Spectral Interpretations of the Interlace polynomial

Constanza Riera and Matthew G. Parker

Abstract

We relate the *interlace polynomials* of a graph to the spectra of a quadratic boolean function with respect to a strategic subset of local unitary transforms. By so doing we establish links between graph theory, cryptography, coding theory, and quantum entanglement. We establish the form of the interlace polynomial for certain functions, provide a new interlace polynomial, Q_{HN}, and propose a generalisation of the interlace polynomial to hypergraphs. We also prove some conjectures from [13] and equate certain spectral metrics with various evaluations of the interlace polynomial.

I. Introduction

The *interlace polynomial* was introduced by Arratia, Bollobás and Sorkin [2], [3], as a variant of Tutte and Tutte-Martin polynomials [6]. They defined the interlace polynomial of a graph G, $q(G)$, by means of a recurrence formula, involving *local complementation* (LC) of the graph. Aigner and van der Holst, in [1], generalised the concept by means of a related interlace polynomial, $Q(G)$, and they show a new and easier way of constructing both polynomials $q(G)$ and $Q(G)$ using a matrix approach. They conclude that the polynomial $q(z)$, when evaluated at $z = 1$, gives the number of induced subgraphs of G with an odd number of perfect matchings (including the empty set), and that $Q(z)$, when evaluated at $z = 2$, gives the (general) induced subgraphs with an odd number of (general) perfect matchings, "general" meaning here that loops are allowed to be part of the matching.

Define the n vertex graph, G, by its $n \times n$ adjacency matrix, Γ. We identify G with a quadratic boolean function $p(x_0, x_1, \ldots, x_{n-1})$, where $p(\mathbf{x}) = \sum_{i<j} \Gamma_{ij} x_i x_j$ [18]. This identification allows us to interpret $q(G, 1)$ as the number of *flat* spectra of $p(\mathbf{x})$ with respect to (w.r.t.) $\{I, H\}^n$, and $Q(G, 2)$ as the number of flat spectra of $p(\mathbf{x})$ w.r.t. $\{I, H, N\}^n$ (for definitions of $\{I, H, N\}^n$ and 'flat spectra', see the end of this section).

In section III we give an equivalent definition of the interlace polynomial Q using the modified adjacency matrix of the graph that we used to compute the number of flat spectra w.r.t. $\{I, H, N\}^n$ in [18], and use it to compute the interlace polynomial of the clique (complete graph), and clique-line-clique.

In section IV we define a new interlace polynomial, the HN-polynomial, denoted by Q_{HN}, that generalises the number of flat spectra w.r.t. $\{H, N\}^n$ in the same way that the interlace polynomials q and Q do with their respective sets. Our motivation for relating the concept of interlace polynomial to

C. Riera is 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.

M. G. Parker is with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: matthew@ii.uib.no. Web: http://www.ii.uib.no/~matthew/

$\{H, N\}^n$ is that this set is related to the *Peak-to-Average Power Ratio* (PAR) w.r.t. both one and multi-dimensional continous Discrete Fourier Transforms, and hence to problems in Telecommunications and Physics for tasks such as channel-sounding, spread-spectrum, and synchronization [17]. We compute Q_{HN} for the clique, line, and clique-line-clique functions. The polynomial Q_{HN} is also the basis for constructing Q for recursive structures.

By Glynn [10], a self-dual *quantum error correcting code (QECC)* $[[n, 0, d]]$ 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 H give equivalent self-dual quantum codes if and only if H and G are LC-equivalent. H and G also map to GF(4) additive codes with identical weight distributions [7]. As the interlace polynomial, Q, is LC-invariant [1], it is also an invariant of the corresponding QECC. This result implies that Q is invariant under the application of certain *Local Unitary* (LU) *transforms* to an associated multipartite quantum state [16], for it turns out that LC-equivalence for graph states can be characterised by LU-transformation via the set of transforms $\{I, H, N\}^n$ [18]. More generally, an analysis of the spectra of a boolean function provides measures of the *entanglement* of the associated quantum multipartite state which, in the case of a quadratic boolean function, is defined by the QECC (the *graph state*) [18], [16], [12].

In section V we show that the interlace polynomial Q is LC-invariant. We then provide spectral interpretations of the interlace polynomial, and define a generalisation to hypergraphs, i.e. to boolean functions of algebraic degree greater than 2. In [11], [15], the *Multivariate Merit Factor (MMF)* and *Clifford Merit Factor (CMF)* are defined, these being measures of the energy of the boolean function w.r.t. $\{H, N\}^n$ and $\{I, H, N\}^n$ respectively. By proving that the *power spectrum* of a quadratic boolean function w.r.t. $\{I, H, N\}^n$ is always flat or two-valued, we show that MMF and CMF can be derived from Q_{HN} and Q evaluated at $z = 4$. We also prove some conjectures proposed by Parker in [13] related to the line function (path graph) and its affine offsets.

Our spectral approach allows us to interpret the interlace polynomial as a descriptor for some of the spectral characteristics of a Boolean function, with application to classical cryptography - for a block cipher, Q relates to attack scenarios where one has full read/write access to a subset of the plaintext bits and access to all ciphertext bits [8]. The analysis of spectra w.r.t. $\{I, H, N\}^n$ tells us more about the boolean function p than is provided by just the spectrum w.r.t. the Walsh-Hadamard Transform (WHT); for instance, identifying relatively higher generalised linear biases for p [14]. As seen in [18], just the analysis of the flat spectra w.r.t. $\{I, H, N\}^n$ provides a good measure of the 'strength' of the function.

II. Definitions and Notation

We recapitulate here some definition and results of [18]:

Let $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ be the Walsh-Hadamard kernel, $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $i^2 = -1$, the Nega-hadamard kernel, and I the 2×2 identity matrix. A boolean function $p(\mathbf{x}) : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$ is *bent* [19] if $P = 2^{-n/2}(\bigotimes_{i=0}^{n-1} H)(-1)^{p(\mathbf{x})}$ has a *flat* spectrum, or, in other words, if $P = (P_{\mathbf{k}}) \in \mathbb{C}^{2^n}$ is such that $|P_{\mathbf{k}}| = 1 \ \forall \ \mathbf{k} \in \mathrm{GF}(2)^n$, where '$\otimes$' indicates the tensor product of matrices. If the function is quadratic, we associate to it a simple non-directed graph, and in this case a flat spectrum is obtained iff Γ, the adjacency matrix of the graph, has maximum rank mod 2. In [18], we generalised this concept, considering not only the Walsh-Hadamard transform $\bigotimes_{i=0}^{n-1} H$, but the complete set of unitary transforms $\{I, H, N\}^n$, comprising all transforms U of the form

$$U = \bigotimes_{j \in \mathbf{R_I}} I_j \bigotimes_{j \in \mathbf{R_H}} H_j \bigotimes_{j \in \mathbf{R_N}} N_j \ ,$$

where sets $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ partition the set of vertices $\{0, \ldots, n-1\}$ [1].

We studied there the number of flat spectra of a function w.r.t. $\{I, H, N\}^n$, or in other words the number of unitary transforms $U \in \{I, H, N\}^n$ such that $P_U = (P_{U,\mathbf{k}}) \in \mathbb{C}^{2^n}$ has $|P_{U,\mathbf{k}}| = 1 \ \forall \ \mathbf{k} \in \mathrm{GF}(2)^n$, where

$$P_{U,\mathbf{k}} = U(-1)^{p(\mathbf{x})} = (\bigotimes_{j \in \mathbf{R_I}} I_j \bigotimes_{j \in \mathbf{R_H}} H_j \bigotimes_{j \in \mathbf{R_N}} N_j)(-1)^{p(\mathbf{x})} \ . \tag{1}$$

We also considered the number of flat spectra w.r.t. some subsets of $\{I, H, N\}^n$, namely $\{H, N\}^n$ (when $\mathbf{R_I} = \emptyset$) and $\{I, H\}^n$ (when $\mathbf{R_N} = \emptyset$). We proved there that a quadratic boolean function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix, Γ, concretely the matrix resultant of the following actions, has maximum rank mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column of Γ.
- for $i \in \mathbf{R_N}$, we substitute 0 for 1 in position $[i, i]$, i.e. we assign $\Gamma_{ii} = 1$.
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column of Γ unchanged.

As we will see, this modified adjacency matrix is also helpful to compute the interlace polynomial of a graph.

III. The interlace polynomial

We give here a definition of the polynomials q and Q, equivalent to the one offered in [1], that relates the interlace polynomial with the spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

Definition 1: The interlace polynomial q of a graph in n variables is

$$q(z) = \sum_{U \in \{I,H\}^n} (z-1)^{co(\Gamma_U)} \ , \tag{2}$$

[1] For instance, if $n = 4$, $\mathbf{R_I} = \{1\}$, $\mathbf{R_H} = \{0, 3\}$, and $\mathbf{R_N} = \{2\}$, then $U = H \otimes I \otimes N \otimes H$, where U is a 16×16 unitary matrix.

where co(Γ_U) stands for the corank of the modified adjacency matrix of the graph w.r.t. the transform $U \in \{I, H\}^n$, Γ_U, obtained by erasing from the adjacency matrix of the graph the rows and columns whose indices are in $\mathbf{R_I}$:

$$\Gamma = \begin{pmatrix} 0 & a_{01} & \dots & a_{0n} \\ a_{01} & 0 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & 0 \end{pmatrix} \quad \rightsquigarrow \quad \Gamma_U = \begin{pmatrix} 0 & a_{r_0r_1} & \dots & a_{r_0r_k} \\ a_{r_0r_1} & 0 & \dots & a_{r_1r_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r_0r_k} & a_{r_1r_k} & \dots & 0 \end{pmatrix} \quad ,$$

where $\{r_0, \dots, r_k\} = \{0, \dots, n-1\} \setminus \mathbf{R_I}$.

Definition 2: The interlace polynomial Q of a graph in n variables is

$$Q = \sum_{V \in \{I,H,N\}^n} (z-2)^{co(\Gamma_V)} \quad , \tag{3}$$

where $co(\Gamma_V)$ means the corank of the modified adjacency matrix of the graph w.r.t. $V \in \{I, H, N\}^n$, Γ_V, obtained by erasing the rows and columns whose indices are in $\mathbf{R_I}$, as before, and then substituting 0 by $v_i \in$ GF(2) in those indices $i \in \mathbf{R_H} \cup \mathbf{R_N}$, where $v_i = 1$ iff $i \in \mathbf{R_N}$:

$$\Gamma = \begin{pmatrix} 0 & a_{01} & \dots & a_{0n} \\ a_{01} & 0 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & 0 \end{pmatrix} \quad \rightsquigarrow \quad \Gamma_V = \begin{pmatrix} v_{r_0} & a_{r_0r_1} & \dots & a_{r_0r_k} \\ a_{r_0r_1} & v_{r_1} & \dots & a_{r_1r_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r_0r_k} & a_{r_1r_k} & \dots & v_{r_k} \end{pmatrix} \quad ,$$

where $\{r_0, \dots, r_k\} = \{0, \dots, n-1\} \setminus \mathbf{R_I}$.

Lemma 1: For the complete graph (7),

$$Q_{n+1} = 2Q_n + z^n, \ n \geq 2, \ \text{with } Q_1 = z \ ,$$

where Q_k means the interlace polynomial of the clique in n variables. The closed form is $Q_n = 2^{n-1} + 2^{n-1}(z-2) + (z-2)^{-1}(z^n - 2^n)$

Remark: When $z = 2$, we get $(n+1)2^{n-1}$, the number of flat spectra w.r.t. $\{I, H, N\}^n$ [18].

Lemma 2: For the n-clique-line-m-clique (8), when $n, \ m \geq 3$, the interlace polynomial Q is:

$$\begin{aligned} Q &= 2^{n+m-2} - 2^{n+m-4}z + 3 \cdot 2^{n+m-4}z^2 + z^{n-1}2^{m-2}(z-1) + z^{m-1}2^{n-2}(z-1) \\ &+ \frac{3 \cdot 2^{m-1}z + z^{m-1} - 2^m}{z-2}(z^{n-1} - 2^{n-1}) + \frac{3 \cdot 2^{n-1}z + z^{n-1} - 2^n}{z-2}(z^{m-1} - 2^{m-1}) + \\ &+ \frac{z+4}{(z-2)^2}(z^{n-1} - 2^{n-1})(z^{m-1} - 2^{m-1}) \ . \end{aligned}$$

IV. The HN-Interlace Polynomial

We now define an interlace polynomial related to the set $\{H,N\}^n$ as q and Q were related to the sets $\{I,H\}^n$ and $\{I,H,N\}^n$ respectively.

Definition 3: The HN-interlace polynomial for a graph in n variables is

$$Q^n_{HN} = \sum_{W\in\{H,N\}^n} (z-2)^{co(\Gamma_W)} \ , \tag{4}$$

where $co(\Gamma_W)$ means the corank of the modified adjacency matrix of the graph w.r.t. $W\in\{H,N\}^n$, Γ_W, obtained by substituting 0 by $v_i\in \mathrm{GF}(2)$ where $v_i=1$ iff $i\in \mathbf{R_N}$:

$$\Gamma = \begin{pmatrix} 0 & a_{01} & \dots & a_{0n} \\ a_{01} & 0 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & 0 \end{pmatrix} \ \rightsquigarrow \ \Gamma_W = \begin{pmatrix} v_0 & a_{01} & \dots & a_{0n} \\ a_{01} & v_1 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & v_{n-1} \end{pmatrix} \ .$$

Lemma 3: Let G be a graph such that it is the union of two disjoint graphs, G_1 and G_2, in n and m variables respectively. Then, $Q^{n+m}_{HN}(G) = Q^n_{HN}(G_1)Q^m_{HN}(G_2)$.

Proof: w.l.o.g. the adjacency matrix of G, denoted by Γ, will be of type: $\Gamma = \begin{pmatrix} \Gamma_1 & \mathbf{0} \\ \mathbf{0} & \Gamma_2 \end{pmatrix}$, where Γ_1 and Γ_2 are the adjacency matrices of graphs G_1 and G_2, respectively, and $\mathbf{0}$ denotes the zero matrix in the appropiate dimensions. Modifications to Γ that produce $\Gamma_{\mathbf{v}}$ do not alter this shape: $\Gamma_{\mathbf{v}} = \begin{pmatrix} \Gamma_{\mathbf{v},\mathbf{1}} & \mathbf{0} \\ \mathbf{0} & \Gamma_{\mathbf{v},\mathbf{2}} \end{pmatrix}$, where $\Gamma_{\mathbf{v},\mathbf{1}}$ and $\Gamma_{\mathbf{v},\mathbf{2}}$ are the generic modified adjacency matrices of graphs G_1 and G_2, respectively. Therefore the corank of $\Gamma_{\mathbf{v}}$ is just the sum of the coranks of $\Gamma_{\mathbf{v},\mathbf{1}}$ and $\Gamma_{\mathbf{v},\mathbf{2}}$. So, if $Q^n_{HN}(G_1) = \sum_{i=0}^n a_i(z-2)^i$, and $Q^m_{HN}(G_2) = \sum_{j=0}^m b_i(z-2)^j$,

$$\begin{aligned} Q^{n+m}_{HN}(G) &= a_0\sum_{j=0}^m b_j(z-2)^j + a_1\sum_{j=0}^m b_j(z-2)^i(z-2)^{j+1} + \dots + a_n\sum_{j=0}^m b_j(z-2)^{n+j} \\ &= \sum_{i=0}^n a_i(z-2)^i Q^m_{HN}(G_2) = Q^n_{HN}(G_1)Q^m_{HN}(G_2) \ . \end{aligned}$$

■

Remark: In the same way we obtain $q^{n+m}(G) = q^n(G_1)q^m(G_2)$ and $Q^{n+m}(G) = Q^n(G_1)Q^m(G_2)$.

The *line function* (or *path graph*), $p_l(\mathbf{x})$ is defined as

$$p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_jx_{j+1} + \mathbf{c}\cdot\mathbf{x} + d \ , \tag{5}$$

where $\mathbf{x},\ \mathbf{c}\in \mathrm{GF}(2)^n$, $\mathbf{x} = (x_0,\dots,x_{n-1})$, and $d\in\mathrm{GF}(2)$.

Lemma 4: The HN-interlace polynomial for the path graph (5) is

$$Q^{n+1}_{HN} = 2^n - Q^n_{HN}, \text{ with } Q^1_{HN} = z-1 \ .$$

In closed form,

$$Q^n_{HN} = \frac{1}{3}\left(2^n + (-1)^{n-1}\right) z + (-1)^n \ .$$

Proof: The proof for the number of flat spectra w.r.t. the line [18] tells us that,

$$D_n = v_0 D_{n-1} + D_{n-2} \bmod 2 \ , \tag{6}$$

where

$$D_n = \begin{vmatrix} v_0 & 1 & 0 & \dots & 0 \\ 1 & v_1 & 1 & \dots & 0 \\ 0 & 1 & v_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & v_{n-1} \end{vmatrix}$$

is the determinant of the generic modified adjacency matrix of the line on n variables. We will see that if the corank is not 0, it cannot be other than 1, and that, if $D_n = 0$, then $D_{n-1} = 1$. For suppose that $D_n = 0 = D_{n-1}$. Then, by (6), $D_{n-2} = 0$. But $D_{n-1} = v_1 D_{n-2} + D_{n-3}$, so $D_{n-3} = 0$. Similarly, we see that $D_2 = 0 = D_1$. But $D_1 = v_{n-1} = 0$ implies $D_2 = v_{n-1}v_{n-2} + 1 = 1$, so we reach a contradiction. Thus, if $D_n = 0$ (that is, if $\mathrm{co}(\Gamma_{\mathbf{v}}) \neq 0$), then $D_{n-1} = 1$ (that is, $\mathrm{co}(\Gamma_{\mathbf{v}}) = 1$). Therefore the HN-interlace polynomial is $K_n(z-2)^0 + (2^n - K_n)(z-2)^1$, where K_n is the number of flat spectra of the line w.r.t. $\{H, N\}^n$. By [18], $K_n = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$, and the formula follows. ■

The *clique function* (*complete graph*) is defined as:

$$p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j \ , \tag{7}$$

where $\mathbf{x} = (x_0, \dots, x_{n-1}) \in \mathrm{GF}(2)^n$.

Lemma 5: For the complete graph (7),

$$Q^{n+1}_{HN} = Q^n_{HN} + (z-1)^n + (-1)^n(z-3), \text{ with } Q^1_{HN} = z - 1 \ .$$

In closed form,

$$Q^n_{HN} = \begin{cases} 1 + (z-2)^{-1}((z-1)^n - 1), & \text{for } n \text{ even} \\ z - 2 + (z-2)^{-1}((z-1)^n - 1), & \text{for } n \text{ odd} \end{cases}$$

Remark: When $z = 2$, we get $n + \frac{1+(-1)^n}{2}$, the number of flat spectra w.r.t. $\{H, N\}^n$, as seen in [18].

Define the *n-clique-line-m-clique* as

$$p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1}x_n + \sum_{n \le i < j \le n+m-1} x_i x_j \ , \tag{8}$$

where $\mathbf{x} = (x_0, \dots, x_{n+m-1}) \in \mathrm{GF}(2)^{n+m}$

Lemma 6: For the n-clique-line-m-clique (8), the HN-interlace polynomial is, when both n and m are odd:

$$Q_{HN}^{n,m} = 1 + z + \frac{z+1}{(z-2)^2}\left((z-1)^{n-1}-1)((z-1)^{m-1}-1\right) + \frac{z+1}{z-2}\left((z-1)^{n-1}+(z-1)^{m-1}-2\right) \ ;$$

when n is odd and m even:

$$Q_{HN}^{n,m} = 2z-2+\frac{z+1}{(z-2)^2}\left((z-1)^{n-1}-1)((z-1)^{m-1}-1\right)+\frac{2z-2}{z-2}((z-1)^{n-1}-1)+\frac{z+1}{z-2}((z-1)^{m-1}-1) \ ;$$

when n is even and m is odd:

$$Q_{HN}^{n,m} = 2z-2+\frac{z+1}{(z-2)^2}\left((z-1)^{n-1}-1)((z-1)^{m-1}-1\right)+\frac{z+1}{z-2}((z-1)^{n-1}-1)+\frac{2z-2}{z-2}((z-1)^{m-1}-1) \ ;$$

when both n and m are even:

$$Q_{HN}^{n,m} = 4 + \frac{z+1}{(z-2)^2}\left((z-1)^{n-1}-1)((z-1)^{m-1}-1\right) + \frac{2z-2}{z-2}\left((z-1)^{n-1}+(z-1)^{m-1}-2\right) \ .$$

Remark: The result can be summarized as:

$$\begin{aligned} Q_{HN}^{n,m} = & - 2 + 6\chi_n\chi_m + 3\chi_{n+1}\chi_{m+1} + (2 - 2\chi_n\chi_m - \chi_{n+1}\chi_{m+1})z \\ & + \frac{z+1}{(z-2)^2}\left((z-1)^{n-1}-1)((z-1)^{m-1}-1\right) \\ & + \frac{z+1+z\chi_m-3\chi_m}{z-2}((z-1)^{n-1}-1) + \frac{z+1+z\chi_n-3\chi_n}{z-2}((z-1)^{m-1}-1) \ , \end{aligned}$$

where $\chi_k = \dfrac{1+(-1)^k}{2}$.

V. Spectral Interpretations of the Interlace polynomial

As we saw in definition 2 in section III, the interlace polynomial Q is closely related to the set of transforms $\{I, H, N\}^n$. We now give further spectral interpretations of Q. This allows us to extend the concept to hypergraphs (or boolean functions of higher degree than two). Given a graph G with adjacency matrix Γ, its *complement* is defined 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.

Definition 4: The action of *Local Complementation (LC)* (or *vertex-neighbour-complement (VNC)*) on a graph G at vertex v is defined as the graph transformation obtained by replacing the subgraph $G[\mathcal{N}(v)]$ (i.e., the induced subgraph of the neighbourhood of the v^{th} vertex of G) by its complement.

Theorem 1: [1] The interlace polynomial Q is invariant under LC.

Proof: From definition 2 and [18], one can show that Q is invariant w.r.t. $\{I, H, N\}^n$. But, as seen in [18], this set defines the LC operation. ■

Definition 5: [2], [4] The action of *pivot* on a graph, G, at two connected vertices, u and v, (i.e. where G contains the edge uv), is given by $LC(v)LC(u)LC(v)$ - that is the action of LC at vertex v, then vertex u, then vertex v again.

Theorem 2: [2] The interlace polynomial q is invariant under pivot.

Proof: By considering definition 2 it is possible to show that q is invariant w.r.t. $\{I, H\}^n$. One can then show that pivot can be defined by $\{I, H\}^n$. ■

Theorem 3: The corank of the modified adjacency matrix is $\mathrm{co}(\Gamma_U) = \log_2(\max_{\mathbf{k}} |P_{U,\mathbf{k}}|^2)$, where $P_{U,\mathbf{k}}$ are the entries of P_U as defined in (1).

Definition 6: [9] The *Peak-to-Average Power Ratio* of a vector $s \in \mathbb{C}^{2^n}$, with respect to a set of $2^n \times 2^n$ unitary transforms $\mathbf{T}$, is

$$\mathrm{PAR}_{\mathbf{T}}(s) = 2^n \max_{\substack{U \in \mathbf{T} \\ \mathbf{k} \in \mathbb{Z}_2^n}} (|P_{U,\mathbf{k}}|^2), \quad \text{where } P_U = (P_{U,\mathbf{k}}) = Us \in \mathbb{C}^{2^n} \ . \tag{9}$$

Corollary 1: Let $p(\mathbf{x})$ be a quadratic boolean function, and let $s = (-1)^{p(\mathbf{x})}$. Then, by theorem 3, the Peak-to-Average Power Ratio of s, $\mathrm{PAR}_{\mathbf{T}}(s)$ is equal to the maximum degree of the interlace polynomial q, Q_{HN}, or Q, for $\mathbf{T} = \{I, H\}^n$, $\{H, N\}^n$ or $\{I, H, N\}^n$, respectively.

The "GDJ sequences", as defined in [13], can be identified, without loss of generality, with the path graph. Here we use (6) to prove Conjectures 1,2, and 3 of [13]

Lemma 7: (Conjecture 1 of [13]) PAR_H of the path graph is 1.0 for even n and 2.0 for odd.

Proof: By (6), and as in this case $v_i = 0$ for all i, we get that $D_n = D_{n-2}$, mod 2. Expanding, we see that, when n is even, $D_n = D_2 = 1$; when n is odd, $D_n = D_1 = 0$. Now, from the proof of the Q_{HN} of the line (lemma 4), we know that the rank of the matrix cannot be lower than $n - 1$. ■

Lemma 8: (Conjecture 2 of [13]) PAR_N of the path graph is 1.0 for $n \neq 2$ mod 3 and 2.0 for $n = 2$ mod 3.

Proof: From (6), and as in this case $v_i = 1$ for all i, we get that $D_n = D_{n-1} + D_{n-2}$ mod 2. It is clear that $D_1 = 1$, $D_2 = 0$ and $D_3 = D_2 + D_1 = 1$. For $n > 3$, $D_n = D_{n-1} + D_{n-2} = D_{n-2} + D_{n-3} + D_{n-2} = D_{n-3}$. Expanding the argument, when $n = 0$ mod 3, $D_n = D_3 = 1$; when $n = 1$ mod 3, $D_n = D_1 = 1$; when $n = 2$ mod 3, $D_n = D_2 = 0$. ■

Corollary 1: (Conjecture 3 of [13]) From lemmas 7 and 8 it follows that PAR_H and PAR_N of the path graph are both 1.0 for n even, $n \neq 2$ mod 3.

[5], [1] show that $q(-1) = (-1)^r 2^{n-r}$ where r is the rank of $\Gamma + I$. From [18] and this paper it is therefore clear that $\mathrm{PAR}_N(s) = |q(-1)|$ and that, for quadratics, PAR_N is pivot-invariant.

Theorem 4: Let $p(\mathbf{x})$ be a quadratic boolean function. Let $s = (-1)^{p(\mathbf{x})}$, and let $U \in \mathbf{T}$, where $\mathbf{T} = \{I, H, N\}^n$ or one of its subsets. Then, the *power spectrum* $|P_U|^2 = (|P_{U,\mathbf{k}}|^2)$, where $P_U = (P_{U,\mathbf{k}}) = Us \in \mathbb{C}^{2^n}$ is the spectrum of p under U, is either flat (one-valued) or two-valued. Furthermore, if it is two-valued, one of the values is 0 and the other value is equal to $2^{co(\Gamma_U)}$.

Proof: We prove that the power-spectrum is one or two-valued w.r.t. $\{H,N\}^n$ as the case for $\{I,H,N\}^n$ then follows trivially. Firstly, we characterise the possible sets of spectral values produced via the action of the partial transforms $H\otimes I\otimes\cdots\otimes I$ and $N\otimes I\otimes\cdots\otimes I$ on any boolean function. Then we show that, for a quadratic, the subsequent actions of $I\otimes H\otimes\cdots\otimes I$ or $I\otimes N\otimes\cdots\otimes I$ on these partial spectra produce identically-structured sets of values for the power spectra which can be one or two-valued with one value equal to zero. Further action by H or N on the remaining tensor positions leaves the structure of these sets invariant. The evaluation to the corank follows from theorem 3. ■

Definition 7: [11], [15] The *Multivariate Merit Factor (MMF)* and the *Clifford Merit Factor (CMF)* as $\text{MMF}=\dfrac{4^n}{2\sigma}$, and $\text{CMF}=\dfrac{6^n}{2E}$, where

$$2\sigma=\sum_{\substack{U\in\{H,N\}^n\\ \mathbf{k}\in\mathbb{Z}_2^n}}|P_{U,\mathbf{k}}|^4-4^n,\qquad 2E=\sum_{\substack{U\in\{I,H,N\}^n\\ \mathbf{k}\in\mathbb{Z}_2^n}}|P_{U,\mathbf{k}}|^4-6^n\ .$$

Corollary 2: $\text{MMF}=\dfrac{4^n}{2^nQ_{HN}(4)-4^n}$, and $\text{CMF}=\dfrac{6^n}{2^nQ(4)-6^n}$.

Proof: By theorems 3 and 4, and the fact that $\sum_{\mathbf{k}}|P_{U,\mathbf{k}}|^2=2^n$. ■

Remark: In the same way that we obtain the *L_4-norm* of the spectra w.r.t. $\{I,H,N\}^n$ (resp. $\{H,N\}^n$) by evaluating $(2^nQ(4))^{\frac{1}{4}}$, we can obtain the *L_p-norms*, for all $1\le p<\infty$, as $(2^nQ(2^{\frac{p-2}{2}}+2))^{\frac{1}{p}}$. Analogously, we can evaluate the L_p-norms w.r.t. $\{H,N\}^n$ and $\{I,H\}^n$ as $(2^nQ_{HN}(2^{\frac{p-2}{2}}+2))^{\frac{1}{p}}$ and $(2^nq(2^{\frac{p-2}{2}}+1))^{\frac{1}{p}}$, respectively.

Theorem 4, together with theorem 3, tells us that, for quadratics, the interlace polynomial encapsulates much of the information about the spectrum. But for higher degree boolean functions, the number of values of the spectrum grows with the number of variables, and concretely, for each function, with the number of variables we have to fix to get a quadratic function. So, for higher-degree functions, we lose information by just considering the maximum of the spectrum - we require a more detailed generalisation of the interlace polynomial. We defer the complete solution of this problem to future work but offer an initial generalisation to hypergraphs below from which, by theorem 3, we can still compute the number of flat spectra and the PAR:

Definition 8: The *interlace polynomial*[2] of a hypergraph is

$$Q=\sum_{U\in\{I,H,N\}^n}(z-2)^{\log_2(\max_{\mathbf{k}}|P_{U,\mathbf{k}}|^2)}$$

Remark: The generalisation preserves the property $Q(G)=Q(G_1)Q(G_2)$, if G_1 and G_2 are disjoint.

[2]Note that, in general, it will not be really a polynomial, because some of the exponents might be non-integer, and even irrational. In some cases, though, they are rational, so we can, by multiplying by a certain $(z-2)^l$, get a polynomial.

VI. Conclusions

We have shown that the interlace polynomial can be used to summarise many of the spectral properties of quadratic boolean functions with respect to a special subset of tensor transforms. We also derived interlace polynomials for the clique and clique-line-clique functions. We then defined the HN-interlace polynomial, and derived its form for the clique, the line, and the clique-line-clique functions. We proved some conjectures of [13], and presented other spectral interpretations of the interlace polynomial. Finally we generalised the interlace polynomial to hypergraphs.

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", *Proc. 11th Annual ACM-SIAM Symp. on Discrete Math.*, pp. 237–245, 2000.

[3] 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. Preprint: http://arxiv.org/abs/math/0209045, v2, 13 Aug. 2004.

[4] R. Arratia, B. Bollobas and G.B. Sorkin, "Two-Variable Interlace Polynomial", *Combinatorica*, **24**, 4, pp. 567–584, 2004. Preprint: http://arxiv.org/abs/math/0209054, v3, 13 Aug. 2004.

[5] P.N. Balister, B. Bollobas, J. Cutler and L. Pebody, "The Interlace Polynomial of Graphs at -1", *Europ. J. Combinatorics*, **23**, pp. 761–767, 2002.

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

[7] 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, (preprint: http://xxx.soton.ac.uk/abs/quant-ph/?9608006).

[8] L.E. Danielsen,T.A. Gulliver and M.G. Parker, "Aperiodic Propagation Criteria for Boolean Functions," *ECRYPT Document Number: STVL-UiB-1-APC-1.0*, http://www.ii.uib.no/~matthew/GenDiff2.ps, August 2004.

[9] 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, Accepted for Proceedings of SETA04, Lecture Notes in Computer Science, Springer-Verlag, 2005*, http://www.ii.uib.no/~matthew/seta04-parihn.ps, October 2004.

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

[11] T.A. Gulliver and M.G. Parker, "The Multi-Dimensional Aperiodic Merit Factor of Binary Sequences," (preprint), 2003.

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

[13] M. G. Parker, "Constabent Properties of Golay-Davis-Jedwab Sequences", *ISIT2000, Sorrento, Italy*, June, 2000.

[14] 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.

[15] M.G. Parker, "Aperiodic Univariate and Multivariate Merit Factors", *SETA'04, Sequences and their Applications, Seoul, Accepted for Proceedings of SETA04, Lecture Notes in Computer Science, Springer-Verlag, 2005*, http://www.ii.uib.no/~matthew/seta04-parihn.ps, October 2004.

[16] 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/BergDM2.ps, June 2001.

[17] 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.

[18] C. Riera, G. Petrides and M.G. Parker, "Generalised Bent Criteria for Boolean Functions", *Technical Report No 285, Dept. of Informatics, University of Bergen, Norway*, http://www.ii.uib.no/publikasjoner/texrap/pdf/2004-285.pdf, Nov 2004.

[19] O.S. Rothaus, "On Bent Functions", *J. Comb. Theory*, **20A**, pp. 300–305, 1976.