One and Two-Variable Interlace Polynomials: A Spectral Interpretation

Constanza Riera and Matthew G. Parker

Depto. de Álgebra, Facultad de Matemáticas, Universidad Complutense de Madrid, Avda. Complutense s/n, 28040 Madrid, Spain. E-mail: criera@mat.ucm.es
Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. matthew@ii.uib.no
http://www.ii.uib.no/\~{}matthew

Abstract. We relate the one- and two-variable *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 new one and two-variable interlace polynomials, and propose a generalisation of the interlace polynomial to hypergraphs. We also prove conjectures from [15] and equate certain spectral metrics with various evaluations of the interlace polynomial.

1 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 showed 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 number of (general) induced subgraphs with an odd number of (general) perfect matchings, "general" meaning here that loops are allowed to be part of the matching.

In [4], Arratia, Bollobas and Sorkin defined an extension of the interlace polynomial q, defined by themselves in [3], to a new polynomial $q(x, y)$. Here we propose a similar extension of Q as defined by Aigner and Van der Holst in [1] to a new polynomial $Q(x, y)$. We also propose the HN-interlace polynomial Q^{HN} and its corresponding two-variable extension, $Q^{HN}(x, y)$. Also, we define the IN-interlace polynomial $Q^{IN}(x, y)$.

A main goal of this paper is to re-state the problem of constructing an interlace polynomial for a graph as a problem in transform theory. To be precise, the interlace polynomial of a graph summarises the spectra of the *Boolean function*

associated with that graph, where the spectra are computed w.r.t. (with respect to) a certain well-chosen set of *Local Unitary* (LU) transforms. This re-statement allows us to propose new interlace polynomials, as mentioned above, to suggest new applications for these polynomials, and even to extend the problem in a natural way to hypergraphs. We focus on LU transforms which are formed from tensor products of the matrices I, H, and N, where,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \text{is the } \textit{Walsh-Hadamard} \text{ kernel,}$$

$$N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, i^2 = -1, \qquad \text{is the } \textit{Negahadamard} \text{ kernel,}$$

and I is the 2×2 identity matrix.

Definition 1 *The set of 3^n LU transforms, $\{I, H, N\}^n$, is the set comprising all transforms, U, of the form $U = \prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j$, each of size $2^n \times 2^n$, where, say, $V_j = I \otimes \ldots \otimes I \otimes V \otimes I \otimes \ldots \otimes I$, with V in the jth position, '$\otimes$' means the tensor product of matrices, and where the sets $\mathbf{R_I}, \mathbf{R_H}$, and $\mathbf{R_N}$, partition the set of vertices $\{0, \ldots, n-1\}$* [1].

Transform subsets such as $\{I, H\}^n$ ...etc are then defined in the obvious way.

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 $p(\mathbf{x}) = \sum_{i<j} \Gamma_{ij} x_i x_j$ [20]. This identification allows us to interpret $q(G, 1)$ as the number of *flat spectra* of $p(\mathbf{x})$ w.r.t. the transform set, $\{I, H\}^n$, and $Q(G, 2)$ as the number of flat spectra of $p(\mathbf{x})$ w.r.t. the transform set $\{I, H, N\}^n$.

In section 3 we re-define the interlace polynomials q and Q using the modified adjacency matrix of the graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$, respectively, as defined in [20, 21], and use them to compute the interlace polynomial of the clique (complete graph), and clique-line-clique.

In section 4 we define a new interlace polynomial, Q^{HN}, that summarises 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 $\{H, N\}^n$ is that this set is related to the *Peak-to-Average Power Ratio* (PAR) w.r.t. both one and multi-dimensional continuous *Discrete Fourier Transforms*, and hence to problems in telecommunications and physics for tasks such as channel-sounding, spread-spectrum, and synchronization [19]. 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 [11], a self-dual *quantum error correcting code (QECC)* $[[n, 0, d]]$ corresponds to a graph on n vertices, this being a so-called *graph state* [13] 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 if and only

[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.

if they are LC-equivalent [2] (see definition 9). In this case, G 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 LU *transforms* to the multipartite quantum state associated with the QECC [18], for it turns out that LC-equivalence for graph states can be characterised by LU-transformation via the set of transforms $\{I, H, N\}^n$ [20]. Therefore Q can be used to summarise some important properties of an associated quantum graph state. More specifically, an analysis of the spectra of a Boolean function provides measures of *entanglement* of the associated quantum multipartite state, as defined by the QECC and/or its associated quadratic Boolean function [13, 18, 20].

In section 5 we provide spectral interpretations of interlace polynomials, and generalise to hypergraphs, i.e. to Boolean functions of algebraic degree greater than 2. We prove conjectures proposed by Parker in [15] related to the line function (path graph) and its affine offsets. In [12, 17], the *Multivariate Merit Factor (MMF)* and *Clifford Merit Factor (CMF)* are defined, these being inverse 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 one or two-valued, we show that MMF and CMF can be derived from $Q^{HN}(4)$ and $Q(4)$, respectively.

In section 6 we propose the new two-variable interlace polynomial $Q(x, y)$, and derive some lemmas.

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 instance, one often wants to approximate a Boolean function, p, of n variables, by a simpler function. One way to do this is to use an *annihilator* Boolean function, g, such that $gp \approx 0$ or $g(p+1) \approx 0$. A generalisation of this is to look for a function g such that $g(p+a) \approx 0$, where a is a low degree Boolean function. These approximations provide a generalised measure of *probabilistic algebraic immunity* for a function, p. In particular, in the context of transforms w.r.t. $\{I, H\}^n$, with $\mathbf{R_I}$ and $\mathbf{R_H}$ integer sets that partition $\{0, 1, \ldots, n-1\}$, then $g = \prod_{j \in \mathbf{R_I}} (x_j + c_j)$ is a degree $|\mathbf{R_I}|$ Boolean function of $|\mathbf{R_I}|$ variables, $c_j \in$ GF(2), and $a = d + \sum_{j \in \mathbf{R_H}} x_j$ is a degree-one Boolean function of $|\mathbf{R_H}|$ variables, with $d \in$ GF(2). In this case the transform spectra w.r.t. $\{I, H\}^n$ quantify the accuracy of all possible (g, a) pairs of the above form w.r.t. the approximation $g(p + a) \approx 0$. The spectra, in turn, are summarised by the interlace polynomial, q. Similarly, Q can be used to summarise the accuracy of approximations w.r.t. $\{I, H, N\}^n$, where a is now an affine function from $\mathrm{GF}(2)^{|\mathbf{R_H}|+|\mathbf{R_N}|} \to \mathcal{Z}_4$. Q can also be used to assess the block cipher attack scenario where one has full read/write access to a subset of plaintext bits and access to all ciphertext bits [9]. Using similar arguments, Q^{HN} summarises all possible $\mathcal{Z}_4$-linear approximations to a Boolean function, i.e. w.r.t. $\{H, N\}^n$ [16]. Thus, the spectra w.r.t. $\{I, H, N\}^n$ or its subsets tell us more about the Boolean

[2] Referred to as "Vertex-Neighbour-Complementation" (VNC)-equivalent in [11].

function, p, than is provided by just the spectrum w.r.t. the *Walsh-Hadamard transform* (WHT), and such spectra are conveniently summarised by their respective interlace polynomials. As seen in [20], just an enumeration of the flat spectra of a function w.r.t. $\{I, H, N\}^n$ or its subsets provides a good measure of the 'strength' of the function in various contexts.

2 Definitions and Notation

We recapitulate here some definition and results of [20, 21]:

Definition 2 *[23] A Boolean function* $p(\mathbf{x}) : GF(2)^n \rightarrow GF(2)$ *is* bent *iff* $P = 2^{-n/2}(\bigotimes_{i=0}^{n-1} H)(-1)^{p(\mathbf{x})}$ *has a* flat *spectrum, or, in other words, if* $P = (P_{\mathbf{k}}) \in \mathbb{C}^{2^n}$ *is such that* $|P_{\mathbf{k}}| = 1 \ \forall \ \mathbf{k} \in GF(2)^n$.

If the function is quadratic, we associate to it a simple non-directed n-vertex graph, and in this case a flat spectrum is obtained iff Γ, the $n \times n$ adjacency matrix of the graph, has maximum rank mod 2 [14]. In [20], we generalised this concept, considering not only the Walsh-Hadamard transform $\bigotimes_{i=0}^{n-1} H$, but the complete set of unitary transforms w.r.t. $\{I, H, N\}^n$. 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

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

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 maximal 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.

This modified adjacency matrix is also helpful to compute the interlace polynomial of a graph.

3 The interlace polynomial

We define polynomials q and Q, equivalently to definitions offered in [1], but relate the interlace polynomial with the spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

Definition 3 *The interlace polynomial q of a graph G in n variables is*

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

where $co(\Gamma_U)$ 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 $\mathbf{R_I}$ (see [20]).

Remark: $q(G;1)$ is the number of flat spectra of the function w.r.t. $\{I,H\}^n$.

Definition 4 *The* line function *(or* path graph*), $p_l(\mathbf{x})$ is*

$$p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c}\cdot\mathbf{x} + d \ , \tag{3}$$

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

Definition 5 *The* clique function *(*complete graph*) is*

$$p_c(\mathbf{x}) = \sum_{0\le i<j\le n-1} x_i x_j \ , \tag{4}$$

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

Remark: [3] The interlace polynomial q for the path graph satisfies, for $n \ge 2$, $q_n(z) = q_{n-1}(z) + zq_{n-2}(z)$, with $q_1(z) = 1, q_2(z) = 2z$; for the complete graph, $q_n(z) = 2^{n-1}z$.

Definition 6 *The* n-clique-line-m-clique *is*

$$p_{n,m}(\mathbf{x}) = \sum_{0\le i<j\le n-1} x_i x_j + x_{n-1}x_n + \sum_{n\le i<j\le n+m-1} x_i x_j \ , \tag{5}$$

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

We consider the clique-line-clique function to be structurally interesting due to the results on page 31 of [8] which tend to suggest that the best QECCs (and most entangled graph states) have a graph in their LC-orbit which can be described as a *nested-clique graph* - more generally, *nested-regular graph*. So an investigation of the clique-line-clique structure is an attempt to understand these graphical structures more.

Lemma 1 *For the n-clique-line-m-clique (5), $q_n(z) = 3\cdot 2^{n+m-4}z^2 + 2^{n+m-3}z$.*

Definition 7 *The interlace polynomial Q of a graph G in n variables is*

$$Q_n(G;z) = \sum_{V \in \{I,H,N\}^n} (z-2)^{co(\Gamma_V)} \ , \tag{6}$$

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 the diagonal, in those indices $i \in \mathbf{R_H} \cup \mathbf{R_N}$, where $v_i = 1$ iff $i \in \mathbf{R_N}$ (see [20]).

Remark: $Q(G;2)$ is the number of flat spectra of the function w.r.t. $\{I,H,N\}^n$.
Remark: The formula of Q for the path graph is found in [1].

Lemma 2 *For the complete graph (4),*

$$Q_{n+1}(z) = 2Q_n(z) + z^n, \ n \geq 2, \ \textit{with } Q_1(z) = z \ .$$

The closed form is $Q_n = 2^{n-1}(z-1) + (z-2)^{-1}(z^n - 2^n)$.

Remark: When $z = 2$, we get $(n+1)2^{n-1}$, the number of flat spectra for the complete graph w.r.t. $\{I,H,N\}^n$ [21].

Lemma 3 *For the n-clique-line-m-clique (5), when $n,\ m \geq 3$, the interlace polynomial Q is:*

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

4 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 8 *The HN-interlace polynomial for a graph G in n variables is*

$$Q_n^{HN}(G;z) = \sum_{W \in \{H,N\}^n} (z-2)^{co(\Gamma_W)} \ , \tag{7}$$

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 $v_i \in GF(2)$ in the diagonal, in those indices $i \in \mathbf{R_H} \cup \mathbf{R_N}$, where $v_i = 1$ iff $i \in \mathbf{R_N}$ (see [20]).

Remark: $Q^{HN}(G;2)$ is the number of flat spectra of the function w.r.t. $\{H,N\}^n$.

Lemma 4 *The HN-interlace polynomial for the path graph (3) is*

$$Q^{HN}_{n+1}(z) = 2^n - Q^{HN}_n(p_l;z), \text{ with } Q^{HN}_1(p_l;z) = z-1 \ .$$

In closed form,

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

Lemma 5 *For the complete graph (4),*

$$Q^{HN}_{n+1}(z) = Q^{HN}_n(z) + (z-1)^n + (-1)^n(z-3), \text{ with } Q^{HN}_1(z) = z-1 \ .$$

In closed form,

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

Remark: When $z=2$, we get $n + \frac{1+(-1)^n}{2}$, the number of flat spectra for the complete graph w.r.t. $\{H,N\}^n$, as seen in [21].

Lemma 6 *For the n-clique-line-m-clique (5), the HN-interlace polynomial is*

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

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

5 Spectral Interpretations of the One-Variable Interlace Polynomial

In definition 7 in section 3, the interlace polynomial Q was related to the set of transforms $\{I,H,N\}^n$. We now give further spectral interpretations of q, Q, and Q^{HN}. This allows us to extend the interlace 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 9 *[6,11,13] The action of* Local Complementation (LC) *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 7 and [20], one can show that Q is invariant w.r.t. $\{I, H, N\}^n$. But, as seen in [20], this set defines the LC operation.

Definition 10 *[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 3 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 $\{I, H\}^n$ [22].

Theorem 3 *The corank of the modified adjacency matrix is*

$$co(\Gamma_U) = \log_2(\max_{\mathbf{k}} |P_{U,\mathbf{k}}|^2) \ ,$$

where $P_{U,\mathbf{k}}$ are the entries of P_U as defined in (1).

Proof. We prove the theorem for $U \in \{H, N\}^n$, as the case for $U \in \{I, H, N\}^n$ then follows trivially. First, we must recall the autocorrelation of a boolean function $p(\mathbf{x})$ w.r.t $\{H, N\}^n$:

$$A_{\mathbf{k}} = \sum_{\mathbf{x} \in GF(2)^n} (-1)^{p(\mathbf{x})+p(\mathbf{x}+\mathbf{k})+\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i) k_i (x_i+1)} \ ,$$

where $\mathbf{k} = (k_0, k_1, \ldots, k_{n-1}) \in \mathrm{GF}(2)^n$, and $\chi_{\mathbf{R_N}}(i)$ is the characteristic function of $\mathbf{R_N}$, i.e,

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

We use extensively the *Wiener-Kinchine* property

$$\begin{pmatrix} A_{0\ldots0} \\ A_{0\ldots1} \\ \vdots \\ A_{1\ldots1} \end{pmatrix} \begin{array}{c} U \\ \longrightarrow \\ \longleftarrow \\ U^{-1} \end{array} \begin{pmatrix} |P_{0\ldots0}|^2 \\ |P_{0\ldots1}|^2 \\ \vdots \\ |P_{1\ldots1}|^2 \end{pmatrix} \tag{8}$$

Let $\mathrm{co}(\Gamma_U) = c$. Then, from [20], we can deduce that exactly 2^c of the autocorrelation values $A_{\mathbf{k}}$ are different from zero, and furthermore that, for those $\mathbf{k}$'s, $A_{\mathbf{k}} = \pm 2^n$. Clearly, $A_{0\ldots0} = 2^n$.

We differentiate two cases. First, let $U = H \otimes \cdots \otimes H$. Then, in U there always exists a row i with entries in ± 1 ordered in such a way that, when multiplying by $(A_{0\ldots0}, A_{0\ldots1}, \ldots, A_{1\ldots1})^T$, we get $2^{n/2}2^c$. By (8), this is $|P_{\mathbf{k}}|^2$, for some $\mathbf{k}$. Then, after normalization, we get 2^c. Clearly, this value is the maximum value that we can obtain, so the theorem is true for $U = H \otimes \cdots \otimes H$.

Now, let any $U \in \{H, N\}^n$ except $H \otimes \cdots \otimes H$. By (8), we can obtain the autocorrelation vector from the power spectrum as $(A_{0\ldots0}, A_{0\ldots1}, \ldots, A_{1\ldots1})^T = U^{-1}(|P_{0\ldots0}|^2, |P_{0\ldots1}|^2, \ldots, |P_{0\ldots0}|^2)^T$. Because of the shape of N, in U^{-1} half of the rows have purely imaginary entries. Since both the $|P_{\mathbf{k}}|^2$'s and the $A_{\mathbf{k}}$'s are real, we have that the corresponding $A_{\mathbf{k}}$'s must be equal to zero. Trivially, the rows in U^{-1} that have purely imaginary entries correspond to the columns in U with purely imaginary entries, the rest being real. Now, as in the previous case, we can always find a row i such that, when multiplying by $(A_{0\ldots0}, A_{0\ldots1}, \ldots, A_{1\ldots1})^T$, we get $2^{n/2}2^c$, and this is the maximum value we can get.

Definition 11 *[8, 10, 16, 18] The* Peak-to-Average Power Ratio [3] *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*

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

Corollary 1. *Let $p(\mathbf{x})$ be a quadratic Boolean function, and let $s = (-1)^{p(\mathbf{x})}$. Then, by theorem 3, the logarithm (base 2) of the Peak-to-Average Power Ratio of s, $log_2(PAR_{\mathbf{T}}(s))$, is equal to the 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.*

Remark: It follows, trivially, that $\deg(q) \leq \deg(Q)$ and $\deg(Q^{HN}) \leq \deg(Q)$. [4]

Lemma 7 *Let G be a graph which is the union of two disjoint graphs, G_1 and G_2, in n and m variables respectively. Then, $q^{n+m}(G; z) = q^n(G_1; z)q^m(G_2; z)$, $Q^{n+m}(G; z) = Q^n(G_1; z)Q^m(G_2; z)$ and $Q^{HN}_{n+m}(G; z) = Q^{HN}_n(G_1; z)Q^{HN}_m(G_2; z)$.*

It follows from corollary 1 and lemma 7 that PAR is *multiplicative* on the union of disjoint graphs.

The "GDJ sequences", defined in [15], can be identified, without loss of generality, with the path graph. Using a result of [21], we prove Conjectures 1 – 3 of [15].

[3] PAR_{IHN} can be used as a lower bound on PAR_l (where PAR_l is the PAR w.r.t. the infinite set of local unitary transforms - see [8, 18]) and therefore as an upper bound on the *geometric measure* $1 - I^2_{\max}$ (after normalisation), because $\mathrm{PAR}_l = 2^n(1 - I^2_{\max})$. The geometric measure is an *entanglement monotone* for quantum states (see [24, 25])

[4] It also follows from previous comments that $n - \deg(Q)$ can be used as an upper bound on the log form of the geometric measure of quantum entanglement, $E_{\log_2}$, as defined in [24], where $E_{\log_2} \leq n - \deg(Q)$.

Lemma 8 *(Conjecture 1 of [15]) PAR_H of the path graph is 1.0 for even n and 2.0 for odd.*

Proof. The proof for the number of flat spectra w.r.t. the path graph [21] tells us that

$$D_n = v_0 D_{n-1} + D_{n-2} \bmod 2 \ , \tag{10}$$

where D is the determinant of the generic modified adjacency matrix of the line on n variables w.r.t. $\{H, N\}^n$. As in this case $v_i = 0$ for all i, we get that $D_n = D_{n-2}$, mod 2. Expanding for n even, $D_n = D_2 = 1$; for n odd, $D_n = D_1 = 0$. From the proof of Q^{HN} for the path graph (lemma 4), we know that the rank of the matrix cannot be lower than $n - 1$.

Lemma 9 *(Conjecture 2 of [15]) 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 (10), 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 [15]) From lemmas 8 and 9 it follows that PAR_H and PAR_N of the path graph are both* 1.0 *for n even, $n \neq 2$ mod* 3*.*

Lemma 10 *$PAR_N(s) = |q(-1)|$. Furthermore, for quadratics, PAR_N is pivot-invariant.*

Proof. In [5] and [1] it is shown that $q(-1) = (-1)^r 2^{n-r}$, where r is the rank of $\Gamma + I$. From [20] and the results above it follows that $\mathrm{PAR}_N(s) = |q(-1)|$. The last part follows from [22], as we prove there that the pivot orbit lies within $\{I, H\}^n$, and q is invariant w.r.t. this set.

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 transforms H_0 and N_0 on any Boolean function. Then we show that, for a quadratic, the subsequent actions of H_1 or N_1 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 12 *(see [8]) An* independent set (IS) *of a graph G is a subset of the set of vertices V such that no two vertices in the subset are adjoint.*

Lemma 11 *$PAR_{IH} = 2^{\max|IS|}$.*

Proof. $log_2(\mathrm{PAR}_{IH})$ is, as we saw in theorem 3, the maximal value of the corank of the modified adjacency matrix over all transforms in $\{I, H\}^n$. But the corank is maximal when the graph has been completely separated, and its value will tell us the least possible number of fixings we have to do to get a completely disjoint graph. But this is exactly the maximal size independent set, $\max|IS|$, that is, the maximal number of variables that such a graph can have.

Corollary 2. *$deg(q) = \max|IS|$.*

Proof. By corollary 1 and lemma 11.

Furthermore:

Theorem 5 *[8] If the maximum independent set over all graphs in the LC orbit of the graph G has size $\lambda(G)$, then all functions corresponding to graphs in the orbit will have $PAR_{IHN} = 2^{\lambda(G)}$.*

Corollary 3. *$deg(Q) = \lambda(G)$.*

Proof. By corollary 1 and theorem 5.

Definition 13 *[12, 17] The* Multivariate Merit Factor (MMF) *and the* Clifford Merit Factor (CMF) *are $MMF = \dfrac{4^n}{2\sigma}$, and $CMF = \dfrac{6^n}{2E}$, 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 4. *$MMF = \dfrac{4^n}{2^n Q^{HN}(4) - 4^n}$, and $CMF = \dfrac{6^n}{2^n Q(4) - 6^n}$.*

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

σ and E are derived from their respective L_4-norms, (e.g. $\mathrm{L}_4\text{-norm}_{IHN} = (2^n Q(4))^{\frac{1}{4}}$). We can generalise the result to express the L_p norms in terms of the interlace polynomials.

Lemma 12 *The L_p-norms w.r.t. $\{I, H, N\}^n$, $\{H, N\}^n$, and $\{I, H\}^n$ for all $1 \leq p < \infty$, are,*

$$\begin{aligned} L_p\text{-}norm_{IHN} &= (2^n Q(2^{\frac{p-2}{2}} + 2))^{\frac{1}{p}}, \\ L_p\text{-}norm_{HN} &= (2^n Q^{HN}(2^{\frac{p-2}{2}} + 2))^{\frac{1}{p}} \\ L_p\text{-}norm_{IH} &= (2^n q(2^{\frac{p-2}{2}} + 1))^{\frac{1}{p}}, \end{aligned}$$

respectively.

Theorem 4, together with theorem 3, tell us that, for quadratics, the interlace polynomial encapsulates much of the information about the spectrum. But for higher degree Boolean functions (i.e. hypergraphs), 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, and that preserves the property $Q(G) = Q(G_1)Q(G_2)$, if G_1 and G_2 are disjoint hypergraphs:

Definition 14 *The* interlace polynomial[5] *of a hypergraph is*

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

6 Two-variable Interlace Polynomials

6.1 Interlace Polynomial $q(x, y)$

We offer a definition of $q(x, y)$ equivalent to the one proposed in [4]:

Definition 15 *The 2-variable interlace polynomial $q(G; x, y)$ of a graph G in n variables is defined as*

$$q(G; x, y) = \sum_{U \in \{I,H\}^n} (x-1)^{rk(\Gamma_U)} (y-1)^{co(\Gamma_U)} \quad , \tag{11}$$

where $co(\Gamma_V)$ and $rk(\Gamma_V)$ stand respectively for corank and rank 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 $\mathbf{R_I}$ (see definition 3).

Remark: $q(2, y) = q(y)$. Therefore, $\deg(q(2, y)) = log_2(\mathrm{PAR}_{IH})$.

Lemma 13 *$q(x, 1)$ gives the number of flat spectra of the function w.r.t. $\{I, H\}^n$ partitioned according to their weight in I's. Furthermore, $n - deg(q(x, 1))$ is the least number of fixings that we have to do to get a flat spectrum.*

Proof. From the definition

$$q(x, 1) = \sum_{U, co(\Gamma_U)=0} (x-1)^{rk(\Gamma_U)} \quad .$$

Now, when $co(\Gamma_U) = 0$, it is clear that the matrix has full rank, and therefore that $rk(\Gamma_U) = n - |R_{\mathbf{I}}|$. Thus, $q(x, 1)$ tells you where to locate the flat spectra, and the degree is maximal when the number of fixings is minimal.

[5] 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.

Lemma 14 *$q(1,y)$ gives the number of independent sets partitioned according to their size (i.e. according to their weight in I's). Furthermore, $deg(q(1,y))$ gives the maximal size of an independent set.*

Proof.

$$q(1,y) = \sum_{U, rk(\Gamma_U)=0} (y-1)^{co(\Gamma_U)} \ .$$

But the only subgraph such that $rk(\Gamma_U) = 0$ is the empty graph. Thus, $q(1,y)$ tells us how to separate totally the graph and how many fixings we have to make to do so, and as $co(\Gamma_U) = n - |R_{\mathbf{I}}|$, the degree of $q(1,y)$ tells us the least number of fixings we have to do to get a completely disjoint graph; i.e., how many variables can have such a graph.

Lemma 15 *$deg(q(2,y)) = deg(q(1,y))$.*

Proof. As can be deduced from [4], the degree of $q(1,y)$ is equal to $\max|IS|$. The lemma follows by taking into account lemma 11.

Remark: $q(x,y)$ gives us the bentness of the function. That is, if x^n appears in $q(x,y)$, then the function is bent. Otherwise, it is not bent.

Lemma 16 *The following equality holds:*

$$q_x(G;1,1) = \#\{U : rk(\Gamma_U) = 1, co(\Gamma_U) = 0\} = 0 \ ,$$

where the subindex means derivative w.r.t. x.

Proof. The first equality follows trivially. The second equality follows from the fact that $rk(U) + co(U) = dim(U)$, and that any modified adjacency matrix (w.r.t. $\{I,H\}^n$) of dimension 1 is the 1×1 matrix (0), which has rank 0 and corank 1.

6.2 Interlace Polynomial $Q(x,y)$

Definition 16 *The 2-variable interlace polynomial $Q(G;x,y)$ of a graph G in n variables is defined as*

$$Q(G;x,y) = \sum_{V \in \{I,H,N\}^n} (x-2)^{rk(\Gamma_V)}(y-2)^{co(\Gamma_V)} \ , \tag{12}$$

where $co(\Gamma_V)$ and $rk(\Gamma_V)$ stand respectively for the corank and rank 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 $i \in \mathbf{R_N}$ (see definition 7).

Remark: $Q(3,y) = Q(y)$ as defined in (6).

Lemma 17 $Q(2,y) = q(1,y-1)$.

Proof. Clearly,

$$Q(2,y) = \sum_{V, rk(\Gamma_V)=0} (y-2)^{co(\Gamma_V)} \ .$$

The only subgraph such that $rk(\Gamma_V) = 0$ is the empty graph. Moreover, $rk(\Gamma_V) = 0$ iff $\mathbf{R_N} = \emptyset$. Thus, $Q(2,y) = \sum_{V \in \{I,H\}^n, rk(\Gamma_V)=0} (y-2)^{co(\Gamma[S])} = q(1,y-1)$.

Lemma 18 *The following equalities hold:*

$$Q_x(G;2,2) = \#\{V : rk(\Gamma_V) = 1, co(\Gamma_V) = 0\} = n \ ,$$
$$Q_{x,y}(G;2,2) = \#\{V : rk(\Gamma_V) = 1, co(\Gamma_V) = 1\} = \#edges = \#\ terms\ p(\mathbf{x}) \ ,$$

where the subindex means derivative w.r.t. the corresponding variable.

Proof. For both equations, the first equality follows trivially. For the first equation, the second equality comes from the fact that the modified adjacency matrix cannot have rank 1 and corank 0 unless in the case $V = N_j$ for some j, so there are n possibilities. For the second equation, as all the modified adjacency matrices are symmetric, then both the rank and the corank being 1 can only happen in the case $\Gamma_V = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$; that is, when $V = N_i N_j$ for each edge ij. Now, the number of edges is precisely the number of terms of the quadratic boolean function $p(\mathbf{x})$.

7 Conclusions

We have shown that one and two-variable interlace polynomials 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 [15], and presented other spectral interpretations of the interlace polynomial. We also 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. http://arxiv.org/pdf/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. http://arxiv.org/pdf/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, http://xxx.soton.ac.uk/pdf/quant-ph/?9608006.
8. L. E. Danielsen, "On Self-Dual Quantum Codes, Graphs, and Boolean Functions," *Master's Thesis*, Selmer Centre, Inst. for Informatics, University of Bergen, Bergen, Norway, March 2005. http://arxiv.org/pdf/quant-ph/0503236.
9. L. E. Danielsen, T. A. Gulliver and M. G. Parker, "Aperiodic Propagation Criteria for Boolean Functions," *Accepted for Inform. Comput.*, Sept. 2005. http://www.ii.uib.no/ matthew/apcpaper.pdf.
10. 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, Lecture Notes in Computer Science, LNCS 3486, 2005. http://xxx.soton.ac.uk/ps/cs.IT/0504102.
11. 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.
12. T. A. Gulliver and M. G. Parker, "The Multivariate Merit Factor of a Boolean Function", IEEE ITSOC Information Theory Workshop 2005 on Coding and Complexity, Rotorua, New Zealand, 29th Aug. - 1st Sept., 2005. http://www.ii.uib.no/~matthew/NZRecursionsCamera1.pdf.
13. 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/pdf/quant-ph/0307130.
14. F. J. MacWilliams and N. J. A. Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, 1977.
15. M. G. Parker, "Constabent Properties of Golay-Davis-Jedwab Sequences", *ISIT2000, Sorrento, Italy*, June, 2000. http://www.ii.uib.no/~matthew/BentGolayISIT.ps.
16. 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.
17. M. G. Parker, "Univariate and Multivariate Merit Factors", *SETA'04, Sequences and their Applications, Seoul, Proceedings of SETA04, Lecture Notes in Computer Science, LNCS 3486, Springer-Verlag, 2005*, http://www.ii.uib.no/~matthew/seta04-mf.pdf.
18. 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/ps/quant-ph/?0107106 or http://www.ii.uib.no/~matthew/BergDM3.ps, June 2001.
19. 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.

20. C. Riera and M. G. Parker, "Generalised Bent Criteria for Boolean Functions", accepted for IEEE Trans Inform. Theory, July, 2005. http://xxx.soton.ac.uk/pdf/cs.IT/0502049.
21. C. Riera, G. Petrides and M. G. Parker, "Generalised Bent Criteria for Boolean Functions (II)". http://xxx.soton.ac.uk/pdf/cs.IT/0502050.
22. C. Riera and M. G. Parker, "On Pivot Orbits of Boolean Functions", *Proceedings of the Fourth International Workshop on Optimal Codes and Related Topics (OC 2005), Pamporovo, Bulgaria*, June 2005. http://www.ii.uib.no/ matthew/octalk4.ps.
23. O. S. Rothaus, "On Bent Functions", *J. Comb. Theory*, **20A**, pp. 300–305, 1976.
24. T. Wei, M. Ericsson, P. M. Goldbart, and W. J. Munro, "Connections between relative entropy of entanglement and geometric measure of entanglement", *Quantum Information and Computation*, **4**, pp. 252–272, 2004. http://xxx.soton.ac.uk/pdf/quant-ph/0405002.
25. T. Wei, and P. M. Goldbart, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states", *Physical Review*, **A 68**, 2003. http://xxx.soton.ac.uk/pdf/quant-ph/0307219.