}a_{0,n-1} \\ a_{02} & a_{12} + a_{01}a_{02} & \dots & a_{2n} + a_{02}a_{0,n-1} \\ a_{03} & a_{13} + a_{01}a_{03} & \dots & a_{3n} + a_{03}a_{0,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,n-1} & a_{1,n-1} + a_{01}a_{0,n-1} & \dots & 0 \end{pmatrix}.$$

The general algorithm, mod 2, is

$$\begin{cases} \Gamma_v(i,j) = \Gamma(i,j) + \Gamma(v,i) * \Gamma(v,j), \ i < j \\ \Gamma_v(i,i) = 0 \ \ \forall i \\ \Gamma_v(j,i) = \Gamma_v(i,j), \quad i > j \end{cases}$$

where Γ_v is the adjacency matrix of the function after doing LC to vertex x_v.

III. Local Complementation (LC) and Local Unitary (LU) Equivalence

[28] states that LC-Equivalence (and therefore local unitary (LU) equivalence [5]) of graph states can be obtained via successive transformations of the form,

$$U_v(G) = (-i\sigma_x^{(v)})^{1/2} \prod_{b\in\mathcal{N}_v} (i\sigma_z^{(b)})^{1/2} \ , \qquad (2)$$

where $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ are Pauli matrices, the superscript (v) in their notation indicates that the Pauli matrix acts on qubit v (with I acting on all other qubits) [6] , and $\mathcal{N}_v$ comprises the neighbours of qubit v in the graphical representation. Define matrices x and z as follows:

$$x = \pm(-i\sigma_x)^{1/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & i \\ i & -1 \end{pmatrix}$$

and

$$z = \pm(i\sigma_z)^{1/2} = \begin{pmatrix} w & 0 \\ 0 & w^3 \end{pmatrix} \ ,$$

where $w = e^{2\pi i/8}$. Observe that x and z are generators of the local Clifford group, $\mathbf{C}_1$. Furthermore, let $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

In this section we show that the LC-orbit of an n-vertex graph, G, is contained within the flat spectra of $(-1)^p$ w.r.t. $\{I, x, xz\}^n$, where G is the graph associated to p. We then show that, as we are only interested in the multi-set of power spectral values w.r.t. each member of $\{I, x, xz\}^n$, then one can replace $\{I, x, xz\}^n$ by $\{I, \lambda, \lambda^2\}^n$, and also by $\{I, H, N\}^n$. Finally, we show that successive application of N to $(-1)^p$ generates the LC-orbit as a subset of the complete $\{I, H, N\}^n$ spectra.

A. The Diagonal Group

Definition 8: $\mathbf{D}_1$ is the subgroup of the local Clifford group, $\mathbf{C}_1$, , and $\mathbf{D}_1$ is generated by ω, σ_x, and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$, where $\omega = e^{2\pi i/8}$ and $|\mathbf{D}_1| = 64$. Let $\mathbf{D}$ be the infinite set of 2×2 matrices such that every element in the set is either of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ or of the form $\left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right)$, where $a, b \in \mathbb{C}, |a| = |b| = 1$.

We call $\mathbf{D}$ the *diagonal set* and $\mathbf{D}_1$ the *diagonal group*, where $\mathbf{D}_1 \subset \mathbf{D}$. $\mathbf{D}_1$ is also a *Sylow-2 subgroup* of the local Clifford group [7] .

Following (1), let $s = m(\mathbf{x})\gamma^{p(\mathbf{x})}$. Let $\Delta \in \mathbf{D}_1$, and $\Delta_j = I \otimes \cdots \otimes I \otimes \Delta \otimes I \cdots \otimes I$, with Δ at position j of the tensor product. W.lo.g, let $j = 0$, and let $s' = \Delta_0 s = m'(\mathbf{x})\mu^{p'(\mathbf{x})}$, where μ is some complex root of one.

Lemma 1: The multi-set of 2^n magnitude values $\{|s'_{0\ldots00}|, |s'_{0\ldots01}|, \ldots |s'_{1\ldots11}|\}$ is equal to the multi-set of 2^n magnitude values $\{|s_{0\ldots00}|, |s_{0\ldots01}|, \ldots |s_{1\ldots11}|\}$.

Lemma 2: Let $p(\mathbf{x})$ be a function of degree d. Then $p'(\mathbf{x})$ differs from $p(\mathbf{x})$ by terms of degree $< d$.

Remark: In particular, if p is quadratic then p' only differs from p by affine terms.

Proof: (of lemmas 1 and 2) Let $\Delta = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in \mathbf{D}$. To within sufficient precision let $a = e^{2\pi i\alpha/\xi}$ and $b = e^{2\pi i\beta/\xi}$, with ξ, α and β integers. Then,

$$\begin{aligned} \Delta_0 m(\mathbf{x})\gamma^{p(\mathbf{x})} &= \Delta_0 \begin{pmatrix} m_0(\mathbf{x})\gamma^{p_0(\mathbf{x})} \\ m_1(\mathbf{x})\gamma^{p_1(\mathbf{x})} \end{pmatrix} \\ &= \begin{pmatrix} m_0(\mathbf{x})e^{2\pi i\alpha/\xi}\gamma^{p_0(\mathbf{x})} \\ m_1(\mathbf{x})e^{2\pi i\beta/\xi}\gamma^{p_1(\mathbf{x})} \end{pmatrix} = m(\mathbf{x})\mu^{p'(\mathbf{x})}, \end{aligned} \qquad (3)$$

where $\mu = e^{2\pi i/u}$, $u = \text{lcm}(\xi, r)$, 'lcm' means 'least common multiple', and $p'(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{Z}_u$ satisfies

$$p'(\mathbf{x}) = u\left(\frac{p(\mathbf{x})}{r} + \frac{\alpha + x_0(\beta - \alpha)}{\xi}\right). \qquad (4)$$

Let now $\Delta = \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right)$. Then,

$$\begin{aligned} \Delta_0 m(\mathbf{x})\mu^{p(\mathbf{x})} &= \begin{pmatrix} m_1(\mathbf{x})e^{2\pi i\beta/\xi}(-1)^{p_1(\mathbf{x})} \\ m_0(\mathbf{x})e^{2\pi i\alpha/\xi}(-1)^{p_0(\mathbf{x})} \end{pmatrix} \\ &= m(\mathbf{x} + (1, 0\ldots, 0))\mu^{p'(\mathbf{x})}, \end{aligned} \qquad (5)$$

where

$$p'(\mathbf{x}) = u\left(\frac{p(\mathbf{x} + (1, 0\ldots, 0))}{r} + \frac{\beta + x_0(\alpha - \beta)}{\xi}\right). \qquad (6)$$

Lemma 1 is proved by equations (3) and (5), as these equations demonstrate that the action of Δ_0 leaves $m(\mathbf{x})$ unchanged or permutes its outputs. Lemma 2 is proved from equations (4) and (6) as the only extra terms introduced are linear or constant or, via $p(\mathbf{x} + (1, 0\ldots, 0))$, terms of degree $< \deg(p(\mathbf{x}))$. ■

Remark: Observe that we have proved w.r.t. $\mathbf{D}$, but trivially the proof also holds w.r.t. $\mathbf{D}_1$, as $\mathbf{D}_1 \subset \mathbf{D}$.

Example: Let $m(\mathbf{x}) = 1$ and let $p : \mathbb{F}_2^2 \to \mathbb{Z}_4$, $p(\mathbf{x}) = 2x_0x_1 + x_0 + 1(\text{ mod } 4)$. Then $p(0,0) = 1$, $p(1,0) = 2$, $p(0,1) = 1$ and $p(1,1) = 0$, so $i^{p(x)} = \begin{pmatrix} i \\ -1 \\ i \\ 1 \end{pmatrix}$. Let $\Delta = \left(\begin{smallmatrix} i & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathbf{D}_1$. Then, $(\Delta \otimes I)i^{p(\mathbf{x})} = \begin{pmatrix} -1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = i^{g(\mathbf{x})}$, with $g : \mathbb{F}_2^2 \to \mathbb{Z}_4$, $g(\mathbf{x}) = 2x_0x_1 + 2$. We can re-write $i^{g(\mathbf{x})}$ as $(-1)^{g'(\mathbf{x})}$, with $g'(\mathbf{x})$ Boolean, $g'(\mathbf{x}) = x_0x_1 + 1$. It is straightforward to verify that this example satisfies lemmas 1 and 2.

From lemmas 1 and 2 we conclude that a final multiplication of a vector by a member of $\mathbf{D}_n = \{\mathbf{D}_1\}^n$ leaves invariant the multi-set of power spectra values, and also leaves invariant the underlying graphical interpretation of a vector described by a quadratic function, as the graphical interpretation is dependent only on terms of degree 2. We introduce the symbol '$\simeq$'.

Definition 9: Let u and v be two 2×2 unitary matrices. Then,

$$u \simeq v \quad \Leftrightarrow \quad u = \Delta v, \qquad \Delta \in \mathbf{D} \ .$$

Remark: Note that $u \simeq v$ cannot be deduced from (and does not imply) $u = v\Delta$.

[5] It remains an open problem to establish whether LU-equivalence of two graph states implies LC-equivalence of the same two states (see Chapter 6 of [55] and [58]).

[6] For instance, $\sigma_x^{(2)} = I \otimes I \otimes \sigma_x \otimes I \otimes \ldots \otimes I$.

[7] Thanks to Patrick Sole for pointing this out, and similary w.r.t. the transform group.

B. The Transform Group

Definition 10: $\mathbf{T}_1$ is the subgroup of the local Clifford group, $\mathbf{C}_1$, generated by $\lambda = \omega^5 N = \frac{\omega^5}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $|\mathbf{T}_1| = 3$. We call $\mathbf{T}_1$ the *transform group* because it represents the unique maximal subgroup of transforms within the local Clifford group that do not, in general, leave the multi-set of power spectral values invariant. Observe that $\lambda = N^{16}$. $\mathbf{T}_1$ is also a *Sylow-3 subgroup* of the local Clifford group.

Remark: As $\mathbf{C}_1 = \mathbf{D}_1 \times \mathbf{T}_1$, every element of $\mathbf{C}_1$ can be represented uniquely by $\Delta\lambda^j$, $0 \leq j < 3$, for some j and some $\Delta \in \mathbf{D}_1$. This fact leads directly to theorem 1, and is used implicitly in the proof of theorem 1.

In this paper we are interested in the set of multi-sets of power spectral values of a vector s w.r.t. the transform set $\mathbf{T}_n = \{\mathbf{T_1}\}^n$. As $x \simeq \lambda$ and $xz \simeq \lambda^2$, we can, without loss, focus on such sets w.r.t. the transform set $\{I, x, xz\}^n$, as is done in the next subsection. As $N \simeq \lambda$ and $H \simeq \lambda^2$, we can also, without loss, focus on such sets w.r.t. the transform set $\{I, H, N\}^n$, as is done primarily in this paper.

C. The LC-orbit Occurs Within the $\{I, x, xz\}^n$ Set of Transform Spectra

Summarising (2),

Lemma 3: Given graphs G and G' as represented by quadratic Boolean functions, $p(\mathbf{x})$ and $p'(\mathbf{x})$, then G and G' are in the same LC-orbit iff $(-1)^{p'(\mathbf{x})} \simeq U_{v_{t-1}} U_{v_{t-2}} \dots U_{v_0} (-1)^{p(\mathbf{x})}$ for some series of t local unitary transformations, U_{v_i}.

Thus by applying $U_v(G)$ successively for various v to an initial state, one can generate all LC-equivalent graphs within a finite number of steps. (It is evident that the action of LC generates an LC-orbit of finite size). Instead of applying U successively, it would be nice to identify a (smaller) transform set in which all LC-equivalent graphs exist as spectra, to within a post-multiplication by a member of $\mathbf{D}_n$. One can deduce from definition 9 that $zx \simeq x$. Therefore,

Lemma 4: $zxx \simeq I$, and $xzx \simeq zxz$.

We can now derive the following.

Theorem 1: To within subsequent transformation by a member of $\mathbf{D}_n$, the LC-orbit of the graph, G, over n qubits occurs within the spectra of all possible tensor product combinations of the 2×2 matrices, I, x, and xz. There are 3^n such transform spectra.

Proof: For each vertex in G, consider every possible product of the two matrices, x, and z. Using the equivalence relationship, '$\simeq$', and lemma 4,

$xxx \simeq x$	$zxx \simeq I$
$xxz \simeq I$	$zxz \simeq xz$
$xzx \simeq zxz \simeq xz$	$zzx \simeq x$
$xzz \simeq zxzz \simeq xzxz \simeq xxzx \simeq x$	$zzz \simeq I$.

Thus, any product of three or more instances of x and/or z can always be reduced to I, x, or xz. Theorem 1 follows by recursive application of (2) with these rules, and by noting that the rules are unaffected by tensor product expansion over n vertices. ∎

Theorem 1 gives a trivial and very loose upper bound on the maximum size of any LC-orbit over n qubits, this bound being 3^n. It has been computed by Danielsen in [16] that, up to graph isomorphism, the number of LC-orbits for connected graphs for $n = 1$ to $n = 12$ is $1, 1, 1, 2, 4, 11, 26, 101, 440, 3132, 40457$, and 1274068, respectively (see also [28], [25], [29], [15], [52], [19]).

D. The LC-orbit Occurs Within the $\{I, H, N\}^n$ Set of Transform Spectra

As $x \simeq \lambda$ and $xz \simeq \lambda^2$, and as $N \simeq \lambda$ and $H \simeq \lambda^2$, and, as it also follows that $N \simeq x$ and $H \simeq xz$, we can, without change, replace the transform set $\{I, x, xz\}^n$ with the transform set $\{I, H, N\}^n$, as the set of multi-sets of power spectral values remain invariant under such a change. This is of theoretical interest because H defines a 2-point (periodic) discrete Fourier transform matrix, and N defines a 2-point negaperiodic discrete Fourier transform matrix. In other words a basis change from rows of x and xz to rows of N and H provides a more natural set of multidimensional axes in some contexts. Observe that, for t a non-negative integer,

$$N^{3t} = \omega^t I \simeq I, \quad N^{3t+1} \simeq N, \quad N^{3t+2} \simeq H, \quad N^{24} = I, \tag{7}$$

where $\omega = e^{2\pi i/8}$. The $\{I, H, N\}^n$ transform set over n binary variables has been used to analyse the resistance of certain S-boxes to a form of generalised linear approximation in [40]. It also defines the basis axes under which aperiodic autocorrelation of Boolean functions is investigated in [17], and has been used to define the *Clifford merit factor* - an entanglement measure [41]. The *negahadamard transform*, $\{N\}^n$, was introduced in [35] and, in [46], [47], it is noted that the peak-to-average power ratio of the spectrum of a vector s w.r.t. the negahadamard transform is given by $q(-1)$, where q is the interlace polynomial of the associated graph. Constructions for Boolean functions with favourable spectral properties w.r.t. $\{H, N\}^n$ have been proposed in [39], and [38] showed that Boolean functions that are LU-equivalent to indicators for distance-optimal binary error-correcting codes yield favourable spectral properties w.r.t. $\{I, H\}^n$. *Pivot orbits* of a graph w.r.t $\{I, H\}^n$ have been characterised in [48], [49].

E. A Spectral Derivation of LC

We now derive LC by examining the repetitive action of N on the vector form of the graph states, interspersed with the actions of certain matrices from $\mathbf{D}_1$. These repeated actions not only generate the LC-orbit of the graph but, more generally, also generate the $\{I, H, N\}^n$ transform spectra. The LC-orbit can be identified with a subset of the flat transform spectra w.r.t. $\{I, H, N\}^n$. Let $s = (-1)^{p(\mathbf{x})}$, where $p(\mathbf{x})$ is Boolean quadratic and represents a graph G. Then the action of N_v on G is equivalent to $U_v s$, where:

$$U_v \simeq U'_v = I \otimes \dots \otimes I \otimes N \otimes I \otimes \dots \otimes I \ ,$$

where N occurs at position v in the tensor product decomposition. Let us write $p(\mathbf{x})$, uniquely, as,

$$p(\mathbf{x}) = x_v \mathcal{N}_v(\mathbf{x}) + q(\mathbf{x}) \ ,$$

where $q(\mathbf{x})$ and $\mathcal{N}_v(\mathbf{x})$ are independent of x_v ($\mathcal{N}_v(\mathbf{x})$ has nothing to do with the negahadamard kernel, N_v). We shall

state a theorem that holds for $p(\mathbf{x})$ of any degree, not just quadratic, and then show that its specialisation to quadratic $p(\mathbf{x})$ gives the required single LC operation. Express $\mathcal{N}_v(\mathbf{x})$ as the sum of r monomials, $e_i(\mathbf{x})$, as follows,

$$\mathcal{N}_v(\mathbf{x}) = \sum_{i=0}^{r-1} e_i(\mathbf{x}) \ .$$

For $p(\mathbf{x})$ of any degree, the $e_i(\mathbf{x})$ are of degree $\leq n-1$. In the sequel we mix arithmetic, mod 2, and mod 4 so, to clarify, anything in square brackets is computed mod 2. The $\{0,1\}$ result is then embedded in mod 4 arithmetic for subsequent operations outside the square brackets. Define,

$$\mathcal{N}'_v(\mathbf{x}) = \sum_{i=0}^{r-1} [e_i(\mathbf{x})] \qquad (\text{ mod } 4) \ .$$

Theorem 2: Let $s' = U_v s$, where $s = (-1)^{p(\mathbf{x})}$ and $s' = \omega i^{\tilde{p'}(\mathbf{x})}$, where $\omega = e^{2\pi i/8}$. Then,

$$\tilde{p'}(\mathbf{x}) = 2\left[p(\mathbf{x}) + \textstyle\sum_{j\neq k} e_j(\mathbf{x})e_k(\mathbf{x})\right] + 3\mathcal{N}'_v(\mathbf{x}) + 3[x_v], \quad (\text{ mod } 4) \ . \tag{8}$$

Proof: Assign to A and B the evaluation of $p(\mathbf{x})$ at $x_v = 0$ and $x_v = 1$, respectively. Thus,

$$A = p(\mathbf{x})_{x_v=0} = q(\mathbf{x}) \ .$$

Similarly,

$$B = p(\mathbf{x})_{x_v=1} = \mathcal{N}_v(\mathbf{x}) + q(\mathbf{x}) \ .$$

We need the following equality between mod 2 and mod 4 arithmetic.

Lemma 5:

$$\textstyle\sum_{i=0}^{t-1}[A_i] \ (\text{ mod } 4) = \left[\sum_{i=0}^{t-1} A_i\right] + 2\left[\sum_{i\neq j} A_i A_j\right] \ (\text{ mod } 4), \quad \text{where } A_i \in \mathbb{F}_2, t > 0 \ .$$

Observe the following action of N:

$$\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = w\begin{pmatrix} 1 \\ -i \end{pmatrix} \ ,$$

where $w = e^{2\pi i/8}$. For the moment we ignore the global constant, w, so that N maps $(-1)^{00}$ to i^{03} and, similarly, $(-1)^{10}$ to i^{12}, $(-1)^{01}$ to i^{30} and $(-1)^{11}$ to i^{21}, where by c^{ab} we mean $\begin{pmatrix} c^a \\ c^b \end{pmatrix}$. In general, for $A, B \in \mathbb{F}_2$, $\alpha, \beta \in \mathbb{Z}_4$, $(-1)^{AB}$ is mapped by N_v to $i^{\alpha\beta}$, where,

$$\begin{aligned} \alpha &= 2[AB] + [A] + 3[B] && (\text{ mod } 4) \\ \beta &= 2[AB] + 3[A] + [B] + 3 && (\text{ mod } 4) \ . \end{aligned}$$

Substituting the previous expressions for A and B into the above and making use of Lemma 5 gives,

$$\begin{aligned} \alpha(\mathbf{x}) &= 2[q(\mathbf{x})] + 3[\mathcal{N}_v(\mathbf{x})] && (\text{ mod } 4) \\ \beta(\mathbf{x}) &= 2[q(\mathbf{x})] + [\mathcal{N}_v(\mathbf{x})] + 3 && (\text{ mod } 4) \ . \end{aligned}$$

$\tilde{p'}(\mathbf{x})$ can now be written as,

$$\tilde{p'}(\mathbf{x}) = (3[x_v] + 1)\alpha(\mathbf{x}) + [x_v]\beta(\mathbf{x}) \qquad (\text{ mod } 4) \ .$$

Substituting for α and β gives,

$$\tilde{p'}(\mathbf{x}) = 2[q(\mathbf{x})] + 2[x_v\mathcal{N}_v(\mathbf{x})] + 3[\mathcal{N}_v(\mathbf{x})] + 3[x_v] \quad (\text{ mod } 4) \ .$$

Applying Lemma 5 to the term $3[\mathcal{N}_v(\mathbf{x})]$,

$$3[\mathcal{N}_v(\mathbf{x})] = 2\left[\sum_{j\neq k} e_j(\mathbf{x})e_k(\mathbf{x})\right] + 3\mathcal{N}'_v(\mathbf{x}) \qquad (\text{ mod } 4) \ .$$

Furthermore, Lemma 5 implies that,

$$2\left[\textstyle\sum_{i=0}^{t-1} A_i\right] (\text{ mod } 4) = 2\textstyle\sum_{i=0}^{t-1}[A_i] (\text{ mod } 4), \quad \text{where } A_i \in \mathbb{F}_2, t > 0 \ .$$

Thus we obtain $\tilde{p'}(\mathbf{x})$, and re-introducing the global phase, ω, this establishes that $s' = \omega i^{\tilde{p'}}$. ∎

For $p(\mathbf{x})$ a quadratic function, $\mathcal{N}_v(\mathbf{x})$ has degree one, so $\mathcal{N}'_v(\mathbf{x})$ is a sum of degree-one terms over $\mathbb{Z}_4$. Therefore the $\mathbb{Z}_4$ degree-one terms, $\mathcal{N}'_v(\mathbf{x})$ and $3[x_v]$, can be eliminated from (8) by appropriate subsequent action by a member of $\mathbf{D}_n$ to s'. As all monomials, $e_i(\mathbf{x})$, are then of degree one, (8) reduces to,

$$p'(\mathbf{x}) = p(\mathbf{x}) + \sum_{j,k\in\mathcal{N}_v, j\neq k} x_j x_k \qquad (\text{ mod } 2) \ , \tag{9}$$

where $\tilde{p'}(\mathbf{x}) \simeq 2[p'(\mathbf{x})]$. (9) precisely defines the action of a single LC operation at vertex v of G, where we have used $\simeq$ to mean that $i^{\tilde{p'}(\mathbf{x})} = B(-1)^{p'(\mathbf{x})}$, for some $B \in \mathbf{D}_n$. As $p'(\mathbf{x})$ is also quadratic Boolean, we can realise successive LC operations on chosen vertices in G via successive actions of N at these vertices, where each action of N must be interspersed with the action of a matrix from $\mathbf{D}_n$ to eliminate $\mathbb{Z}_4$-linear terms from (8) and the residual $\mathbb{Z}_8$ constant term introduced by ω. In particular, one needs to intersperse with tensor products of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$.

Theorem 3: Given a graph, G, as represented by $s = (-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ quadratic, the LC-orbit of G comprises graphs which occur as a subset of the spectra w.r.t. $\{I, H, N\}^n$ acting on s.

Proof: Define $\mathbf{D}' \subset \mathbf{D}_1$ such that

$$\mathbf{D}' = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \ \middle| \ a = 1, b = \pm 1\right\} \ .$$

Similarly, define $\mathbf{D}'' \subset \mathbf{D}_1$ such that

$$\mathbf{D}'' = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \ \middle| \ a = 1, b = \pm i\right\}, \quad \text{where } i^2 = -1 \ .$$

Then for any $\Delta_1, \Delta'_1 \in \mathbf{D}'$, any $\Delta_2, \Delta'_2 \in \mathbf{D}''$, and any $c \in \{1, i, -1, -i\}$,

$$\begin{aligned} N\Delta_1 &= c\Delta'_1 N & \qquad H\Delta_1 &= c\Delta'_1 H \\ N\Delta_2 &= c\Delta_1 H & \qquad H\Delta_2 &= c\Delta_1 N \ . \end{aligned} \tag{10}$$

Let $\Delta_* \in \mathbf{D}' \bigcup \mathbf{D}''$. Then successive applications of $\Delta_* N$ can, using (10), be re-expressed as,

$$\prod(\Delta_* N) = c\Delta_* \prod N \simeq \prod N \ .$$

But, from (7), successive powers of N generate I, H, or N, to within a final multiplication by a member of $\mathbf{D}_1$. It follows that successive LC actions on arbitrary vertices can be described by the action on s of a member of the transform set, $\{I, H, N\}^n$, and therefore that the LC-orbit occurs within the $\{I, H, N\}^n$ transform spectra of s. ∎

F. LC on Hypergraphs

For $p(\mathbf{x})$ of degree > 2, $\mathcal{N}_v(\mathbf{x})$ will typically have degree higher than 1, and therefore the expansion of the sum will contribute higher degree terms. For such a scenario we can no longer eliminate the nonlinear and non-Boolean term, $\mathcal{N}'_v(\mathbf{x})$, from the right-hand side of (8) by subsequent actions from $\mathbf{D}_n$. Therefore, it is typically not possible to iterate LC graphically beyond one step. We would like to identify hypergraph equivalence w.r.t. local unitary transforms, in particular w.r.t. $\{I, H, N\}^n$. Computations have shown that orbits of Boolean functions of degree > 2 and size > 1 do sometimes exist with respect to $\{I, H, N\}^n$, although they appear to be significantly smaller in size compared to orbits for the quadratic case [17].

An interesting open problem is to characterise a 'LC-like' equivalence for hypergraphs.

Further spectral symmetries of Boolean functions w.r.t. $\{I, H, N\}^n$ are discussed in Appendix II.

IV. Generalised Bent Properties of Boolean Functions

A. Bent Boolean Functions

A bent Boolean function can be defined by using the WHT. Let $p(\mathbf{x})$ be our function over n binary variables. Define the WHT of $p(\mathbf{x})$ *at position* $\mathbf{k}$ by,

$$P_{\mathbf{k}} = 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{p(\mathbf{x}) + \mathbf{k} \cdot \mathbf{x}} \ , \qquad (11)$$

where $\mathbf{x}, \mathbf{k} \in \mathbb{F}_2^n$, and $\cdot$ implies the scalar product. The WHT of $p(\mathbf{x})$ can alternatively be defined by $P = (\prod_{i=0}^{n-1} H_i)(-1)^{p(\mathbf{x})}$.

$p(\mathbf{x})$ is *bent* if $|P_{\mathbf{k}}| = 1 \ \forall \mathbf{k}$, in which case we say that $p(\mathbf{x})$ has a *flat spectra* w.r.t. the WHT. In other words, $p(\mathbf{x})$ is bent if P is *flat*.

Let Γ be the binary adjacency matrix associated to $p(\mathbf{x})$ when $p(\mathbf{x})$ is a quadratic.

Lemma 6: [32]

$p(\mathbf{x})$ is *bent* $\Leftrightarrow$ Γ has maximum rank as a binary matrix.

All bent quadratics are equivalent under affine transformation to the Boolean function $\left(\sum_{i=0}^{\frac{n}{2}-1} x_{2i} x_{2i+1}\right) + \mathbf{c} \cdot \mathbf{x} + d$ for n even, where $\mathbf{c} \in \mathbb{F}_2^n$, and $d \in \mathbb{F}_2$ [32]. More generally, bent Boolean functions only exist for n even. It is interesting to investigate other bent symmetries where affine symmetry has been omitted. In particular, in the context of LC, we are interested in the existence and number of flat spectra of Boolean functions with respect to the $\{H, N\}^n$-transform set (*bent*$_4$), the $\{I, H\}^n$-transform set (*I-bent*), and the $\{I, H, N\}^n$-transform set (*I-bent*$_4$).

B. Bent Properties with respect to $\{H, N\}^n$

$\{H, N\}^n$ is the set of 2^n transforms of the form $\prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j$, where the sets $\mathbf{R_H}$ and $\mathbf{R_N}$ partition $\{0, \ldots, n-1\}$.

The following is trivial to verify:

$$p(\mathbf{x}) \text{ is bent } \Leftrightarrow p(\mathbf{x}) + \mathbf{k} \cdot \mathbf{x} + d \quad \text{is bent} \ ,$$

where $\mathbf{k} \in \mathbb{F}_2^n$ and $d \in \mathbb{F}_2$. In other words, if $p(\mathbf{x})$ is bent then so are all its affine offsets, mod 2. However the above does not follow if one considers every possible $\mathbb{Z}_4$-linear offset of $p(\mathbf{x})$. The WHT of $p(\mathbf{x})$ at position $\mathbf{k}$, with a $\mathbb{Z}_4$-linear offset, as specified by $\mathbf{c}$, can be defined by,

$$P_{\mathbf{k},\mathbf{c}} = 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (i)^{2[p(\mathbf{x}) + \mathbf{k} \cdot \mathbf{x}] + [\mathbf{c} \cdot \mathbf{x}]} \qquad \mathbf{k}, \mathbf{c} \in \mathbb{F}_2^n \ . \quad (12)$$

Definition 11:

$p(\mathbf{x})$ is *bent*$_4$ $\Leftrightarrow$ $\forall \mathbf{k} \in \mathbb{F}_2^n \ \exists \mathbf{c}$ such that $|P_{\mathbf{k},\mathbf{c}}| = 1$.

Let $\mathbf{R_N}$ and $\mathbf{R_H}$ partition $\{0, 1, \ldots, n-1\}$. Let,

$$U = \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j \ .$$

$$s' = U(-1)^{p(\mathbf{x})} \ . \qquad (13)$$

Lemma 7: $p(\mathbf{x})$ is bent$_4$ if there exists one or more partitions, $\mathbf{R_N}, \mathbf{R_H}$ such that s' is *flat*.

Proof: The rows of U, $U[t]$, can be described by $(i)^{f_t(\mathbf{x})}$, where the f_t's are linear, $f_t : \mathbb{F}_2^n \to \mathbb{Z}_4$, and the coefficient of x_j in any $f_t \in \{0, 2\}$ for $j \in \mathbf{R_H}$ and $\in \{1, 3\}$ for $j \in \mathbf{R_N}$. Therefore s' can always, equivalently, be expressed as $s' = (\prod_j H_j)(i)^{2p[\mathbf{x}] + [f'(\mathbf{x})]}$, where f' is linear, $f' : \mathbb{F}_2^n \to \mathbb{F}_2$, and the coefficient of x_j in any f' is 0 for $j \in \mathbf{R_H}$, and 1 for $j \in \mathbf{R_N}$. ∎

An alternative way to define the bent$_4$ property for $p(\mathbf{x})$ quadratic is via a modified form of the adjacency matrix.

Lemma 8: For quadratic $p(\mathbf{x})$,

$$p(\mathbf{x}) \text{ is bent}_4 \quad \Leftrightarrow \quad \Gamma_{\mathbf{v}} \text{ has maximum rank as a binary matrix, for some } \mathbf{v} \in \mathbb{F}_2^n \ ,$$

where $\Gamma_{\mathbf{v}}$ is a modified form of Γ with v_i in position $[i, i]$, where $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

Proof: We first show that the transform of $(-1)^{p(\mathbf{x})}$ by tensor products of H and N produces a flat spectra iff the associated periodic and negaperiodic [8] autocorrelation spectra have zero out-of-phase values. We then show how these autocorrelation constraints lead directly to constraints on the associated adjacency matrix.

Consider a function, p, of just one variable, x_0, and let $s = (-1)^{p(x_0)}$. Define the *periodic autocorrelation function* by,

$$a_k = \sum_{x_0 \in \mathbb{F}_2} (-1)^{p(x_0) + p(x_0 + k)}, \qquad k \in \mathbb{F}_2 \ .$$

Claim 1: It is well-known that $s' = Hs$ is a flat spectrum iff $a_k = 0$ for $k \neq 0$.

The *negaperiodic autocorrelation function* is less well-known. It has been investigated in, for instance, [36], and in multivariate form, in [35]. Whereas the periodic autocorrelation compares a sequence with its cyclic shifts, the negaperiodic autocorrelation compares a sequence with its modified cyclic shifts, where the elements wrapped round

[8] or *odd-periodic*.

are multiplied by -1. Define the negaperiodic autocorrelation function by,

$$b_k = \sum_{x_0 \in \mathbb{F}_2} (-1)^{p(x_0)+p(x_0+k)+k(x_0+1)}, \qquad k \in \mathbb{F}_2 \ .$$

Claim 2: $s' = Ns$ is a flat spectrum iff $b_k = 0$ for $k \neq 0$ [9].

We now elaborate on claims 1 and 2. Define $s(z) = s_0 + s_1 z$, $a(z) = a_0 + a_1 z$, and $b(z) = b_0 + b_1 z$. Then the periodic and negaperiodic relationships between autocorrelation and fourier spectra, as claimed above, follow because periodic autocorrelation can be realised by the polynomial multiplication, $a(z) = s(z)s(z^{-1})$ mod (z^2-1), with associated residue reduction, mod $(z-1)$ and mod $(z+1)$, realised by $s' = Hs = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} s$, with the Chinese remainder theorem (CRT) realised by $H^\dagger s'$, where '$\dagger$' means transpose conjugate. By Parseval, s' can only be flat if $a_1 = 0$. Similarly, negaperiodic autocorrelation can be realised by the polynomial multiplication, $b(z) = s(z)s(z^{-1})$ mod (z^2+1), with associated residue reduction, mod $(z-i)$ and mod $(z+i)$, realised by $s' = Ns = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} s$, with the CRT realised by $N^\dagger s'$. By Parseval, s' can only be flat if $b_1 = 0$.

We now extend this autocorrelation $\leftrightarrow$ Fourier spectrum duality to n binary variables by defining multivariate forms of the above polynomial relationships. If we choose periodic autocorrelation for indices in $\mathbf{R_H}$ and negaperiodic autocorrelation for indices in $\mathbf{R_N}$, we obtain the autocorrelation spectra,

$$A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{p(\mathbf{x})+p(\mathbf{x}+\mathbf{k})+\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i)k_i(x_i+1)} \ , \tag{14}$$

where $\mathbf{k} = (k_0, k_1, \ldots, k_{n-1}) \in \mathbb{F}_2^n$, and $\chi_{\mathbf{R_N}}(i)$ is the characteristic function of $\mathbf{R_N}$, i.e,

$$\chi_{\mathbf{R_N}}(i) = \begin{cases} 1, & i \in \mathbf{R_N} \\ 0, & i \notin \mathbf{R_N} \end{cases}$$

In polynomial terms, with $\mathbf{z} \in \mathbb{F}_2^n$ and $s(\mathbf{z}) = \sum_{\mathbf{j} \in \mathbb{F}_2^n} s_{\mathbf{j}} \prod_{i=0}^{n-1} z_i^{j_i}$, we have,

$$\begin{aligned} A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) &= \sum_{\mathbf{k} \in \mathbb{F}_2^n} A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} \prod_{i=0}^{n-1} z_i^{k_i} \\ &= s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1}) \\ &\qquad \text{mod} \ \prod_{i=0}^{n-1} (z_i^2 - (-1)^{\chi_{\mathbf{R_N}}(i)}) \ . \end{aligned} \tag{15}$$

Then, by appealing to a multivariate version of Parseval's theorem, s' as defined in (13) is flat iff $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0, \forall \ \mathbf{k} \neq \mathbf{0}$.

These constraints on the autocorrelation coefficients of s translate to requiring a maximum rank property for a modified adjacency matrix, as follows. The condition $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$ for $\mathbf{k} \neq \mathbf{0}$ is equivalent to requiring that, if we compare the function with its multidimensional periodic and negaperiodic rotations (but for the identity rotation), the remainder should be a balanced function. When dealing with quadratic Boolean functions, the remainder is always linear or constant. This gives us a system of linear equations represented by the binary adjacency matrix, Γ, of $p(\mathbf{x})$, with a modified diagonal, that is with $\Gamma_{i,i} = 1$ for all $i \in \mathbf{R_N}$, and $\Gamma_{i,i} = 0$ otherwise. Let

$$\begin{aligned} &p(x_0, x_1, \ldots, x_{n-1}) = \\ &a_{01}x_0x_1 + \cdots + a_{ij}x_ix_j + \cdots + a_{n-2,n-1}x_{n-2}x_{n-1} \ . \end{aligned}$$

Therefore,

$$\begin{aligned} &p(\mathbf{x}) + p(\mathbf{x}+\mathbf{k}) + \textstyle\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i)k_ix_i = \\ &k_0(\chi_{\mathbf{R_N}}(0)x_0 + a_{01}x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) \\ &+k_1(a_{01}x_0 + \chi_{\mathbf{R_N}}(1)x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) + \cdots \\ &+k_{n-1}(a_{0,n-1}x_0 + \cdots + a_{n-2,n-1}x_{n-2} + \chi_{\mathbf{R_N}}(n-1)x_{n-1}) \ . \end{aligned}$$

This is equal to:

$$\begin{aligned} &x_0(\chi_{\mathbf{R_N}}(0)k_0 + a_{01}k_1 + \cdots + a_{0n}k_n) + \\ &x_1(a_{01}k_0 + \chi_{\mathbf{R_N}}(1)k_1 + \cdots a_{1,n-1}k_{n-1}) + \cdots + \\ &x_{n-1}(a_{0,n-1}k_0 + \cdots + a_{n-2,n-1}k_{n-2} + \chi_{\mathbf{R_N}}(n-1)k_{n-1}), \end{aligned}$$

which is balanced unless constant. The constant $\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i)k_i$ will not play any role in the equation $A_{\mathbf{k}} = 0$, and can be ignored. We have the the following system of equations:

$$\begin{aligned} &\chi_{\mathbf{R_N}}(0)k_0 + a_{01}k_1 + a_{02}k_2 + \cdots + a_{0,n-1}k_{n-1} = 0 \\ &a_{01}k_0 + \chi_{\mathbf{R_N}}(1)k_1 + a_{12}k_2 + \cdots + a_{1,n-1}k_{n-1} = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_{0,n-1}k_0 + a_{1,n-1}k_1 + \cdots + a_{n-2,n-1}k_{n-2} \\ &\qquad + \chi_{\mathbf{R_N}}(n-1)k_{n-1} = 0 \ . \end{aligned}$$

Writing this system as a matrix, we have:

$$\begin{pmatrix} \chi_{\mathbf{R_N}}(0) & a_{01} & a_{02} & \ldots & a_{0,n-1} \\ a_{01} & \chi_{\mathbf{R_N}}(1) & a_{12} & \ldots & a_{1,n-1} \\ a_{02} & a_{12} & \chi_{\mathbf{R_N}}(2) & \ldots & a_{2,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,n-1} & a_{1,n-1} & a_{2,n-1} & \ldots & \chi_{\mathbf{R_N}}(n-1) \end{pmatrix} .$$

This is a modification of Γ, with 1 or 0 in position i of the diagonal depending on whether $i \in \mathbf{R_N}$ or $i \in \mathbf{R_H}$. ■

In general,

$$p(\mathbf{x}) \text{ is bent} \ \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \ p(\mathbf{x}) \text{ is bent}_4 \ .$$

Theorem 4: All Boolean functions of degree ≤ 2 are bent$_4$.

Proof: Degree zero and degree one functions are trivial. Consider the adjacency matrix, Γ, associated with the quadratic Boolean function, $p(\mathbf{x})$. We now prove that $\Gamma_{\mathbf{v}}$ has maximum rank as a binary matrix for at least one choice of $\mathbf{v}$, where $\Gamma_{\mathbf{v}} = \Gamma + \text{diag}(\mathbf{v})$ as before. Let M be the minor associated with the first entry of Γ; in other words, let $\Gamma = \begin{pmatrix} 0 & \\ & M \end{pmatrix}$. We prove by induction that there exists at least one choice of v such that $\Gamma_{\mathbf{v}}$ has maximum rank as a binary matrix. The theorem is true for $n = 2$: in this case, $\Gamma = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$. Then, either $\det(\Gamma) = 1$, in which case we choose $\mathbf{v} = (0,0)$, or we have $a = 0$ (empty graph). In the last case we choose $\mathbf{v} = (1,1)$, so $det(\Gamma_{\mathbf{v}}) = 1 + a = 1$. Suppose the theorem is true for $n-1$ variables. We will see that it is true for n variables. If the determinant of Γ is 1 we

[9] In fact, for p a Boolean function of just one variable, Hs is never flat and Ns is always flat.

take $\mathbf{v} = (0, \ldots, 0)$ and we are done. If $\det(\Gamma) = 0$, then we have two cases:

- $\det(M) = 1$: Take $\mathbf{v} = (1, 0, \ldots, 0)$.
- $det(M) = 0$: By the induction hypothesis there is at least one choice of $\mathbf{v}(M) \in \mathbb{F}_2^{n-1}$, where $\mathbf{v}(M) = (v_1, \ldots, v_{n-1})$ such that $M_{\mathbf{v}(M)}$ has full rank. Let $\mathbf{v}' = (0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_2^n$. If $\det(\Gamma_{\mathbf{v}'}) = 1$ we have finished. If $\det(\Gamma_{\mathbf{v}'}) = 0$ we are in the first case again, so we take $\mathbf{v} = (1, v_1, \ldots, v_{n-1})$, and we are done.

The theorem follows from lemma 8. ∎

Remark: Theorem 4 is true even for Boolean functions associated with non-connected or empty graphs.

Lemma 9: Not all Boolean functions of degree > 2 are bent$_4$.

Proof: Counter-example - by computation there are no bent$_4$ cubics of three variables. ∎

Further computations show that there are no bent$_4$ Boolean functions of four variables of degree > 2. Similarly, there are only 252336 bent$_4$ cubic Boolean functions in five variables (out of a possible $2^{20} - 2^{10}$, not including affine offsets), and no bent$_4$ Boolean functions of degree ≥ 4 in five variables. Bent$_4$ cubics of six variables do exist. Lemma 9 identifies an open problem:

What is the maximum algebraic degree of a bent$_4$ Boolean function of n variables?

Theorem 5: There is no Boolean function $p(\mathbf{x})$ such that $|P_{\mathbf{k},\mathbf{c}}| = 1 \ \forall \mathbf{c}, \mathbf{k} \in \mathbb{F}_2^n$.

Proof: This is trivial for degree zero and degree one functions.

Let $p(\mathbf{x})$ be a quadratic. Consider the adjacency matrix, Γ, associated with $p(\mathbf{x})$. For degree 2, the theorem is equivalent to proving that there is a $\mathbf{v}$ such that $\Gamma_{\mathbf{v}}$ has rank less than maximal. Then:

1) if $p(\mathbf{x})$ is not bent, then we take $\mathbf{v} = (0, \ldots, 0)$ and we are done.
2) if $p(\mathbf{x})$ is bent, we take M as in the proof for Theorem 4. If $det(M) = 1$, we take $\mathbf{v} = (1, 0, \ldots, 0)$ and we are done; if $det(M) = 0$, modify the diagonal as in the proof for Theorem 4. If the determinant of the new matrix is equal to 0, we are done; if not, we are in case 1.

Let $p(\mathbf{x})$ be a function of degree higher than quadratic. Consider the proof of Lemma 8. We have established that, for a fixed choice of $\mathbf{R_H}$ and $\mathbf{R_N}$, s', as defined in (13), is flat if and only if $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall\ \mathbf{k}$, $\mathbf{k} \neq \mathbf{0}$. Therefore $p(\mathbf{x})$ is such that $|P_{\mathbf{k},\mathbf{c}}| = 1\ \forall \mathbf{c}, \mathbf{k} \in \mathbb{F}_2^n$ iff $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall \mathbf{k}$, $\mathbf{k} \neq \mathbf{0}$, for **all** partitions $\{\mathbf{R_H}, \mathbf{R_N}\}$. In particular, if $p(\mathbf{x})$ is such that $|P_{\mathbf{k},\mathbf{c}}| = 1\ \forall \mathbf{c}, \mathbf{k} \in \mathbb{F}_2^n$, then the polynomials, $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z})$, as defined in (15), satisfy $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) = 2^n$ for all choices of $\mathbf{R_H}$ and $\mathbf{R_N}$ (i.e. their out-of-phase coefficients are all zero). By the CRT we can combine theses polynomials for each choice of $\mathbf{R_H}$ and $\mathbf{R_N}$ to construct the polynomial,

$$r(\mathbf{z}) \bmod \prod_{j=0}^{n}(z_j^4 - 1) = \text{CRT}\{A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) \mid \forall \mathbf{R_H}, \mathbf{R_N}\} \ , \tag{16}$$

where $r(\mathbf{z}) = s(z_0, z_1, \ldots, z_{n-1})s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$.

But as $r(\mathbf{z})$ comprises monomials containing only z_i^{-1}, z_i^0, z_i^1, the modular restriction in (16) has no effect on coefficient magnitudes, and

$$r(\mathbf{z}) \equiv r(\mathbf{z}) \bmod \prod_{j=0}^{n}(z_j^4 - 1) \ .$$

to within a multiplication of the coefficients by ± 1. It follows, by application of the CRT to (16) that, if $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) = 2^n$, $\forall \mathbf{R_H}, \mathbf{R_N}$, then $r(\mathbf{z}) = 2^n$ also, i.e. $r(\mathbf{z})$ is integer. But this is impossible as the coefficients of the maximum degree terms, $\prod_j z_j^{-1^{u_j}}$, $u_j \in \mathbb{F}_2$, in $r(\mathbf{z})$ can never be zero, but are always ± 1. ∎

Remark: Although we proved it only for Boolean functions, it is possible to generalise theorem 5 for functions $\mathbb{F}_2^n \to \mathbb{Z}_q$, for any even integer q.

C. Bent Properties with respect to $\{I, H\}^n$

$\{I, H\}^n$ is the set of 2^n transforms of the form $\prod_{j\in\mathbf{R_I}} I_j \prod_{j\in\mathbf{R_H}} H_j$, where the sets $\mathbf{R_I}$ and $\mathbf{R_H}$ partition $\{0, \ldots, n-1\}$. [38] has investigated other spectral properties w.r.t. $\{I, H\}^n$, such as *weight hierarchy* of an associated binary linear code if the graph is bipartite.

The WHT of the subspace of a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, can be defined as follows. Let $\theta \in \mathbb{F}_2^n$ be such that $\theta_j = 1$ iff $j \in \mathbf{R_I}$. Let $\mathbf{r} \preceq \theta$, where '$\preceq$' means that θ '*covers*' $\mathbf{r}$, i.e. $r_i \leq \theta_i$, $\forall i$. Then,

$$P_{\mathbf{k},\mathbf{r},\theta} = 2^{-(n-\text{wt}(\theta))/2} \sum_{\substack{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}}} (-1)^{p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}}, \quad \mathbf{k} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \quad . \tag{17}$$

Definition 12:

$$p(\mathbf{x}) \text{ is } \textit{I-bent} \quad \Leftrightarrow \quad \begin{array}{l} \forall \mathbf{k} \preceq \bar{\theta}, \forall \mathbf{r} \preceq \theta, \\ \exists \theta \text{ such that } |P_{\mathbf{k},\mathbf{r},\theta}| = 1, \\ \quad \text{where wt}(\theta) < n. \end{array}$$

Let

$$U = \prod_{j\in\mathbf{R_I}} I_j \prod_{j\in\mathbf{R_H}} H_j \ . \tag{18}$$

$$s' = U(-1)^{p(\mathbf{x})} \ . \tag{19}$$

Lemma 10: $p(\mathbf{x})$ is I-bent if there exist one or more partitions, $\mathbf{R_I}, \mathbf{R_H}$ such that s' is flat, where $|\mathbf{R_I}| < n$.

An alternative way to define the I-bent property of $p(\mathbf{x})$ is via its associated adjacency matrix, Γ. Let Γ_I be the adjacency matrix obtained from Γ by deleting all rows and columns of Γ with indices in $\mathbf{R_I}$.

Lemma 11: For quadratic $p(\mathbf{x})$,

$p(\mathbf{x})$ is I-bent $\Leftrightarrow$ Γ_I has maximum rank as a binary matrix for one or more choices of $\mathbf{R_I}$, where $|\mathbf{R_I}| < n$.

In general,

$$p(\mathbf{x}) \text{ is bent } \begin{array}{c}\Rightarrow \\ \not\Leftarrow\end{array} \quad p(\mathbf{x}) \text{ is I-bent} \ .$$

Theorem 6: All quadratic Boolean functions are I-bent.

Proof: It is easy to show that all quadratic Boolean functions of 2 variables are I-bent. The theorem follows by observing that all adjacency matrices, Γ, representing quadratic functions of $n > 2$ variables contain 2×2 non-zero submatrices, obtained from Γ by deleting all rows and columns of Γ with indices $\mathbf{R_I}$, for $|\mathbf{R_I}| = n-2$. ■

Remark: An I-bent function is a Boolean function $p : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that there exists (w.l.o.g.) a decomposition of $\mathbb{F}_2^n = \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2}$ in such a way that

$$p(x, y = a) : \mathbb{F}_2^{n_1} \rightarrow \mathbb{F}_2$$

is bent for all $a \in \mathbb{F}_2^{n_2}$.

Remark: An I-bent function is a Boolean function in n variables such that the function, after fixing the subset of variables indexed by $\mathbf{R_I}$, $|\mathbf{R_I}| > 0$, is bent in the remaining variables indexed by $\mathbf{R_H}$. Thereby, one can create I-bent functions by choosing $2^{|\mathbf{R_I}|}$ arbitrary bent functions and concatenating them, or even by taking a bent function in a set of variables and any non-bent function in the remaining variables and adding them.

Theorem 7: The maximum degree of an I-bent Boolean function in n variables, where $n > 2$, is $n-1$.

Proof: First, we show an I-bent Boolean function in n variables of degree $n-1$:

$$p(\mathbf{x}) = x_0 x_1 + x_1 x_2 \cdots x_{n-1} \ .$$

Let $p(\mathbf{x})|_{\mathbf{R_I}}$ be a restriction of p where the variables indexed by members of $\mathbf{R_I}$ have been arbitrarily fixed. If we take $\mathbf{R_I} = \{2, \ldots, n-1\}$, we see that

$$p(\mathbf{x})|_{\mathbf{R_I}} = \begin{cases} p'(x_0, x_1) = x_0 x_1 \\ p'(x_0, x_1) = x_0 x_1 + x_1 \end{cases}$$

Both are bent, so p is I-bent.

We now show that there is no I-bent Boolean function of n variables, when $n > 2$, of degree n. A Boolean function p of degree n in n variables can be written as $p(\mathbf{x}) = x_0 \cdots x_{n-1} + g(\mathbf{x})$, with $\deg(g) < n$. W.l.o.g., let $\mathbf{R_I} = \{0, \ldots, n_1 - 1\}$. Then, after fixing the variables in $\mathbf{R_I}$, the possible functions we get are: $p(\mathbf{x})|_{\mathbf{R_I}} = \begin{cases} p'_1(x_{n_1}, \ldots, x_{n-1}) = x_{n_1} \cdots x_{n-1} + g'(x_{n_1}, \ldots, x_{n-1}) \\ p'_2(x_{n_1}, \ldots, x_{n-1}) = g'(x_{n_1}, \ldots, x_{n-1}) \end{cases}$ with $g'(x_{n_1}, \ldots, x_{n-1}) = g(\mathbf{x})|_{\mathbf{R_I}}$. Both must be bent for p to be I-bent. Suppose that $n - n_1 > 2$: then either p'_1 or p'_2 are functions of degree $n - n_1$ in $n - n_1$ variables, so p cannot be bent. Therefore $n - n_1 \leq 2$. Suppose $n - n_1 = 2$ or 1. Then, either p'_1 or p'_2 (or both) are affine, and there are no affine bent functions. $n - n_1 = 0$ would imply $\mathbf{R_I} = \{0, \ldots, n-1\}$, and by definition $|\mathbf{R_I}| < n$. Therefore p cannot be I-bent, so there are no I-bent functions of n variables of degree n. ■

Computations show that there are 416 I-bent cubics in four variables, and that there are 442640 I-bent cubics, and 1756160 I-bent quartics in five variables.

Lemma 12: There is no Boolean function $p(\mathbf{x})$ with the property $|P_{\mathbf{k},\mathbf{r},\theta}| = 1 \ \forall \ \theta, \mathbf{k}, \mathbf{r}, \ \mathbf{k} \preceq \bar{\theta}, \mathbf{r} \preceq \theta$.

Proof: Let $s = (-1)^{p(\mathbf{x})}$. Let $|\mathbf{R_I}| = n-1$. Then for U as defined in (18), s' cannot be flat. ■

D. Bent Properties with respect to $\{I, H, N\}^n$

The $\{H, N\}^{n-|\mathbf{R_I}|}$ set of transforms of the subspace of a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, is defined as follows. Let $\theta \in \mathbb{F}_2^n$ be such that $\theta_j = 1$ iff $j \in \mathbf{R_I}$. Let $\mathbf{r} \preceq \theta$. Then,

$$P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta} = \ 2^{-(n-\mathrm{wt}(\theta))/2} \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (i)^{2[p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}]+[\mathbf{c}\cdot\mathbf{x}]}, \quad \mathbf{k}, \mathbf{c} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \ . \tag{20}$$

Definition 13:

$$p(\mathbf{x}) \text{ is } \textit{I-bent}_4 \quad \Leftrightarrow \quad \forall \mathbf{k} \preceq \bar{\theta}, \forall \mathbf{r} \preceq \theta, \ \exists \mathbf{c}, \theta \text{ such that } |P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta}| = 1 \ ,$$

where $\mathrm{wt}(\theta) < n$.

Let $\mathbf{R_I}$, $\mathbf{R_H}$ and $\mathbf{R_N}$ partition $\{0, 1, \ldots, n-1\}$. Let,

$$U = \prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j \ . \tag{21}$$

$$s' = U(-1)^{p(\mathbf{x})} \ . \tag{22}$$

Lemma 13: $p(\mathbf{x})$ is I-bent$_4$ if there exists one or more partitions, $\mathbf{R_I}, \mathbf{R_H}, \mathbf{R_N}$ such that s' is *flat*, where $|\mathbf{R_I}| < n$. As a generalization of (14), we get flat spectra for one or more partitions $\mathbf{R_I}, \mathbf{R_H}, \mathbf{R_N}$ iff

$$A_{k,\mathbf{R_I},\mathbf{R_H},\mathbf{R_N}} = \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (-1)^{p(\mathbf{x})+p(\mathbf{x}+\mathbf{k})+\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i) k_i (x_i+1)} = 0, \quad \forall \mathbf{k} \neq \mathbf{0} \ ,$$

where $\theta_j = 1$ iff $j \in \mathbf{R_I}$, $\mathbf{r} \preceq \theta$, and $r_j = k_j$ if $j \in \mathbf{R_I}$.

An alternative way to define the I-bent$_4$ property when $p(\mathbf{x})$ is quadratic is via its associated adjacency matrix, Γ. Let $\Gamma_{I,\mathbf{v}}$ be the matrix obtained from $\Gamma_{\mathbf{v}}$ when we erase the i^{th} row and column if $i \in \mathbf{R_I}$.

Lemma 14: For quadratic $p(\mathbf{x})$,

$$p(\mathbf{x}) \text{ is I-bent}_4 \quad \Leftrightarrow \quad \Gamma_{I,\mathbf{v}} \text{ has maximum rank as a binary matrix where, } \mathbf{v} \preceq \bar{\theta} \text{ for one or more choices of } \mathbf{v} \text{ and } \theta, \text{ where } \mathrm{wt}(\theta) < n.$$

In general,

$$p(\mathbf{x}) \text{ is bent} \ \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \ p(\mathbf{x}) \text{ is bent}_4 \ \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \ p(\mathbf{x}) \text{ is I-bent} \ \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \ p(\mathbf{x}) \text{ is I-bent}_4.$$

Theorem 8: All Boolean functions are I-bent$_4$.

Proof: From Theorem 2, the action of a single U_v on a Boolean function, $p(\mathbf{x})$, of any degree, always gives a flat output spectra, for any value of v. This gives (at least) n flat spectra for any Boolean function. ■

Corollary 1: There are no Boolean functions $p(\mathbf{x})$ such that $|P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta}| = 1 \ \forall \theta, \mathbf{c}, \mathbf{k}, \mathbf{r}, \ \mathbf{k}, \mathbf{c} \preceq \bar{\theta}, \mathbf{r} \preceq \theta$.

Proof: Follows from theorem 5 or lemma 12. ■

It is natural to ask whether, for a given quadratic, $p(\mathbf{x})$, there exists at least one member of its LC-orbit which is bent. If so, then we state that the graph state, $p(\mathbf{x})$, and its associated LC-orbit, is *LC-bent*. More formally,

Definition 14: The graph state, $p(\mathbf{x})$ (a quadratic Boolean function), and its associated LC-orbit is *LC-bent* if $\exists \ p'(\mathbf{x})$

such that $p'(\mathbf{x}) \in$ LC-orbit$(p(\mathbf{x}))$, and such that $p'(\mathbf{x})$ is bent.

For example, the bent function $x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3$ is in the same LC-orbit as $x_0x_1 + x_0x_2 + x_0x_3$ so, although $x_0x_1 + x_0x_2 + x_0x_3$ is not bent, it is LC-bent.

In general, for $p(\mathbf{x})$ quadratic,

$$p(\mathbf{x}) \text{ is bent } \begin{array}{c}\Rightarrow \\ \not\Leftarrow\end{array} \quad p(\mathbf{x}) \text{ is LC-bent } .$$

Theorem 9: Not all quadratic Boolean functions are LC-bent.

Proof: By computation, the LC-orbit associated with the $n = 6$-variable Boolean function, $x_0x_4+x_1x_5+x_2x_5+x_3x_4+x_4x_5$ is not LC-bent. ∎

By computation it was found that all quadratic Boolean functions of $n \leq 5$ variables are LC-bent. Table I lists the orbit representatives for those orbits which are not LC-bent, for $n = 2$ to 9, and provides a summary for $n = 10$, where the Boolean functions are presented in algebraic normal form (ANF) and abbreviated so that, say, ab, de, fg is short for $x_ax_b + x_dx_e + x_fx_g$. For those orbits which are not LC-bent we provide the maximum rank satisfied by a graph within the orbit.

n	ANF for the orbit representative	Max. Rank within Orbit
2-5	-	-
6	04,15,25,34,45	4
7	-	-
8	07,17,27,37,46,56,67	6
	06,17,27,37,46,56,67	6
	07,17,25,36,46,57,67	6
	06,17,27,36,45,46,47,56,57,67	6
	07,16,26,35,45,47,67	6
9	08,18,28,38,47,57,67,78	6
	08,18,26,37,47,56,68,78	6
10	08,19,29,39,49,58,68,78,89	6
	51 other orbits	8

TABLE I
REPRESENTATIVES FOR ALL LC-ORBITS WHICH ARE NOT LC-BENT FOR $n = 2$ TO 10

An interesting open problem is to characterise those graphs which are not LC-bent.

V. CONCLUSION

This paper has examined the spectral properties of Boolean functions with respect to the transform set formed by tensor products of the identity, I, the Walsh-Hadamard kernel, H, and the negahadamard kernel, N (the $\{I, H, N\}^n$ transform set). In particular, the idea of a bent Boolean function was generalised to $\{I, H, N\}^n$ and its subsets. Various theorems about the generalised bent properties of Boolean functions were established. It was shown how a quadratic Boolean function maps to a graph and it was shown how the local unitary equivalence of these graphs can be realised by successive application of the LC operation - local complementation - or, alternatively, by identifying a subset of the flat spectra with respect to $\{I, H, N\}^n$. For quadratic Boolean functions it was further shown how the $\{I, H, N\}^n$ set of transform spectra could be characterised by looking at the ranks of suitably modified versions of the adjacency matrix. In part II [45], we apply this method to enumerate the flat spectra w.r.t. $\{I, H\}^n$, $\{H, N\}^n$ and $\{I, H, N\}^n$ for certain concrete functions.

APPENDIX I
VARIOUS INTERPRETATIONS OF THE GRAPH STATES

In this section we summarise the different interpretations of graph states, following [7], [8], [9], [11], [14], [24], [25], [34], [38], [54], [55].

A. Interpretation as a Graph

Given a graph G on n vertices with adjacency matrix Γ, one defines n commuting Pauli operators

$$\begin{aligned} K_{G_j} &= \sigma_x^{(j)} \prod_{k\in\mathcal{N}_j} \sigma_z^{(k)} \\ &= \sigma_x^{(j)} \prod_{k=0}^{n-1} (\sigma_z^{(k)})^{\Gamma_{jk}} \ , \end{aligned} \tag{23}$$

where $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and the superindex (i) implies that the operator has the corresponding matrix on the i^{th} position in the tensor product and the identity elsewhere.

Definition 15: [28] Graph states associated with the n-vertex graph, G, are the set of pure n-qubit quantum states that are stabilized by a stabilizer of hermitian operators, K_G, generated by $\{K_{G_j}, 0 \leq j < n\}$.

It follows that the pure state of n qubits, $|\psi\rangle$, is a graph state iff

$$K_G|\psi\rangle = \pm|\psi\rangle.$$

B. Interpretation as a Quadratic Boolean Function

Theorem 10: [55] (Proposition 2.14). To within normalisation, a graph state can be represented by the pure state $s = (-1)^p$, where p is a quadratic Boolean function such that $p = \sum_{j<k} \Gamma_{jk}x_jx_k + a(\mathbf{x})$, where $a(\mathbf{x})$ is an arbitrary affine Boolean function.

Theorem 11: A pure state s of n qubits is an eigenvector of a stabilizer of hermitian operators K_G, and hence a graph state, iff $s = (-1)^p$, with p a quadratic Boolean function.

Proof: To within normalisation, let $s = m(\mathbf{x})\gamma^{p(\mathbf{x})}$, where γ is a rth complex root of 1, r arbitrary but even, $m : \mathbb{F}_2^n \to \mathbb{Z}$, and $p : \mathbb{F}_2^n \to \mathbb{Z}_r$, such that $s_{\mathbf{i}} = m(\mathbf{x} = \mathbf{i})\gamma^{p(\mathbf{x}=\mathbf{i})}$. We show that no state with non-constant magnitude, m, and/or algebraic degree, p, other than two (i.e. with $\deg(p) \neq 2$) can be an eigenvector for K_G.

Apply K_{G_v} to s. First, w.l.o.g., apply all phase-flips, σ_z, to the neighbours of qubit v to get

$$s' = m(\mathbf{x})\gamma^{p(\mathbf{x})+\frac{r}{2}\sum_k \Gamma_{vk}x_k}.$$

Our question then reduces to: For what states, s', can a subsequent bit-flip to qubit x_v take s' to s'' such that $s'' = \lambda s$, for some scalar coefficient, λ? For the phase part, p can always be written as

$$p(\mathbf{x}) = x_v\mathcal{N}_v(\mathbf{x}) + q(\mathbf{x}),$$

where $q(\mathbf{x})$ and $\mathcal{N}_v(\mathbf{x})$ are independent of x_v. It follows that, considering bit-flip on v, (note that bit-flip is done mod 2 and the result embedded mod r),

$$p(x_0,\ldots,x_v+1,\ldots,x_{n-1}) - p(x_0,\ldots,x_v,\ldots,x_{n-1}) \\ = (1-2x_v)\mathcal{N}_v(\mathbf{x}).$$

We therefore arrive at our first condition:

- $s'' = \lambda s$ iff $(1-2x_v)\mathcal{N}_v(\mathbf{x}) = \frac{-r}{2}\sum_k \Gamma_{vk}x_k + c$, where $c \in \mathbb{Z}_r$. As the right-hand does not depend on x_v, it follows that $2x_v\mathcal{N}_v(\mathbf{x}) = 0$, implying that $\mathcal{N}_v(\mathbf{x})$ is a Boolean function. Moreover, as the right-hand is of degree ≤ 1, then $\deg(\mathcal{N}_v) \leq 1$.

If $m(\mathbf{x})$ is dependent on x_v then $m(\mathbf{x})$ must change after bit-flip on v (the bit positions are permuted); in that case, $\frac{m'}{m}$ cannot be a constant, so s cannot be an eigenvector of K_{G_v}, and therefore cannot be an eigenvector of K_G. Therefore,

- m must be independent of x_v.

By considering the above two conditions over all qubits, v, we conclude that s can only be an eigenvector of K_G if $m(\mathbf{x}) = 1$ and $p(\mathbf{x})$ is quadratic, where the degree-2 monomials in $p(\mathbf{x})$ are uniquely defined by Γ. The coefficients of p are $\frac{-r}{2}$ (but for a constant that can be neglected), and so $\gamma^{p(\mathbf{x})} = (-1)^{p_b(\mathbf{x})}$, with p_b a quadratic Boolean function. The theorem is proved by observing that the set of all simple graphs is as large as the set of all homogenous quadratic functions. ■

C. Interpretation as a Quantum Error Correcting Code

Let E be a $2n$-dimensional binary vector space, whose elements are written as $(a|b)$, where $a,\ b \in \mathbb{F}_2^n$, and E is equiped with the (symplectic) inner product $((a|b),(a'|b')) = a\cdot b' + a'\cdot b$. Define the *weight* of $(a|b) = (a_1,\ldots,a_n|b_1,\ldots,b_n)$ as the number of coordinates i such that at least one of the a_i or b_i is 1. The distance between two elements $(a|b)$ and $(a'|b')$ is defined to be the weight of their difference.

Theorem 12: [11] Let S be a $(n-k)$-dimensional linear subspace of E, contained in its dual $S^\perp$ (with respect to the inner product), such that there are no vectors of weight less than d in $S\backslash S^\perp$. By taking an eigenspace of S (for any chosen linear character) we obtain a quantum error-correcting code mapping k qubits to n qubits that corrects $[(d-1)/2]$ errors. Such a code is called an *additive quantum error-correcting code (QECC)*, and is described by its parameters, $[[n,k,d]]$, where d is the *minimal distance* of the code.

We show, later, that a $[[n,0,d]]$ QECC can be represented by a graph. First we re-express the QECC as a $\mathbb{F}_4$ additive code.

D. Interpretation as a $\mathbb{F}_4$ Additive Code

From [11] we see how to interpret the binary space E as the space $\mathbb{F}_4^n$ and thereby how to derive a QECC from an additive (classical) code over $\mathbb{F}_4^n$. Let $\mathbb{F}_4 = \{0,1,\omega,\bar{\omega}\}$, with $\omega^2 = \omega+1$, $\omega^3 = 1$; and conjugation defined by $\bar{\omega} = \omega^2 = \omega+1$. The *Hamming weight* of a vector in $\mathbb{F}_4^n$, written $wt(u)$, is the number of non-zero components, and the *Hamming distance* between $u,u' \in \mathbb{F}_4^n$ is $\text{dist}(u,u') = wt(u+u')$. Define the *trace function* as: $tr(x) : \mathbb{F}_4 \to \mathbb{F}_2,\ tr(x) = x + \bar{x}$. To each vector $v = (a|b) \in E$ we associate the vector $\phi(v) = a\omega + b\bar{\omega}$. The weight of v is the Hamming weight of $\phi(v)$, and the distance between two vectors in E is the Hamming distance of their images. If S is a subspace of E then $C = \phi(S)$ is a subset of $\mathbb{F}_4^n$ that is closed under addition (defining thus an additive code). The *trace inner product* of $u,v \in \mathbb{F}_4^n$ is

$$u \star v = Tr(u\cdot\bar{v}) = \sum_{i=1}^{n}(u_i\bar{v_i} + \bar{u_i}v_i)\ ,$$

Define the *dual code* $C^\perp$ as

$$C^\perp = \{u \in \mathbb{F}_4^n : u\star v = 0\ \forall v \in C\}\ .$$

Now one can reformulate Theorem 12.

Theorem 13: Let C be an additive self-orthogonal subcode of $\mathbb{F}_4^n$, containing 2^{n-k} vectors, such that there are no vectors of weight $< d$ in $C\setminus C^\perp$. Then any eigenspace of $\phi^{-1}(C)$ is a QECC with parameters $[[n,k,d]]$.

By Glynn (see [24], [25]), we have: Let S be a stabilizer matrix, that is $(n-k)\times n$ over $\mathbb{F}_4$ and such that its rows are $\mathbb{F}_2$-linearly independent. Then we define a QECC with parameters $[[n,k,d]]$ as the set of all $\mathbb{F}_2$-linear combinations of the rows of S. The code is *self-dual* when $k = 0$.

E. The QECC as a Graph via Projective Geometry

Assume that each column of S contains at least two non-zero values, for the columns that do not have this property may be deleted to obtain a better code. Following [24], a self-dual quantum code $[[n,0,d]]$ corresponds to a graph on n vertices, which may be assumed to be connected if the code is indecomposable. Let $\text{PG}(m,q)$ be the finite projective space defined from the vector space of rank $m+1$ over the field $\mathbb{F}_q$. Then the *Grassmannian* of lines of $\text{PG}(n-1,2)$, $G_1(\text{PG}(n-1,2))$, regarded as a variety immersed in $\text{PG}(\binom{n}{2},2)$ is as follows: each line l_i is defined by two points, a_i and b_i. We associate to the set of lines all products $a_ib_j + a_jb_i,\ i \neq j \pmod 2$. Define a mapping from a column of an $n\times n$ stabilizer matrix S over $\mathbb{F}_4$ to a vector of length $\binom{n}{2}$ with coefficients in $\mathbb{F}_2$: We write each column over $\mathbb{F}_4$ as $a + b\omega$, where $a,b \in \mathbb{F}_2^n$.

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \omega \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}\ .$$

Taking all 2×2 subdeterminants found when we put the two vectors into a matrix, we get the points of the Grassmannian. A point in $G_1(\text{PG}(n-1,2)) \equiv$ a line in $\text{PG}(n-1,2) \equiv$ a column of length n over $\mathbb{F}_4$ (with at least two different non-zero components). A quantum self-dual code $[[n,0,d]]$ corresponds to some set of n lines that generate $\text{PG}(n-1,2)$. As each line of $\text{PG}(n-1,2)$ corresponds to a (star) kind of graph, the set corresponds to a graph in n vertices.

F. Interpretation as a Generator Matrix over $\mathbb{F}_2$ and over $\mathbb{F}_4$

From any connected graph we obtain an indecomposable code. Let Γ be the adjacency matrix of a graph G in n variables. Then, $G_T = (I \mid \Gamma)$ (where I is the $n \times n$ identity matrix) is the generator matrix of a binary linear code [54]. In other words,

$$G_T = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & a_{01} & \dots & a_{0n} \\ 0 & 1 & \dots & 0 & a_{01} & 0 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_{0n} & a_{1n} & \dots & 0 \end{pmatrix}$$

generates a code over $\mathbb{F}_2^n$. Alternatively, we can interpret G_T as a generating matrix of an additive code over $\mathbb{F}_4^n$, as follows [11]:

$$G = \Gamma + \omega I = \begin{pmatrix} \omega & a_{01} & \dots & a_{0n} \\ a_{01} & \omega & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & \omega \end{pmatrix}$$

is the generating matrix of an additive code over $\mathbb{F}_4^n$. Different graphs may define the same code, but this relation is 1-1 with respect to LC-equivalence between graphs, as defined in section II. Of the two interpretations, G_T and G, the interpretation using G more precisely reflects the properties of the graph state.

G. Interpretation as a Modified Adjacency Matrix over $\mathbb{Z}_4$

Define from a graph with adjacency matrix, Γ, the generating matrix of an additive code over $\mathbb{Z}_4^n$ as $2\Gamma + I$. This code has the same weight distribution over $\mathbb{Z}_4^n$ as $\Gamma + \omega I$ over $\mathbb{F}_4^n$. Once again, LC-equivalent graphs define equivalent $\mathbb{Z}_4$ additive codes.

H. Interpretation as an Isotropic System

The graph state can also be viewed as an isotropic system (see [7], [9], [8], [14], [34]).

Let A be a 2-dimensional vector space over $\mathbb{F}_2$. For $x, y \in A$, define a bilinear form, $<,>$, by

$$< x, y >= \begin{cases} 1 & \text{if } x \neq y, x \neq 0 \text{ and } y \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

Let V be a finite set. Define the space of $\mathbb{F}_2$-homomorphisms $A^V : V \to A$. Define in this $\mathbb{F}_2$-vector space a bilinear form as:

$$\text{for } \phi, \psi \in A^V, \ < \phi, \psi >= \sum_{v \in V} < \phi(v), \psi(v) > \pmod 2 \ .$$

Definition 16: Let L be a subspace of A^V. Then, $I = (V, L)$ is an *isotropic system* if dim $(L) = |V|$ and $< \phi, \psi >= 0 \ \forall \ \phi, \psi \in L$.

For a graph G, $V(G)$ denotes the set of vertices of G. If $v \in V(G)$, $\mathcal{N}(v)$ denotes the *neighbourhood* of vertex v, that is, the set of all its neighbours. For $P \subseteq V$, we set $\mathcal{N}(P) = \sum_{v \in P} \mathcal{N}(v)$. Let $K = \{0, x, y, z\}$ be the Klein group, which is a 2-dimensional vector space, and set $K' = K \setminus \{0\}$. Note that $x + y + z = 0$.

Lemma 15: ([9]) Let G be a simple graph with vertex set V. Let $\phi, \psi \in K'^V$ such that $\phi(v) \neq \psi(v) \ \forall v \in V$, and set $L = \{\phi(P) + \psi(\mathcal{N}(P)) \ : \ P \subseteq V\}$. Then $S = (V, L)$ is an isotropic system.

The triple $\Pi = (G, \phi, \psi)$ is called a *graphic presentation* of S.

For $\phi \in K^V$, we set $\widehat{\phi} = \{\phi(P) \ : \ P \subseteq V\}$. $\widehat{\phi}$ is a vector subspace of K^V.

Definition 17: For $\psi \in K'^V$, the restricted Tutte-Martin polynomial $m(S, \psi; x)$ is defined by

$$m(I, \psi; x) = \sum (x-1)^{dim(L \cup \widehat{\phi})} \ ,$$

where the sum is over $\phi \in K'^V$ such that $\phi(v) \neq \psi(v), \ v \in V$.

Theorem 14: ([9]) If G is a simple graph and I is the isotropic system defined by a graphic presentation (G, ϕ, ψ), then

$$q(G; x) = m(I, \phi + \psi; x) \ ,$$

where $q(G; x)$ is the interlace polynomial of G.

We mention the interlace polynomial and its relation to our work in [46], [50].

I. Interpretation of a Bipartite Graph State as a Binary Linear Code

Quadratic ANFs, as represented by bipartite graphs, have an interpretation as binary linear codes [38]: Let $\mathbf{T_C}, \ \mathbf{T_{C^\perp}}$ be a bipartite splitting of $\{0, \dots, n-1\}$, and let us 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 $\mathbf{x_{C^\perp}} = \{x_i : i \in \mathbf{T_{C^\perp}}\}$. Let $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, where $\deg(q_k(\mathbf{x_C})) = \deg(r_k(\mathbf{x_{C^\perp}})) = 1 \ \forall k$ (clearly, such a function corresponds to a bipartite graph), and let $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$. Then the action of the transform $\prod_{i \in \mathbf{T}} H_i$, with $\mathbf{T} = \mathbf{T_C}$ or $\mathbf{T_{C^\perp}}$, on $s(\mathbf{x})$ gives $s'(\mathbf{x}) = m(\mathbf{x})$, with m the ANF of a Boolean function. s' is the binary indicator for a binary linear $[n, n - |\mathbf{T}|, d]$ error correcting code. [10]

APPENDIX II
FURTHER SPECTRAL SYMMETRIES OF BOOLEAN FUNCTIONS WITH RESPECT TO $\{I, H, N\}^n$

The *power spectrum* of the WHT of a Boolean function is invariant to within a re-ordering of the spectral elements after an invertible affine transformation of the variables of the Boolean function [11]. This implies that bent Boolean functions remain bent after affine transform. However, the set of $\{I, H, N\}^n$ power spectra are not an invariant of affine transformation.

Let $\mathbf{Q} = \{\mathbf{q}_{II\dots,I}, \mathbf{q}_{HI\dots,I}, \mathbf{q}_{NI\dots,I}, \mathbf{q}_{IN\dots,I}, \dots, \mathbf{q}_{NN\dots N}\}$ be the set of 3^n multi-sets, $\mathbf{q}_{**\dots*}$, where each $\mathbf{q}$ comprises 2^n power spectral values of a length 2^n vector w.r.t. a specific transform in $\{I, H, N\}^n$.

Let $\mathbf{S} = \mathbf{q}_{II\dots,I} \cup \mathbf{q}_{HI\dots,I} \cup \mathbf{q}_{NI\dots,I} \cup \mathbf{q}_{IN\dots,I} \cup \dots, \mathbf{q}_{NN\dots N}$ be the multi-set of $3^n \times 2^n$ power spectral values of a vector,

[10] There is also an equivalent interpretation of bipartite graphs as *binary matroids* (e.g. [12]).

[11] The *power* of the k^{th} spectral element, P_k, is given by $|P_k|^2$, where P_k is defined in (11).

being the union of all multi-sets, $\mathbf{q}$, w.r.t. transforms in the transform set $\{I, H, N\}^n$.

In this section we ascertain for which transformations of the input vector (other than LC), $\mathbf{Q}$ and/or $\mathbf{S}$ are invariant. If $\mathbf{Q}$ is invariant under some transformation of the input vector, then $\mathbf{S}$ is also invariant under the same transformation.

We emphasise that $\mathbf{Q}$ and $\mathbf{S}$, are not ordered, nor do they contain phase information as we are dealing with power values.

The following is clear.

Lemma 16: Let $p(\mathbf{x})$ be a Boolean function of any degree over n variables.
Let $\pi(\mathbf{x}) = (x_{\pi(0)}, x_{\pi(1)}, \ldots, x_{\pi(n-1)})$ be a permutation of Boolean variables, $\mathbf{x}$. Then $\mathbf{S}$ of $(-1)^{p(\mathbf{x})}$ and of $(-1)^{p(\pi(\mathbf{x}))}$ are identical.

From the discussion of sections III-C and III-D it is evident that $\mathbf{S}$ is LC-invariant for a quadratic Boolean function. More generally, we have the following lemma.

Lemma 17: Let $p(\mathbf{x})$ be a Boolean function of any degree over n variables. Let $U \in \mathbf{C}_n$. Then $\mathbf{S}$ of $(-1)^p$ and of $U(-1)^p$ are identical.

We now identify special cases of lemma 17.

Lemma 18: Let $p(\mathbf{x})$ be a Boolean function of any degree over n variables. Then both $\mathbf{Q}$ and $\mathbf{S}$ of $(-1)^{p(\mathbf{x})}$ and of $(-1)^{p(\mathbf{x}+\mathbf{a})}$ are identical, where $\mathbf{a} \in \mathbb{F}_2^n$.

Proof: Replacing x_j with $x_j + 1$ within any $p(\mathbf{x})$ is equivalent to the action of the bit-flip operator, $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, at position j of the transform on $(-1)^{p(\mathbf{x})}$, applying I in all other positions.

From (10), we can rewrite $H\sigma_x$ as $\sigma_z H$. In other words, a bit-flip (or periodic shift) followed by the action of H is identical to the action of H followed by a phase-flip. (This is well-known to quantum code theorists). The final phase-flip is a member of the set $\mathbf{D}_1$ (see Section III) so does not change the magnitude of the spectral values produced by H. Therefore the power spectra produced by H is invariant to prior periodic shift.

We can rewrite $N\sigma_x$ as $-\sigma_y N$. In other words, a bit-flip (or periodic shift) followed by the action of N is identical to the action of N followed by a member of $\mathbf{D}_1$. Therefore the power spectra produced by N is invariant to prior periodic shift.

The above argument is trivial with respect to I. In all three cases, the transform kernel, I, H, or N, remains unchanged after passing the bit-flip through the kernel. So both $\mathbf{Q}$ and $\mathbf{S}$ are invariant to such a transformation. The argument extends naturally to $\{I, H, N\}^n$. ∎

Lemma 19: Let $p(\mathbf{x})$ be a Boolean function of any degree. Then both $\mathbf{Q}$ and $\mathbf{S}$ of $(-1)^{p(\mathbf{x})}$ and of $(-1)^{p(\mathbf{x})+l(\mathbf{x})}$ are identical, where l is any affine Boolean function of its arguments.

Proof: The argument follows similarly to that for lemma 18, by appealing to (10) for a prior phase-flip. ∎

Lemma 20: Let $p(\mathbf{x})$ be a Boolean function of any degree over n variables. The output of p can be lifted to $\mathbb{Z}_4$ by replacing p with $2p$. Let $l(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{Z}_4$ be any generalised affine Boolean function outputting to $\mathbb{Z}_4$, such that 2 does not divide l. Then $\mathbf{S}$ of $i^{2p(\mathbf{x})}$ and of $i^{2p(\mathbf{x})+l(\mathbf{x})}$ are identical, but $\mathbf{Q}$ is not kept invariant.

Proof: The argument follows similarly to those for lemmas 18 and 19, but this time the prior phase-flip is of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pm i \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 1 \\ \pm i & 0 \end{smallmatrix}\right)$. From (10) one can ascertain that the transformations under consideration are in the set $\mathbf{D}''$, and therefore the roles of H and N are swapped when any such transformation is passed through H or N. So $\mathbf{Q}$ is not kept invariant, whilst $\mathbf{S}$ is. ∎

Let $p(\mathbf{x})$ be a Boolean function of *any* degree over n variables. Let us lift p to $\mathbb{Z}_4$. We perform a combination of affine offset and periodic shift on $2p(\mathbf{x})$ by the following operation:

$$2p(\mathbf{x}) \Rightarrow 2p(\mathbf{x} + \mathbf{a}) + \mathbf{c} \cdot \mathbf{x} + d, \qquad (\bmod 4) \ ,$$

where $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{c} \in \mathbb{Z}_4^n$, $d \in \mathbb{Z}_4$, and '$\cdot$' is the scalar product. By lemmas 18, 19, and 20, the resultant function has the same $\mathbf{S}$ as $2p(\mathbf{x})$ mod 4. The symmetries generated by affine offset and periodic shift include the symmetries generated by any combination of certain constaperiodic shifts, because we perform these constaperiodic shifts on $p(\mathbf{x})$ by the following operation:

$$p(\mathbf{x}) \Rightarrow 2p(\mathbf{x} + \mathbf{a}) + \mathbf{c} \cdot \mathbf{x} - \ \mathrm{wt}(\mathbf{c}), \qquad \mathbf{c} \preceq \mathbf{a} \ ,$$

where $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{c} \in \mathbb{Z}_4^n$, '$\mathbf{c} \preceq \mathbf{a}$' means that $c_i = 0$ if $a_i = 0$, $\forall i$ (i.e. a *covers* c), and $\mathrm{wt}(\mathbf{c})$ is the sum of the elements of $\mathbf{c}$, mod 4. The one positions in $\mathbf{a}$ identify variables x_i which are to undergo constaperiodic shift, and the non-zero positions in $\mathbf{c}$ identify the variables x_i which are to undergo periodic, constaperiodic, negaperiodic, or constaperiodic shift if $c_i = 0, 1, 2$ or 3, respectively. The constaperiodic symmetry is induced by $\{H, N\}^n$ and can be generalised to a fixed-constaperiodic symmetry w.r.t. $\{I, H, N\}^n$, where the $\{I, H, N\}^n$ spectra encapsulate the fixed-aperiodic properties of p, as discussed further in [17] and [41].

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers who helped to improve the quality of this manuscript. Thanks also to the reviewer who suggested the remarks leading up to theorem 7.

REFERENCES

[1] M. Aigner and H. van der Holst, "Interlace Polynomials", *Linear Algebra and its Applications*, **377**, pp. 11–30, 2004.
[2] R. Arratia, B. Bollobas, and G. B. Sorkin, "The Interlace Polynomial: a new graph polynomial", *Proceedings of the Eleventh Annual ACM–SIAM Symposium on Discrete Algorithms (San Francisco, CA)*, pp. 237–245, Jan. 2000.
[3] R. Arratia, B. Bollobas, D. Coppersmith, and G. B. Sorkin, "Euler Circuits and DNA Sequencing by Hybridization", *Disc. App. Math.*, **104**, pp. 63–96, 2000.
[4] R. Arratia, B. Bollobas, and G. B. Sorkin, "The Interlace Polynomial of a Graph", *J. Combin. Theory Ser. B*, **92**, 2, pp. 199–233, 2004. http://arxiv.org/abs/math/0209045, v2, 13 Aug. 2004.
[5] R. Arratia, B. Bollobas, and G. B. Sorkin, "Two-Variable Interlace Polynomial", *Combinatorica*, **24**, 4, pp. 567–584, 2004. http://arxiv.org/abs/math/0209054, v3, 13 Aug. 2004.
[6] H. -J. Briegel and R. Raussendorf, "Persistent Entanglement in Arrays of Interacting Particles", *Physical Review Letters*, **86**, 910 2001. http://xxx.soton.ac.uk/pdf/quant-ph/0004051.

[7] A. Bouchet, "Isotropic Systems", *European J. Combin.*, **8**, pp. 231–244, 1987.

[8] A. Bouchet, "Transforming trees by succesive local complementations", *J. Graph Theory*, **12**, pp. 195-207, 1988.

[9] A. Bouchet, "Graphic Presentation of Isotropic Systems", *J. Combin. Theory B*, **45**, pp. 58–76, 1988.

[10] A. Bouchet, "Tutte-Martin Polynomials and Orienting Vectors of Isotropic Systems", *Graphs Combin.*, **7**, pp. 235–252, 1991.

[11] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum Error Correction Via Codes Over GF(4)", *IEEE Trans. on Inform. Theory*, **44**, pp. 1369–1387, 1998, http://xxx.soton.ac.uk/abs/quant-ph/9608006.

[12] P. J. Cameron, "Cycle Index, Weight Enumerator, and Tutte Polynomial", *Electronic Journal of Combinatorics*, **9**, 2, 2002.

[13] C. Carlet, "Two New Classes of Bent Functions", *Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science, Springer-Verlag*, **765**, pp. 77–101, 1994.

[14] B. Courcelle and S. Oum, "Vertex-minors, Monadic Second-order Logic and Seese's Conjecture", *To appear in J. comb. Theory B*, 2006. http://www.labri.fr/perso/courcell/Textes/BC-Oum(2006).pdf.

[15] L. E. Danielsen, "Database of Self-Dual Quantum Codes", *http://www.ii.uib.no/˜larsed/vncorbits/*, 2004.

[16] L. E. Danielsen, "On Self-Dual Quantum Codes, Graphs, and Boolean Functions", *Master's Thesis, University of Bergen*, March, 2005. http://arxiv.org/abs/quant-ph/0503236.

[17] L. E. Danielsen,T. A. Gulliver and M. G. Parker, "Aperiodic Propagation Criteria for Boolean Functions", *Inform. Comput.*, **204**, 5, pp. 741–770, May 2006. http://www.ii.uib.no/˜matthew/apcpaper.pdf.

[18] L. E. Danielsen and M. G. Parker, "Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with respect to the $\{I, H, N\}^n$ Transform", *SETA'04, Sequences and their Applications, Seoul, Proceedings of SETA04, October 2004, Lecture Notes in Computer Science, Springer-Verlag*, LNCS **3486**, pp. 373–388, 2005. http://www.ii.uib.no/˜matthew/seta04-parihn.ps.

[19] L. E. Danielsen and M. G. Parker, "On the classification of all self-dual additive codes over GF(4) of length up to 12",, *Journal of Combinatorial Theory, Series A*, Available online, 10 Jan. 2006, http://arxiv.org/abs/math.CO/0504522.

[20] J. F. Dillon, "Elementary Hadamard Difference Sets", *Ph.D. Dissertation, Univ. Maryland, College Park*, 1974.

[21] H. Dobbertin, "Construction of Bent Functions and Balanced Functions with High Nonlinearity", *Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag* LNCS **1008**, pp. 61–74, 1994.

[22] D. Fon-der-Flaas, "On Local Complementation of Graphs", *A. Hajnal, L. Lovasz, V.T. Sos (Eds.), Combinatorics (Eger, 1987), Colloquia Mathematica Societatis Janos Bolyai, North-Holland, Amsterdam*, **52**, pp. 257–266, 1988.

[23] H. de Fraysseix, "Local Complementation and Interlacement Graphs", *Discrete Math.*, **33**, pp. 29–35, 1981.

[24] D. G. Glynn, "On Self-Dual Quantum Codes and Graphs", *Submitted to the Electronic Journal of Combinatorics*, http://homepage.mac.com/dglynn/quantum_files/Personal3.html, April 2002.

[25] D. G. Glynn, T. A. Gulliver, J. G. Maks and M. K. Gupta, *The Geometry of Additive Quantum Codes - Connections with Finite Geometry*, submitted to Springer-Verlag, 2004.

[26] M. Grassl, A. Klappenecker and M. Rötteler, "Graphs, Quadratic Forms, and Quantum Codes", Proc. IEEE Int. Symp. on Inform. Theory, Lausanne, Switzerland, June 30-July 5, 2002.

[27] M. Grassl, "Bounds on dmin for additive $[[n, k, d]]$ QECC",, http://iaks-www.ira.uka.de/home/grassl/QECC/TableIII.html, Feb. 2003.

[28] M. Hein, J. Eisert and H. J. Briegel, "Multi-Party Entanglement in Graph States", *Phys. Rev. A*, **69**, 6, 2004. http://xxx.soton.ac.uk/abs/quant-ph/0307130.

[29] G. Höhn, "Self-Dual Codes over the Kleinian Four Group", Mathematische Annalen, **327**, pp. 227–255, 2003.

[30] A. Klappenecker and M. Rötteler, "Clifford Codes", Chapter 10, **Mathematics of Quantum Computation**, R. Brylinski, G. Chen (eds.), CRC Press, 2002.

[31] Nils Gregor Leander, "Monomial Bent Functions", *IEEE Trans. Inform. Theory*, **52**, 2, pp. 738–743, Feb. 2006.

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

[33] W. Meier, O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions", *Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag*, LNCS **434**, pp. 549–562, 1990.

[34] J. Monaghan, I. Sarmiento, "Properties of the interlace polynomial via isotropic systems", http://academics.smcvt.edu/jellis-monaghan/#Papers

[35] M. G. Parker, "The Constabent Properties of Golay-Davis-Jedwab Sequences", *Int. Symp. Inform. Theory, Sorrento, Italy*, p. 302, June 25–30, 2000. http://www.ii.uib.no/˜matthew/BentGolayISIT.ps

[36] M. G. Parker, "Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation", *AAECC-14, Nov 26–30, Melbourne, Australia, Lecture Notes in Computer Science,*, LNCS **2227**, pp. 200–209, 2001. http://www.ii.uib.no/˜matthew/NPAutMel4.ps

[37] M. G. Parker, "Quantum Factor Graphs", *Annals of Telecom.*, pp. 472–483, July-Aug 2001, (originally 2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France Sept 4–7, 2000), http://xxx.soton.ac.uk/ps/quant-ph/0010043.

[38] M. G. Parker and V. Rijmen, "The Quantum Entanglement of Binary and Bipolar Sequences", short version in *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science Series, Springer-Verlag, 2001, long version at http://xxx.soton.ac.uk/abs/quant-ph/0107106 or http://www.ii.uib.no/˜matthew/BergDM3.ps, June 2001.

[39] M. G. Parker and C. Tellambura, "A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio", *Technical Report No 242, Dept. of Informatics, University of Bergen, Norway*, http://www.ii.uib.no/publikasjoner/texrap/ps/2003-242.ps, Feb 2003.

[40] M. G. Parker, "Generalised S-Box Nonlinearity", *NESSIE Public Document - NES/DOC/UIB/WP5/020/A*, https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase2/SBoxLin.pdf, 11 Feb, 2003.

[41] M. G. Parker, "Univariate and Multivariate Merit Factors", *Proceedings of SETA04, Lecture Notes in Computer Science,*, LNCS **3486**, pp. 72–100, 2005. http://www.ii.uib.no/˜matthew/seta04-mf.pdf

[42] Laurent Poinsot and Sami Harari, "Generalized Boolean Bent Functions", *INDOCRYPT 2004, Lecture Notes in Computer Science, A. Canteaut and K. Viswanathan (Eds), Springer*, LNCS **3348**, pp. 107–119, 2004.

[43] R. Raussendorf and H. -J. Briegel, "Quantum Computing via Measurements Only", *Phys. Rev. Lett.*, **86**, 5188, 2000, http://xxx.soton.ac.uk/abs/quant-ph/0010033, 7 Oct 2000.

[44] R. Raussendorf, D. E. Browne, and H. -J. Briegel, "Measurement-based quantum computation on cluster states", *Physical Review A*, **68**, 022312 2003. http://xxx.soton.ac.uk/pdf/quant-ph/0301052.

[45] C. Riera, G. Petrides, and M. G. Parker, "Generalised Bent Criteria for Boolean Functions (II)", http://xxx.soton.ac.uk/ps/cs.IT/0502050, 2004.

[46] C. Riera and M. G. Parker, "Spectral Interpretations of the Interlace Polynomial", *Proceedings of the Workshop on Coding and Cryptography (WCC), Bergen*, http://www.ii.uib.no/˜matthew/WCC7.pdf, March 2005.

[47] Constanza Riera and Matthew G. Parker, "One and Two-Variable Interlace Polynomials: A Spectral Interpretation", *accepted for Proceedings of the Workshop on Coding and Cryptography (WCC), WCC2005, Bergen, Lecture Notes in Computer Science, LNCS*, http://www.ii.uib.no/˜matthew/paperwcc4final.pdf October 2005.

[48] Constanza Riera and Matthew G. Parker, "On Pivot Orbits of Boolean Functions", *Optimal Codes and Related Topics, Pamporovo, Bulgaria*, June 2005. http://www.ii.uib.no/˜matthew/octalk4.pdf

[49] Constanza Riera, Lars Eirik Danielsen, and Matthew G. Parker, "On Pivot Orbits of Boolean Functions", *Submitted to Designs, Codes and Cryptography*, http://arxiv.org/math.CO/0604396, April 2006.

[50] C. Riera, "On Spectral Properties of Boolean Functions, Graphs and Graph States", *Ph.D. dissertation, Universidad Complutense de Madrid*, Jan. 2006.

[51] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs", *Phys. Rev. A*, **65**, 2002, http://xxx.soton.ac.uk/abs/quant-ph/0012111, Dec. 2000.

[52] N. J. A. Sloane, "The On-Line Encyclopedia of Integer Sequences", http://www.research.att.com/˜njas/sequences/, 2004.

[53] A. M. Steane, "Introduction to Quantum Error Correction", *Phil. Trans. Roy. Soc. Lond. A*, **356**, pp. 1739–1758, 1997.

[54] V. D. Tonchev, "Error-correcting codes from graphs", *Discrete Math.*, **257**, 2–3, pp. 549–557, 28 Nov. 2002.

[55] M. Van den Nest, "Local Equivalences of Stabilizer States and Codes", PhD thesis, Faculty of Engineering, K.U.Leuven (Leuven, Belgium), May 2005.

[56] M. Van den Nest, J. Dehaene and B. De Moor, "Graphical description of the action of local Clifford transformations on graph states", *Phys. Rev. A*, **69**, 2, 2004. http://xxx.soton.ac.uk/abs/quant-ph/0308151.

[57] Maarten Van den Nest and Bart De Moor, "Edge-local equivalence of graphs", http://uk.arxiv.org/pdf/math.CO/0510246, October, 2005.

[58] D. Schlingemann, "Local Equivalence of Graph States", *R. Werner: Open Problems in Quantum Information Web Page*, http://www.imaph.tu-bs.de/qi/problems/28.html, 2005.
[59] J. Wolfmann, "Difference Sets in $\mathbb{Z}_4^m$ and $\mathbb{F}_2^{2m}$", *Designs, Codes and Cryptography*, **20**, 73-88, 2000.

Constanza Riera is a post-doctoral fellow at the Selmer Center, University of Bergen (Norway). She received a PhD degree in Mathematics from the Universidad Complutense de Madrid (Spain) in 2006. She researches into Boolean functions, graph theory, coding theory, and quantum computation and communication.

Matthew G. Parker has been a researcher at the Selmer Centre, Institute for Informatics, University of Bergen, Norway, since 1998. He received his PhD from the University of Huddersfield, UK, in 1995 and, prior to Bergen, was a researcher with the telecommunications research group at the University of Bradford, UK. His interests include quantum information theory, sequence design, cryptography, coding theory, communications, and combinatorics.