Spectral Properties of Boolean Functions, Graphs and Graph States

Constanza Riera

December 9, 2005

Acknowledgements

I feel that I have to thank a lot of people, but I cannot list them all here. Nevertheless, I want to express my warmest thanks to some of them.

Tusen takk til Tor Helleseth og Matthew G. Parker. I would like to gratefully acknowledge their support, encouraging and understanding. Thanks for helping me to come back to Bergen as often as I did, and making me feel at home in Bergen. I owe a lot to you, both at a scientific and a personal level. I'm very grateful to Matthew for his enthusiasm, for sharing his knowledge with me, and for providing me a fascinating subject of research, and also for his sense of humour. Agradezco también la ayuda y la formación que me proporcionó mi director Ignacio Luengo, que me acogió como alumna y me dio la oportunidad de descubrir el mundo de los códigos y la criptografía, y de quien partió la idea de enviarme a Bergen.

I wish to thank my colleagues and friends, both at Selmersenteret in the Universitetet i Bergen and at the Universidad Complutense de Madrid, for their friendship and for providing a stimulating and fun environment to work in; especially, I'd like to thank Ángel, John Erik, Helena, Giorgos, Mikael, Marion, Hans Georg, Eirik, Qingshu, Manuel, Sofía, Eva, Jorge, Johannes, Miguel, Antonio, Håvard, Enrique, Lars Eirik, Pål and so many others... Takk til alle! I'd also like to thank Dragan for all his help in research and many other things, and to my previous colleagues and friends at the Universidad Autónoma de Madrid, not to forget Orlando, who encouraged me to start a master in Mathematics. Special thanks to Marian for all her help.

I want to thank all those who have put up with my drifting a long way away from my original thesis subject.

Gracias a mi familia por su apoyo y su paciencia, y a mis amigos en Bergen y Madrid: Dag, Mariángel, Marina, Rocío, Juliane, Kåre, Cachi, Alberto, Rolf, Patricia, Diana, Jens, Jesús, Iván, Álex...

Thanks also to the program of F.P.U. (Formación del Profesorado Universitario) grants of the Spanish Government, and the Marie Curie Training Site (FASTSEC) in Bergen, for financial support during my PhD.

Abstract

Generalisations of the *bent* property of a Boolean function are presented, by proposing spectral analysis of the Boolean function 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 some graph transforms can be found within the spectra of certain unitary transform sets. The *flat spectra* of a quadratic Boolean function with respect to those transforms are related to modified versions of its associated *adjacency matrix*. The flat spectra of concrete recursive structures are found using this method. We derive a spectral interpretation of the *interlace polynomials* (in one or two variables) of a graph and we relate to one of them a quantum measure of entanglement of the associated *quantum state*. We characterise the values of the spectra of a quadratic Boolean function. We give a formula for the *weight hierarchy* for a binary linear code in terms of a modified interlace polynomial. We derive as well a spectral interpretation of the *pivot* operation on a graph and generalise this operation to hypergraphs. We enumerate the number of inequivalent pivot orbits for small numbers of vertices. We also construct a family of Boolean functions of degree higher than two with a large number of flat spectra with respect to the $\{I, H\}^n$ set of transforms, and compute a lower bound on this number. We show how to change the degree of a Boolean function via pivot operation. Finally, we give concrete formulae for the spectra of a wide range of vectors with respect to well-chosen transforms sets.

Contents

Chapter 1

Introduction

There are many equivalences between subjects laying in different fields, and it is always interesting to connect and exploit them. This thesis deals with objects belonging to different areas of research, such as Boolean functions, cryptography, graphs, classical and quantum error-correcting codes, quantum information theory and linear algebra, and their connections. While some of these relationships are known, others will be established for the first time in this thesis. The main idea behind our work is to explicitly state relationships between objects so that we can make use of techniques in the associated fields.

The areas discussed in this thesis have received a lot of attention recently. *Boolean functions*, for instance, are of great interest to cryptographers, since they can be used, among other purposes, to add non-linearity to systems based on *stream ciphers*, or to analyse and construct *S-boxes* in block ciphers. For stream cipher-based systems a high degree Boolean function is usual, but for other systems like *HFE* [70] the functions used are quadratic. Recently, so-called *generalised Boolean functions* have been employed for *wireless communication*, concretely for *OFDM (Orthogonal Frequency Division Multiplexing)*[22, 23] systems.

Recent applications of *graph theory* are for instance DNA sequencing by hybridization [3, 2], and the distributed networks in wireless communication. As we shall see, there is a close relationship between *non-directed simple graphs* and *quadratic Boolean functions*. In the same way, *hypergraphs* can be constructed from Boolean functions of degree higher than two. Non-directed simple graphs are used as well to define a certain type of *quantum*

state, namely *graph states*[93], of great relevance for the construction of *quantum error-correcting codes (QECCs)*. Some graph operations such as *Local Complementation* play an important role in the study of *local equivalence* of pure quantum states.

In modern communication, *error-correcting codes* play a very important role. Nowadays more than ever, information must be both fast and reliable, so one must guarantee that communications systems can detect and correct as many errors as possible. In this thesis, we shall deal mainly with *binary linear error-correcting codes*, though as can be seen in the interpretation of *graph states* (see chapter 10) the objects presented here are also directly related with *GF(4) additive error-correcting codes*. One important concept for the study of binary linear codes is the *weight hierarchy* for a binary linear code, and we shall see how it can be computed from the study of the graph associated to the code.

There has recently been a lot of interest in *quantum information theory (QIT)* and concretely in *quantum computing*, especially since the discovery of *Shor's algorithm* [85], which can factor an integer in polynomial time, and thus, in theory, break the *RSA* cryptographic system. For the time being, practical quantum computers have not yet been built, but the construction of *quantum error-correcting* codes is already an active area of research in the field. The classification of such codes is of great importance, and the study of the graphs associated to them can yield such a classifying method (see for instance [27]).

Turning now to the last subject, *linear algebra* is a classical area of research, and is mainly used here as a tool. As we point out here, talking about a non-directed simple graph is the same as talking about a symmetric binary matrix, the *adjacency matrix* of the graph. In this thesis, we shall relate a modification of this matrix with some graph invariants, such as the *interlace polynomials* [2, 1, 5], as well as with spectral properties of the quadratic Boolean function associated to the graph. This modification of the adjacency matrix will depend on a set of transforms, the set $\{I, H, N\}^n$ (definition 2.1).

As we shall show, the values of the autocorrelation of the associated Boolean function with respect to $\{I, H, N\}^n$ will be highly related to the corank of the modified adjacency matrix of the graph.

We shall work mainly with the following equivalent interpretations of a quadratic Boolean function, $p(\mathbf{x}) : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$, in n variables:

- Algebraic Normal Form (ANF): $p(\mathbf{x}) = \sum_{0 \le i < j \le n-1} a_{ij} x_i x_j$, with $a_{ij} \in \{0, 1\}$.
- Graph: Define G as:
  - Vertices: $\{0, \cdots, n-1\}$
  - Edges: There is an edge between i and j iff $a_{ij} = 1$
- Matrix: The *adjacency matrix* Γ of G is defined as:
  - $\Gamma(i, j) = \Gamma(j, i) = a_{ij},\ i < j$, $\Gamma(i, i) = 0$
- Generator matrix for a GF(4)-additive code:
  - $M(i, j) = M(j, i) = a_{ij},\ i < j$, $M(i, i) = \omega$, where $\omega \in$ GF(4)$= \{0, 1, \omega, \bar{\omega}\}$
- The variables $x_0, \ldots, x_{n-1}$ can be seen as n qubits, whose state is fully entangled if the graph G is connected. From M, we can get an additive Quantum Error Correcting Code (QECC), by taking the GF(2)-linear combinations of the rows.

The equivalences between these objects are developed in the thesis. As a preface, we now offer some background on the different areas involved:

Remark: Definitions of most of the terms used here can be found in chapter 2.

1.1 The Cryptographic Context

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. To be precise, define the Boolean function of n variables $p : \text{GF}(2)^n \to \text{GF}(2)$, and the WHT by the $2^n \times 2^n$ unitary matrix $U = H \otimes H \ldots \otimes H = \bigotimes_{i=0}^{n-1} H$, where the *Walsh-Hadamard kernel* $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, '$\bigotimes$' indicates the tensor product of matrices, and unitary means that $UU^\dagger = I_n$, where '$\dagger$' means transpose-conjugate and I_n is the $2^n \times 2^n$ identity matrix. We further define a length 2^n vector, the *bipolar vector* of the function, as $s = (s_{0\ldots00}, s_{0\ldots01}, s_{0\ldots11}, \ldots, s_{1\ldots11})$ such that $s_{\mathbf{i}} = (-1)^{p(\mathbf{i})}$, where $\mathbf{i} \in \text{GF}(2)^n$. 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 $\mathbf{k} \in \mathrm{GF}(2)^n$.

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 as far away as it can be from the affine functions [57], which is a desirable cryptographic design goal. It is an open problem to classify all bent Boolean functions, although many results are known [32, 53, 21, 34].

Functions with a flat WHT spectrum are crucial in the design of cryptosystems to avoid *linear cryptanalysis*. This type of attack was first devised by Matsui and Yamagishi [55] in an attack on FEAL, and extended by Matsui [54] to attack *DES*. It is a known plaintext/ciphertext attack, meaning that the attacker must be able to obtain encrypted ciphertexts for some set of plaintexts of his choosing. The idea as conceived by Matsui is based on finding affine approximations to the action of a cipher, and attempting to recover key bits by approximating core rounds of the block cipher by a series of binary linear expressions, and then concatenating these linear approximations. The block cipher to be approximated is parameterised by a secret key which is typically added into the cipher by means of XOR. If this is the case, then the binary linear approximation to the block cipher core is key-invariant to within a global constant[1]. If the spectrum w.r.t. WHT is not flat, the probability that the approximation is correct will be biased (that is, $\frac{1}{2} \pm \epsilon$), and then, given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained. Increased amounts of data will usually give a higher probability of success. Attacks using linear cryptanalysis have been developed for block ciphers and stream ciphers.

There have been a variety of enhancements and improvements to the basic attack. Langford and Hellman [52] introduced an attack called differential-linear cryptanalysis, combining elements of differential cryptanalysis (see below) with those of linear cryptanalysis. Also, Kaliski and Robshaw [48] showed that a linear cryptanalytic attack using

[1] If some subsets of the key bits are not added using XOR, then this subset is often taken to be fixed, so that a complete linear approximation can be established that holds for a subset of all possible key configurations.

multiple approximations might allow for a reduction in the amount of data required for a successful attack. Other issues such as protecting ciphers against linear cryptanalysis have been considered by Nyberg [61], Knudsen [50], and O'Conner [63].

The autocorrelation of the function w.r.t. the WHT is used for *differential cryptanalysis*. This is a type of attack applicable primarily to iterative block ciphers, but also to stream ciphers and cryptographic hash functions. The technique of differential cryptanalysis was first introduced by Murphy [59] in an attack on FEAL-4, but was later improved and perfected by Biham and Shamir [11, 12] who used it to attack DES. Differential cryptanalysis is basically a chosen plaintext attack (there are, however, extensions that would allow a known plaintext or even a ciphertext-only attack) and relies on an analysis of the evolution of the differences between two related plaintexts as they are encrypted under the same key. By careful analysis of the available data, probabilities can be assigned to each of the possible keys and eventually the most probable key is identified as the correct one.

Differential cryptanalysis has been used against a great many ciphers with varying degrees of success. In attacks against DES, its effectiveness is limited by what was very careful design of the S-boxes during the design of DES [24]. Studies on protecting ciphers against differential cryptanalysis have been conducted by Nyberg and Knudsen [62] as well as Lai, Massey and Murphy [51]. Differential cryptanalysis has also been useful in attacking other cryptographic algorithms such as hash functions, as shown by Wang and Yu [95].

The analysis of spectra w.r.t. $\{I, H, N\}^n$ tells us more about $p(\mathbf{x})$ than is provided by the spectrum w.r.t. the WHT; for instance, the analysis of the spectra w.r.t. $\{I, H\}^n$ is related to a probabilistic version of the so-called algebraic immunity [56], as it identifies the linear or affine approximations to a Boolean function after fixing some of the variables (that is, taking $x_i = 0$ or 1 for some i). More generally, $\{I, H, N\}^n$ can improve linear cryptanalysis by identifying relatively high generalised linear biases for p as proposed by Parker [69, 28], using not only binary linear approximations but linear approximations over any weighted alphabet. In [28], Danielsen, Gulliver and Parker propose a generalised differential cryptanalysis based on the set $\{I, H, N\}^n$. 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, using as in [69] not only binary linear approximations but approximations over more general alphabets (see [28] for more details).

In chapter 3, our aim is to introduce new generalised bent criteria. In chapter 4, we enumerate the flat spectra w.r.t. $\{I, H, N\}^n$ and its subsets of some structures such as the *line*, the *clique* and the *clique-line-clique*.

Remark: A row of $U_0 \otimes U_1 \otimes \ldots \otimes U_{n-1}$ for U_i a 2×2 unitary matrix can always be written as $u = (a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})$, where a_i, b_i are complex numbers. For α an r^{th} complex root of 1, we can approximate an unnormalised version of u by $u \simeq m(\mathbf{x})\alpha^{p(\mathbf{x})}$, for some appropriate choice of integers s and r, where $m : \mathrm{GF}(2)^n \to \mathrm{GF}(s)$, $p : \mathrm{GF}(2)^n \to \mathrm{GF}(r)$, and $\mathbf{x} \in \mathrm{GF}(2)^n$, such that the $\mathbf{j}^{th}$ element of u, $u_{\mathbf{j}} = m(\mathbf{j})\alpha^{p(\mathbf{j})}$, where $\mathbf{j} \in \mathrm{GF}(2)^n$ and $u_{\mathbf{j}}$ is interpreted as a complex number.

Definition 1 *[67] In the context above, when u is fully-factorised using the tensor product, then m and p are affine functions and we say that u represents a* generalised affine function.

We are trying to answer the question: which Boolean functions are as far away as possible from the set of generalised affine functions as defined by the rows of $\{I, H, N\}^n$?

1.2 The Quantum Context

In chapter 2, we give an introduction to some concepts in *quantum mechanics* and *quantum information theory*, used in this thesis. We refer for definitions to this chapter. We are specially interested in the concept of *quantum entanglement* (see definition 2.9). Intuitively, it is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. This leads to correlations between observable physical properties of the systems. For a formal definition, see definition 2.9.

Quantum entanglement of qubits is the basis for emerging technologies such as *quantum computing* and *quantum cryptography*. For instance, in the so-called *one-way quantum computer* [73], quantum algorithms are implemented by performing single qubits measurements on a highly entangled stabilizer state (for a description of stabilizer states, see for instance [93]).

In quantum cryptography, the process of sending and storing information is always carried out by physical means, for example photons in optical fibres or electrons in electric current. Eavesdropping can be viewed as measurements on a physical object—in this case the carrier of the information. Using quantum phenomena such as *quantum superposition* (definition 2.8) or *quantum entanglement* (definition 2.9) one can design and implement a communication system which can always detect eavesdropping. This is because measurements on the quantum carrier of information disturb it and so leave traces.

Entanglement of qubits has also been used in *quantum teleportation* (see [8, 18] for the teleportation of a single qubit, or [79] for the teleportation of N qubits).

As in classical communication, an important element in quantum information theory is the correction of errors. While classical error-correction employs redundancy, this is not possible with quantum information, for, as stated by the no-cloning theorem, the information cannot be copied:

Theorem 1 *[101] There is no quantum operation that takes $|\phi\rangle$ to $|\phi\rangle \otimes |\phi\rangle$, where $|\phi\rangle$ is any quantum state.*

However, as proven by Peter Shor, the information of one qubit can be spread onto several physical qubits by using a *Quantum Error-Correcting Code (QECC)* (see definition 2.18) [40, 19]. Now, if *noise* or *decoherence* (interaction with the environment) corrupts one qubit, the information is not lost.

The choice of I, H, and N, is motivated by their relevance to the set of equivalent Quantum Error-Correcting Codes (QECCs) of the *stabilizer type* (definition 2.20). This is because I, H, and N are generators of the *Local Clifford Group* [19, 49] (see definition 2.21), that *stabilizes* the *group of Pauli matrices on one qubit* (see definitions 2.19 and 2.13).This group, in turn, forms a basis for the set of local errors that act on the quantum code. This stabilizing property of the Local Clifford Group allows one error of the Pauli Group to be 'swapped' with another, whilst leaving invariant the weight distribution of the stabilizer code. In other words the action of the Local Clifford Group generates the fundamental symmetries of the stabilizer code. It follows that all states that occur as spectra w.r.t. $\{I, H, N\}^n$ represent stabilizer states which are equally robust to quantum errors from the Pauli set.

To evaluate the quantum *entanglement* of a *pure n-qubit state* (see definition 2.10) one should really examine the spectra w.r.t. the infinite set of n-fold tensor products of all 2×2 unitary matrices [67]. Those states which minimise all spectral magnitudes w.r.t. this infinite transform set are as far away as possible from all generalised affine functions and can be considered to be highly entangled as the probability of observing (measuring) any specific qubit configuration is as small as possible, in any local measurement basis. However it is computationally intractable to evaluate, to any reasonable approximation, this continuous local unitary spectrum beyond about $n = 4$ qubits (although approximate results up to $n = 6$ are given in [67]). Therefore we choose, in chapter 3, a well-spaced subset of spectral points, as computed by the set of $\{I, H, N\}^n$ transforms, from which to ascertain approximate entanglement measures. Complete spectra for such a transform set can be computed up to about $n = 10$ qubits using a standard desk-top computer, although partial results for higher n are possible if the n-qubit quantum state is represented by, say, a quadratic Boolean function over n variables: let p be a Boolean function of n variables such that $s = (-1)^{p(\mathbf{i})}$, where $\mathbf{i} \in \mathrm{GF}(2)^n$. We say that s represents the pure quantum state of n qubits such that a joint measurement of s in the computational basis (that is, the basis implied by the vector s) evaluates to $\mathbf{i}$ with probability $2^{-n}|(-1)^{p=\mathbf{i}}|^2$. We sometimes say that p represents the same quantum state, where the meaning will be clear from the context. It has been shown by Van der Nest in Proposition 2.14 of [93] that all graph states (definition 2.22) are equivalent under local unitaries to quadratic forms expressed as $(-1)^p$, where p is a Boolean function. We further show (see chapter 10) that no graph state is equivalent to a state $(-1)^p$ if the algebraic degree of p is other than 2.

Papers in the physics literature have recently proposed a measure of entanglement for the pure multipartite state, s, which measures distance of s to the nearest *product state* (definition 2.9) over the infinite set of product states [7, 9, 96, 97, 98]. It is called, by some authors, the *geometric measure* and has been shown to be an *entanglement monotone* [96]. It has been extended by [7, 96, 97, 98] to a measure of entanglement for *mixed states* (definition 2.10). An entanglement measure for pure multipartite states was proposed in [67] called PAR_l and, in logarithmic form, *linear entanglement*. The PAR_l is, essentially, the geometric measure, although [67] did not prove that the measure is also an entanglement monotone. PAR_l is the maximum *Peak-to-Average Power Ratio (PAR)* (definition

2.1) over the output spectra of s w.r.t. the infinite set of local unitary transforms. In contrast, the geometric measure is defined in [98] to be $1 - \Lambda^2_{\max}$, where $\Lambda_{\max}$ is called the *entanglement eigenvalue*, and is the cosine of the angle between the state s and any closest separable (i.e. product) state. It is clear by comparing equation (8) of [98] and Definition 10 of [67] that $2^n\Lambda^2_{\max} = \mathrm{PAR}_l$. [98] also provides a logarithmic form of the geometric measure, namely $E_{\log_2} = -\log_2(\Lambda^2_{\max})$, which is precisely the same as the linear entanglement of [67] which was defined as $n - \log_2(\mathrm{PAR}_l)$. As shown in [98], $E_{\log_2}$ acts as a lower bound on *relative entropy* (w.r.t. separable states), both for pure and mixed multipartite states and, in some cases, this bound is exact. [67, 27] have shown that, for states represented by Boolean functions, (i.e. graph states), whose associated multipartite graph is bipartite, the PAR_l and associated linear entanglement can be computed exactly by using just tensor products of I and H. Similar techniques have been used in [45] but this time w.r.t. a multipartite version of the *Schmidt measure*.

In this thesis, we do not examine the PAR_l which, in general, appears to be computationally intractable. Instead we examine spectra w.r.t. just tensor products of I, H, and N. In the first part of the thesis (chapters 3 and 4), we do not consider the PAR but instead simply count the number of spectra which are flat, taken over all transforms of s w.r.t. $\{I, H, N\}^n$. Such a measure is not an entanglement monotone but we call it an *entanglement criteria* for a pure quantum state in the same way that cryptographers refer to *cryptographic criteria* for Boolean functions. Entanglement criteria give an indication of the amount of entanglement of a state, but other criteria should also be taken into account when assessing entanglement. As is shown in chapter 4, 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 degree of p, with the enumeration maximised if $\deg(p) = 2$. Chapter 4 also shows experimentally that, for graph states, those states which represent QECCs with highest distance also have the most number of flat spectra w.r.t. $\{I, H, N\}^n$. Therefore, as experimental results suggest that distance is optimised for those graph states with lowest PAR_l [27], then the number of flat spectra w.r.t. $\{I, H, N\}^n$ can be considered to be an entanglement criteria but not an entanglement measure.

1.3 The Graphical Context

Structures that can be represented as graphs are ubiquitous, and many problems of practical interest can be represented by graphs. For instance, as we stated before, quadratic Boolean functions can be represented by graphs, and some of their spectral properties can be computed in graph terms. One of the first results in graph theory appeared in Leonhard Euler's paper on *Seven Bridges of Königsberg*, published in 1736. Here we present some problems in graph theory that are strongly related to the content of this thesis.

We offer a brief introduction of graph theory in chapter 2, section 2.3.

Definition 2 *The* clique function *or* complete graph *is defined as the graph in which an edge connects every pair of vertices.*

Definition 3 *Given a graph G, an* independent set (IS) *is a subset of its vertices that are pairwise not adjacent.*

The *k-clique problem* is the problem of determining, given a graph G and an integer k, whether G contains a clique of at least a given size k. The *k-independent set problem* is the problem of finding an independent set of size at least k. These two problems are equivalent, because there is a clique of size at least k if and only if there is an independent set of size at least k in the complement graph. Both problems are NP-complete.

The corresponding optimization problem to the clique problem is the *maximum clique problem*, that is the problem of finding the largest clique in a graph. Equivalent to this problem, the *independent set problem* is the problem of determining the largest independent set in a graph.

Definition 4 *[71] The* Ramsey number*, $r = R(m, n)$, is the number such that all simple undirected graphs on at least r vertices will have either an independent set of size m or a clique of size n.*

The Ramsey number is also highly related to the independent set problem, where we now consider not only a single graph, but the whole orbit of the graph under a graph operation. This is of significant relevance to the subject of this thesis (see chapters 3 and 5):

Definition 5 *Define the action of* Local Complementation (LC) *[16, 15] (or* vertex-neighbour-complement (VNC) *[37]) on a graph G at vertex v, LC_v, as the graph transformation obtained by replacing the subgraph defined by restricting the set of vertices to $\mathcal{N}_v$, $G[\mathcal{N}_v]$, by its complement; that is, the graph transformation obtained by complementing the relationships between the vertices in $\mathcal{N}_v$ (the neighbourhood of v).*

Let Λ_n be the minimum value of λ over all LC orbits of graphs on n vertices, λ being the size of the largest independent set in the corresponding LC orbit of graphs. Then:

Lemma 1 *[30] If r is the Ramsey number $R(k, k+1)$, then $\Lambda_n \geq k$ for $n \geq r$.*

A *vertex covering* for a graph G is a set of vertices V so that every edge of G is adjacent to at least one vertex in V. The *vertex cover problem* is the problem of finding the smallest vertex covering and is NP-complete. This problem is strongly related to the independent set problem, because for any graph $G := (V, E)$, the size of the smallest vertex covering plus the size of the maximum independent set equals the size of V [36].

Graphs have an important application in quantum mechanics, as a certain significant type of quantum state can be described by a simple graph (see chapter 10). The graphical description of certain pure quantum states was investigated by Parker and Rijmen [67]. They proposed partial entanglement measures for such states and made observations about a *Local Unitary (LU) Equivalence* between graphs describing the states w.r.t. the tensor product of 2×2 local unitary transforms. These graphs were interpreted as quadratic Boolean functions and it was noted that bipartite quadratic functions are LU-equivalent to indicators for *binary linear error-correcting codes*. It was further observed that physical quantum graph arrays were already under investigation in the guise of *cluster states*, by Raussendorf and Briegel [72, 13]. These clusters form the 'substrate' for *measurement-driven* quantum computation.

Measurement-driven quantum computation on a *quantum factor graph*[2] has been discussed by Parker [66]. Independent work by Schlingemann and Werner [82], Glynn [37, 38], and by Grassl, Klappenecker, and Rotteler [41] proposed to describe *stabilizer* Quantum

[2]A factor graph is the diagram showing how a function of several variables can be factored into a product of "smaller" functions in less variables.

Error-Correcting Codes (QECCs) (definition 2.20) using graphs and, for QECCs of dimension zero, the associated graphs can be referred to as *graph states* (see definition 2.22). The graph states are equivalent to the graphs described by [67] and therefore have a natural representation using quadratic Boolean functions (see [93]).

In reference [67] it was observed that the complete graph, the star graph, and generalised GHZ (short for Greenberger-Horne-Zeilinger) states are all LU-equivalent. It turns out [93] that LU-equivalence for graph states can be characterised, graphically, via the *Vertex-Neighbour-Complement (VNC)* transformation, which was defined by Glynn, in the context of QECCs (definition 4.2 in [37]), and also, independently, by Hein, Eisert and Briegel [45], and also by Van Den Nest and De Moor under the name of *Local Clifford operation* [94, 93]. VNC is another name for *Local Complementation (LC)*, as investigated by Bouchet [14, 15, 16] in the context of *isotropic systems*. 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 GF(4) additive codes that keeps the weight distribution of the code invariant [19]. There has been recent renewed interest in Bouchet's work motivated, in part, by the application of *interlace polynomials* (see chapters 5 and 6) 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 chapter 4.

1.4 The Coding Theory Context

In this section, we give a summary of binary linear codes, one of the topics related to the thesis.

The aim of coding theory is the reliable transmission of information across noisy channels. Shannon [83] was the first to formulate information theory mathematically. Ideally, one wishes to find codes which transmit quickly, contain many valid codewords and can correct or at least detect many errors. However, these aims are mutually exclusive, so different codes are optimal for different applications, depending mainly on the probability of errors happening during transmission. An error-correcting code is an algorithm for expressing a sequence of numbers such that any errors (within certain limitations) produced during transmission can be detected and corrected based on the information received.

The motivation behind creating (binary) linear codes is to allow for *syndrome decoding*, minimum distance decoding using a reduced (because of the linearity of the code) lookup table.

Definition 6 *A* $[n, k]$ binary linear code*,* $n \geq 1$*,* $1 \leq k \leq n$*, is a linear subspace* C *with dimension* k *of the vector space* $\mathbb{F}_2^n$*. The elements of* C *are known as* codewords*,* n *is called the* length *of the code and* k *its* rank*.*

Taking a base over $\mathbb{F}_2^n$ (usually, the canonical base $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is on the i^{th} position), C can be expressed by means of its *generator matrix*, G, a binary $k \times n$ matrix defined by the property that $c \in C$ iff c is a linear combination of the rows of G.

Definition 7 *The* dual code *of a* $[n, k]$ *linear code* C *is the* $[n, n-k]$ *linear code defined by*

$$C^{\perp} = \{x \in \mathbb{F}_2^n : \langle x, c \rangle = 0 \ \forall \ c \in C\} \ .$$

It can be shown that each bipartite graph with k variables on one side and $n-k$ on the other is related to a binary $[n, k]$ linear code, C, via a simple transform from the set of $\{I, H\}^n$ transforms [67]. Likewise, the dual $[n, n-k]$ code, $C^{\perp}$, can also be obtained from the same graph via another transform from the set of $\{I, H\}^n$ transforms (see section 10.8). Viceversa, from any binary linear code we can define a bipartite graph.

One can also show that C and $C^{\perp}$ are invariant under *pivot* of the associated bipartite graph, where pivot is a graphical operation, as defined in definition 5.12. Consequently, such a graph remains bipartite under pivot, as stated in Lemma 7.3. It is therefore of interest to enumerate the number of pivot orbits of bipartite graphs, in order to get a classification of binary linear codes. In chapter 7, we give an enumeration of all pivot orbits of unlabelled and labelled connected bipartite graphs for some values of n (see table 7.1). A list of bipartite pivot orbit representatives for unlabelled and labelled connected graphs is available at http://www.ii.uib.no/∼matthew/bipivotorbits/files.html.

1.5 Outline of the thesis

In chapter 3, 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 the choice of unitary transforms that are typically used to action a local basis change for a pure n-qubit quantum state. Then, we shall apply such transforms to an n-variable Boolean function, and examine the resultant spectra accordingly. In particular we shall apply all possible transforms formed from n-fold tensor products of the 2×2 identity matrix I, the *Walsh-Hadamard kernel*, H, and the *Negahadamard kernel* N [64], where

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

with $i^2 = -1$. We refer to this set of transforms as the $\{I, H, N\}^n$ *transform set*. That is, the set $\{I, H, N\}^n$ consists of all transforms $U = \prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j$, where the sets $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ partition $\{0, \ldots, n-1\}$, and H_j, say, stands for the transform $I \otimes \ldots \otimes I \otimes H \otimes I \otimes \ldots \otimes I$, with H in the j^{th} position. There are 3^n such transforms which act on a Boolean function of n variables to produce 3^n spectra, each spectrum of which comprises 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 just 2^n spectral elements.

One of the main aims of chapter 3 is to provide a technique to study 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

$$P_{U,\mathbf{k}} = U \; 2^{-n/2}(-1)^{p(\mathbf{x})} = (\prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j) 2^{-n/2}(-1)^{p(\mathbf{x})} \; . \tag{1.1}$$

Chapter 4 can be regarded as the application of the above-mentioned technique to some concrete recursive graph structures, such as the *line* or the *clique*, and to a new structure, the *clique-line-clique*, defined from the two previous graphs, and that in general inherits from them good qualities, inherent to those structures with respect to some specific subsets of $\{I, H, N\}^n$, and that avoids the less positive behaviour that they show with respect to

the total of $\{I, H, N\}^n$. We summarize the results for this chapter in the appendix of the chapter (section 4.6).

Chapter 5 exploits further the connection between graph structures and Boolean functions, relating some objects derived from the structure of a graph, the *interlace polynomials* (see [2, 4] and [1]) to the spectra of a quadratic Boolean function with respect to $\{I, H, N\}^n$. With this purpose in mind, we give a new and equivalent definition of the different interlace polynomials that are based on the linear algebra techniques used in chapters 3 and 4 to compute the number of flat spectra with respect to some subsets of $\{I, H, N\}^n$.

We prove as well that, if $p(\mathbf{x})$ is a quadratic Boolean function, its *power spectrum* with respect to any transform in $\{I, H, N\}^n$ is either flat (one-valued) or two-valued, and when it is two-valued one of these values is 0 and the other one can be computed explicitly from the modified adjacency matrix proposed in chapter 3. This allows us to derive a formula for computing the *Clifford Merit Factor (CMF)* and the *Multivariate Merit Factor (MMF)* [43, 65], with the interlace polynomials. Next, we prove some conjectures proposed by Parker in [64] related to the line function (path graph) and its affine offsets.

Chapter 6 shows a similar relationship between the two-variable interlace polynomial (see [5]), and the spectra of a quadratic Boolean function with respect to the set $\{I, H\}^n$. We also introduce new two-variable interlace polynomials by analogy, and investigate some of their properties. Next, for bipartite graphs, we develop a three-variable interlace polynomial and from it derive the *weight hierarchy* [46, 99] of the associated binary code, thereby expanding on the results of Parker and Rijmen [67].

Chapter 7 gives an expression of the pivot operation on graphs using the ANF of its associated (quadratic) Boolean function. By using this form, we generalise the pivot operation to hypergraphs, and we state the (necessary and sufficient) condition that a function of degree higher than two must fulfill in order to allow such an operation. We give as well a spectral interpretation of the pivot operation on a (hyper)graph. Based on the above mentioned condition for pivot and on the spectral interpretation, we construct a family of Boolean functions that have a large number of flat spectra w.r.t. $\{I, H\}^n$, and we compute this number. Also, we enumerate pivot orbits of unlabelled and labelled connected bipartite graphs for some values of n. Finally, we study the pivot orbit trajectory

of structures that include a clique and develop lower bounds on the number of flat spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

Chapter 8 offers a description of the conditions that allow a Boolean function to change its degree by pivoting on its associated hypergraph, or to reduce or increase the number of high degree terms. We describe as well the explicit formula for the result of applying a transform $U \in \{I, N\}^n$ to the APF (Algebraic Polar Form) [67] (see section 8.3) of any vector with entries in the set $\{0, \pm 1\}$. Together with the results proposed by Parker and Rijmen in [67], and using iteration, this formula allows the computation of the result of the application of a $U \in \{I, H, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$. Finally, we show how to use these results for computing the result of the application of a $U \in \{I, H, N\}^n$ to i^p for $p : \{0, 1\}^n \to \mathbb{Z}_4$.

In the Appendix (chapter 10), we summarise the different interpretations of graph states, with more detail than in the Introduction. As the matters dealt with in this thesis are interdisciplinary, and as the equivalences displayed here are scattered among many papers published in different areas, it is useful to gather them together, although the results presented in this chapter are not new.

Chapter 2

Preliminaries

2.1 Boolean functions

For better comprehension of the thesis, we state some definitions related to Boolean functions, as well as some important transforms that act on them.

Definition 2.1 *Let*

- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *be the* 2×2 *identity matrix,*
- $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ *the* Walsh-Hadamard kernel*, and*
- $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ *the* Negahadamard kernel *[69].*

Let $U \in \{I, H, N\}$*. We define* U_j *as the tensor product*

$$U_j = I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I \ ,$$

where the U *occurs in position* j *in the tensor product. Then, the set of transforms* $\{I, H, N\}^n$ *is defined as the set of tensor products of all possible combinations of the matrices* I*,* H *and* N*, that is,*

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

where the sets $\mathbf{R_I}, \mathbf{R_H}$ *and* $\mathbf{R_N}$ *partition the set of vertices* $\{0, \ldots, n-1\}$*, and '*$\prod$*' represents the usual matrix product.*

Definition 2.2 *Let* $p : GF(2)^n \to GF(2)$ *be a Boolean function on* n *variables. We define the* bipolar vector *of the function, as the length* 2^n *vector with coefficients in* $\{+1, -1\}$*,* $s = (s_{0\ldots00}, s_{0\ldots01}, s_{0\ldots11}, \ldots, s_{1\ldots11})$ *such that* $s_{\mathbf{i}} = (-1)^{p(\mathbf{i})}$*, where* $\mathbf{i} \in GF(2)^n$*.*

Definition 2.3 *The* Walsh Hadamard Transform (WHT)*,* $WHT : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$*, is defined by the* $2^n \times 2^n$ *unitary matrix* $U = H \otimes H \ldots \otimes H = \bigotimes_{i=0}^{n-1} H$*, where '*$\otimes$*' indicates the tensor product of matrices, and unitary means that* $UU^\dagger = I_n$*, where '*$\dagger$*' means transpose-conjugate and* I_n *is the* $2^n \times 2^n$ *identity matrix.*

Definition 2.4 *The* Walsh-Hadamard spectrum *of* p *is given by the matrix-vector product* $P = Us \in \mathbb{C}^{2^n}(\mathbb{R}^{2^n})$*, where* $s = (-1)^{p(\mathbf{k})}$ *as before, with* $\mathbf{k} \in GF(2)^n$*. In general, the* spectrum *of a function w.r.t. a transform* $T : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ *is given by the matrix-vector product* $P = Ts$*. The* spectral coefficients *are defined as the entries of the vector* P*,* $P_{\mathbf{k}}$*.*

Definition 2.5 *A Boolean function* $p : GF(2)^n \to GF(2)$ *is said to have a* flat spectrum *w.r.t. a transform* $T : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ *iff* $|P_{\mathbf{k}}| = 1 \ \forall \mathbf{k} \in GF(2)^n$*. The function will be called* bent *iff it has a flat spectra w.r.t. the transform WHT.*

Definition 2.6 *[29] The* Peak-to-Average Power Ratio (PAR) *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*

$$PAR_{\mathbf{T}}(s) = 2^n \max_{\substack{U \in \mathbf{T} \\ \mathbf{k} \in \mathbb{Z}_2^n}} (|P_{U,\mathbf{k}}|^2), \quad \text{where } P_U = (P_{U,\mathbf{k}}) = Us \in \mathbb{C}^{2^n} \ . \tag{2.1}$$

2.2 Quantum theory

We offer here a brief introduction to some of the concepts in quantum theory, more concretely in quantum information theory, that are more relevant to this work. We refer to [33, 93, 40] for a more extended view of these subjects.

Definition 2.7 *[33] A* quantum state $|\phi\rangle$ *is a unit vector*[1] *in a complex Hilbert space* $\mathcal{H}$*.*

[1]It is enough to take a unit vector as representative for a state, because for any $\alpha \in \mathbb{C} \setminus \{0\}$, $\alpha |\phi\rangle$ is defined equivalent to $|\phi\rangle$.

Remark: The space $\mathcal{H}$ is in general not finite, but under laboratory conditions one can consider the space as finite, and then $\mathcal{H} \cong \mathbb{C}^n$, for some n. This is the convention that most of the papers in the literature use, and we shall adopt this convention from this point onwards.

The notation $|\ \rangle$ is known as the *bra-ket notation*, because the *inner product* of two states is denoted by a bracket, $\langle\psi|\phi\rangle$, consisting of a left part, $\langle\psi|$, called the *bra*, and a right part, $|\phi\rangle$, called the *ket*. It is also known as *Dirac notation*. The bra vector belongs to the dual space of $\mathcal{H}$, $\mathcal{H}^*$. $|\phi\rangle$ should be thought of as a column vector,

$$|\phi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} ,$$

and $\langle\psi|$ as a row vector, $\langle\psi| = (b_0, \ldots, b_{n-1})$. $\langle\psi|\phi\rangle$ will be computed as the matrix product $\langle\psi| \cdot |\phi\rangle$.

Given a ket $|\phi\rangle$ with coordinates as before, its corresponding bra $\langle\phi|$ is defined as $\langle\phi| = (\overline{a_0}, \ldots, \overline{a_{n-1}})$, where $\overline{a_i}$ means the complex conjugate of a_i.

Definition 2.8 *[33] A ket state $|\varphi\rangle$ is a* superposition *of $|\phi\rangle$ and $|\psi\rangle$ if*

$$|\varphi\rangle = \alpha\,|\phi\rangle + \beta\,|\psi\rangle\,,\ \textit{with } \alpha,\, \beta \in \mathbb{C}\ .$$

Two (ket) states $|\phi\rangle$ and $|\psi\rangle$, say in N-, respectively M-dimensional spaces V, W, can be *composed* by a tensor product, $|\phi\rangle \otimes |\psi\rangle$. This vector will be in the tensor product of V and W, $V \otimes W$, of dimension NM. The tensor product of the states will be alternatively denoted by $|\phi\rangle\,|\psi\rangle$, $|\phi\psi\rangle$ or $|\phi, \psi\rangle$. Given the coordinates of $|\phi\rangle$ and $|\psi\rangle$, we can compute the coordinates of $|\phi\rangle \otimes |\psi\rangle$ as the set of all pairwise products of coordinates of $|\phi\rangle$ and $|\psi\rangle$.

Definition 2.9 *[35] A state $|\rho\rangle$ in $V \otimes W$ that can be written as $|\phi\rangle \otimes |\psi\rangle$ is called a* product state. *If $|\rho\rangle$ is not a product state, it is* entangled.

Definition 2.10 *A* pure quantum state *is a state which can be described by a single ket vector, or as a sum of basis states. A* mixed quantum state *is a statistical distribution of pure states.*

Definition 2.11 *A* quantum bit, qubit *(sometimes denoted as* qbit*) is a unit of quantum information, described by a state in a 2-dimensional space, whose standard basis vectors are labelled* $|0\rangle$ *and* $|1\rangle$*. A* pure qubit state *is a linear quantum superposition of those two states. This means that each qubit can be represented as a linear combination of* $|0\rangle$ *and* $|1\rangle$*:*

$$\alpha\,|0\rangle + \beta\,|1\rangle\,,\ \textit{with}\ |\alpha|^2 + |\beta|^2 = 1\ .$$

If $A : \mathcal{H} \to \mathcal{H}$ is a linear operator, we can apply A to the ket $|\phi\rangle$ to obtain the ket $(A\,|\phi\rangle)$. In this thesis, we deal mainly with the 2×2 linear operators I, H, and N and combinations of their tensor products (see definition 2.1).

We introduce briefly the theory of *quantum error-correction*. For more detailed information, we refer for instance to [90, 89, 40, 93].

Definition 2.12 *A* quantum error *in a state of* n *qubits is a map* $E : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$*, where* $m \geq n$*.*

Definition 2.13 *The* Pauli matrices *on one qubit are defined as the* 2×2 *matrices*

$$\sigma_I = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \textit{and}\ \sigma_y = i\sigma_x\sigma_z\ . \tag{2.2}$$

The Pauli group on one qubit*,* $\mathcal{P}_1$*, is defined as the (finite) multiplicative group generated by the Pauli matrices.*

Definition 2.14 *A* bit-flip X *is defined as the (linear) transform:* $X\,|a\rangle = |a \oplus 1\rangle$*, for* $|a\rangle = |0\rangle$ *or* $|1\rangle$*. A* phase-flip Z *is defined as the (linear) transform:* $X\,|a\rangle = (-1)^a\,|a\rangle$*, for* $|a\rangle = |0\rangle$ *or* $|1\rangle$*.*

Remark: It is easy to see that the matricial expression for a bit-flip X is the Pauli matrix σ_x, and for a phase-flip Z is σ_z, while a bit-flip followed by a phase-flip is represented by $i\sigma_x\sigma_z$. The matrix I would represent the case that no error is made on the qubit, that is, the qubit does not change.

Lemma 2.15 *[90] A completely arbitrary change in a general state $|\phi\rangle$ of one qubit can be written as:*

$$|\phi\rangle \simeq |\phi\rangle |\psi_0\rangle_e \rightarrow \sum_{i\in\{I,x,y,z\}} (\sigma_i |\phi\rangle) |\psi_i\rangle_e \ , \tag{2.3}$$

where $|\psi_i\rangle_e$ are called states of the environment*, and they are unconstrained, that is, they are not necessarily either normalised or orthogonal.*

Note: The second system, with states $|\psi_i\rangle_e$, is introduced simply to allow us to write using the language of kets a general change in the state.

Definition 2.16 *The* Pauli group on n qubits *is the group*

$$\mathcal{P}_n = \{\alpha U_0 \otimes \cdots \otimes U_{n-1} : U_i \in \mathcal{P}_1, \alpha \in \{\pm 1, \pm i\}\} \ .$$

Note: [90] Generalising lemma 2.15, a *completely arbitrary change on n qubits* can be expressed as

$$|\phi\rangle |\psi_0\rangle_e \rightarrow \sum_i (E_i |\phi\rangle) |\psi_i\rangle_e \ , \tag{2.4}$$

where each *error operator* $E_i \in \mathcal{P}_n$, $|\phi\rangle$ is the initial state of the qubits, and $|\psi\rangle_e$ are states of a second system, not necessarily orthogonal or normalised. This implies that arbitrary changes, which form a continuous set, can be 'digitized' by expressing them as a weighted sum of discrete errors.

Definition 2.17 *The* weight *of a transform E on n qubits is the maximal number $\omega \in \{0, \ldots, n\}$ such that E can be written as $I^{\otimes n-m} \otimes E'$, up to a permutation of qubits, for some matrix E'.*

Definition 2.18 *A (general)* Quantum Error-Correcting Code (QECC) *is an orthonormal set of n-qubit states (*quantum codewords*) which allow correction of all members of a set $S = \{E_i\}$ of* correctable errors*. A code that corrects all errors (including X, Y or Z and combinations thereof for different qubits) of weight up to some maximum ω is called a* ω-QECC*.*

Note: [90] Using some auxiliary qubits (called *ancilla*), and *projective measuring* (that is, projection on some orthogonal base, in this case the Pauli group), a system that can correct the Pauli errors acting on each qubit separately can correct the most general possible noise (eq. (2.4)).

Definition 2.19 *Given a group $\mathcal{G}$, and an element $g \in \mathcal{G}$, the* stabilizer subgroup of g *is the set of all elements that fix g:*

$$G_g = \{h \in \mathcal{G} : h \cdot g = g\} \ .$$

Let $X \subseteq G$. Then, the stabilizer subgroup of X *is the set of all elements that fix X:*

$$G_X = \{h \in \mathcal{G} : h \cdot X = X\} \ .$$

Remark: Note that, for $g \in X$ and $h \in G_X$, it is not true in general that $h \cdot g = g$.

Definition 2.20 *A* stabilizer *QECC is a QECC such that all codewords are simultaneous eigenstates with eigenvalue 1 of all the operators in a stabilizer on n qubits.*

Definition 2.21 *[19, 49] The* Local Clifford Group *is defined to be the set of matrices that stabilizes the Pauli group on one qubit.*

This stabilizing property of the Local Clifford Group allows one error of the Pauli Group to be 'swapped' with another, whilst leaving invariant the weight distribution of the stabilizer code.

We now give a definition of a certain type of quantum state, the *graph state*, of high relevance in quantum information theory (see [93] for details), and to this thesis, as this is one of the objects that is equivalent to a quadratic Boolean function (see chapter 10):

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

$$\begin{aligned} K_i &= \sigma_x^{(i)} \prod_{j \in \mathcal{N}_i} \sigma_z^{(j)} \\ &= \sigma_x^{(i)} \prod_{k=0}^{n-1} (\sigma_z^{(k)})^{\Gamma[k,i]} \ , \end{aligned} \tag{2.5}$$

where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, 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. A *graph state* is defined as:

Definition 2.22 *[45] The* graph state $|G\rangle$, *also known as* cluster state, *is the unique (modulo an overall phase factor) common eigenvector with eigenvalue* 1 *of all operators in the subgroup generated by the K_i operators.*

2.3 Graph Theory

We recall here some definition of graph theory, used profusely in this thesis:

A *graph* on n vertices is a pair $G = (V, E)$ of sets, where $V = \{0, \ldots, n-1\}$ and the elements of E are 2-element subsets of V. The elements of V are called the *vertices* of the graph, and the elements of E its *edges*. All graphs considered in this thesis will be *simple* graphs, that are graphs with no multiple edges (i.e. repetitions in E) and no loops (i.e. edges of the form (i, i), for $i \in V$). We also consider our graphs to be *non-directed*; that is, if $(i, j) \in E$, it follows that $i < j$. Two vertices $i, j \in V$ are called *adjacent* or *neighbours* if $(i, j) \in E$. The *neighbourhood* $\mathcal{N}_i$ of a vertex i is the set of all neighbours of i. The *adjacency matrix* Γ_G (denoted simply by Γ when no confusion is possible) is a symmetric binary $n \times n$ matrix defined by

$$\begin{cases} \Gamma[i, j] = \Gamma[j, i] = 1 \text{ if } (i, j) \in E \\ \Gamma[i, j] = \Gamma[j, i] = 0 \text{ otherwise} \end{cases}$$

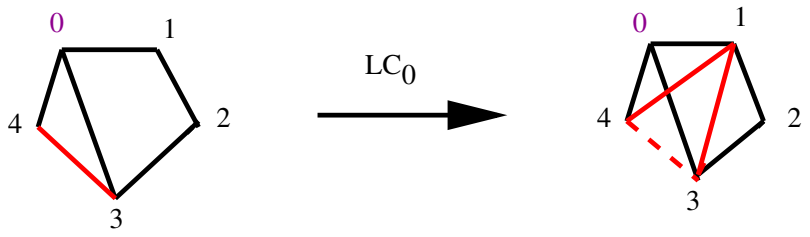
The *complement* or *inverse* of a graph G is a graph H on the same vertices such that two vertices of H are adjacent if and only if they are not adjacent in G.

Definition 2.23 *The* clique function *or* complete graph *is defined as the graph in which an edge connects every pair of vertices.*

Definition 2.24 *Given a graph G, an* independent set (IS) *is a subset of its vertices that are pairwise not adjacent.*

Definition 2.25 *Define the action of* Local Complementation (LC) *(or* vertex-neighbour-complement (VNC)*) on a graph G at vertex v, LC_v, as the graph transformation obtained by replacing the subgraph defined by restricting the set of vertices to $\mathcal{N}_v$, $G[\mathcal{N}_v]$, by its complement; that is, the graph transformation obtained by complementing the relationships between the vertices in $\mathcal{N}_v$.*

Example: with $v = 0$,



2.4 Code Theory

We recall here some definitions of code theory, related to the spectral interpretation of a quadratic, as we shall see in this thesis (for the statement of the relationship, see section 10.8). We refer to [53] for more information about coding theory.

Definition 2.26 *A* $[n, k]$ binary linear code, $n \geq 1$, $1 \leq k \leq n$, *is a linear subspace* C *with dimension* k *of the vector space* $\mathbb{F}_2^n$. *The elements of* C *are known as* codewords, n *is called the* length *of the code and* k *its* rank.

Taking a base over $\mathbb{F}_2^n$ (usually, the canonical base $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is on the i^{th} position), C can be expressed by means of its *generator matrix*, G, a binary $k \times n$ matrix defined by the property that $c \in C$ iff c is a linear combination of the rows of G.

Definition 2.27 *The dual code of a* $[n, k]$ *linear code* C *is the* $[n, n-k]$ *linear code defined by*

$$C^{\perp} = \{x \in \mathbb{F}_2^n : \langle x, c \rangle = 0 \ \forall \ c \in C\} \ .$$

Definition 2.28 *Let* $GF(4) = \{0, 1, \omega, \bar{\omega}\}$, *with* $\bar{\omega} = \omega^2 = \omega + 1$. *A* GF(4)-additive code *of length* n *is an additive subgroup of* $GF(4)^n$.

Chapter 3

Generalised Bent Criteria for Boolean Functions

The results for this chapter can be found in [74].

3.1 Overview

The classification of bent quadratic (degree-two) Boolean functions is well-known [53], and is made easier because the bent criterion is an invariant of affine transformation of the input variables. On the other hand, 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 with respect to affine transformation of the inputs. Chapter 3 characterises these generalised bent criteria for both quadratic and more general Boolean functions. By associating a quadratic Boolean function to an undirected graph, we can interpret spectral flatness with respect to $\{I, H, N\}^n$ as a *maximum rank* property of suitably modified adjacency matrices. We interpret *Local Complementation (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, of the WHT of all subspaces of Boolean functions that can be obtained by fixing a subset of the variables, of the WHT of all $\mathbb{Z}_4$-linear offsets of all of the above subspace Boolean functions, of 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.

In Section 3.2 we review LC as an operation on an undirected graph [37, 38], and provide an algorithm for LC in terms of the adjacency matrix of the graph. In Section 3.3, 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 $\sqrt{i\sigma_z}$, where σ_x and σ_z are Pauli matrices (definition 2.2). We also show, equivalently, that the orbit lies within the flat spectra w.r.t. $\{I, H, N\}^n$. We show that applying LC to vertex x_v can be obtained 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.

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

where $p(\mathbf{x})$ and $p'(\mathbf{x})$ are quadratic, $p'(\mathbf{x})$ is obtained by applying LC to variable x_v, $\omega = \sqrt{i}$, and $a(\mathbf{x})$ is any offset over $\mathbb{Z}_8$. In Section 3.5 we identify spectral symmetries that hold for $p(\mathbf{x})$ of any degree w.r.t. $\{I, H, N\}^n$. In Section 3.4, we introduce the concepts of *bent*$_4$, *I-bent*, *I-bent*$_4$, and *LC-bent* Boolean functions, and show how, for quadratic Boolean functions, the first three properties can be evaluated by examining the ranks of suitably modified versions of the adjacency matrix.

3.2 Local Complementation (LC)

3.2.1 Definition

We recall here some definitions (see chapter 1):

Given a 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.

We recall definition 2.25:

Definition 3.1 *Define the action of* LC *[16, 15] (or* vertex-neighbour-complement (VNC) *[37]) on a graph G at vertex v, LC_v, as the graph transformation obtained by replacing the*

subgraph defined by restricting the set of vertices to $\mathcal{N}_v$, $G[\mathcal{N}_v]$, by its complement; that is, the graph transformation obtained by complementing the relationships between the vertices in $\mathcal{N}_v$.

Definition 3.2 *We say that two graphs G and H are* LC-equivalent *iff there is a graph transform U such that $G = UH$, with U a succession of transforms LC.*

By Glynn (see [37]), 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 H give equivalent self-dual quantum codes if and only if H and G are LC-equivalent.

For a study of the group of compositions of local complementations, see [14, 16, 15, 25], which describe the relation between local complementation and *isotropic systems*. Essentially, a suitably-specified isotropic system has graph presentations G and G' iff G and G' are locally equivalent w.r.t. local complementation.

3.2.2 LC in terms of the adjacency matrix

Let $p(\mathbf{x}) : \mathbb{F}_2^n \to \mathbb{F}_2$ be a (homogeneous) quadratic Boolean function, defined by,

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

We can express $p(\mathbf{x})$ by the adjacency matrix of its associated graph, Γ, defined as the symmetric $n \times n$ binary matrix with coefficients $\Gamma(i,j) = \Gamma(j,i) = a_{ij}$, $i < j$, $\Gamma(i,i) = 0$. The LC operation on the graph associated to $p(\mathbf{x})$ can be expressed in terms of the adjacency matrix. Without loss of generality, we show how the matrix changes from Γ to Γ_0 after applying LC on vertex x_0:

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

The general algorithm, mod 2, is

$$\begin{cases} \Gamma_v(i,j) = \Gamma(i,j) + \Gamma(v,i) * \Gamma(v,j), & i < j, \quad i,j = 1,\ldots,n \\ \Gamma_v(i,i) = 0 \ \ \forall i \\ \Gamma_v(j,i) = \Gamma_v(i,j), & i > j \end{cases}$$

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

3.3 LC and Local Unitary (LU) Equivalence

Hein et al [45] state that LC-Equivalence (and therefore Local Unitary (LU) Equivalence) of graph states is obtained via successive transformations of the form,

$$U_v(G) = (-i\sigma_x^{(v)})^{1/2} \prod_{b \in \mathcal{N}_v} (i\sigma_z^{(b)})^{1/2} \ , \tag{3.1}$$

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) indicates that the Pauli matrix acts on qubit v (with I acting on all other qubits) [1] , and $\mathcal{N}_v$ comprises the neighbours of qubit v in the graphical representation. Define matrices x and z as follows:

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

and

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

where $w = e^{2\pi i/8}$. Furthermore, let $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$.

These matrices are the usual choice for representatives of the Local Clifford Group; however, we take as representatives I, H and N due mainly to the following properties:

- the flat spectra wrt $\{I,H,N\}^n$ identify Local Unitary (LU)-equivalent graph states, i.e. LU-equivalent stabilizer QECCs (see chapter 10), so one can explicitly use the $\{I,H,N\}^n$ spectrum to construct equivalent QECCs.

- $\{I,H,N\}$, identify the Local Clifford Group explicitly with multivariate *Discrete Fourier Transform* matrices (alternatively, to polynomial residue number systems),

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

whereas I, x, and z do not. Consider the bit-flip error. This can be modelled by multipliying a degree-one polynomial in z_i by z_i, mod z_i^2-1. The modulus, z_i^2-1 is a cyclic modulus, and $z_i^2-1=(z_i-1)(z_i+1)$, so the multiplication can be split over the residues of z_i^2-1, and this residue computation is defined precisely by cyclically transforming by H. Consider now the phase-flip followed by bit-flip error. This is the same as multiplying by z_i, mod z_i^2+1. Now $z_i^2+1=(z_i-i)(z_i+i)$, so computing the polynomial residues, mod z_i^2+1, is realised by negacyclically transforming by the matrix N. So H and N are the natural transforms intrinsically linked with bit-flip and phase-flip-then-bit-flip errors, respectively. The I is of course where no error happens. Note that phase-flip is (trivially) phase-flip-then-bit-flip followed by bit-flip. The use of I, H, and N allows one to examine the Pauli errors in the 'transform' domain. The use of I, H, and N bridges to the concept of generalised linear cryptanalysis, for which one would typically measure nonlinearity of a Boolean function w.r.t. the WHT. This is one of the aims of chapter 3 (see section 1.1).

- H and N are chosen because the rows of the matrices formed from tensor products of H and N can be written as $i^{p(\mathbf{x})}$, where p is a linear function from $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_4$. In fact this is just another way of stating the Fourier property mentioned above.

The idea of expressing the Clifford operations as a set of transforms, whether as tensor products of I, x, and xz, or as tensor products of I, H, and N, has not, to our knowledge, appeared in the QECC literature before. Clearly it is implicit by the transversal property of the Clifford Group, but we think that this would not be obvious to many readers.

Define $\mathbf{D}$ to be the set of 2×2 diagonal or anti-diagonal local unitary matrices, i.e. of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ or $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, for some a and b in $\mathbb{C}$, such that $|a|=|b|=1$. We make extensive use of the fact that a final multiplication of a spectral vector by tensor products of members of $\mathbf{D}$ does not change spectral coefficient magnitudes, due to the equations $|a|=|b|=1$. However, it does change the linear terms of the corresponding function. We include here a simple example to clarify this fact:

Example: Let $p:\mathbb{Z}_2\rightarrow\mathbb{Z}_4$, $p(x)=x+1(\text{ mod } 4)$. Then, $p(0)=1$, $p(1)=2$, so

$i^{p(x)} = \begin{pmatrix} i \\ -1 \end{pmatrix}$. Now, let $d = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \in \mathbf{D}$. Then,

$$di^{p(x)} = \begin{pmatrix} -1 \\ -1 \end{pmatrix} = i^{g(x)} \ ,$$

with $g(x) : \mathbb{Z}_2 \to \mathbb{Z}_4$, $g(x) = 2$. We can write this last term of the equation as $(-1)^{g'(x)}$, with $g'(x)$ Boolean, $g'(x) = 1$. So, by applying a member of $\mathbf{D}$ we have obtained a constant Boolean function from an affine generalised Boolean function. Observe that the spectral coefficients magnitude has not changed, as $|i^{p(x)}| = |i^{g(x)}|$.

In this sense a final multiplication by tensor products of members of $\mathbf{D}$ has no effect on the final spectrum and does not alter the underlying graphical interpretation. For instance, applying x twice to the same qubit is the same as applying $x^2 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, which is in $\mathbf{D}$. Therefore we can equate x^2 with the identity matrix, i.e. $x^2 \simeq I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Similarly, the action of any 2×2 matrix from $\mathbf{D}$ on a specific vertex is 'equivalent' to the action of the identity on the same vertex. Note that $z \in \mathbf{D}$. The same equivalence holds over n vertices, so we define an equivalence relation with respect to a tensor product of members of $\mathbf{D}$ by the symbol '$\simeq$'.

Definition 3.3 *Let u and v be two 2×2 unitary matrices. Then,*

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

This equivalence relation allows us to simplify the concatenation of actions of x and z on a specific qubit.

Remark: Note that $u \simeq v$ cannot be deduced from (and does not imply) $u = vd$ for some $d \in \mathbf{D}$.

We now show that the LC-orbit of an n-vertex graph is found as the transform spectra w.r.t. $\{I, x, xz\}^n$. Subsequently, it will be shown that we can alternatively find the LC-orbit as a subset of the transform set w.r.t. $\{I, H, N\}^n$. We then re-derive the single LC operation on a graph from the application of x (or N) on a single vertex.

3.3.1 The LC-orbit Occurs Within $\{I, x, xz\}^n$

We summarise the result of the beginning of section 3.3:

Lemma 3.4 *Given graphs G and G' as represented by the quadratic Boolean functions, $p(\mathbf{x})$ and $p'(\mathbf{x})$ respectively, then G and G' are in the same LC-orbit if and only if $(-1)^{p'(\mathbf{x})} \simeq U_{v_{t-1}} U_{v_{t-2}} \ldots U_{v_0} (-1)^{p(\mathbf{x})}$, where U_{v_i} are local unitary transformations as defined in (3.1).*

From Lemma 3.4 we see that, 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 from the action of LC on a graph that any LC-orbit must be 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 the spectra, to within a post-multiplication by the tensor product of matrices from $\mathbf{D}$. One can deduce from definition 3.3 that $zx \simeq x$, and it is easy to verify that

Lemma 3.5 *$zxx \simeq I$, and $xzx \simeq zxz$.*

With these definitions and observations we can derive the following theorem.

Theorem 3.6 *To within subsequent transformation by tensor products of matrices from $\mathbf{D}$, the LC-orbit of the graph, G, over n qubits (vertices) 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 and lemma 3.5,

$$\begin{aligned} xxx &\simeq x & zxx &\simeq I \\ xxz &\simeq I & zxz &\simeq xz \\ xzx &\simeq zxz \simeq xz & zzx &\simeq x \\ xzz &\simeq zxzz \simeq xzxz \simeq xxzx \simeq x & zzz &\simeq I \ . \end{aligned}$$

Thus, any product of three or more instances of x and/or z can always be reduced to I, x, or xz. Theorem 3.6 follows by recursive application of (3.1) with these rules, and by noting that the rules are unaffected by the tensor product expansion over n vertices. ∎

For instance, for $n = 2$, the LC-orbit of the graph represented by the quadratic function $p(\mathbf{x})$ is found as a subset of the $3^2 = 9$ transform spectra of $(-1)^{p(\mathbf{x})}$ w.r.t. the transforms

$I \otimes I$, $I \otimes x$, $I \otimes xz$, $x \otimes I$, $x \otimes x$, $x \otimes xz$, $xz \otimes I$, $xz \otimes x$, and $xz \otimes xz$. Theorem 3.6 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 in [27] that the number of LC-orbits for connected graphs for $n = 1$ to $n = 12$ are $1, 1, 1, 2, 4, 11, 26, 101, 440, 3132, 40457$, and 1274068, respectively (see also [45, 38, 47, 26, 87]).

3.3.2 The LC-orbit Occurs Within $\{I, H, N\}^n$

One can verify that $N \simeq x$ and $H \simeq xz$. Therefore one can replace x and xz with N and H, respectively, so the transform set, $\{I, xz, x\}$ becomes $\{I, H, N\}$. 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 the rows of x and xz to the rows of N and H provides a more natural set of multidimensional axes in some contexts. For t a non-negative integer,

$$N^{3t} \simeq I, \qquad N^{3t+1} \simeq N, \qquad N^{3t+2} \simeq H, \qquad N^{24} = I \ , \tag{3.2}$$

so N could be considered a 'generator' of $\{I, H, N\}$. 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 [69]. It also defines the basis axes under which aperiodic autocorrelation of Boolean functions is investigated in [28]. The *Negahadamard Transform*, $\{N\}^n$, was introduced in [64]. Constructions for Boolean functions with favourable spectral properties w.r.t. $\{H, N\}^n$ (amongst others) have been proposed in [68], and [67] showed that Boolean functions that are LU-equivalent to indicators for distance-optimal binary error-correcting codes yield favourable spectral properties w.r.t. $\{I, H\}^n$.

3.3.3 A Spectral Derivation of LC

We now re-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 $\mathbf{D}$. We will show that, as with Lemma 3.4, these repeated actions not only generate the LC-orbit of the graph, but 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 quadratic and represents a graph G. Then the action of N_v on G is equivalent to $U_v s$,

where:

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

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 Nega-hadamard 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, $m_i(\mathbf{x})$, as follows,

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

For $p(\mathbf{x})$ of any degree, the $m_i(\mathbf{x})$ are of degree $\leq n-1$. In the sequel we mix arithmetic, mod 2, and mod 4 so, to clarify the formulae for equations that mix moduli, 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. We must also define,

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

Theorem 3.7 *Let $s' = U_v s$, where $s = (-1)^{p(\mathbf{x})}$ and $s' = i^{p'(\mathbf{x})}$. Then,*

$$p'(\mathbf{x}) = 2 \left[p(\mathbf{x}) + \sum_{j \neq k} m_j(\mathbf{x}) m_k(\mathbf{x}) \right] + 3\mathcal{N}'_v(\mathbf{x}) + 3[x_v] \qquad (\ mod\ 4) \ . \tag{3.3}$$

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 3.8

$$\sum_{i=1}^{n}[A_i] \quad (\ mod\ 4) \qquad = \qquad [\sum_{i=1}^{n} A_i] + 2[\sum_{i\neq j} A_i A_j] \quad (\ mod\ 4) \quad \textit{where } A_i \in \mathbb{Z}_2 \ .$$

Observe the following action of N:

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

where $w = e^{2\pi i/8}$. We ignore the global constant, w, so that N maps $(-1)^{00}$ to i^{03} and $(-1)^{10}$ to i^{12}, and consequently $(-1)^{01}$ 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 $A, B \in \mathbb{Z}_2$, $\alpha, \beta \in \mathbb{Z}_4$, $(-1)^{AB}$ is mapped by N_v to $i^{\alpha\beta}$, where,

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

Substituting the previous expressions for A and B into the above and making use of Lemma 3.8 gives,

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

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

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

Substituting for α and β gives,

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

Applying Lemma 3.8 to the term $3[\mathcal{N}_v(\mathbf{x})]$,

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

Furthermore, Lemma 3.8 implies that,

$$2\left[\sum_{i=1}^{n} A_i\right] (\text{ mod } 4) = 2\sum_{i=1}^{n}[A_i](\text{ mod } 4) \quad \text{where } A_i \in \mathbb{Z}_2 \ .$$

■

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 (as shown in the example of section 3.3, the $\mathbb{Z}_4$ degree-one terms, $\mathcal{N}'_v(\mathbf{x})$ and $3[x_v]$, can be eliminated from (3.3) by appropriate subsequent action by members of $\{\mathbf{D}\}^n$ to s'. As all monomials, $m_i(\mathbf{x})$, are then of degree one, (3.3) reduces to,

$$p'(\mathbf{x}) \simeq p(\mathbf{x}) + \sum_{j,k \in \mathcal{N}_v, j \neq k} x_j x_k \qquad (\text{ mod } 2) \ . \tag{3.4}$$

(3.4) precisely defines the action of a single LC operation at vertex v of G, where we have used $\simeq$ to mean that $(-1)^{p'(\mathbf{x})} = BU(-1)^{p(\mathbf{x})}$, for some fully tensor-factorisable matrix, U, and 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 (3.3). In particular, one needs to intersperse with tensor products of the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

Theorem 3.9 *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 $D_1 \subset \mathbf{D}$ such that

$$D_1 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \quad | \quad a = 1, b = \pm 1\} \ .$$

Similarly, define $D_2 \subset \mathbf{D}$ such that

$$D_2 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \quad | \quad a = 1, b = \pm i\}, \quad \text{where } i^2 = -1 \ .$$

Then it is straightforward to establish that, for any $\Delta_1, \Delta'_1 \in D_1$, any $\Delta_2, \Delta'_2 \in D_2$, and any $c \in \{1, i, -1, -i\}$,

$$\begin{aligned} N\Delta_1 &= c\Delta'_1 N \qquad & H\Delta_1 &= c\Delta'_1 H \\ N\Delta_2 &= c\Delta_1 H \qquad & H\Delta_2 &= c\Delta_1 N \ . \end{aligned} \tag{3.5}$$

Let $\Delta_* \in D_1 \bigcup D_2$. Then, for a vertex, succesive applications of $\Delta_* N$ can, using (3.5), be re-expressed as,

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

But, from (3.2), successive powers of N generate I, H, or N, to within a final multiplication by a member of $\mathbf{D}$. 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. ∎

The question of how to generalise LC to hypergraphs will be treated in section 8.4.

Further spectral symmetries of Boolean functions w.r.t. $\{I, H, N\}^n$ are discussed in Section 3.5.

3.4 Generalised Bent Properties of Boolean Functions

3.4.1 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 $p(x)$ *at position* $\mathbf{k}$ by,

$$P_{\mathbf{k}} = 2^{-n/2} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{p(\mathbf{x}) + \mathbf{k} \cdot \mathbf{x}} \ , \tag{3.6}$$

where $\mathbf{x}, \mathbf{k} \in \mathrm{GF}(2)^n$, and $\cdot$ implies the scalar product of vectors.

The WHT of $p(\mathbf{x})$ can alternatively be defined as a multiplication of the vector $(-1)^{p(\mathbf{x})}$ by $H \otimes H \otimes \ldots \otimes H$. In other words,

$$P = (H \otimes H \otimes \ldots \otimes H)(-1)^{p(\mathbf{x})} = (\bigotimes_{i=0}^{n-1} H)(-1)^{p(\mathbf{x})} \ , \tag{3.7}$$

where $P = (P_{(0,\ldots,0)}, \ldots, P_{(1,\ldots,1)}) \in \mathbb{C}^{2^n}$.
Then, $p(\mathbf{x})$ is defined to be *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 3.10 *[53]* $p(\mathbf{x})$ *is* bent $\quad \Leftrightarrow \quad det(\Gamma) = 1 \ mod \ 2$.

It is well-known [53] that 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 $\mathbf{c} \in \mathrm{GF}(2)^n$, and $d \in \mathrm{GF}(2)$. 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*$_4$).

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

We now investigate certain spectral properties of Boolean functions with respect to the set of transforms $\{H,N\}^n$, that 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 assertion 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 $\mathbf{k} \in \mathrm{GF}(2)^n$ and $d \in \mathrm{GF}(2)$. In other words, if $p(\mathbf{x})$ is bent then so it is when we add any affine offset, mod 2. However the above assertion does not follow when one considers every possible $\mathbb{Z}_4$-linear offset of the Boolean function. The WHT of $p(\mathbf{x})$ with a $\mathbb{Z}_4$-linear offset can be defined as follows.

$$P_{\mathbf{k},\mathbf{c}} = 2^{-n/2} \sum_{\mathbf{x}\in GF(2)^n} (i)^{2[p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}]+[\mathbf{c}\cdot\mathbf{x}]} \qquad \mathbf{k},\mathbf{c} \in \mathrm{GF}(2)^n \ . \tag{3.8}$$

Definition 3.11

$$p(\mathbf{x}) \textit{ is } \text{bent}_4 \quad \Leftrightarrow \quad \forall\ \mathbf{k} \in GF(2)^n \ \ \exists \mathbf{c} \textit{ such that } |P_{\mathbf{k},\mathbf{c}}| = 1 \qquad .$$

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

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

$$s' = U(-1)^{p(\mathbf{x})} \ . \tag{3.9}$$

Lemma 3.12 *$p(\mathbf{x})$ 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 $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, and where the f_t's are linear, $f_t : \mathrm{GF}(2)^n \rightarrow \mathbb{Z}_4$, and the coefficient of x_j in any $f_t \in \{0, 2\}$ for $j \in \mathbf{R_H}$ and $f_t \in \{1, 3\}$ for $j \in \mathbf{R_N}$. Therefore s' can always be expressed, equivalently, as $s' = (\prod H_i)(i)^{2p[\mathbf{x}]+[f'_t(\mathbf{x})]}$, where the f'_t's are linear, $f'_t : \mathrm{GF}(2)^n \rightarrow \mathrm{GF}(2)$, and the coefficient of x_j in any f'_t 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 3.13 *Let $p(\mathbf{x})$ be a quadratic Boolean function. Then, $p(\mathbf{x})$ is bent$_4$ if and only if $det(\Gamma_\mathbf{v}) = 1$ mod 2, for some $\mathbf{v} \in GF(2)^n$, where $\Gamma_\mathbf{v}$ is a modified form of Γ with v_i in position $[i, i]$, and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.*

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

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

$$a_k = \sum_{x_0 \in GF(2)} (-1)^{p(x_0)+p(x_0+k)}, \qquad k \in \mathrm{GF}(2) \ .$$

Then it is well-known that $s' = Hs$ is a flat spectrum if and only if $a_k = 0$ for $k \neq 0$.

Define the negaperiodic autocorrelation function as follows,

$$b_k = \sum_{x_0 \in GF(2)} (-1)^{p(x_0)+p(x_0+k)+k(x_0+1)}, \qquad k \in \mathrm{GF}(2) \ .$$

Then $s' = Ns$ is a flat spectrum if and only if $b_k = 0$ for $k \neq 0$. (For p a Boolean function of just one variable, Hs is never flat and Ns is always flat, but this only holds for one variable).

We now elaborate on the two claims above. 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, $a(z) = s(z)s(z^{-1}) \bmod (z^2-1)$, 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 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, $b(z) = s(z)s(z^{-1}) \bmod (z^2+1)$, 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 Chinese Remainder Theorem realised by $N^\dagger s'$). By Parseval, s' can only be flat if $b_1 = 0$.

We 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,

$$A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = \sum_{\mathbf{x} \in GF(2)^n} (-1)^{p(\mathbf{x})+p(\mathbf{x}+\mathbf{k})+\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i) k_i (x_i+1)} \quad , \tag{3.10}$$

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,

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

In polynomial terms, with $\mathbf{z} \in \mathrm{GF}(2)^n$ and $s(\mathbf{z}) = \sum_{\mathbf{j} \in GF(2)^n} s_{\mathbf{j}} \prod_{i=0}^{n-1} z_i^{j_i}$, we have,

$$\begin{aligned} A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) &= \sum_{\mathbf{k} \in GF(2)^n} A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} \prod_{i=0}^{n-1} z_i^{k_i} \\ &= s(z_0, \ldots, z_{n-1}) s(z_0^{-1}, \ldots, z_{n-1}^{-1}) \bmod \prod_{i=0}^{n-1} (z_i^2 - (-1)^{\chi_{\mathbf{R_N}}(i)}) \ . \end{aligned} \tag{3.11}$$

Then, by appealing to a multivariate version of Parseval's Theorem, s' as defined in (3.9) is flat if and only if $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall\ \mathbf{k} \neq \mathbf{0}$.

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

$$p(x_0, x_1, \ldots, x_{n-1}) = a_{01}x_0x_1 + a_{02}x_0x_2 + \cdots + a_{ij}x_ix_j + \cdots + a_{n-2,n-1}x_{n-2}x_{n-1} \ .$$

Therefore,

$$\begin{aligned}
&p(\mathbf{x}) + p(\mathbf{x}+\mathbf{k}) + \textstyle\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i)k_ix_i = \\
&k_0(\chi_{\mathbf{R_N}}(0)x_0 + a_{01}x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) \\
&+k_1(a_{01}x_0 + \chi_{\mathbf{R_N}}(1)x_1 + a_{03}x_3 + \cdots + a_{0,n-1}x_{n-1}) \\
&+\cdots \\
&+k_{n-1}(a_{0,n-1}x_0 + a_{1,n-1}x_{n-1} + \cdots + a_{n-2,n-1}x_{n-2} + \chi_{\mathbf{R_N}}(n-1)x_{n-1}) \ .
\end{aligned}$$

This is equal to:

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

which is balanced unless it is 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 then the following system of equations:

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

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,

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

Theorem 3.14 *All Boolean functions of degree ≤ 2 are bent$_4$.*

Proof: Degree zero and degree one functions are trivial. Now, let $p(\mathbf{x})$ be a quadratic in n variables. Consider then the adjacency matrix, Γ, associated with $p(\mathbf{x})$. We now prove that $\Gamma_{\mathbf{v}}$ has maximum rank (mod 2) for at least one choice of $\mathbf{v}$, where $\Gamma_{\mathbf{v}} = \Gamma + \mathrm{diag}(\mathbf{v})$ as before. Let M be the $(n-1) \times (n-1)$ minor associated with the first entry of Γ; in other words, let $\Gamma = \begin{pmatrix} 0 & A \\ A^T & M \end{pmatrix}$, where A is a matrix $1 \times (n-1)$, A^T its transpose and M a matrix $(n-1) \times (n-1)$.

We prove by induction that there exists at least one choice of v such that $\Gamma_{\mathbf{v}}$ has maximum rank (mod 2). 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, and we will see that it is true for n variables. If the determinant of Γ is 1 we 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 $\mathbf{v}(M) \in \mathrm{GF}(2)^{n-1}$, where $\mathbf{v}(M) = (v_1, \ldots, v_{n-1})$ such that $M_{\mathbf{v}(M)}$ has full rank. Let $\mathbf{v}' = (0, v_1, \ldots, v_{n-1}) \in \mathrm{GF}(2)^n$. 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 3.13. ∎

Remark: Theorem 3.14 is true even for Boolean functions associated with non-connected or empty graphs.

Lemma 3.15 *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 3.15 identifies an open problem:

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

Theorem 3.16 *For $P_{\mathbf{k},\mathbf{c}}$ as defined in 3.8, there is no Boolean function $p(\mathbf{x})$ such that $|P_{\mathbf{k},\mathbf{c}}| = 1$ $\forall \mathbf{c}, \mathbf{k} \in GF(2)^n$.*

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 3.14. 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 3.14. 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 3.13. We have established that, for a fixed choice of $\mathbf{R_H}$ and $\mathbf{R_N}$, s', as defined in (3.9), 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 $|P_{\mathbf{k},\mathbf{c}}| = 1$ $\forall \mathbf{c}, \mathbf{k} \in \mathrm{GF}(2)^n$ 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 $|P_{\mathbf{k},\mathbf{c}}| = 1$ $\forall \mathbf{c}, \mathbf{k} \in \mathrm{GF}(2)^n$, then the polynomials, $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z})$, as defined in (3.11), 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 Chinese Remainder Theorem (CRT) we can combine these polynomials for each choice of $\mathbf{R_H}$ and $\mathbf{R_N}$ to construct the polynomial,

$$r(\mathbf{z}) \bmod \prod_{j=0}^{n} (z_j^4 - 1) = \mathrm{CRT}\{A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) \mid \forall \mathbf{R_H}, \mathbf{R_N}\} \ , \tag{3.12}$$

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 (3.12) 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 (3.12) 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, $\prod_j z_j^{-1^{u_j}}$, $u_j \in \mathbb{Z}_2$, in $r(\mathbf{z})$ can never be zero, but are always ± 1. ∎

Remark: Although we proved theorem 3.16 only for Boolean functions, it is possible to generalise the theorem for functions $\mathrm{GF}(2)^n \to \mathrm{GF}(q)$, for any even integer q.

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

We now investigate certain spectral properties of Boolean functions with respect to the set of transforms $\{I, H\}^n$, that 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 $\{0, \ldots, n-1\}$. [67] has investigated other spectral properties w.r.t. $\{I, H\}^n$, such as *weight hierarchy* if the graph is bipartite.

The WHT of the subspace of a function from $\mathrm{GF}(2)^n$ to $\mathrm{GF}(2)$, obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, can be defined as follows. Let $\theta \in \mathrm{GF}(2)^n$ 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,

$$P_{\mathbf{k},\mathbf{r},\theta} = 2^{-(n-\mathrm{wt}(\theta))/2} \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (-1)^{p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}} \qquad \mathbf{k} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \ . \tag{3.13}$$

Definition 3.17

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

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

Let

$$U = \prod_{j\in\mathbf{R_I}} I_j \prod_{j\in\mathbf{R_H}} H_j \ . \tag{3.14}$$

Lemma 3.18 $p(\mathbf{x})$ *is I-bent if there exist one or more partitions,* $\mathbf{R_I}, \mathbf{R_H}$ *such that* $s' = U(-1)^{p(\mathbf{x})}$ *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 3.19 *For quadratic $p(\mathbf{x})$,*

$$p(\mathbf{x}) \text{ is I-bent} \quad \Leftrightarrow \quad \Gamma_I \text{ has maximum rank, mod 2}$$

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 3.20 *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 $|\mathbf{R_I}| = n - 2$. ∎

Lemma 3.21 *Not all Boolean functions of degree > 2 are I-bent.*

Proof: Counter-example - by computation there are no I-bent cubics of three variables. ∎ Further computations show that there are only 416 I-bent cubics in four variables, and no I-bent quartics in four variables. There are only 442640 I-bent cubics, only 1756160 I-bent quartics in five variables, and no I-bent quintics in five variables. I-bent cubics in six variables do exist. Lemma 3.21 indicates an open problem:

What is the maximum algebraic degree of an I-bent Boolean function of n variables?

Theorem 3.22 *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 (3.14), s' cannot be flat. ∎

3.4.4 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 GF(2)^n to GF(2), obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, is defined as follows. Let $\theta \in$ GF(2)^n be such that $\theta_j = 1$ iff $j \in \mathbf{R_I}$. Let $\mathbf{r} \preceq \theta$. Then,

$$P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta} = 2^{-(n-\mathrm{wt}(\theta))/2} \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (i)^{2[p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}]+[\mathbf{c}\cdot\mathbf{x}]} \qquad \mathbf{k}, \mathbf{c} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \ . \tag{3.15}$$

Definition 3.23

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

where $wt(\theta) < n$.

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

$$U = \prod_{j\in\mathbf{R_I}} I_j \prod_{j\in\mathbf{R_H}} H_j \prod_{j\in\mathbf{R_N}} N_j \ . \tag{3.16}$$

$$s' = U(-1)^{p(\mathbf{x})} \ . \tag{3.17}$$

Lemma 3.24 $p(\mathbf{x})$ *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 (3.10), we get flat spectra for one or more partitions $\mathbf{R_I}, \mathbf{R_H}, \mathbf{R_N}$ iff

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

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 3.25 *For quadratic* $p(\mathbf{x})$,

$$p(\mathbf{x}) \textit{ is I-bent}_4 \quad \Leftrightarrow \quad \Gamma_{I,\mathbf{v}} \textit{ has maximum rank, mod 2,} \quad \textit{where } \mathbf{v} \preceq \bar{\theta}$$

for one or more choices of $\mathbf{v}$ *and* θ *where* $wt(\theta) < n$.

In general,

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

Lemma 3.26 *All Boolean functions are I-bent$_4$.*

Proof: From Theorem 3.7, 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 3.27 *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 theorems 3.16 or 3.22. ∎

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 3.28 *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 3.29 *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 16.1 lists 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 abbreviated so that, say, ab, de, fg is short for $x_a x_b + x_d x_e + x_f x_g$. 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 3.1: Representatives for all LC-Orbits which are not LC-bent for $n = 2$ to 10

3.5 Further Spectral Symmetries of Boolean Functions

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 [2]. 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. In this section we ascertain for which binary transformations (other than LC) the power spectra of the $\{I, H, N\}^n$ transform remains invariant to within a re-ordering of the spectral elements within each spectrum. We refer to the complete set of $3^n \times 2^n$ power spectral values w.r.t. $\{I, H, N\}^n$ as $\mathbf{S_{IHN}}$. Moreover, 'invariance' is to within any re-ordering of the $3^n \times 2^n$ spectral elements. From the discussion of sections

[2] The *power* of the k^{th} spectral element, P_k, is given by $|P_k|^2$, where P_k is defined in (3.6).

3.3.1 and 3.3.2 it is evident that $\mathbf{S_{IHN}}$ of a quadratic Boolean function is LC-invariant. However the LC-orbit is not the only spectral symmetry exhibited with respect to $\mathbf{S_{IHN}}$. We identify the following symmetries.

Lemma 3.30 *Let $p(\mathbf{x})$ be a Boolean function of* any *degree. Then $\mathbf{S_{IHN}}$ of $p(\mathbf{x})$ and $\mathbf{S_{IHN}}$ of $p(\mathbf{x}) + l(\mathbf{x})$ are equivalent, where l is any affine function of its arguments.*

Lemma 3.31 *Let $p(\mathbf{x})$ be a Boolean function of* any *degree over n variables. Then $\mathbf{S_{IHN}}$ of $p(\mathbf{x})$ and $\mathbf{S_{IHN}}$ of $p(\mathbf{x} + \mathbf{a})$ are equivalent, where $\mathbf{a} \in GF(2)^n$.*

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 the rest of the positions.

We can rewrite $H\sigma_x$ as follows,

$$\begin{aligned} H\sigma_x &= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} H = \sigma_z H \ . \end{aligned}$$

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 $\mathbf{D}$ (see section 3.3 for a definition of $\mathbf{D}$) 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 follows,

$$\begin{aligned} N\sigma_x &= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \\ &= \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} N = -\sigma_y N \ , \end{aligned}$$

where σ_y is one of the four Pauli matrices. 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 the set $\mathbf{D}$. Therefore the power spectra produced by N is invariant to a prior periodic shift.

The above argument is trivial with respect to I. The argument extends naturally to any n-dimensional tensor product of I, H, and N. ∎

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

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

where $\mathbf{a}, \mathbf{c} \in \mathrm{GF}(2)^n$, $d \in \mathrm{GF}(2)$, and '$\cdot$' is the scalar product.

The symmetries generated by affine offset and periodic shift include all symmetries generated by any combination of periodic and negaperiodic shift, because we perform periodic and negaperiodic shifts on $p(\mathbf{x})$ by the following operation:

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

where $\mathbf{a}, \mathbf{c} \in \mathrm{GF}(2)^n$, '$\mathbf{c} \preceq \mathbf{a}$' means that $c_i \leq a_i$, $\forall i$ (i.e. *a covers c*), and $\mathrm{wt}(\mathbf{c})$ is the binary weight of $\mathbf{c}$. The one positions in $\mathbf{a}$ identify variables x_i which are to undergo periodic or negaperiodic shift, and the one positions in $\mathbf{c}$ identify the variables x_i which are to undergo negaperiodic shift. The combined periodic and negaperiodic symmetry induced by $\{I, H, N\}^n$ implies an aperiodic symmetry, as discussed in [28].

3.6 Conclusion

This chapter 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 has been generalised in a number of ways to $\{I, H, N\}^n$. Various theorems about the generalised bent properties of Boolean functions have been established. We showed how a quadratic Boolean function maps to a graph and 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. Concretely, we prove that a function

will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix, concretely the matrix resultant of the following actions, has non-zero determinant mod 2:

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

In chapter 4, we shall apply this method to enumerate the flat spectra w.r.t. $\{I, H\}^n$, $\{H, N\}^n$ and $\{I, H, N\}^n$ for certain specific functions.

Chapter 4

Generalised Bent Criteria – Recursive Relationships

The results for this chapter can be found in [75].

4.1 Overview

In this chapter, we apply the techniques presented in chapter 3, to prove that, for certain recursive quadratic Boolean constructions, one can establish simple recursive relationships for the number of flat spectra w.r.t. the $\{I, H, N\}^n$ transform set. For those Boolean constructions, we prove simple recursions for the number of flat spectra w.r.t. the $\{I, H, N\}^n$ transform set or subsets thereof. We also observe that optimal *Quantum Error-correcting Codes* (QECCs), interpreted as quadratic Boolean functions, appear to maximise the number of flat spectra w.r.t. $\{I, H, N\}^n$. Very loosely, for Boolean functions of fixed degree, the more flat (or near-flat) spectra w.r.t. $\{I, H, N\}^n$ we obtain for the function, the stronger it is cryptographically, and the more *entangled* it is when interpreted as a quantum state [67, 45].

In sections 4.2, 4.3 and 4.4, we compute, by means of a modified adjacency matrix, the number of flat spectra for some Boolean functions w.r.t $\{H, N\}^n$, $\{I, H\}^n$ and $\{I, H, N\}^n$ respectively. It is desirable to identify Boolean functions which maximise the number of flat spectra w.r.t. $\{I, H, N\}^n$, as this is a criterion for high *entanglement* for the corresponding pure multipartite quantum states which are represented by Boolean functions [67, 45]. We

will see that the quadratic line and clique functions appear to maximise the number of flat spectra w.r.t. $\{H, N\}^n$ and $\{I, H\}^n$, respectively, and that the quadratic functions representing high-distance QECCs appear to maximise the number of flat spectra w.r.t. $\{I, H, N\}^n$. Recent graphical descriptions for these optimal QECCs [29] suggest that *nested-clique* structures may maximise the number of flat spectra w.r.t. $\{I, H, N\}^n$. As an initial step towards the analysis of such functions we provide recursive formulae for the number of flat spectra for the 'clique-line-clique' structure.

Some recent papers [2, 1, 4, 5] have proposed *interlace polynomials* to describe some properties of graphs. In particular, polynomials $q(x)$ and $Q(x)$ are defined, and proven to be certain *Martin polynomials*, as proposed by Bouchet [17]. It can be shown that $q(x)$ and $Q(x)$ summarise certain aspects of the spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$, respectively. In particular, $q(1)$ and $Q(2)$ evaluate the number of flat spectra w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$, respectively. We develop these ideas in chapter 5.

Section 4.5 contains a few concluding remarks. The results of this chapter are summarised in the appendix of the chapter (section 4.6).

4.2 Number of Flat Spectra: $\{H, N\}^n$

We wish to construct Boolean functions that have flat spectra w.r.t. the largest possible subset of $\{H, N\}^n$ transforms. The multivariate complementary set constructions of [68] provide candidate functions. The simplest and strongest of these is the line function (or path graph) [81, 39, 31].

4.2.1 Line

The *line function* in n variables, $p_n^l(\mathbf{x})$, is defined as

$$p_n^l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d \ , \tag{4.1}$$

where $\mathbf{x},\ \mathbf{c} \in \mathrm{GF}(2)^n$, $\mathbf{x} = (x_0, \ldots, x_{n-1})$, and $d \in \mathrm{GF}(2)$. Its number of flat spectra with respect to $\{H, N\}^n$ is as follows:

Lemma 4.1 *The number of flat spectra of the line w.r.t.* $\{H,N\}^n$, $K_n^{HN}(p_n^l(\mathbf{x}))$, *is* $K_n^{HN}(p_n^l(\mathbf{x})) = 2^n - K_{n-1}^{HN}(p_{n-1}^l(\mathbf{x}))$, *with* $K_1^{HN}(p_1^l(\mathbf{x})) = 1$*; in closed form,*

$$K_n^{HN}(p_n^l(\mathbf{x}))) = \frac{1}{3}\left(2^{n+1} + (-1)^n\right) \ .$$

Proof: The generic modified matrix of the line for $\{H,N\}^n$ is as follows:

$$\Gamma_{\mathbf{v}} = \begin{pmatrix} v_0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & v_1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & v_2 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & v_{n-1} \end{pmatrix} \ ,$$

where $\mathbf{v} = (v_0, \dots, v_{n-1}) \in \mathrm{GF}(2)^n$.

Computing the determinant, we get the recursion formula

$$D_n = v_0 D_{n-1} + D_{n-2} \bmod 2 \ , \tag{4.2}$$

where D_{n-j} is the determinant of the generic modified matrix of the line in the variables $x_j, \dots, x_{n-1}$. The spectrum will be flat iff $D_n = 1$. In order to get this, we consider the following cases:

1. $D_{n-1} = 0, D_{n-2} = 0$. In this case, $D_n = 0$, so the spectrum cannot be flat.
2. $D_{n-1} = 0, D_{n-2} = 1$. In this case, v_0 can be 0 or 1.
3. $D_{n-1} = 1, D_{n-2} = 1$. In this case, $v_0 = 0$.
4. $D_{n-1} = 1, D_{n-2} = 0$. In this case, $v_0 = 1$.

We then have $K_n^{HN}(p_n^l(\mathbf{x})) = 2K1 + K2 + K3$, where Ki is the number of times the i^{th} case is true. Note that

$$\{v_1, \dots, v_{n-1} | D_{n-1} = D_{n-2} = 1\} \cup \{v_1, \dots, v_{n-1} | D_{n-1} = 1, D_{n-2} = 0\} = \{v_1, \dots, v_{n-1} | D_{n-1} = 1\} \ ,$$

and therefore $K2 + K3 = K_{n-1}^{HN}(p_{n-1}^l(\mathbf{x}))$.

We see now that

$$\{v_1, \dots, v_{n-1} | D_{n-1} = 0, D_{n-2} = 1\} = \{v_1, \dots, v_{n-1} | D_{n-1} = 0\} \ ,$$

and so $K1 = 2^{n-1} - K_{n-1}$. Suppose $D_{n-1} = D_{n-2} = 0$. By the equation $D_{n-1} = v_1 D_{n-2} + D_{n-3}$ (obtained from 4.2), this implies $D_{n-3} = 0$. By the same argument, we must have $D_i = 0,\ 1 \leq i \leq n-1$. However, if $D_1 = v_{n-1} = 0$ then $D_2 = v_{n-2}v_{n-1} + 1 = 1$, which leads to a contradiction.

Finally, we get $K_n^{HN}(p_n^l(\mathbf{x})) = 2(2^{n-1} - K_{n-1}^{HN}(p_{n-1}^l(\mathbf{x}))) + K_{n-1}^{HN}(p_{n-1}^l(\mathbf{x})) = 2^n - K_{n-1}^{HN}(p_{n-1}^l(\mathbf{x}))$. Expanding this recurrence relation, and using the fact that $K_1^{HN}(p_1^l(\mathbf{x})) = 1$, we get $K_n^{HN}(p_n^l(\mathbf{x})) = \sum_{k=0}^{n}(-1)^{n+k}2^k = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$, as claimed. ∎

4.2.2 Clique

We recall here definition 2.23: the *clique function* or *complete graph* is defined as the graph in which an edge connects every pair of vertices. In ANF terms, this is equivalent to:

Definition 4.2 *The* clique function *or* complete graph *is defined as*

$$p_n^c(\mathbf{x}) = \sum_{0 \leq i < j \leq n-1} x_i x_j \ , \tag{4.3}$$

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

For this function, the number of flat spectra with respect to $\{H, N\}^n$ is given as follows:

Lemma 4.3 *The number of flat spectra of the clique function w.r.t. the set* $\{H, N\}^n$, $K_n^{HN}(p_n^c(\mathbf{x}))$, *is* $K_n^{HN}(p_n^c(\mathbf{x})) = K_{n-1}^{HN}(p_{n-1}^c(\mathbf{x})) + 1 + (-1)^n$*; in closed form,*

$$K_n^{HN}(p_n^c(\mathbf{x})) = n + \frac{1 + (-1)^n}{2} \ .$$

Proof: The generic modified adjacency matrix of the clique is as follows:

$$\Gamma_{\mathbf{v}} = \begin{pmatrix} v_0 & 1 & 1 & 1 & \ldots & 1 \\ 1 & v_1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & v_2 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \ldots & v_{n-1} \end{pmatrix} \ .$$

Applying N to the bipolar vector of the clique function, $(-1)^{p_n^c(\mathbf{x})}$, in the position i is equivalent to making $v_i = 1$. If two or more of the v_i's are 1, then the matrix will not have

full rank, so $|\mathbf{R_N}| \leq 1$. We will denote as D the determinant of the modified adjacency matrix $\Gamma_\mathbf{v}$.

First, suppose $|\mathbf{R_N}| = 1$. Let $v_i \in \mathbf{R_N}$. In this case, we get $D = \det(\Gamma_\mathbf{v}) = \det(\Gamma) + m$, where m is the minor corresponding to v_i. Obviously, m is the determinant of the adjacency matrix of a clique in $n-1$ variables. It is easy to show that the clique in n variables is bent iff n is even. So, if n is even, we have $\det(\Gamma) = 1,\ m = 0$, and so $D = 1$. On the other hand, if n is odd, we have $\det(\Gamma) = 0,\ m = 1$, and so $D = 1$. This means that for every position in which we choose to apply N, we have a flat spectrum, and therefore we get n flat spectra for this case.

Now, suppose $|\mathbf{R_N}| = 0$. Since the clique is bent in an even number of variables, we have flat spectra iff n is even.

From the preceding argument, we see that $K_n^{HN}(p_n^c(\mathbf{x})) = n + \frac{1+(-1)^n}{2}$. The recurrence formula follows trivially. ∎

4.2.3 Clique-Line-Clique

By combining the clique and line graphs in certain ways we can get an improvement in the number of flat spectra of a clique in the same number of variables, though we are still far from the number of flat spectra of a line in the same number of variables.

Specifically, if we define the *n clique-line-m clique* as

$$p_{n,m}(\mathbf{x}) = \sum_{0 \leq i < j \leq n-1} x_i x_j + x_{n-1}x_n + \sum_{n \leq i < j \leq n+m-1} x_i x_j \ , \tag{4.4}$$

where $\mathbf{x} = (x_0, \ldots, x_{n+m-1}) \in \mathrm{GF}(2)^{n+m}$, the number of flat spectra w.r.t. $\{H, N\}^{n+m}$ is as given as follows:

Lemma 4.4 *The number of flat spectra of the n clique-line-m clique w.r.t.* $\{H, N\}^n$, $K_n^{HN}(p_{n,m}(\mathbf{x}))$, *for* $n,\ m \geq 1$, *is*

$$\begin{aligned} K_{n,m}^{HN}(p_{n,m}(\mathbf{x})) &= 3nm - n(\tfrac{1+(-1)^m}{2}) - m(\tfrac{1+(-1)^n}{2}) \\ &+ 3(\tfrac{1+(-1)^n}{2})(\tfrac{1+(-1)^m}{2}) \ . \end{aligned}$$

Proof: The generic modified adjacency matrix of the graph is as follows:

$$\Gamma_{\mathbf{v}} = \begin{pmatrix} v_0 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & v_1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & v_{n-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 & v_n & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & \ddots & 0 & 1 & v_{n+1} & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots & v_{n+m-1} \end{pmatrix}.$$

Solving the determinant by minors along the n^{th} column or row, we see that $|\Gamma_{\mathbf{v}}| = |G_c| + C$, where G_c is the generic modified adjacency matrix of the two independent cliques:

$$G_c = \begin{pmatrix} v_0 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & v_1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & v_{n-1} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & v_n & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & \ddots & 0 & 1 & v_{n+1} & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots & v_{n+m-1} \end{pmatrix}$$

and C is the product of the first $(n-1) \times (n-1)$ minor and the last $(m-1) \times (m-1)$ minor:

$$C = \begin{vmatrix} v_0 & 1 & 1 & \dots & 1 \\ 1 & v_1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & v_{n-2} \end{vmatrix} \cdot \begin{vmatrix} v_{n+1} & 1 & 1 & \dots & 1 \\ 1 & v_{n+2} & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & v_{n+m-1} \end{vmatrix}.$$

The first minor corresponds to the determinant of a clique in $n-1$ variables, say C_1, and the second to that of a clique in $m-1$ variables, say C_2.

As seen in the proof of lemma 4.3, we have to look separately at the different cases that arise from the parities of n and m. For brevity, we will denote by K_n^c the number of flat spectra of the clique in n variables w.r.t. $\{H, N\}^n$.

- Case n, m odd: Here, $C = 0$ iff two or more of the $v_0, v_1, \ldots, v_{n-2}$ and/or two or more of $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to 1. In that case $|G_c| = 0$ as well, since there will be linear dependence in the rows of G_c. Therefore the only case in which we obtain $|\Gamma_{\mathbf{v}}| = 1$ is when $C = 1$ and $|G_c| = 0$.
  The number of times $|C_1| = 1$ is K^c_{n-1}, and the number of times $|C_2| = 1$ is K^c_{m-1}. Hence, we can have $C = 1$ in $K^c_{n-1}K^c_{m-1}$ ways, and the rank of $\Gamma_{\mathbf{v}}$ will depend on its rows containing the variables v_{n-1} and v_n. The way to get $|G_c| = 0$ is to make the choice of v_{n-1} and v_n such that it makes the first and/or second cliques within G_c not flat. Therefore,

$$K^{HN}_{n,m} = K^c_{n-1}(2K^c_{m-1}) + K^c_{m-1}(2K^c_{n-1} - K^c_{n-1}) = 3(n - 1 + \tfrac{1+(-1)^{n-1}}{2})(m - 1 + \tfrac{1+(-1)^{m-1}}{2}) \ .$$

- Case n even, m odd: Here, $C = 0$ as above and also iff $v_0 = v_1 = \ldots = v_{n-2} = 0$. In the last case it is possible to have $|G_c| = 1$ iff both cliques within G_c have flat spectra. This happens $2K^c_m$ times: for the first clique we have $v_0 = v_1 = \ldots = v_{n-2} = 0$ and so v_{n-1} can be 0 or 1. Adding this to the number we found above, we get $3(n - 1 + \frac{1+(-1)^{n-1}}{2})(m - 1 + \frac{1+(-1)^{m-1}}{2}) + 2m + 1 + (-1)^m$.

- Case n odd, m even: As in the previous case, we get

$$3(n - 1 + \tfrac{1+(-1)^{n-1}}{2})(m - 1 + \tfrac{1+(-1)^{m-1}}{2}) + 2n + 1 + (-1)^n \ .$$

- Case n, m even: In this case we have all the flat spectra of the second case, plus the number of flat spectra coming from $v_{n+1} = v_{n+2} = \ldots = v_{n+m-1} = 0$ which are not already counted. This number is $2(K^c_{n-1} - 2)$. Adding it to the rest we get

$$3(n - 1 + \tfrac{1+(-1)^{n-1}}{2})(m - 1 + \tfrac{1+(-1)^{m-1}}{2}) + 2(m + n - 1) + (-1)^m + (-1)^n \ .$$

Summing up and simplifying, we get the desired formula. ∎

Note: The formula is still valid for n or m equal to 1, if we consider $K^c_0 = 1$.

4.2.4 Comparison

Table 4.1 summarises our results for the $\{H, N\}^n$ transform set. Further computational results show that, for $n \leq 8$ and $n \leq 5$, the line has the maximum number of flat spec-

tra w.r.t. $\{H, N\}^n$ over the set of quadratics and over the set of all Boolean functions, respectively. We can therefore conjecture the following:

Conjecture 4.5 *Over the set of all Boolean functions, the line function, as defined in (4.1), maximizes the number of flat spectra w.r.t.* $\{H, N\}^n$.

4.3 Number of Flat Spectra: $\{I, H\}^n$

As in the previous section, it would also be interesting to construct Boolean functions with the largest possible number of flat spectra w.r.t. $\{I, H\}^n$. Note that for the *interlace polynomial*, $q(x)$, of a graph, as defined in [4], one can show that $q(1)$ is the number of flat spectra w.r.t. $\{I, H\}^n$.

4.3.1 Line

The number of flat spectra of the line function, as defined by (4.1), with respect to $\{I, H\}^n$, is the Fibonacci recurrence:

Lemma 4.6 *The number of flat spectra of the line function in n variables w.r.t.* $\{I, H\}^n$, $K_n^{IH}(p_n^l(\mathbf{x}))$, *follows the relationship* $K_n^{IH}(p_n^l(\mathbf{x})) = K_{n-1}^{IH}(p_{n-1}^l(\mathbf{x})) + K_{n-2}^{IH}(p_{n-2}^l(\mathbf{x}))$, *with initial values* $K_0^{IH}(p_0^l(\mathbf{x})) = K_1^{IH}(p_1^l(\mathbf{x})) = 1$*; in closed form,*

$$K_n^{IH}(p_n^l(\mathbf{x})) = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}} \ .$$

Proof: We are first going to see that

$$K(k) = \sum_{\sum_{\lambda=0}^{k} t_\lambda = n-k} \prod_{j=0}^{k} K_{t_j}^H \ ,$$

where $K(k)$ is the number of flat spectra when $|R_I| = k$, and K_i^H is the number of flat spectra in i variables of the line function, after the fixing of the variables in R_I, w.r.t. $\{H\}^i$. It is easy to see that $K_i^H = \frac{1+(-1)^i}{2}$, with $K_0^H = 1$.

Let $R_I = \{i_0, \ldots, i_{k-1}\}$. Then,

$$D(k) = \det(\Gamma_I) = D^{0,\ldots,i_0-1} D^{i_0+1,\ldots,i_1-1} \cdots D^{i_k+1,\ldots,n-1} \ , \tag{4.5}$$

where $D^{k_0,\ldots,k_t}$ is the determinant of the generic modified matrix of the line, Γ_I, in the variables $x_{k_0},\ldots,x_{k_t}$. With a slight abuse of notation, in the cases $i_0 = 0, i_{j+1} = i_j + 1$ or $i_k = n-1$, we will consider the corresponding determinant of the empty matrix to be equal to 1. To prove this formula we use induction on k:

Case $k = 0$ ($R_I = \emptyset$). Evidently, $D(0) = D^{0,\ldots,n-1}$.

Case $k = 1$. In this case $R_I = \{i_0\}$. When we 'cross out' the i_0^{th} row and column from the matrix, we get a block matrix of four blocks in which both anti-diagonal blocks are zero. $D(1) = 1$ if and only if the rows of the matrix are linearly independent. But because of the anti-diagonal blocks being zero, that happens if and only if in each of the other two blocks the rows are linearly independent, that is if the determinants of both blocks are equal to 1. In other words, $D(1) = D^{0,\ldots,i_0-1}D^{i_0+1,\ldots,n-1}$.

Suppose the statement holds for $|R_I| = m$: let $R_I = \{j_0,\ldots,j_{m-1}\}$; then, we have $D(m) = D^{0,\ldots,j_0-1}\cdots D^{j_{m-1}+1,\ldots,n-1}$. We will see that it is true for $|R_I| = m+1$:

Let $R_I = \{i_0,\ldots,i_m\} = \{j_0,\ldots,j_l,\lambda,j_{l+1},\ldots,j_{m-1}\}$. Then, by induction hypothesis $D(m+1) = D^{0,\ldots,j_0-1}\cdots D_\lambda^{j_l+1,\ldots,j_{l+1}-1}\cdots D^{j_{m-1}+1,\ldots,n-1}$, where $D_\lambda^{j_l+1,\ldots,j_{l+1}-1}$ represents the determinant $D^{j_l+1,\ldots,j_{l+1}-1}$ with the λ^{th} row and column crossed out. From the case $k = 1$, we see that

$$D_\lambda^{j_l+1,\ldots,j_{l+1}-1} = D^{j_l+1,\ldots,\lambda-1}D^{\lambda+1,\ldots,j_{l+1}-1} \ ,$$

and that concludes the proof of equation (4.5).

The determinant on the left hand side of equation (4.5) is equal to 1 iff each one of the determinants on the right hand side is equal to 1. But each determinant $D^{k_0,\ldots,k_t}$ will be equal to 1 exactly $K^H_{k_t-k_0+1}$ times. Consequently, for $R_I = \{i_0,\ldots,i_{k-1}\}$, the number of flat spectra is $K^H_{i_0}K^H_{i_1-i_0-1}\cdots K^H_{n-1-i_{k-1}}$ and so

$$K(k) = \sum_{|R_I|=k} K^H_{i_0}K^H_{i_1-i_0-1}\cdots K^H_{n-1-i_{k-1}} \ .$$

The summands that appear in $K(k)$ are all possible products $\prod K_i^H$ such that the sum of the indices is $n-k$, so we have

$$K(k) = \sum_{\sum_{\lambda=0}^{k} t_\lambda = n-k} \prod_{j=0}^{k} K^H_{t_j} \ .$$

If we write the indices as a vector, $(t_0,\ldots,t_{n-1})$, where $\sum_{l=0}^{n-1} t_l = n-k$, then for $(t_1,\ldots,t_{n-1})$ we have that $\sum_{l=1}^{n-1} t_l = n-k-t_0$. Hence, for all possible vectors in

$K_n^{IH} = \sum_{k=0}^{n-1} K(k)$, we have all possible vectors in the lesser indices, as follows:

$$K_n^{IH} = K_n^H + K_{n-1}^H K_0^{IH} + K_{n-2}^H K_1^{IH} + \ldots + K_0^H K_{n-1}^{IH} = K_n^H + \sum_{i=0}^{n-1} K_{n-1-i}^H K_i^{IH} \quad , \quad (4.6)$$

where $K_n^{IH} = K_n^{IH}(p_n^l(\mathbf{x}))$. For the rest of the proof, we are going to omit the superscript H for K_n^H; we will use extensively that $K_n + K_{n+1} = 1$.

Using (4.6), we get

$$\begin{aligned}
K_{n+2}^{IH} = & \quad K_{n+2} + \sum_{i=0}^{n+1} K_{n+1-i} K_i^{IH} \\
= & \quad K_{n+2} + \sum_{i=0}^{n} K_{n+1-i} K_i^{IH} + K_0 K_{n+1}^{IH} \\
= & \quad K_{n+2} + \sum_{i=0}^{n} K_{n+1-i} K_i^{IH} + K_{n+1} + \sum_{i=0}^{n} K_{n-i} K_i^{IH} \\
= & \quad K_{n+1} + K_{n+2} + \sum_{i=0}^{n} K_i^{IH} (K_{n-i} + K_{n+1-i}) \\
= & \quad 1 + \sum_{i=0}^{n} K_i^{IH} = 1 + \sum_{i=0}^{n-1} K_i^{IH} + K_n^{IH} \\
= & \quad 1 + \sum_{i=0}^{n-1} K_i^{IH} (K_{n-1-i} + K_{n-i}) + K_n^{IH} K_0 \\
= & \quad K_n + K_{n+1} + \sum_{i=0}^{n-1} K_{n-1-i} K_i^{IH} + \sum_{i=0}^{n} K_{n-i} K_i^{IH} \\
= & \quad K_n^{IH} + K_{n+1}^{IH}
\end{aligned}$$

This gives us the recurrence relation, and from there we get the closed formula. ∎

Remark: This result was obtained independently in [4] as the evaluation of the interlace polynomial $q(x)$ for the path graph at $x = 1$ (see chapter 5).

4.3.2 Clique

The clique function, as defined in (4.2) satisfies the following lemma:

Lemma 4.7 *The number of flat spectra of the clique function in n variables w.r.t. the set* $\{I, H\}^n$*, denoted by* $K_n^{IH}(p_n^c(\mathbf{x}))$*, is* $K_n^{IH}(p_n^c(\mathbf{x})) = 2^{n-1}$.

Proof: It is easy to show from its adjacency matrix that the clique function of n variables is bent for n even. Consider the sub-functions of the n-variable clique function, obtained by fixing a subset of the input variables, $\mathbf{R_I}$. These sub-functions will also be cliques and will be bent iff $n-|\mathbf{R_I}|$ is even. The lemma follows by straightforward counting arguments.

■

Remark: This result was obtained independently in [4] as the evaluation of the interlace polynomial $q(x)$ for the complete graph at $x = 1$.

4.3.3 Clique-Line-Clique

For the n-clique-line-m-clique, as defined in (4.4), we get:

Lemma 4.8 *The number of flat spectra of the n-clique-line-m-clique w.r.t. $\{I, H\}^n$, $K^{IH}_{n,m}(p_{n,m}(\mathbf{x}))$, for $n,\ m \geq 1$ such that $n + m \geq 4$, satisfies*

$$K^{IH}_{n,m}(p_{n,m}(\mathbf{x})) = 2K^{IH}_{n-1,m}(p_{n-1,m}(\mathbf{x})) = 2K^{IH}_{n,m-1}(p_{n,m-1}(\mathbf{x}))\ ;$$

in closed form,

$$K^{IH}_{n,m}(p_{n,m}(\mathbf{x})) = 5 \cdot 2^{n+m-4}\ .$$

Proof: We begin the proof with some observations. Firstly, note that by fixing one of the connecting variables, x_{n-1} or x_n, we get two independent cliques, either in $n-1$ and m variables respectively or in n and $m-1$ variables respectively. Secondly, if we fix any of the other variables instead, we get the same kind of clique-line-clique graph. Thirdly, from the proof of lemma 4.4, we can deduce that $p_{n,m}$ is bent iff $n + m$ is even.

By the first and second observations, and considering that the order in which we fix doesn't matter, we get three separate cases:

- Case 1: We can fix any variables but x_{n-1} and x_n, the connecting variables. Then, by the second and third observations, we have flat spectra by fixing t variables iff $n + m - 2 - t$ is even; that is, if $n + m - t$ is even. Therefore the number of flat

spectra for this case is:

$$N1 = \begin{cases} \sum_{k=0}^{(n+m)/2} \binom{n+m-2}{2k} & \text{if } n+m \text{ even} \\ \sum_{k=0}^{(n+m-1)/2} \binom{n+m-2}{2k+1} & \text{if } n+m \text{ odd} \end{cases}$$

- Case 2: We fix x_n, and we can fix any variables but x_{n-1}. First, we fix x_n. We then get two independent cliques, one of n and the other of $m-1$ variables. We can now fix any of the remaining variables but x_{n-1}; when we fix t_1 variables in the first clique and t_2 in the second, we obtain a flat spectrum iff $n-t_1$ and $m-1-t_2$ are both even. Thus,

$$N2 = 2^{m-2} \cdot \begin{cases} \sum_{k=0}^{(n-1)/2} \binom{n-1}{2k} & \text{if } n \text{ odd} \\ \sum_{k=0}^{(n-2)/2} \binom{n-1}{2k+1} & \text{if } n \text{ even} \end{cases}$$

- Case 3: We fix x_{n-1}, and we can fix any of the remaining variables. First, we fix x_{n-1}. We thus have two independent cliques, one of $n-1$ and the other of m variables. We can then fix any of the remaining variables; when we fix t_1 variables in the first clique and t_2 in the second, we obtain a flat spectrum iff $n-1-t_1$ and $m-t_2$ are both even. Thus,

$$N3 = 2^{n-2}2^{m-1} \ .$$

Clearly, $K^{IH}_{n,m}(p_{n,m}(\mathbf{x})) = K1+K2+K3$; in principle, the result depends on the parity of n and m. However,

$$\sum_{k=0}^{s/2} \binom{s}{2k} = 1 + \sum_{k=1}^{s/2} \left[\binom{s-1}{2k} + \binom{s-1}{2k-1} \right] = 1 + \sum_{i=1}^{s-1} \binom{s-1}{i} = 2^{s-1} \ ,$$

and in the same way

$$\sum_{k=0}^{(s-1)/2} \binom{s}{2k+1} = \sum_{k=1}^{(s-1)/2} \left[\binom{s-1}{2k+1} + \binom{s-1}{2k} \right] = \sum_{i=0}^{s-1} \binom{s-1}{i} = 2^{s-1} \ .$$

Therefore, in all cases, we get $K^{IH}_{n,m}(p_{n,m}(\mathbf{x})) = 5 \cdot 2^{n+m-4}$, and from here, trivially, the recurrence relation. ∎

4.3.4 Comparison

Table 4.1 summarises our results for the $\{I, H\}^n$ transform set. Given the results obtained, and as there are no bent functions in an odd number of variables, we arrive at the following:

Theorem 4.9 *Over the set of all Boolean functions, the clique function, as defined in (4.2), maximises the number of flat spectra w.r.t.* $\{I, H\}^n$.

Proof: From the proof of Lemma 4.7, the spectrum is flat iff $n' = n - |\mathbf{R_I}|$ is even, in which case the constituent $2^{n-n'}$ sub-functions over n' variables, obtained from the clique function by considering all possible fixings of the variables in $\mathbf{R_I}$, are all bent. But it is well-known that no Boolean function over n' variables is bent if n' is odd. So the clique function obtains the maximum possible number of flat spectra w.r.t. $\{I, H\}^n$. ∎

Remark: Note that we have not proved that no other Boolean function exists with the same number of flat spectra w.r.t. $\{I, H\}^n$ as the clique function, but the existence of such a function seems unlikely.

4.4 Number of Flat Spectra: $\{I, H, N\}^n$

As deduced from computational results, high-distance stabilizer quantum codes (optimal additive codes over GF(4)) are associated to quadratic Boolean functions with large number of flat spectra w.r.t. $\{I, H, N\}^n$. In fact Hein et al [45] have already argued that high-distance QECCs will represent highly-entangled pure multipartite quantum states, and one indication of this entanglement strength will be an 'evenly-spread' power spectrum w.r.t. all *Local Unitary Transforms* [67], of which $\{I, H, N\}^n$ is a strategic subset. Therefore, the problem of maximising the number of flat spectra w.r.t. $\{I, H, N\}^n$ is of significant importance. As a means of comparison, we first consider the number of flat spectra for the near-worst and worst-case functions, namely the constant function and the monomial function of degree n, respectively.

4.4.1 Constant function

Lemma 4.10 *The* constant function *in n variables, that is* $p(\mathbf{x}) = 0$ *or* 1, *for* $\mathbf{x} \in GF(2)^n$, *has* 2^n *flat spectra with respect to* $\{I, H, N\}^n$.

Proof: Any $\{I, N\}^n$ transform of the constant function is flat, and none of the others: as seen in chapter 3, we get flat spectra iff $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \sum_{i=1}^{n-1} \chi_{\mathbf{R_N}}(i) k_i x_i$ is balanced for all $\mathbf{k} \neq \mathbf{0}$, where $\mathbf{k} = (k_0, \ldots, k_{n-1}) \in \mathrm{GF}(2)^n$, $\chi_{\mathbf{R_N}}$ is the characteristic function of the set $\mathbf{R_N}$ and p_I is the restriction of the function when fixing the variables whose indices are in $\mathbf{R_I}$. In our case, for any choice of $\mathbf{R_I}$, we get $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) = 0$. Thus, we get flat spectra iff $\sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i) k_i x_i$ is balanced for all $\mathbf{k} \neq \mathbf{0}$. Clearly, if $\chi_{\mathbf{R_N}}(i) = 1$ for all $i \in \{0, \ldots, n-1\} \setminus \mathbf{R_I}$, we get a balanced function for all $\mathbf{k} \neq \mathbf{0}$. But if $i \in \mathbf{R_H}$ for some i, $\chi_{\mathbf{R_N}}(i) = 0$, and by taking $\mathbf{k} = (0, \ldots, 1, \ldots, 0)$, where the 1 is in the i^{th} position, we get an unbalanced function. ∎

4.4.2 Monomial function

Lemma 4.11 *The* monomial function *of degree n in n variables, that is the function $p(\mathbf{x}) = x_0 \ldots x_{n-1}$, where $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in GF(2)^n$, has $n+1$ flat spectra w.r.t. $\{I, H, N\}^n$, except for the case $n = 2$.*

Proof: Throughout this proof, we will use the same notation as in the previous one. We first let $n = 1$. Then, the monomial function becomes the linear function x_0 in one variable. This will have the same flat spectra as the constant function in one variable, that is $2^1 = n + 1$.

Next, we let $n = 2$. Then the monomial is the same as the line in two variables, and will be considered in lemma 4.12.

Now, we let $n > 2$ and $\mathbf{R} = \{i_0, \ldots, i_l\} = \{0, \ldots, n-1\} \setminus \mathbf{R_I}$. Suppose that we fix $x_i = 1$ for all $i \in \mathbf{R_I}$, and that $|\mathbf{R}| > 2$. If we take $\mathbf{k} = (1, 0, \ldots, 0)$, the function $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \sum_{i=0}^{n-1} \chi_{\mathbf{R_N}}(i) k_i x_i$ becomes $x_{i_1} \cdots x_{i_l} + \chi_{\mathbf{R_N}}(i_0) x_{i_0}$, which is balanced iff $\chi_{\mathbf{R_N}}(i_0) = 1$. Similarly, we see that we must have $\chi_{\mathbf{R_N}}(i) = 1$ for all $i \in \mathbf{R}$ (that is, $\mathbf{R} = \mathbf{R_N}$). Consider now $\mathbf{k} = (1, 1, 0 \ldots, 0)$. The function we will get is $x_{i_1} \cdots x_{i_l} + x_{i_0} x_{i_2} \cdots x_{i_l} + x_{i_2} \cdots x_l + x_{i_0} + x_{i_1}$, which is not balanced.

Therefore, for $n > 2$, we need to fix at least $n-2$ variables in order to obtain flat spectra; that is, we need $|\mathbf{R_I}| \geq n-2$. Suppose now $|\mathbf{R_I}| = n-2$: By symmetry, we can suppose, w.l.o.g., that we fix $x_2, \ldots, x_{n-1}$. If any of the $x_i = 0$, then our new function is a constant, $p_I = 0$. As we have just seen, the only possibility for

$p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \chi_{\mathbf{R_N}}(0)k_0x_0 + \chi_{\mathbf{R_N}}(1)k_1x_1$ to be balanced for all $\mathbf{k} \neq (0,0)$ is that $\chi_{\mathbf{R_N}}(0) = \chi_{\mathbf{R_N}}(1) = 1$. On the other hand, if $x_i = 1$ for all $i \geq 2$, $p_I = x_0x_1$, the line in two variables; as we can easily deduce from the generic modified adjacency matrix, it has a flat spectrum iff $\chi_{\mathbf{R_N}}(i) = 0$ for at least one of the i's. Thus we get a contradiction, and so in fact $|\mathbf{R_I}| \geq n-1$. When $|\mathbf{R_I}| = n-1$, by fixing we now get either $p_I = 0$ or $p_I = x_i$. Both have a flat spectrum iff $\chi_{\mathbf{R_N}}(i) = 1$, and from here we get n flat spectra. Finally, for $|\mathbf{R_I}| = n$, we get another flat spectrum. ∎

Remark: It can be shown that $n+1$ is the minimal number of flat spectra possible for a Boolean function w.r.t. $\{I,H,N\}^n$.

4.4.3 Line

As opposed to the case of $\{H,N\}^n$, the number of flat spectra of the line w.r.t. $\{I,H,N\}^n$ does not seem to be maximal:

Lemma 4.12 *The number of flat spectra of the line w.r.t.* $\{I,H,N\}^n$, $K_n^{IHN}(p_n^l(\mathbf{x}))$, *satisfies* $K_n^{IHN}(p_n^l(\mathbf{x})) = 2(K_{n-1}^{IHN}(p_{n-1}^l(\mathbf{x})) + K_{n-2}^{IHN}(p_{n-2}^l(\mathbf{x})))$, *with* $K_0^{IHN} = 1$ *and* $K_1^{IHN} = 2$*; in closed form,*

$$K_n^{IHN}(p_n^l(\mathbf{x})) = \frac{(1+\sqrt{3})^{n+1} - (1-\sqrt{3})^{n+1}}{2\sqrt{3}} \ .$$

Proof: Following the same arguments as in the proof of Lemma 4.6, we arrive at the formula:

$$K_n^{IHN} = K_n + \sum_{i=0}^{n-1} K_{n-1-i}K_i^{IHN} \ , \tag{4.7}$$

where here, K_i will represent the number of flat spectra in i variables w.r.t. $\{H,N\}^n$.

In the sequel we are going to use the fact that $K_n = 2^n - K_{n-1}$ (see Lemma 4.1), or more accurately its consequence

$$K_{n+1} + K_{n+2} = 2^{n+2} = 2(K_n + K_{n+1}) \ .$$

We shall also use the fact that $K_0 = K_1 = 1$.

Using (4.7) we get

$$
\begin{aligned}
& 2K_n^{IHN} + 2K_{n+1}^{IHN} \\
&= 2K_n + 2K_{n+1} + 2\sum_{i=0}^{n-1} K_{n-1-i}K_i^{IHN} + 2\sum_{i=0}^{n} K_{n-i}K_i^{IHN} \\
&= K_{n+2} + K_{n+1} + \sum_{i=0}^{n-1} K_i^{IHN} 2(K_{n-1-i} + K_{n-i}) + 2K_n^{IHN}K_0 \\
&= K_{n+2} + \sum_{i=0}^{n-1} K_i^{IHN}(K_{n-i} + K_{n-i+1}) + K_n^{IHN}(K_0 + K_1) + K_{n+1} \\
&= K_{n+2} + \sum_{i=0}^{n} K_i^{IHN}(K_{n-i} + K_{n-i+1}) + K_{n+1} \\
&= K_{n+2} + \sum_{i=0}^{n} K_i^{IHN}K_{n-i+1} + K_{n+1} + \sum_{i=0}^{n} K_i^{IHN}K_{n-i} \\
&= K_{n+2} + \sum_{i=0}^{n} K_i^{IHN}K_{n-i+1} + K_{n+1}^{IHN} \\
&= K_{n+2} + \sum_{i=0}^{n+1} K_i^{IHN}K_{n-i+1} \\
&= K_{n+2}^{IHN}
\end{aligned}
$$

From the recursion formula, we arrive easily at the closed formula. ∎

Remark: This result can be gleaned, indirectly, from page 23 of [1] as the evaluation of the interlace polynomial $Q(x)$ for the path graph at $x = 2$.

4.4.4 Clique

Although the clique function as defined in (4.2) maximizes the number of flat spectra w.r.t. $\{I, H\}^n$, it does not do so well w.r.t. $\{I, H, N\}^n$:

Lemma 4.13 *The number of flat spectra of the clique w.r.t.* $\{I, H, N\}^n$, $K_n^{IHN}(p_n^c(\mathbf{x}))$, *satisfies* $K_n^{IHN}(p_n^c(\mathbf{x})) = 2K_{n-1}^{IHN}(p_{n-1}^c(\mathbf{x})) + 2^n$; *in closed form,*

$$K_n^{IHN}(p_n^c(\mathbf{x})) = (n+1)2^{n-1} \quad .$$

Proof: As stated above, if we have a clique in n variables and we fix a subset in the set of variables (that is, we choose $\mathbf{R_I}$), we get a clique in $n - |\mathbf{R_I}|$ variables. Thereby, for

each selection of $\mathbf{R_I}$ we have as many flat spectra as the number of flat spectra w.r.t. $\{H,N\}^{n-|\mathbf{R_I}|}$, in $n-|\mathbf{R_I}|$ variables. Therefore,

$$\#\text{ flat spectra}(p_c(\mathbf{x}))\text{ w.r.t. }\{I,H,N\}^n = \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) K_{n-i}\ ,$$

where K_{n-i} is the number of flat spectra of the clique in $n-i$ variables w.r.t. $\{H,N\}^{n-i}$. Now,

$$\begin{aligned}
\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) K_{n-i} &= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ n-i \end{array}\right) K_i = \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) K_i \\
&= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\left(i+\frac{1+(-1)^i}{2}\right) \\
&= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i + \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\frac{1}{2} + \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\frac{(-1)^i}{2} \\
&= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i + 2^{n-1} + 0
\end{aligned}$$

Expanding the first term,

$$\begin{aligned}
\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i &= \left(\begin{array}{c} n \\ 0 \end{array}\right) 0 + \left(\begin{array}{c} n \\ n \end{array}\right) n + \sum_{i=1}^{n-1}\left(\begin{array}{c} n \\ i \end{array}\right) i \\
&= n + \sum_{i=1}^{n-1}\left[\left(\begin{array}{c} n-1 \\ i \end{array}\right) + \left(\begin{array}{c} n-1 \\ i-1 \end{array}\right)\right] i \\
&= n + \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) i + \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i-1 \end{array}\right) i \\
&= n + 2\sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) i - \left(\begin{array}{c} n-1 \\ n-1 \end{array}\right)(n-1) + \sum_{i=0}^{n-2}\left(\begin{array}{c} n-1 \\ i \end{array}\right) \\
&= 2\sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) + 1 + 2^{n-1} - \left(\begin{array}{c} n-1 \\ n-1 \end{array}\right)
\end{aligned}$$

Hence, we get that $K_n^{IHN} = 2K_{n-1}^{IHN} + 2^n$. From the recurrence relation we get the desired formula. ∎

Remark: For the cases $n = 2,\ 3$, and $4,\ K_n^{IHN}$ of the clique function can be found by evaluating the interlace polynomial $Q(x)$ for the complete graph at $x = 2$ ([1], p.21).

4.4.5 Clique-Line-Clique

For the n-clique-line-m-clique structure, as defined in (4.4), the number of flat spectra is as follows:

Lemma 4.14 *The number of flat spectra of the n-clique-line-m-clique w.r.t. the set* $\{I, H, N\}^n$, $K_{n,m}^{IHN}(p_{n,m}(\mathbf{x}))$, *satisfies*

$$K_{n,m}^{IHN}(p_{n,m}(\mathbf{x})) = 2^{n+m-3}(3nm + 2n + 2m + 2) \ .$$

Proof: Suppose that one or both of the connecting variables are in $\mathbf{R_I}$: when we fix one of the connecting variables, we get two independent cliques, so from this case we get

$$K_{n-1,C}^{IHN}K_{m,C}^{IHN} + K_{n,C}^{IHN}K_{m-1,C}^{IHN} - K_{n-1,C}^{IHN}K_{m-1,C}^{IHN} = 2^{m+n-4}(3nm + 2n + 2m) \ ,$$

where $K_{k,C}^{IHN}$ is the number of flat spectra of the clique in k variables w.r.t. $\{I, H, N\}^k$.

On the other hand, when none of the connecting variables are in $\mathbf{R_I}$, we get another clique-line-clique: suppose that we fix i variables in the first clique and j in the second one. In that case, we will have as many flat spectra as the number of flat spectra w.r.t. $\{H, N\}^{n+m-i-j}$ of an $(n-i)$-clique-line-$(m-j)$-clique. Considering all possible fixings in this case, we get:

$$\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right)\left(\begin{array}{c} m-1 \\ j \end{array}\right)K_{n-i,m-j}^{HN} = 2^{m+n-4}(3nm + 2n + 2m + 4) \ .$$

■

4.4.6 Comparison

It is well-known that optimal GF(4)-additive codes make optimal QECCs [19]. The mapping from a quadratic Boolean function to a GF(4)-additive code is as follows. Let $p(\mathbf{x})$ be a quadratic function over n variables with associated adjacency matrix, Γ. Then the generator matrix for a $[n, 2^n, d]$ GF(4)-additive code is given by $\Gamma + \omega I_n$, where $\omega^2 + \omega + 1 = 0$ over GF(4) and I_n is the $n \times n$ identity matrix. This GF(4)-additive code can be interpreted as a $[[n, 0, d]]$ QECC of the stabilizer type. Using the database at [26],

an exhaustive computer search for n variable quadratic Boolean functions, $4 \leq n \leq 9$, finds one unique Local complementation (LC) orbit of functions for each n, whose number of flat spectra with respect to $\{I, H, N\}^n$ is optimal. A representative for each of these orbits is listed in Table 4.2. All of these functions map to additive zero-dimension QECCs with optimal distances (see [42] and [26]).

It remains open as to whether the quadratic function with the optimal number of flat spectra w.r.t. $\{I, H, N\}^n$ will always have optimal distance when viewed as a QECC, and vice versa. In any case, the approximate correspondence is to be expected as the QECC distance is equal to the *aperiodic propagation criteria (APC) distance* of the quadratic Boolean functions, as presented in [28].

Tables 4.3 to 4.5 show an exhaustive computer search for Boolean functions that achieve the optimal number of flat spectra w.r.t. $\{I, H, N\}^n$ for cubics, quartics, and quintics respectively, where one representative function is given per LC orbit. As expected, the maximum number of flat spectra decreases as the algebraic degree of the Boolean function rises. Also shown is the distance of the Boolean function when viewed as a zero-dimensional (non-stabilizer) QECC. As with the quadratics, this distance parameter can be interpreted as the APC distance of a Boolean function (see [28] for more details). In all cases, the Boolean functions shown in the tables achieve the maximum possible distance for their given algebraic degree.

4.5 Conclusion

We derived simple recursions for the number of flat spectra with respect to $\{I, H, N\}^n$ for certain recursive quadratic Boolean constructions, and we observed that Quantum Error Correcting Codes with optimal distance appear to have the most flat spectra with respect to $\{I, H, N\}^n$, at least for small n. In subsequent work we hope to develop recursive formulae for nested-clique structures of the type highlighted in [29], as we expect that these will have many flat spectra w.r.t. $\{I, H, N\}^n$.

We also showed computationally that, for small n, the number of flat spectra decreases when the algebraic degree of the Boolean function increases. Future work should seek to establish constructions for Boolean functions of degree greater than two that have as large a number of flat spectra as possible w.r.t. $\{I, H, N\}^n$. More generally, it would be of interest

to relax the criteria somewhat, and look for those functions which have many spectra with respect to $\{I, H, N\}^n$ with a worst-case spectral power peak less than some low upper bound (see [29]). One would expect, in this case, that many more Boolean functions of degree > 2 would be found that do well for this relaxed criteria. One promising line of inquiry in this context would be to apply and specialise the construction proposed at the end of [29], which takes a global graph structure, where the graph 'nodes' partition the set of Boolean variables, and where the nodes are 'linked' by permutations over these variable subsets, thereby obtaining higher-degree Boolean functions with potentially favourable $\{I, H, N\}^n$ spectra.

Finally we have indirectly answered a question posed at the end of [4] as to a simple combinatorial explanation of the interlace polynomial q. It is evident that q summarises some of the spectral properties of the graph w.r.t. $\{I, H\}^n$ (see chapter 5). Similarly the interlace polynomial Q, as defined in [1], summarises some of the spectral properties of the graph w.r.t. $\{I, H, N\}^n$. More details about this and further discussion is showed in chapter 5. Furthermore our work provides a natural setting for future investigations into the generalisation of the interlace polynomial to hypergraphs, as we shall see as well in chapter 5.

4.6 Appendix: Tables

Function	Monomial ($n > 2$)	Constant	Line	Clique	n clique-Line-m clique
ANF	$x_0 \dots x_{n-1}$	0	$\sum_{j=0}^{n-2} x_j x_{j+1}$	$\sum_{0 \le i < j \le n-1} x_i x_j$	$\sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1}x_n + \sum_{n \le i < j \le n+m-1} x_i x_j$
$K_n^{HN}(K_{n,m}^{HN})$	0	2^n	$\frac{1}{3}\left(2^{n+1} + (-1)^n\right)$	$n + \frac{1+(-1)^n}{2}$	$3nm - n(\frac{1+(-1)^m}{2}) - m(\frac{1+(-1)^n}{2})$ $+3(\frac{1+(-1)^n}{2})(\frac{1+(-1)^m}{2})$
$K_n^{IH}(K_{n,m}^{IH})$	1	1	$\frac{(1+\sqrt{5})^{n+1}+(1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$	2^{n-1}	$5 \cdot 2^{n+m-4}$
$K_n^{IHN}(K_{n,m}^{IHN})$	$n+1$	2^n	$\frac{(1+\sqrt{3})^{n+1}-(1-\sqrt{3})^{n+1}}{2\sqrt{3}}$	$(n+1)2^{n-1}$	$2^{n+m-3}(3nm + 2n + 2m + 2)$

Table 4.1: The Number of Flat Spectra w.r.t. $\{H, N\}^n$, $\{I, H\}^n$, and $\{I, H, N\}^n$ for some Quadratic Boolean Functions

n	distance	Quadratics Optimal for K_n^{IHN}	K_n^{IHN}	K_n^{IHN} for the line
4	2	02,13,23	44	44
5	3	01,02,13,24,34	132	120
6	4	01,02,05,13,15,24,25,34,35,45	396	328
7	3	03,06,14,16,25,26,34,35,45	1096	896
8	4	02,03,04,12,13,15,26,37,46,47,56,57,67	3256	2448
9	4	04,07,08,14,16,18,25,26,28,34,35,37,57,58,67,68	9432	6688

Table 4.2: The Maximum Number of Flat Spectra w.r.t. $\{I, H, N\}^n$ for Quadratic Boolean Functions

n	distance	Cubics Optimal for K_n^{IHN}	K_n^{IHN}
3	1	012	4
4	2	012,03,13,23	20
5	2	012,03,14,23,24	72
6	3	012,03,04,13,15,24,25	248

Table 4.3: The Maximum Number of Flat Spectra w.r.t. $\{I, H, N\}^n$ for Cubic Boolean Functions

n	distance	Quartics Optimal for K_n^{IHN}	K_n^{IHN}
4	1	All Quartics	5
5	2	0123,01,04,14,23,24,34	30
		0123,02,04,13,14,23,24,34	
		0123,04,14,23,24,34	

Table 4.4: The Maximum Number of Flat Spectra w.r.t. $\{I, H, N\}^n$ for Quartic Boolean Functions

n	distance	Quintics Optimal for K_n^{IHN}	K_n^{IHN}
5	1	All Quintics	6

Table 4.5: The Maximum Number of Flat Spectra w.r.t. $\{I, H, N\}^n$ for Quintic Boolean Functions

Chapter 5

Spectral Interpretations of the Interlace Polynomial

The results for this chapter can be found in [76] and [78].

5.1 Overview

The (one-variable) *interlace polynomial* was introduced by Arratia, Bollobás and Sorkin [2, 4], as a variant of Tutte and Tutte-Martin polynomials [17]. They defined the interlace polynomial of a graph G, $q(G;z)$, 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, $Q(G;z)$, and showed a new and easier way of constructing both polynomials $q(G;z)$ and $Q(G;z)$ using a matrix approach. They concluded that the polynomial $q(G;z)$, 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 $Q(G;z)$, 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.

As in the previous chapters, we 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 $p(\mathbf{x}) = \sum_{i<j} \Gamma_{ij} x_i x_j$ (see chapter 1). 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. $\{I, H, N\}^n$ (see chapters 3 and 4).

In section 5.2 we give an equivalent definition of the interlace polynomials q and Q using the modified adjacency matrix of the graph that we used to compute the number of flat spectra w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$ respectively in chapters 3 and 4, and use it to compute the interlace polynomial Q of the clique (complete graph), and clique-line-clique.

In section 5.3 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 $\{H, N\}^n$ 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 both Telecommunications and Physics for tasks such as channel-sounding, spread-spectrum, and synchronization [68]. 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 [37], 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 [19]. 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 [67], for it turns out that LC-equivalence for graph states can be characterised by LU-transformation via the set of transforms $\{I, H, N\}^n$ (see chapter 3). 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*) [67, 45].

In section 5.4 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 [43, 65], 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 [64] 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 [28]. 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, by identifying relatively higher generalised linear biases for p [69]. As seen in chapter 3, just the analysis of the flat spectra w.r.t. $\{I, H, N\}^n$ provides a good measure of the 'strength' of the function.

5.2 Interlace Polynomials q and Q

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

Definition 5.1 *The interlace polynomial q of a graph in n variables is*

$$q(z) = \sum_{U \in \{I,H\}^n} (z-1)^{co(\Gamma_U)} \ , \tag{5.1}$$

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 $\mathbf{R_I}$:

$$\Gamma = \begin{pmatrix} 0 & a_{01} & \dots & a_{0n} \\ a_{01} & 0 & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0n} & a_{1n} & \dots & 0 \end{pmatrix} \rightsquigarrow \Gamma_U = \begin{pmatrix} 0 & a_{r_0 r_1} & \dots & a_{r_0 r_k} \\ a_{r_0 r_1} & 0 & \dots & a_{r_1 r_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r_0 r_k} & a_{r_1 r_k} & \dots & 0 \end{pmatrix} \ ,$$

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

Definition 5.2 *The interlace polynomial Q of a graph in n variables is*

$$Q = \sum_{V \in \{I,H,N\}^n} (z-2)^{co(\Gamma_V)} \ , \tag{5.2}$$

where $co(\Gamma_V)$ means the corank of the modified adjacency matrix of the graph w.r.t. the transform $V \in \{I,H,N\}^n$, 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 $i \in \mathbf{R_N}$:

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

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

Lemma 5.3 *For the clique or complete graph (4.2),*

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

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. $\{I,H,N\}^n$ (see chapter 4).

Proof: From the proof of lemma 4.13, we see that:

when $n - |\mathbf{R_I}|$ is even, the corank is $\begin{cases} 0, \ |\mathbf{R_N}| = 0, \ n - |\mathbf{R_I}| \text{ even} \\ 1, \ |\mathbf{R_N}| = 0, \ n - |\mathbf{R_I}| \text{ odd} \\ |\mathbf{R_N}| - 1, \ 1 \leq |\mathbf{R_N}| \leq n - |\mathbf{R_I}| \end{cases}$

So, if n is even, we have

$$\begin{aligned} Q_n &= \sum_{k=0}^{n/2} \begin{pmatrix} n \\ 2k \end{pmatrix} (x-2)^0 + \sum_{k=0}^{(n-2)/2} \begin{pmatrix} n \\ 2k+1 \end{pmatrix} (x-2)^1 \\ &+ \sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} \sum_{i=1}^{n-j} \begin{pmatrix} n-j \\ i \end{pmatrix} (x-2)^{i-1} \ . \end{aligned}$$

Now, $\sum_{k=0}^{n/2} \binom{n}{2k} = \sum_{k=0}^{(n-2)/2} \binom{n}{2k+1} = 2^{n-1}$, so the sum of first two terms equals $2^{n-1} + 2^{n-1}(x-2)$. Finally, we compute the last term as: let $y = x-2$. Then,

$$\sum_{i=1}^{n-j} \binom{n-j}{i} y^{i-1} = y^{-1} \left(\sum_{i=0}^{n-j} \binom{n-j}{i} y^i - 1 \right) = y^{-1}((y+1)^{n-j} - 1) \ .$$

Thereby,

$$\sum_{j=0}^{n} \binom{n}{j} \sum_{i=1}^{n-j} \binom{n-j}{i} y^{i-1} = \sum_{j=0}^{n} \binom{n}{j} y^{-1}((y+1)^{n-j} - 1) = y^{-1}((y+2)^n - 2^n) \ .$$

Adding all terms, we get

$$Q_n = 2^{n-1} + 2^{n-1}(x-2) + (x-2)^{-1}(x^n - 2^n) \ .$$

Similarly, when n is odd, we get:

$$\begin{aligned} Q_n &= \textstyle\sum_{k=0}^{(n-1)/2} \binom{n}{2k} (x-2)^1 + \sum_{k=0}^{(n-1)/2} \binom{n}{2k+1} (x-2)^0 + \\ &+ \textstyle\sum_{j=0}^{n} \binom{n}{j} \sum_{i=1}^{n-j} \binom{n-j}{i} (x-2)^{i-1} \\ &= 2^{n-1} + 2^{n-1}(x-2) + (x-2)^{-1}(x^n - 2^n) \ . \end{aligned}$$

From this last formula, we can easily see that $Q_{n+1} = 2Q_n + x^n,\ n \geq 2$, with $Q_1 = x$. ∎

Lemma 5.4 *For the n-clique-line-m-clique (4.4), when $n,\ m \geq 3$, the interlace polynomial Q is:*

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

Proof: As we saw in chapter 4, when we fix one of the connecting variables (x_{n-1} and x_n), we get two independent cliques. When we fix non-connecting variables, say we fix i in the first clique and j in the second one, we get a $(n-i)$-clique-line-$(m-j)$-clique. As the order in which we do the fixing doesn't alter the result, we can differentiate three cases. The interlace polynomial will be the sum of the polynomials obtained in each case, that will be denoted as Q_1, Q_2 and Q_3, respectively:

Case $x_{n-1} \in R_{\mathbf{I}}$: In this case, we get two independent cliques, one in $n-1$ variables and the other in m variables. As a result of lemma 5.6 and lemma 5.3, we get that $Q_1 = Q^c_{n-1}Q^c_m$, where Q^c_k denotes the interlace polynomial for the clique in k variables.

Case $x_{n-1} \notin R_{\mathbf{I}}$, $x_n \in R_{\mathbf{I}}$: In this case, we get a clique in n variables and a clique in $m-1$ variables, that are independent from each other. As we have to avoid the case where $x_{n-1} \in R_{\mathbf{I}}$, and using the recursion formula of lemma 5.3, it follows that $Q_2 = Q^c_n Q^c_{m-1} - Q^c_{n-1}Q^c_{m-1} = Q_{m-1}(x^{n-1} + Q^c_{n-1})$.

Case $x_{n-1}, x_n \notin R_{\mathbf{I}}$: As we said before, in this case we get another clique-line-clique in the appropriate variables. Thereby, using lemma 5.9,

$$\begin{aligned}
Q_3 &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\binom{n-1}{i}\binom{m-1}{j}(-2+6\chi_{n-i}\chi_{m-j}+3\chi_{n-i+1}\chi_{m-j+1} \\
&+ (2-2\chi_{n-i}\chi_{m-j}-\chi_{n-i+1}\chi_{m-j+1})x \\
&+ \frac{x+1}{(x-2)^2}\left((x-1)^{n-i-1}-1\right)\left((x-1)^{m-j-1}-1\right) \\
&+ \frac{x+1+x\chi_{m-j}-3\chi_{m-j}}{x-2}((x-1)^{n-i-1}-1) \\
&+ \frac{x+1+x\chi_{n-i}-3\chi_{n-i}}{x-2}((x-1)^{m-j-1}-1)) \ ,
\end{aligned}$$

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

Finally, as $Q = Q_1 + Q_2 + Q_3 =$, and considering that

$$\sum_{i=0}^{n-1}\binom{n-1}{i} = 2^{n-1},\ \sum_{i=0}^{n-1}\binom{n-1}{i}\chi_{n-i} = 2^{n-2} \ ,$$

$$\text{and } \sum_{i=0}^{n-1}\binom{n-1}{i}(x-1)^{n-i-1} = x^{n-1} \ , \text{ we get:}$$

$$
\begin{aligned}
Q &= 3(2^{n-2}+2^{n-2}(x-2)+(x-2)^{-1}(x^{n-1}-2^{n-1}))(2^{m-2}+2^{m-2}(x-2) \\
&+ (x-2)^{-1}(x^{m-1}-2^{m-1})) \\
&+ (2^{m-2}+2^{m-2}(x-2)+(x-2)^{-1}(x^{m-1}-2^{m-1}))x^{n-1} \\
&+ (2^{n-2}+2^{n-2}(x-2)+(x-2)^{-1}(x^{n-1}-2^{n-1}))x^{m-1} \\
&+ 2^{n+m-4}+5\cdot 2^{n+m-4}x+\frac{x+1}{(x-2)^2}(x^{n-1}-2^{n-1})(x^{m-1}-2^{m-1}) \\
&+ \frac{3\cdot 2^{m-2}x-2^{m-2}}{x-2}(x^{n-1}-2^{n-1})+\frac{3\cdot 2^{n-2}x-2^{n-2}}{x-2}(x^{m-1}-2^{m-1}) \ .
\end{aligned}
$$

Simplifying, we get the desired result. ∎

5.3 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 5.5 *The HN-interlace polynomial for a graph in n variables is*

$$
Q^n_{HN} = \sum_{W\in\{H,N\}^n} (z-2)^{co(\Gamma_W)} \ , \tag{5.3}
$$

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 $v_i \in GF(2)$ where $v_i = 1$ iff $i \in \mathbf{R_N}$:

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

Lemma 5.6 *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: The adjacency matrix of G, denoted by Γ, will be, w.l.o.g., 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 $Q^m_{HN}(G_2) = \sum_{j=0}^{m} b_i(z-2)^j$,

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

■

Remark: By the same method, we can prove as well: $q^{n+m}(G) = q^n(G_1)q^m(G_2)$ and $Q^{n+m}(G) = Q^n(G_1)Q^m(G_2)$.

Lemma 5.7 *The HN-interlace polynomial for the path graph (4.1) is*

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

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 of the line w.r.t. $\{H, N\}^n$ (see chapter 4) tells us that,

$$D_n = v_0 D_{n-1} + D_{n-2} \bmod 2 \ , \tag{5.4}$$

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 must be 1, and that, if $D_n = 0$, then $D_{n-1} = 1$. For suppose that $D_n = 0 = D_{n-1}$. Then, by (5.4), $D_{n-2} = 0$. 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 that 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 chapter 4, $K_n = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$, and the formula follows. ∎

Lemma 5.8 *For the complete graph (4.2),*

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

In closed form,

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

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 chapter 4.

Proof: Taking $|\mathbf{R_I}| = 0$ in the proof of 5.3, we get the HN-interlace polynomial for the complete graph. This means taking all first terms and the term corresponding to $j = 0$ in the formula obtained at the end of the proof. So we get, if n is even,

$$Q_{HN} = \sum_{k=0}^{n/2} \binom{n}{2k} (x-2)^0 + \sum_{k=0}^{(n-2)/2} \binom{n}{2k+1} (x-2)^1 +$$
$$+ \sum_{i=1}^{n} \binom{n}{i} (x-2)^{i-1} = 2^{n-1} + 2^{n-1}(x-2) + (x-2)^{-1}((x-1)^n - 1)$$

Similarly, when n is odd, we get the same formula. ∎

Lemma 5.9 *For the n-clique-line-m-clique (4.4), the HN-interlace polynomial is, when both n and m are odd:*

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

when n is odd and m even:

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

when n is even and m is odd:

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

when both n and m are even:

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

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

Proof: As in the computation for the number of flat spectra of the clique-line-clique w.r.t. $\{H,N\}^n$ in [74], we will consider the generic modified adjacency matrix of the graph, which is as follows:

$$\Gamma_{\mathbf{v}} = \begin{pmatrix} v_0 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ 1 & v_1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & v_{n-1} & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1 & v_n & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 & 1 & v_{n+1} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & v_{n+m-1} \end{pmatrix}.$$

We will get the coefficients of the polynomial by looking at the occurences of the corank of the matrix is a determined value:

$\underline{n \text{ and } m \text{ odd:}}$

As in [74], we consider the v_i's for the first $n-1$ minor and the last $m-1$ minor, $v_0, v_1, \dots, v_{n-2}$ and $v_{n+1}, v_{n+2}, \dots, v_{n+m-1}$.

We consider first the case when all v_i in both minors are 0. In this case, both minors are flat, so of full rank. Thereby, we get a linear combination (l.c.) of the rows of $\Gamma_{\mathbf{v}}$ iff at least one of the $(n-1)^{th}$ or n^{th} rows are implicated. Suppose that the $(n-1)^{th}$ row is a l.c. of the others. Then, we get a system of equations that implies that the n^{th} row is also implicated, and we get that necesarily $v_{n-1} = 1 = v_n$. We get then, in this case, $\text{co}(\Gamma_{\mathbf{v}}) = 1$ exactly once, and $\text{co}(\Gamma_{\mathbf{v}}) = 0$ in 3 cases.

We consider now the case in which all of $v_{n+1}, v_{n+2}, \dots, v_{n+m-1}$ are equal to zero, but not all of $v_0, v_1, \dots, v_{n-2}$. Suppose, w.l.o.g., that $v_0, \dots, v_{r-1} = 1,\ v_{r-1}, \dots, v_{n-2} = 0$. As before, if we have a l.c., it must imply some of the first $n+1$ rows. We get $r-1$ l.c. implying just the first $n-2$ rows. Suppose now that the $(n-1)^{th}$ row is implicated in a l.c.. Then, from the system of equations we get that the n^{th} row is also implicated, and that $v_{n-1} = 0,\ v_n = 1$. We thus obtain from here $\begin{pmatrix} n-1 \\ r \end{pmatrix}$ occurences of $\text{co}(\Gamma_{\mathbf{v}}) = r,\ r \geq 1$, and $3\begin{pmatrix} n-1 \\ r \end{pmatrix}$ occurences of $\text{co}(\Gamma_{\mathbf{v}}) = r-1,\ r \geq 1$.

Similarly, when all of $v_0, v_1, \dots, v_{n-2}$ are equal to zero, but not all of $v_{n+1}, v_{n+2}, \dots, v_{n+m-1}$, we obtain $\begin{pmatrix} m-1 \\ r \end{pmatrix}$ occurences of $\text{co}(\Gamma_{\mathbf{v}}) = r,\ r \geq 1$, and $3\begin{pmatrix} m-1 \\ r \end{pmatrix}$ occurences of $\text{co}(\Gamma_{\mathbf{v}}) = r-1,\ r \geq 1$.

As a last case, we consider the one in which at least one of the $v_0, v_1, \ldots, v_{n-2}$ and of the $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to 1. Let us say that there are exactly r non-zero v_i's within the two minors. Then, one can see that there can not be any l.c. in which the $(n-1)^{th}$ or the n^{th} rows are implied if they are both equal to 0 (so we get $\mathrm{co}(\Gamma_{\mathbf{v}}) = r-1$ in here), and that there is exactly one l.c. of that sort for every $(v_{n-1}, v_n) \neq (0,0)$. The number of l.c. not involving any of these rows is equal to $r-2$.

Finally, we sum up:

$$\begin{aligned}
Q_{HN} &= 3(x-2)^0 + (x-2)^1 + \sum_{i=1}^{n-1}\sum_{j=1}^{m-1} \binom{n-1}{i}\binom{m-1}{j}(x-2)^{i+j-1} \\
&+ 3\sum_{i=1}^{n-1}\sum_{j=1}^{m-1} \binom{n-1}{i}\binom{m-1}{j}(x-2)^{i+j-2} \\
&+ \left(\sum_{r=1}^{n-1}\binom{n-1}{r} + \sum_{r=1}^{m-1}\binom{m-1}{r}\right)(x-2)^r \\
&+ 3\left(\sum_{r=1}^{n-1}\binom{n-1}{r} + \sum_{r=1}^{m-1}\binom{m-1}{r}\right)(x-2)^{r-1} \\
&= 1 + x + (x-2)^{-1}((x-1)^{n-1}-1)((x-1)^{m-1}-1) \\
&+ 3(x-2)^{-2}((x-1)^{n-1}-1)((x-1)^{m-1}-1) + (x-1)^{n-1} - 1 + (x-1)^{m-1} - 1 \\
&+ 3(x-2)^{-1}((x-1)^{n-1}-1) + 3(x-2)^{-1}((x-1)^{m-1}-1) \\
&= 1 + x + \frac{x+1}{(x-2)^2}\left((x-1)^{n-1}-1)((x-1)^{m-1}-1\right) \\
&+ \frac{x+1}{x-2}\left((x-1)^{n-1} + (x-1)^{m-1} - 2\right)
\end{aligned}$$

<u>n odd, m even:</u> The corank of the matrix changes from above only in the cases where all of $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to zero.

When all of $v_0, v_1, \ldots, v_{n-2}$ are equal to zero, but not all of $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$, we get a new l.c. involving the middle rows iff $v_{n-1} = 1$, so we get for this case $2\binom{n-1}{r}$ occurences of $\mathrm{co}(\Gamma_{\mathbf{v}}) = r,\ r \geq 1$, and $2\binom{n-1}{r}$ occurences of $\mathrm{co}(\Gamma_{\mathbf{v}}) = r-1,\ r \geq 1$.

When all of $v_0, v_1, \ldots, v_{n-2}$ and $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to zero, we get exactly one l.c. iff $v_{n-1} = 0$, and no l.c. in the rest of the cases. Thereby, we get for this case $\mathrm{co}(\Gamma_{\mathbf{v}}) = 1$ twice, and $\mathrm{co}(\Gamma_{\mathbf{v}}) = 0$ twice as well.

Summing up, we get the desired result.

<u>n even, m odd:</u> The proof for this case is analogous to the previous case.

n and m even: This case differs from the second case only when all of the variables $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to zero.

When not all of $v_0, v_1, \ldots, v_{n-2}$ are equal to zero, we get a l.c. iff $v_{n-1} = 1$, so we obtain for this case that $2 \begin{pmatrix} m-1 \\ r \end{pmatrix}$ occurences of $\mathrm{co}(\Gamma_{\mathbf{v}}) = r,\ r \geq 1$, and $2 \begin{pmatrix} m-1 \\ r \end{pmatrix}$ occurences of $\mathrm{co}(\Gamma_{\mathbf{v}}) = r-1,\ r \geq 1$.

When all of $v_0, v_1, \ldots, v_{n-2}$ and $v_{n+1}, v_{n+2}, \ldots, v_{n+m-1}$ are equal to zero, there is no l.c. in any of the four cases. Thereby, we get for this case $\mathrm{co}(\Gamma_{\mathbf{v}}) = 0$ four times. ∎

5.4 Spectral Interpretations of the Interlace Polynomial

As we saw in definition 5.2 in section 5.2, 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.

We recall here definition 2.25:

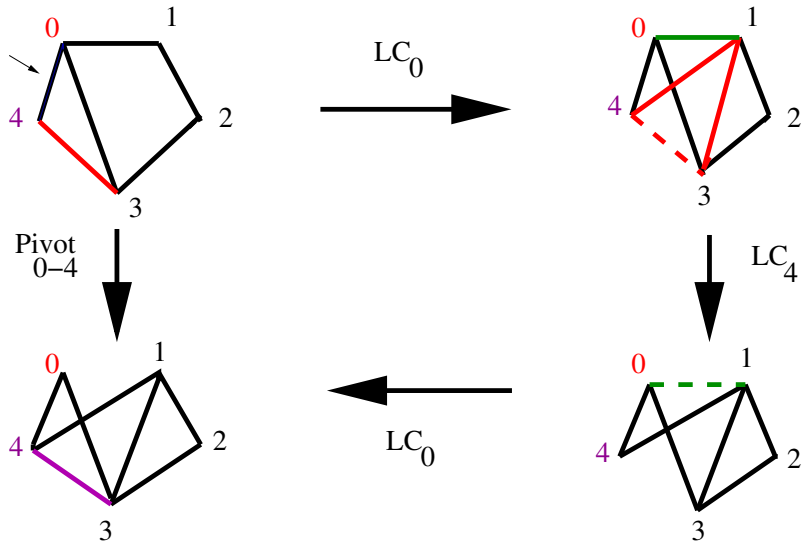
Definition 5.10 *The action of* Local Complementation (LC) *(also known as* vertex-neighbour-complement (VNC)*) on a graph G at vertex v is defined as the graph transformation obtained by replacing the subgraph $G[\mathcal{N}_v]$ (i.e., the induced subgraph of the neighbourhood $\mathcal{N}_v$ of the v^{th} vertex of G) by its complement.*

Theorem 5.11 *[1] The interlace polynomial Q is invariant under LC.*

Proof: From definition 5.2 and chapter 3, one can show that Q is invariant w.r.t. $\{I, H, N\}^n$. But, as seen in section 3.3.3, this set defines the LC operation. ∎

Definition 5.12 *[2, 5] 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.*

Example: with $v = 0, u = 4$



Theorem 5.13 *[2] The interlace polynomial q is invariant under pivot.*

Proof: By considering definition 5.1 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 $\{I, H\}^n$ (see chapter 7). ∎

Theorem 5.14 *The corank of the modified adjacency matrix is given by*

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

where $P_{U,\mathbf{k}}$ are the entries of P_U as defined in (1.1).

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,

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

Let $\mathrm{co}(\Gamma_U) = c$. Then, from chapter 3, we can deduce easily 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 shall extensively use the property

$$\begin{pmatrix} A_{0\ldots0} \\ A_{0\ldots1} \\ \vdots \\ A_{1\ldots1} \end{pmatrix} \quad \begin{matrix} U \\ \longrightarrow \\ \longleftarrow \\ U^{-1} \end{matrix} \quad \begin{pmatrix} |P_{0\ldots0}|^2 \\ |P_{0\ldots1}|^2 \\ \vdots \\ |P_{1\ldots1}|^2 \end{pmatrix} \tag{5.5}$$

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 (5.5), 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 (5.5), we can obtain the autocorrelation vector 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. ∎

Remark: By the proof of the previous theorem, we can see that in all cases but for $U = H \otimes \cdots \otimes H$ the values in the power spectrum are strongly related.

We recall here definition 2.1:

Definition 5.15 *[29] 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*

$$PAR_{\mathbf{T}}(s) = \max_{\substack{U \in \mathbf{T} \\ \mathbf{k} \in \mathbb{Z}_2^n}} (|P_{U,\mathbf{k}}|^2), \quad \textit{where } P_U = (P_{U,\mathbf{k}}) = Us \in \mathbb{C}^{2^n} \ . \tag{5.6}$$

Corollary 5.16 *Let $p(\mathbf{x})$ be a quadratic Boolean function, and let $s = (-1)^{p(\mathbf{x})}$. Then, by theorem 5.14, the Peak-to-Average Power Ratio of s, $PAR_{\mathbf{T}}(s)$ 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.*

The "GDJ sequences", as defined in [64], can be identified, without loss of generality, with the path graph. Here we use (5.4) to prove Conjectures 1,2, and 3 of [64]:

Lemma 5.17 *(Conjecture 1 of [64]) PAR_H of the path graph is 1.0 for even n and 2.0 for odd.*

Proof: By (5.4), and as in this case $v_i = 0$ for all i, we get that $D_n = D_{n-2}$, mod 2. Expanding this relationship, 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 5.7), we know that the rank of the matrix cannot be lower than $n - 1$, so in the even case we get $\mathrm{PAR}_H = 1$ and in the odd case $\mathrm{PAR}_H = 2$. ∎

Lemma 5.18 *(Conjecture 2 of [64]) 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 (5.4), 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 $n > 3$, $D_n = D_{n-1} + D_{n-2} = D_{n-2} + D_{n-3} + D_{n-2} = D_{n-3}$. By iterating the argument, when $n = 0 \bmod 3$, $D_n = D_3 = 1$; when $n = 1 \bmod 3$, $D_n = D_1 = 1$; when $n = 2 \bmod 3$, $D_n = D_2 = 0$. ∎

From lemmas 5.17 and 5.18 it follows that:

Corollary 5.19 *(Conjecture 3 of [64]) PAR_H and PAR_N of the path graph are both* 1.0 *for n even, $n \neq 2$ mod* 3.

Remark: [6, 1] show that $q(-1) = (-1)^r 2^{n-r}$, where r is the rank of $\Gamma + I$. From chapter 3 and the results in this chapter it is therefore clear that $\mathrm{PAR}_N(s) = |q(-1)|$ and that, for quadratics, PAR_N is pivot-invariant.

Theorem 5.20 *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 $2^{co(\Gamma_U)}$.

Remark: Note that this implies that the values in the power spectra are always a power of 2, in the case of quadratics. Computational results show that this is not the case for higher degree Boolean functions.

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. We shall denote the unitary transform by $T_{i_0,\ldots,i_{n-1}}$, where the indices $i_j \in \{0, 1, 2\}$, and $T_{i_0,\ldots,i_{n-1}} = \prod_{i_j=0} I_j \prod_{i_j=1} H_j \prod_{i_j=2} N_j$, where $\{I, H \text{ or } N\}_j$ means that the 2×2 transform is applied to the index j.

The action of the transforms $T_{10\ldots0}$ or $T_{20\ldots0}$ on s give as possible values the following sets: $\frac{1}{\sqrt{2}}\{(2,0),(0,2),(0,-2),(-2,0)\}$ or $\frac{1}{\sqrt{2}}\{(1,-i),(-i,1),(-i,-1),(-1,-i)\}$, respectively. Normalization allows us to ignore global magnitudes and pairwise phase, so we can simplify the above sets to $\{(1,0),(0,1)\}$ and $\{(1,i),(1,-i)\}$. For quadratics, the subsequent action of $T_{010\ldots0}$ or $T_{020\ldots0}$ on the previous sets means that H or N, respectively, act on the previous pair of values (a, b) as (a, a) and (b, b), if the term x_0x_1 is not in $p(\mathbf{x})$, and (b, a) and (a, b) if x_0x_1 is in $p(\mathbf{x})$. Therefore, the action of $T_{110\ldots0}$ or $T_{120\ldots0}$ gives as possible sets of values (depending on whether the term x_0x_1 is included in the function or not) $\{(0,0),(1,0)\}$ and $\{(1,-1),(1,1)\}$, or $\{(0,0),(1,-i)\}$ and $\{(1,-1),(1,1)\}$ (after normalization). By similar arguments, we have that the action of $T_{210\ldots0}$ or $T_{220\ldots0}$ gives the possible sets of values $\{(1,0)\}$ and $\{(1,i),(1,-i)\}$, or $\{(1,-i)\}$ and $\{(1,0),(0,1)\}$ (after normalization). All output sets are one and two-valued and have ocurred before. But all $\{H, N\}^n$ can be covered by sucessive applications of $T_{0\ldots01\ldots0}$ or $T_{0\ldots01\ldots0}$, and as we have seen we obtain every time the same sets of possible values, and taking the square of the (complex) modulus of the values in those sets, we get that the power spectra is one or two-valued. ∎

Definition 5.21 *(see [27]) 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 5.22 $PAR_{IH} = 2^{\max|IS|}$.

Proof: PAR_{IH} is, as we saw in theorem 5.14, the logarithm (base 2) of 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 gives the smallest possible number of fixings we have to do to get a completely disjoint graph. But this is exactly the maximal size along the independent sets, $\max|IS|$, that is, the maximal number of variables that such a graph can have. ∎

Corollary 5.23 *deg*$(q) = 2^{\max|IS|}$.

Proof: By corollary 5.16 and lemma 5.22. ∎

Furthermore:

Theorem 5.24 *[27] 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 5.25 *deg*$(Q) = 2^{\lambda(G)}$.

Proof: By corollary 5.16 and theorem 5.24. ∎

Definition 5.26 *[43, 65] The* Multivariate Merit Factor (MMF) *and the* Clifford Merit Factor (CMF) *are defined as* $MMF = \dfrac{4^n}{2\sigma}$, *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 5.27 $MMF = \dfrac{4^n}{2^n Q_{HN}(4) - 4^n}$, *and* $CMF = \dfrac{6^n}{2^n Q(4) - 6^n}$.

Proof: By theorems 5.14 and 5.20, and the fact that $\sum_{\mathbf{k}} |P_{U,\mathbf{k}}|^2 = 2^n$. ∎

Clearly, σ and E are derived from their respective L_4-norms: e.g.,

$$\sum_{\substack{U \in \{I,H,N\}^n \\ \mathbf{k} \in \mathbb{Z}_2^n}} |P_{U,\mathbf{k}}|^4 = 2^n Q(4) \ .$$

We can generalise the result to express the L_p norms in terms of the interlace polynomials.

Lemma 5.28 *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 5.20, together with theorem 5.14, tells us that, for quadratics, the interlace polynomial encapsulates much of the information about the spectra. 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 5.14, we can still compute the number of flat spectra and the PAR:

Definition 5.29 *The* interlace polynomial[1] *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 is the disjoint union of G_1 and G_2.

[1]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.

5.5 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 [64], and presented other spectral interpretations of the interlace polynomial, including the characterisation of the values of the power spectra for quadratics. Finally we generalised the interlace polynomial to hypergraphs.

Chapter 6

The Two-variable Interlace Polynomial

Some of the results in this chapter can be found in [78].

6.1 Overview

In chapter 5, we showed how to interprete the interlace polynomial from a spectral point of view, and that $q(G;1)$ (resp. $Q(G;2)$) is the number of flat spectra of the function w.r.t. $\{I,H\}^n$ (resp. $\{I,H,N\}^n$). Furthermore, we saw that the Peak-to-Average Power Ratio of $(-1)^p$, $\mathrm{PAR}_{\{I,H\}^n}(-1)^p$ (resp. $\mathrm{PAR}_{\{I,H,N\}^n}(-1)^p$), is equal to the degree of the interlace polynomial $q(z)$ (resp. $Q(z)$). However, it gives no information about the dimension of the set S of variables not fixed (that is, the weight on H's (resp. in H's and N's)) once computed. We shall show that the two-variable interlace polynomial provides this information.

In [5], Arratia, Bollobas and Sorkin defined an extension of the interlace polynomial q [4] (see chapter 5), to a new interlace 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 extension of the HN-interlace polynomial Q_{HN} (see chapter 5) to the two-variable $Q_{HN}(x,y)$. Furthermore, we define the IN-interlace polynomial $Q_{IN}(x,y)$.

In section 6.7, we show how the *weight hierarchy* of the binary linear code associated to a bipartite graph can be derived from an extension of the interlace polynomial, a *three-*

variable interlace polynomial.

6.2 Interlace Polynomial $q(x, y)$

Here we offer a definition of $q(x, y)$ that is equivalent to the one proposed in [5]:

Definition 6.1 *The two-variable interlace polynomial $q(G; x, y)$ of a graph G in n variables is defined as*

$$q(G; x, y) = \sum_{U \in \{I,H\}^n} (x-1)^{rk(\Gamma_U)} (y-1)^{co(\Gamma_U)} \ , \tag{6.1}$$

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 $\mathbf{R_I}$ (see definition 5.1).

Remark: Clearly, we have that $q(2, y) = q(y)$. By applying the results in chapter 5, $\deg(q(2, y))$ =PAR$_{IH}$.

Lemma 6.2 *$deg(q(2, y)) = deg(q(1, y))$.*

Proof: Clearly, $q(2, y) = q(y)$. This implies, using theorem 5.14, that $\deg(q(2, y))$ =PAR$_{IH}$. Now, as can be deduced from [5], the degree of $q(1, y)$ is equal to $2^{\max |IS|}$, and PAR$_{IH}$ = $2^{\max |IS|}$ by lemma 5.22. ∎

Lemma 6.3 *$q(x, 1)$ gives the number of flat spectra, for each $|R_\mathbf{I}|$, of the function w.r.t. $\{I, H\}^n$. Furthermore, $n-deg(q(x, 1))$ is the smallest possible number of fixings that we have to do to get a flat spectrum.*

Proof: From the definition we can see that

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

Now, when $co(\Gamma_U) = 0$, then 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. ∎

Lemma 6.4 *$q(1,y)$ gives the independent sets, and also gives $|R_{\mathbf{I}}|$ for the transform that generates them. Furthermore, $deg(q(1,y))$ gives the maximal size of an independent set.*

Proof: Clearly,

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

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 smallest possible number of fixings we have to do to get a separate graph; i.e., how many variables can have such a graph.■

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 6.5 *The following equality holds:*

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

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

6.3 Interlace Polynomial $Q(x,y)$

Definition 6.6 *The two-variable interlace polynomial $Q(G;x,y)$ of a graph G in n variables is defined as*

$$Q(G;x,y) = \sum_{V \in \{I,H,N\}^n} (x-2)^{rk(\Gamma_V)}(y-2)^{co(\Gamma_V)} \ , \tag{6.2}$$

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 5.2).

Remark: $Q(3,y) = Q(y)$ as defined in [1].

Lemma 6.7 *$Q(2,y) = q(1,y-1)$.*

Proof: Clearly,

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

As before, the only subgraph such that $rk(\Gamma_V) = 0$ is the empty graph. Also, $rk(\Gamma_V) = 0$ 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 6.8 *The following equalities hold:*

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

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

6.4 IN-Interlace Polynomial $Q_{IN}(x,y)$

For completeness, we define the two-variable IN-interlace polynomial (that is, the polynomial w.r.t. $\{I,N\}^n$):

Definition 6.9

$$Q_{IN}(G;x,y) = \sum_{T \in \{I,N\}^n} (x-2)^{rk(\Gamma_T)} (y-2)^{co(\Gamma_T)} \ , \tag{6.3}$$

where $co(\Gamma_T)$ and $rk(\Gamma_T)$ stand respectively for the corank and rank of the modified adjacency matrix of the graph w.r.t. $T \in \{I,N\}^n$, Γ_T, obtained by erasing the rows and columns whose indices are in $\mathbf{R_I}$, as before, and then substituting 0 by 1 in those indices $i \in \mathbf{R_N}$.

Since in this case the rank of the matrix cannot be zero, but for the case when $\mathbf{R_N} = \emptyset$, we get as a first result:

Lemma 6.10 $Q_{IN}(G;2,y) = 1$.

6.5 HN-Interlace Polynomial $Q_{HN}(x,y)$

For completeness, we define as well the two-variable HN-interlace polynomial (that is, the polynomial w.r.t. $\{H,N\}^n$):

Definition 6.11

$$Q_{HN}(G;x,y) = \sum_{W\in\{H,N\}^n} (x-2)^{rk(\Gamma_W)}(y-2)^{co(\Gamma_W)} \ , \tag{6.4}$$

where $co(\Gamma_W)$ *and* $rk(\Gamma_W)$ *stand respectively for the corank and rank of the modified adjacency matrix of the graph w.r.t.* $W \in \{H,N\}^n$, Γ_W, *obtained by substituting 0 by 1 in those indices* $i \in \mathbf{R_N}$.

As in this case the rank cannot be zero, except for the empty graph or a graph in only one variable, then for all graphs but the ones mentioned we get as a first result

Lemma 6.12 $Q_{HN}(G;2,y) = 0$.

6.6 $Q_{HN}(x,y)$ from $Q(x,y)$

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

On the other hand:

$$Q_{HN}(G;x,y) = \sum_{W\in\{H,N\}^n} (x-2)^{rk(\Gamma_W)}(y-2)^{co(\Gamma_W)} \ .$$

$Q_{HN}(G;x,y)$ comprises the summands of $Q(G;x,y)$ such that $\mathbf{R_I} = \emptyset$. That is, such that $rk(\Gamma_V) + co(\Gamma_V) = n$. Such terms will be the "survivors" after deriving n times in total, in the 2 variables. In other words,

$$Q_{HN}(G;x,y) = \sum_{k+l=n} \frac{1}{k!}\frac{1}{l!}\frac{\partial^n}{\partial x^k \partial y^l} Q(G;x,y)$$

6.7 Weight Hierarchy

Let $v = (v_0,\ldots,v_{n-1}) \in \ \mathrm{GF}(2)^n$. We define the *support* of v by

$$\mathrm{supp}\ v = \{i : v_i \neq 0\} \ .$$

For a set $X \subseteq \ \mathrm{GF}(2)^n$, we define then $X = \cup_{v\in X}\mathrm{supp}\ v$.

Definition 6.13 *[46, 99] The* weight hierarchy *of an $[n, k, d]$ binary linear code C is the sequence $(d_1, \ldots, d_k)$, where*

$$d_r = \min\{supp\ D : D \leq C, dim\ D = r\}\ ,$$

where '$\leq$' means here 'subspace of'.

In section 6.2, we saw that the two-variable interlace polynomial offers more information about the spectra than the one-variable polynomials. Still, we can see that if we try to compute the weight hierarchy of a code based on a bipartite graph, $q(x, y)$ does not give enough information. We introduce an extension of the interlace polynomial that contains all necessary information about the weight hierarchy.

The subset of quadratic Boolean functions that can be represented by bipartite graphs, have an interpretation as binary linear codes [67]: Let $\mathbf{T_C}$, $\mathbf{T_{C^\perp}}$ be a bipartite splitting of $\{0, \ldots, n-1\}$, and let us partition the variable set $\mathbf{x} = (x_0, \ldots, x_{n-1})$ as $\mathbf{x} = \mathbf{x_C} \cup \mathbf{x_{C^\perp}}$, where $\mathbf{x_C} = \{x_i : i \in \mathbf{T_C}\}$, and $\mathbf{x_{C^\perp}} = \{x_i : i \in \mathbf{T_{C^\perp}}\}$. For a quadratic bipartite function $p(\mathbf{x})$, we can write $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, with q_k and r_k homogeneous linear Boolean functions where $\deg(q_k(\mathbf{x_C})) = \deg(r_k(\mathbf{x_{C^\perp}})) = 1\ \forall k$ (clearly, such a function $p(\mathbf{x})$ corresponds to a bipartite graph), and let $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$. Then:

Theorem 6.14 *[67] 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, C. In other words, the transform defines a code C such that $s'(x) = 1$ iff $x \in C$. Furthermore, the codes obtained from taking $\mathbf{T} = \mathbf{T_C}$ or $\mathbf{T_{C^\perp}}$ are mutually dual.*

Let $p(\mathbf{x})$ be the quadratic Boolean function associated to a graph in $n + m$ variables. Then, the weight hierarchy of its associated code C is given by:

Theorem 6.15 *[67] Let $[s_C]$ the indicator of the $[n+m, k, d]$ binary linear code associated to the graph, C (see (6.7)). Let $\mathbf{Q} \subset \{0, \ldots, n + m - 1\}$. Let,*

$$m_{\mathbf{Q}} = \frac{|\mathbf{Q}| + \log_2(\mu) - (n + m) + k}{2}, \quad with\ \mu = PAR(s'_C)\ , \tag{6.5}$$

where $s'_C = (\prod_{j \in \mathbf{Q}^c} I_j \prod_{j \in \mathbf{Q}} H_j)[s_C]$, where '$\mathbf{Q}^c$' stands for the complement of the subset $\mathbf{Q}$. Then, the weight hierarchy of the code C, d_j, is given by:

$$d_j = \min_{\mathbf{Q}: m_{\mathbf{Q}} = j} |\mathbf{Q}|\ . \tag{6.6}$$

We suppose that the code C is given by $\mathbf{T_C} = \{n, \ldots, n+m-1\}, \mathbf{T_{C^\perp}} = \{0, \ldots, n-1\}$. That means that the binary indicator $[s_C]$ is obtained as:

$$[s_C] = (\overbrace{I \otimes \cdots \otimes I}^{n} \otimes \overbrace{H \otimes \cdots \otimes H}^{m})(-1)^p = (H_n \cdots H_{n+m-1})(-1)^p \ . \tag{6.7}$$

Note: If the binary indicator of the code is obtained as $[s_{C^\perp}] = (H_0 \cdots H_{n-1})(-1)^p$ (the dual code), by applying a change of variables we are back in the first case.

We want to write the weight hierarchy in terms of the modified adjacency matrix w.r.t. the transforms in $\{I, H\}^{n+m}$. It is important to know whether we have the code C or its dual (whether we apply I's to the 'left' of the graph and H's to the 'right' or viceversa), as the final transform is the product of the transform $\prod_{j \in \mathbf{Q}^c} I_j \prod_{j \in \mathbf{Q}} H_j$ with the transform that converts s into $[s_C]$: in our case, the final transform applied to the bipolar vector of the function will be

$$(\prod_{j \in \mathbf{Q}^c} I_j \prod_{j \in \mathbf{Q}} H_j) \cdot (H_n \cdots H_{n+m-1})(-1)^p \ . \tag{6.8}$$

So even $q(x, y)$ is not enough for computing the weight hierarchy, as it offers no information about the position on which the H's or I's are applied.

Let $U = U_1(H_n \cdots H_{n+m-1})$, which will cover all of $\{I, H\}^{n+m}$ if U_1 does. Then, let $U = (\prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j)$. Furthermore, let $\mathbf{R_H^1} = \mathbf{R_H} \cap \{0, \ldots, n-1\}$, $\mathbf{R_I^1} = \mathbf{R_I} \cap \{0, \ldots, n-1\}$, and let $\mathbf{R_H^2} = \mathbf{R_H} \cap \{n, \ldots, n+m-1\}$, $\mathbf{R_I^2} = \mathbf{R_I} \cap \{n, \ldots, n+m-1\}$. Then, we can rewrite $\mathbf{Q}$ as:

$$|\mathbf{Q}| = |\mathbf{R_H}(U_1)| = |\mathbf{R_H^1}| + (m - |\mathbf{R_H^2}|) \ .$$

Also, $\log_2(\mu) = co(\Gamma_U)$, where Γ_U is the modified adjacency matrix under the transform

$$U = (\prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j)(H_n \cdots H_{n+m-1}) \ .$$

Since p is bipartite, its adjacency matrix will be of the form:

$$\Gamma = \begin{pmatrix} \mathbf{0} & M \\ M^t & \mathbf{0} \end{pmatrix} \ .$$

Definition 6.16 *We define* $q_w(x,y,z)$*, a* three-variable interlace polynomial *which is an extension of the two-variable interlace polynomial, by*

$$q_w(x,y,z) = \sum_U (x-1)^{rk(M_{\mathbf{R_I}})}(y-1)^{\mathbf{R_H^1}+rk(M_{\mathbf{R_I}})}(z-1)^{\mathbf{R_H^2}+rk(M_{\mathbf{R_I}})} \ , \tag{6.9}$$

where $M_{\mathbf{R_I}}$ *is the matrix* M *after erasing in* Γ *the rows and columns of those indices* $i \in \mathbf{R_I}$*.*

Since the blocks of the matrix are independent, we see that $rk(\Gamma_U) = 2rk(M_{\mathbf{R_I}})$ and $co(\Gamma_U) = |\mathbf{R_H^1}| + |\mathbf{R_H^2}| - 2rk(M_{\mathbf{R_I}})$. Therefore, we have that

$$q(x,y) = q_w((x+1)^2 - 1, y, y) \ . \tag{6.10}$$

We now have all the information needed to compute the weight hierarchy, for we can rewrite (6.5) as

$$m_{\mathbf{Q}} = \frac{|\mathbf{R_H^1}| + (m - |\mathbf{R_H^2}|) + co(\Gamma_U) - (n+m) + k}{2} \ . \tag{6.11}$$

Now, $k = n$, as we assume that the code C is given by applying I's to the indices $0, \ldots, n-1$. Substituting the corank in (6.11), we obtain $m_{\mathbf{Q}} = |\mathbf{R_H^1}| - rk(M_{\mathbf{R_I}})$.

We denote $Y = y - 1, Z = z - 1$. We define

$$q_w^0 = Z^m q_w(2, X, Z^{-1}) = \sum_U Y^{|\mathbf{R_H^1}| - rk(M_{\mathbf{R_I}})} Z^{m-(|\mathbf{R_H^2}| - rk(M_{\mathbf{R_I}}))} \ .$$

Then, $m_{\mathbf{Q}} = \deg_Y q_w^0$, where $\deg_Y$ means the degree in the variable Y. Then,

Lemma 6.17

$$d_j = \min_{m_{\mathbf{Q}}=j} |\mathbf{Q}| = \min_{deg_Y q_w^0 = j} deg q_w^0 \ .$$

Example: Following the example on pages 18–19 of [67], we compute the three-variable interlace polynomial for $p = x_0x_2 + x_0x_3 + x_0x_4 + x_1x_2 + x_1x_4$ from the PAR for each transform (see section 5.4); we use the notation $X = x - 1, Y = y - 1, Z = z - 1$:

$$\begin{aligned} q_w &= X^0Y^0Z^3 + 3X^0Y^0Z^2 + 3X^0Y^0Z^1 + X^0Y^0Z^0 + 2X^1Y^0Z^2 \\ &+ 6X^1Y^0Z^1 + 5X^1Y^0Z^0 + 3X^1Y^0Z^1 + X^2Y^0Z^1 + 2X^2Y^0Z^0 \quad . \\ &+ X^1Y^1Z^1 + 3X^1Y^1Z^0 + X^0Y^2Z^0 \end{aligned}$$

Then,

$$q_w^0 = Y^0Z^0 + 5Y^0Z^1 + 13Y^0Z^2 + 8Y^0Z^3 + Y^1Z^2 + 3Y^1Z^3 + Y^2Z^3 \ .$$

We have thus: terms with $\deg_Y q_w^0 = 0 : \{Y^0Z^0, Y^0Z^1, Y^0Z^2, Y^0Z^3\}$, whose minimal degree is 0. So we obtain $d_0 = \min_{\deg_Y q_w^0 = 0} \deg q_w^0 = 0$. Similarly, we get $d_1 = 3$ and $d_2 = 5$.

6.8 Conclusions

As in chapter 5 for the one-variable interlace polynomial, we developed an interpretation of the two-variable interlace polynomial proposed in [5], and extended the concept to define the polynomials $Q(x, y)$, $Q_{IN}(x, y)$ and $Q_{HN}(x, y)$. Also, we showed how to derive the weight hierarchy of the binary code associated with a bipartite graph from an extension of its interlace polynomial, a three-variable interlace polynomial.

Chapter 7

On Pivot Orbits of Boolean Functions

The results for this chapter can be found in [77].

7.1 Overview

The *pivot* operation on a graph G was used by Arratia, Bollobás and Sorkin [2] to define the *interlace polynomial* $q(G, z)$ (see chapter 5), as a variant of Tutte and Tutte-Martin polynomials [17]. In chapter 5, 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, the set $\{I, H, N\}^n$.

In this chapter we characterise the pivot operation using *algebraic normal form (ANF).* We also generalise pivot to hypergraphs, and state the (necessary and sufficient) condition that a function of degree higher than two must fulfill in order to allow such an operation. Then we show how the pivot operation on a (hyper)graph can be written as a transform on the bipolar vector of the function associated to it. Using this, we construct a family of Boolean functions that have a large number of flat spectra w.r.t. $\{I, H\}^n$, and compute this number. We study the pivot orbit trajectory of structures that include a clique and develop lower bounds on the number of flat spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

7.2 Pivot

Here we will see different interpretations of the pivot transform. We recall definition 5.12: 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.

7.2.1 Pivot in Terms of Boolean Functions

Lemma 7.1 *Let p be a quadratic Boolean function. We can write*

$$p = x_i x_j + x_i \mathcal{N}_i + x_j \mathcal{N}_j + R \ ,$$

where $\mathcal{N}_i$, $\mathcal{N}_j$, and R are not functions of x_i or x_j. Then, after pivoting its associated graph on the edge ij, p becomes (equivalent[1] to)

$$p_{iji} = x_i x_j + x_i \mathcal{N}_j + x_j \mathcal{N}_i + \mathcal{N}_i \mathcal{N}_j + R = p + (x_i + x_j)(\mathcal{N}_i + \mathcal{N}_j) + \mathcal{N}_i \mathcal{N}_j \ .$$

7.2.2 A Generalisation to Hypergraphs

Definition 7.2 *Let $p = x_i x_j + q(x_0, \ldots, x_{n-1})$ be a function of any degree (≥ 2) in the variables $\{0, \ldots, n-1\}$ such that $x_i x_j$ is not a multiplying term in q (that is, such that $\frac{\partial^2}{\partial x_i x_j} q = 1$). Then, we can define the* pivot *operation in the associated hypergraph on the edge ij by its ANF as $p_{iji} = x_i x_j + x_i \mathcal{N}_j + x_j \mathcal{N}_i + \mathcal{N}_i \mathcal{N}_j + R = p + (x_i + x_j)(\mathcal{N}_i + \mathcal{N}_j) + \mathcal{N}_i \mathcal{N}_j$, where $p = x_i x_j + x_i \mathcal{N}_i + x_j \mathcal{N}_j + R$ as before.*

Remarks: Note that now there is no restriction in the degree of $\mathcal{N}_i, \mathcal{N}_j$, and also that due to the condition on p (and equivalently to it) $\mathcal{N}_i$ and $\mathcal{N}_j$ are independent of both x_i and x_j and so the formula is well-defined, while if we don't have this condition the definition is ambiguous. When p is quadratic and the vertices i and j are connected, the condition is always fulfilled and the definition is consistent.

Lemma 7.3 *Let G be a bipartite (hyper)graph. Then, after pivoting on any edge of G, the resultant (hyper)graph is bipartite.*

[1] By 'equivalent' we understand here that the graph associated to p_{iji} is the same as the graph obtained from the associated graph of p by pivoting on the edge ij.

7.2.3 Pivot in Spectral Terms

Theorem 7.4 *Let p be a function that fulfills the condition on definition 7.2. Then, the pivot of its associated (hyper)graph lies in the orbit of $\{I, H\}^n$. Concretely, if we call p_{iji} the function result of pivoting on the edge ij of the (hyper)graph associated with p, then* $(-1)^{p_{iji}} = (H_i \cdot H_j)(-1)^p$.

Proof: Let $p = x_i x_j + x_i \mathcal{N}_i + x_j \mathcal{N}_j + R$, and let $s = (-1)^p$. Then, by theorem 18 in [67],

$$s' = H_i s = (x_j + \mathcal{N}_i + x_i + 1)(-1)^{x_j \mathcal{N}_j + R} \ .$$

Now, applying theorem 19 of [67], we get

$$s'' = H_j s' = 1 \cdot (-1)^{R + (\mathcal{N}_i + x_i)(\mathcal{N}_j + x_j)} = (-1)^{x_i x_j + x_i \mathcal{N}_j + x_j \mathcal{N}_i + \mathcal{N}_i \mathcal{N}_j + R} \ ,$$

which is what we wanted. Note that, by the condition on p, $\mathcal{N}_i$ does not depend on x_j, and that ensures that the condition of theorem 19 of [67] is fulfilled. ∎

Proof 2: Here we give an alternative proof of theorem 7.4. As in the first proof, let $p = x_i x_j + x_i \mathcal{N}_i + x_j \mathcal{N}_j + R$, and let $s = (-1)^p$. Then, by theorem 3.7, $N_i s = i^{p'}$, where

$$p' = 2(p(x) + x_j \mathcal{N}_i + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s) + 3\,(x_i + x_j + \mathcal{N}_i) \ .$$

Define $\delta_1 = \prod_{k \in S_1} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}_k \prod_{k \in S_1^c} I_k$, where $S_1 = \mathcal{N}_i \cup \{i\} \cup \{j\}$. Applying δ_1 to $N_i s$, we get $s' = \delta_1 N_i s = (-1)^{p_i}$, where

$$p_i = p(x) + x_j \mathcal{N}_i + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s = x_i x_j + x_i \mathcal{N}_i + x_j(\mathcal{N}_i + \mathcal{N}_j) + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s + R \ .$$

This was the result of the action of LC_i. Now we apply LC_j; that is, we apply N_j to s'. The result is $N_j s' = i^{p''}$, where

$$\begin{aligned} p'' &= 2(x_i x_j + x_i \mathcal{N}_i + x_j(\mathcal{N}_i + \mathcal{N}_j) + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s + R + x_i(\mathcal{N}_i + \mathcal{N}_j) + \\ &+ \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \cup \mathcal{N}_j \\ r \neq s}} x_r x_s) + 3\,(x_i + x_j + \mathcal{N}_i + \mathcal{N}_j) \quad . \end{aligned}$$

Define $\delta_2 = \prod_{k \in S_2} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}_k \prod_{k \in S_2^c} I_k$, where $S_2 = \mathcal{N}_i \cup \mathcal{N}_j \cup \{i\} \cup \{j\}$. Applying δ_2 to $N_j s'$, the result is $s'' = \delta_2 N_j s' = (-1)^{ji}$, where

$$p_{ji} = x_i x_j + x_i \mathcal{N}_j + x_j(\mathcal{N}_i + \mathcal{N}_j) + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \cup \mathcal{N}_j \\ r \neq s}} x_r x_s + R \quad .$$

Finally, we apply LC_i again. The result is $N_i s'' = i^{p'''}$, where

$$\begin{aligned} p''' &= 2(x_i x_j + x_i \mathcal{N}_j + x_j(\mathcal{N}_i + \mathcal{N}_j) + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \\ r \neq s}} x_r x_s + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_i \cup \mathcal{N}_j \\ r \neq s}} x_r x_s + R \\ &+ x_j \mathcal{N}_j + \sum_{\substack{r,\, s \,\in\, \mathcal{N}_j \\ r \neq s}} x_r x_s) + 3\,(x_i + x_j + \mathcal{N}_j) \end{aligned} \quad .$$

Define now $\delta_3 = \prod_{k \in S_3} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}_k \prod_{k \in S_3^c} I_k$, where $S_3 = \mathcal{N}_j \cup \{i\} \cup \{j\}$. Applying it to the previous output, we get $s''' = \delta_3 (-1)^{p_{iji}}$, where

$$p_{iji} = x_i x_j + x_i \mathcal{N}_j + x_j \mathcal{N}_i + \sum_{\substack{r \,\in\, \mathcal{N}_i,\, s \,\in\, \mathcal{N}_j \\ r \neq s}} x_r x_s + R \quad .$$

Let $\Delta_a \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ \pm i & 0 \end{pmatrix} \right\}$, $\Delta_b \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix} \right\}$. Translating the previous results into local unitary transforms, and considering that $N^2 = \Delta_a H$, $\Delta_b \Delta_a = \Delta_a$, we see that we have applied:

- In position i: $\Delta_a N \Delta_a \Delta_a N = \Delta_a N \Delta_b N = \Delta_a \Delta_b N N = \Delta_b \Delta_b H = \Delta_b H$

- In position j: $\Delta_a \Delta_a N \Delta_a = \Delta_b N \Delta_a = \Delta_b \Delta_b H = \Delta_b H$
- Positions $\mathcal{N}_i$ and $\mathcal{N}_j$: $\Delta_a \Delta_a = \Delta_b$.
- Remaining positions: I. ∎

Corollary 7.5 *Let p be a Boolean function of any degree such that it satisfies the conditions of definition 7.2. Then, p has a flat spectrum with respect to the transform $U = H_i \cdot H_j$.*

7.3 Enumeration of Pivot Orbits

We enumerate the number of orbits of connected graphs of n vertices, which are inequivalent with respect to pivot, both for the unlabelled and labelled case, as shown in Table 7.1. It follows from Definition 5.12 that each LC orbit is partitioned into a set of pivot orbits so that, given a list of all LC orbits over n vertices, we can generate and enumerate all pivot orbits over n vertices. For the unlabelled case we make use of the classification of self-dual quantum codes, which is isomorphic to the classification of LC graph orbits, as described in [29, 30] and available at [26]. This classification in turn used *nauty* [60] to deal efficiently with graph isomorphism. The subsequent enumeration of pivot orbits of unlabelled connected graphs is shown in Table 7.1 up to $n = 11$. We have also classified and enumerated all pivot orbits for labelled connected graphs as shown in Table 7.1. A complete list of pivot orbit representatives for both labelled and unlabelled connected graphs is available at http://www.ii.uib.no/∼matthew/pivotorbits/files.html.

It can be shown that each $(k, n-k)$-bipartite graph is related to a binary $[n, k]$ linear code, C, via a simple transform from the set of $\{I, H\}^n$ transforms [67] (see section 10.8). Likewise, the dual $[n, n-k]$ code, $C^\perp$, can also be obtained from the same graph via another transform from the set of $\{I, H\}^n$ transforms. One can also show that C and $C^\perp$ are invariant under pivot of the associated bipartite graph and, consequently, such a graph remains bipartite under pivot, as stated in Lemma 7.3. It is therefore of interest to enumerate the number of pivot orbits of bipartite graphs.

Table 7.1 enumerates pivot orbits of unlabelled and labelled connected bipartite graphs up to $n = 13$, and a list of bipartite pivot orbit representatives for unlabelled and labelled connected graphs is available at

http://www.ii.uib.no/ matthew/bipivotorbits/files.html.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
i_n	1	1	2	4	10	35	134	777	6702	104825	3370317		
j_n	1	1	2	11	119	2303	80923						
k_n	1	1	1	2	3	8	15	43	110	370	1260	5366	25684
l_n	1	1	1	4	26	251	3412						

Table 7.1: Number of pivot-inequivalent labelled/unlabelled connected graphs, i_n: unlabelled, j_n: labelled, k_n: unlabelled-bipartite, l_n: labelled-bipartite

7.4 Construction and Bounds on the Number of Flat Spectra

We now design a family of Boolean functions in n variables of degree less or equal to $\max\{t, 2\}$, where $0 \leq t \leq n-1$, and that have a large number of flat spectra w.r.t. $\{I, H\}^n$.

- $f^{n,t} = \sum_{i=0}^{t-1} \sum_{j=t}^{n-1} x_i x_j + \sum_{i=t}^{n-2} \sum_{j=i+1}^{n-1} x_i x_j + a(x_0, x_1, \ldots, x_{n-1})$, where $\deg(a) \leq 1$.
- Family $\mathcal{F}^{n,t}$: $\mathcal{F}^{n,t} = \{f^{n,t} + h(x_0, x_1, \ldots, x_{t-1})\}$, where h is an arbitrary Boolean function in t variables.

Conjecture 7.6 *Let $f \in \mathcal{F}^{n,t}$. Then the pivot orbit of f occurs within $\bigcup_{k=0}^{n-1} \mathcal{F}^{n,k}$.*

Theorem 7.7 *Let $f \in \mathcal{F}^{n,t}$. Then the number of flat spectra of f w.r.t. $\{I, H\}^n$ is at least $(t+1)2^{n-t-1}$, where the bound is tight if f has degree t.*

Remark: If f has degree t then all the $(t+1)2^{n-t-1}$ flat spectra correspond to restrictions of f down to residual quadratic functions.

Lemma 7.8 *Let $f \in \mathcal{F}^{n,t}$. Then the number of flat spectra of f w.r.t. $\{I, H, N\}^n$ is at least $(n+1)(t+1)2^{n-t-1}$.*

7.5 Number of Flat Spectra w.r.t. $\{I, H\}^n$

We recall here definition 4.2: The *clique* in n variables (or *complete graph*) is defined as $\sum_{0 \leq i < j \leq n-1} x_i x_j$. By lemma 4.7, the clique has 2^{n-1} flat spectra w.r.t. $\{I, H\}^n$, and thus maximises the number of flat spectra w.r.t. $\{I, H\}^n$.

We study here the behaviour of a graph that contains a clique. We consider 3 cases, depending on the positions of the vertices A and B, where we pivot on the edge AB. Let C_r be the clique in r variables contained in the graph. We denote by $\mathcal{N}_A$ and $\mathcal{N}_B$ the neighbourhoods of A and B respectively, and by $\mathcal{N}_{AB}$ the intersection of the neighbourhoods.

- $A, B \in C_r$: The clique remains invariant.
- $A \in C_r,\ B \notin C_r$: Let m be the number of variables of C_r that are in $\mathcal{N}_{AB}$. Then C_r splits and we get the cliques $C_{r-m},\ C_{m+2}$, connected just by B. Moreover $A \notin C_{r-m},\ B \in C_{r-m}$ and $A, B \in C_{m+2}$.
- $A, B \notin C_r$: In this case, C_r remains invariant, independently of whether A or B are connected to it or not.

We give lower bounds on the number of flat spectra w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$ depending on internal structures:

Lemma 7.9 *Consider a graph G and two unconnected subgraphs G_1 and G_2. The number of flat spectra of G w.r.t. $\{I, H\}^n$, K_{IH}, has as lower bound: $K_{IH}(G) \geq K_{IH}(G_1) \cdot K_{IH}(G_2)$*

Corollary 7.10 *If we consider inside the graph unconnected subgraphs $G_1, \ldots, G_t$, then $K_{IH}(G) \geq \prod_{i=1}^{t} K_{IH}(G_i)$. For instance, if we get inside the graph unconnected cliques $C_{r_1}, \ldots, C_{r_t}$, then $K_{IH}(G) \geq \prod_{i=1}^{t} 2^{n_i - 1}$.*

Lemma 7.11 *This is also true for the number of flat spectra w.r.t.* $\{I, H, N\}^n$*: If we consider inside the graph unconnected subgraphs* $G_1, \ldots, G_t$*, then we have that* $K_{IHN}(G) \geq \prod_{i=1}^{t} K_{IHN}(G_i)$.

7.6 Conclusions

We characterised the pivot operation using algebraic normal form (ANF), and generalised the concept to hypergraphs, stating the necessary and sufficient condition that a function of degree higher than two must fulfill in order to allow such an operation. We showed then how the pivot operation on a (hyper)graph can be written as a transform on the bipolar vector of the function associated to it. We construct a family of Boolean functions that have a large number of flat spectra w.r.t. $\{I, H\}^n$, and computed this number. We studied the pivot orbit trajectory of structures that include a clique and developed lower bounds on the number of flat spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

Chapter 8

Further Symmetries for $\{I, H, N\}^n$

8.1 Overview

In this chapter, we show for which cases we can change the degree of a function by pivoting on its associated hypergraph, or reduce or increase the number of high degree terms. We describe as well the explicit formula for the result of applying a transform $U \in \{I, N\}^n$ to the bipolar vector of a Boolean function or, in general, to any vector with entries in the set $\{0, \pm 1\}$. Together with the results proposed by Parker and Rijmen in [67], and by iteration we can compute the result of the application of a $U \in \{I, H, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$. Furthermore, we show how to use these results for computing the result of the application of a $U \in \{I, H, N\}^n$ to i^p for $p : \{0, 1\}^n \to \mathbb{Z}_4$.

8.2 Changing the Degree by Pivoting

In chapter 7, we proposed a generalisation of the pivot transform to hypergraphs. We will see here how in the case of some functions of degree higher than two we can change its degree by pivoting in the associated hypergraph. Those functions will still be equivalent, in the sense that they are $\{I, H\}^n$-equivalent.

Lemma 8.1 *Let p be a Boolean function, such that:*

- *$deg(p) \geq 4$*
- *condition in definition 7.2 is fulfilled for at least one term $x_i x_j$*

- *for a term* $m \in p$ *of degree higher than 4 there* $\exists m_1, m_2$ *s.t.* $m = m_1 m_2$ *and* $x_i m_1, x_j m_2 \in p$

then the term m *will be split into* m_1 *and* m_2 *by pivoting on the edge* ij*.*

Remark: If there is more than one higher degree term, the conditions above must be satisfied for as many edges as necessary (or at least for some sequence of pivoting). If the conditions are not fulfilled for all higher degree terms, at least we can reduce their number by pivoting.

Conversely, if we want to increase the degree of a Boolean function:

Lemma 8.2 *Let* p *be a Boolean function, such that:*

- $deg(p) \geq 3$
- *condition in definition 7.2 is fulfilled for at least one term* $x_i x_j$
- $\exists m_1 \in \mathcal{N}_i, m_2 \in \mathcal{N}_j$ *s.t.* $deg(m_1 m_2) > deg(p)$

then, after pivoting on the edge ij*, the degree of* p *will increase, and its value will be at least* $deg(p_{iji}) \geq deg(m_1 m_2)$*.*

Examples:

1) $p = x_0x_3 + x_0x_1x_2 + x_3x_4x_5 + x_1x_2x_4x_5$ (degree 4) via pivot on the edge 03 gives $p_{030} = x_0x_3 + x_0x_4x_5 + x_3x_1x_2$ (degree 3).

2) $p = x_0x_3 + x_0x_1x_2x_4x_5 + x_3x_6x_7x_8x_9 + x_1x_2x_4x_5x_6x_7x_8x_9$ (degree 8) via pivot on the edge 03 gives $p_{030} = x_0x_3 + x_1x_2x_3x_4x_5 + x_0x_6x_7x_8x_9$ (degree 5).

3) $p = x_0x_3 + x_0x_1x_2 + x_3x_4x_5 + x_3x_6 + x_1x_6$ (degree 3) via pivot on the edge 03 gives $p' = p_{030} = x_0x_6 + x_0x_3 + x_0x_4x_5 + x_1x_2x_3 + x_1x_2x_4x_5 + x_1x_6$ (degree 4); further, via pivot on the edge 16 to this last function gives $p'_{161} = x_1x_6 + x_0x_1 + x_0x_2x_3 + x_0x_2x_4x_5 + x_2x_3x_6 + x_2x_4x_5x_6 + x_2x_3x_4x_5 + x_0x_3 + x_0x_4x_5$ (degree 4: the last pivot does not change the degree but it increases the number of higher degree terms).

As we have seen, two Boolean functions of different degree may be equivalent via the pivot transform. Such an equivalence is counter-intuitive, for we expect equivalent functions to have the same degree, as occurs with affine equivalence.

8.3 $\{I, N\}^n$ Applied to the APF Form

In this section we describe the spectra of a Boolean function of any degree under any tranform in the set $\{I, N\}^n$. That is, for any Boolean function p and any transform $U \in \{I, N\}^n$, we give an explicit formula for $U(-1)^{p(\mathbf{x})}$. Furthermore, for any vector v with entries in the set $\{0, \pm 1\}$ and any $U \in \{I, N\}^n$, we give an explicit formula for Uv.

Following Parker and Rijmen [67], we define the *Algebraic Polar Form (APF)* of a vector v with entries in the set $\{0, \pm 1\}$ as the product $m(\mathbf{x})(-1)^{p(\mathbf{x})}$, where m and p are both Boolean functions. We separate thus the *magnitude* m and the *phase* p of the vector v.

In the sequel we mix arithmetic mod 2 with arithmetic on the complex numbers $\mathbb{C}$ so, to clarify the formulae for equations that mix arithmetic, anything in square brackets is computed mod 2, and the result is computed as complex numbers. For brevity, we will denote by N_j the transform $N_j \prod_{i \neq j} I_i$; that is, the transform that applies N to the index j and I to the remaining indices. For any two transforms $U_1, U_2 \in \{I, N\}^n$, $U_1 \cdot U_2$ will denote the application of U_2 followed by the application of U_1.

Theorem 8.3 *Let m and p be Boolean functions. Then,*

$$N_j m(-1)^p = \frac{1}{\sqrt{2}}([m_0](-1)^{p_0} + i[m_1](-1)^{p_1 + x_j}) \ ,$$

where $m_a = m|_{x_j = a}, p_a = p|_{x_j = a}$, for $a \in \{0, 1\}$.

Proof: Without loss of generality, we set $j = n - 1$. Then, we can write the $1 \times n$ vector

$$m(-1)^p = \begin{pmatrix} m_0(-1)^{p_0} \\ m_1(-1)^{p_1} \end{pmatrix} \ ,$$

where $m_a = m|_{x_{n-1} = a}$, $p_a = p|_{x_{n-1} = a}$, and $a \in \{0, 1\}$.

Let $A = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$. Then,

$$(\prod_{i=0}^{n-2} I_i \cdot N_{n-1}) m(-1)^p = \frac{1}{\sqrt{2}} \begin{pmatrix} A & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & A & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & A \end{pmatrix} \begin{pmatrix} m_0(-1)^{p_0} \\ m_1(-1)^{p_1} \end{pmatrix}$$

$$= \begin{pmatrix} m(0,\ldots,0)(-1)^{p(0,\ldots,0)} + im(0,\ldots,1)(-1)^{p(0,\ldots,1)} \\ m(0,\ldots,0)(-1)^{p(0,\ldots,0)} - im(0,\ldots,1)(-1)^{p(0,\ldots,1)} \\ m(0,\ldots,1,0)(-1)^{p(0,\ldots,1,0)} + im(0,\ldots,1,1)(-1)^{p(0,\ldots,1,1)} \\ m(0,\ldots,1,0)(-1)^{p(0,\ldots,1,0)} - im(0,\ldots,1,1)(-1)^{p(0,\ldots,1,1)} \\ \vdots \\ m(1,\ldots,1,0)(-1)^{p(1,\ldots,1,0)} + im(1,\ldots,1)(-1)^{p(1,\ldots,1,1)} \\ m(1,\ldots,1,0)(-1)^{p(1,\ldots,1,0)} - im(1,\ldots,1,1)(-1)^{p(1,\ldots,1,1)} \end{pmatrix}$$

$$= m_0(-1)^{p_0} + im_1(-1)^{p_1+x_{n-1}} \ .$$

■

Let m and p be Boolean functions. Let $a \in \{0,1\}^t$; then, m_a (respectively p_a) will represent the result of fixing m (respectively p) at $x_{j_k} = a_k$, where $a = \sum_{k=0}^{t-1} a_k 2^k$, and j_k are the indices to which we apply N. Then,

Corollary 8.4

$$(N_{j_{t-1}} \cdots N_{j_0}) m(-1)^p = \frac{1}{2^{t/2}} \sum_{a \in GF(2)^t} i^{\lfloor (a+1)/2 \rfloor} [m_a](-1)^{p_a + x \cdot a}$$

where $x = (x_{j_0}, \ldots, x_{j_{t-1}})$ and $\lfloor (a+1)/2 \rfloor$ means "the floor function for (a+1)/2". The values of the resultant vector are thus in the set $\frac{1}{2^{t/2}}(\{0, \pm 1, \ldots, \pm 2^{t-1}\} + i\{0, \pm 1, \ldots, \pm 2^{t-1}\})$.

Corollary 8.5 *$N_j(-1)^p$ is always flat for p Boolean.*

Proof: $N_j(-1)^p = \frac{1}{\sqrt{2}}((-1)^{p_0} + i(-1)^{p_1+x_j})$, and therefore $|N_j(-1)^p|_{\mathbf{k}} = 1 \ \forall \mathbf{k} \in \mathbb{F}_2^n$, where $|N_j(-1)^p|_{\mathbf{k}}$ means the complex modulus of the $\mathbf{k}^{th}$ component of $N_j(-1)^p$. ■

Remark: Theorem 8.3, together with theorem 17 of [67], allows us to compute $Um(-1)^p$ for any $U \in \{I, H, N\}^n$ and m and p Boolean of any degree, as

$$U = \prod_{i \in \mathbf{R_N}} N_i \prod_{i \in \mathbf{R_H}} H_i \prod_{i \in \mathbf{R_I}} I_i = U_2 \cdot U_1 \ ,$$

where $U_1 = \prod_{j \in \mathbf{R_N}} N_j \prod_{i \neq j} I_i$ and $U_2 = \prod_{j \in \mathbf{R_H}} H_j \prod_{i \neq j} I_i$.

8.4 LC on Hypergraphs

We give in chapter 7 a generalisation over hypergraphs of the pivot operation on graphs. It would be interesting to see how the more general Local Complementation (LC) behaves over hypergraphs. As we will see, the conditions for the generalisation are more restricted. In chapter 3, we give a characterisation of LC on the vertex i as the result of applying N_i to the bipolar vector of the function, $(-1)^p$.

Lemma 8.6 *Let p be a Boolean function. Then, $N_i(-1)^p$ is (equivalent to) a Boolean function iff $\mathcal{N}_i$ is linear.*

Proof: By theorem 3.7 in chapter 3. ∎

This implies that a trivial generalisation by letting

$$p'(\mathbf{x}) = p(\mathbf{x}) + \sum_{j,k \in \mathcal{N}_i, j \neq k} x_j x_k \qquad (\bmod 2)$$

would not be a natural generalisation when $\mathcal{N}_i$ is not linear. As pointed out in chapter 3, in general we get a function $p' : \mathrm{GF}(2)^n \to \mathbb{Z}_4$. This induces difficulties when trying to iterate LC, as it is not known how N_i affects a function $p' : \mathrm{GF}(2)^n \to \mathbb{Z}_4$. This subject will be treated in the following section.

8.5 $\{I, H, N\}^n$ for $p : \{0,1\}^n \to \mathbb{Z}_4$

As in the previous section, the terms inside square brackets are computed $\bmod 2$, and the rest of the operations are understood to be realised over the complex field.

We shall describe here how to compute the effect of the set $\{I, H, N\}^n$ for a class of *generalised Boolean functions*, that is, mappings $p : \{0,1\}^n \to \mathbb{Z}_q$. In this case, $q = 4$. We can, to some extent, generalise this result for any $q \geq 2$, but as q increases the method loses simplicity.

Let $U \in \{I, H, N\}^n$, and let $p : \{0,1\}^n \to \mathbb{Z}_4$. We want to compute the spectrum of Ui^p. Now, as remarked in the previous section, we can compute $Um(-1)^p$ for m and p' Boolean. By means of the following (trivial) result, we can do the same for Ui^p:

Lemma 8.7 *Let $p : \{0,1\}^n \to \mathbb{Z}_4$. Then,*

$$i^p = [m_{\mathcal{R}}](-1)^{p_{\mathcal{R}}} + i[m_{\mathcal{I}}](-1)^{p_{\mathcal{I}}} \ ,$$

with $m_{\mathcal{R}}, m_{\mathcal{I}}, p_{\mathcal{R}}$ and $p_{\mathcal{I}}$ Boolean functions.

Now, taking into account that U is linear, by lemma 8.7

$$Ui^p = U([m_{\mathcal{R}}](-1)^{p_{\mathcal{R}}}) + iU([m_{\mathcal{I}}](-1)^{p_{\mathcal{I}}}) \ .$$

Remark: Note that $N_j i^p$ is not flat in general for $p : \{0,1\}^n \to \mathbb{Z}_4$. E.g, for $x_0x_1 : \{0,1\}^n \to \mathbb{Z}_4$, we get

$$\begin{aligned} N_j i^{x_0x_1} &= N_j(1,1,1,i)^T = N_j[x_0x_1+1](-1)^0 + iN_j[x_0x_1](-1)^0 \\ &= [1] + i[x_1+1](-1)^{x_0} + [0] + i[x_1](-1)^{x_0} = (1+i, 0, 1-i, 2)^T \end{aligned} \ ,$$

where v^T means the transpose of v.

Clearly, we can generalise this for $U[m]i^p$, with m Boolean and $p : \{0,1\}^n \to \mathbb{Z}_4$, using the same decomposition: $[m]i^p = [m_{\mathcal{R}}](-1)^{p_{\mathcal{R}}} + i[m_{\mathcal{I}}](-1)^{p_{\mathcal{I}}}$.

Remark: For $m, p : \{0,1\}^n \to \mathbb{Z}_4$, we can decompose m as the sum of binary monomials and repeat the previous process.

As a first result on flat spectra we can say that if both the spectra of $Um_{\mathcal{R}}(-1)^{p_{\mathcal{R}}}$ and $Um_{\mathcal{I}}(-1)^{p_{\mathcal{I}}}$ are Boolean flat then Umi^p has a flat spectrum as well.

In general, for $p : \{0,1\}^n \to \mathbb{Z}_q$, we want to compute $U\omega^p$ for $U \in \{I, H, N\}^n$, where $\omega = e^{2\pi i/q}$. As for the case $q = 4$, we can decompose ω^p into suitable vectors. For instance, for $q = 8$, the entries of the vector are in the set $\{\pm 1, \pm i, \frac{\pm 1 \pm i}{\sqrt{2}}\}$. From here we can decompose

$$\omega^p = [m_1](-1)^{p_1} + i[m_2](-1)^{p_2} + \frac{1}{\sqrt{2}}[m_3](-1)^{p_3} + i\frac{1}{\sqrt{2}}[m_4](-1)^{p_4} \ ,$$

where m_i and p_i are Boolean for all $i = 1, 2, 3, 4$. Note that, in general, this decomposition will be simpler when q is even, by symmetry.

8.6 Conclusions

We showed for which cases we can change the degree of a function by pivoting on its associated hypergraph, and/or reduce or increase the number of high degree terms. We

described as well the explicit formula for the result of applying a transform $U \in \{I, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$ (which is a generalisation of the bipolar vector of a Boolean function). This, together with the results of [67], allows to compute the result of the application of a $U \in \{I, H, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$. Furthermore, we showed how to compute the result of applying a $U \in \{I, H, N\}^n$ to i^p for $p : \{0, 1\}^n \to \mathbb{Z}_4$.

Chapter 9

Conclusions

9.1 Summary of the results

We have 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 in a number of ways to $\{I, H, N\}^n$. 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. Concretely, we prove that a function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix, concretely the matrix resultant of the following actions, has non-zero determinant mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column
- for $i \in \mathbf{R_N}$, we subsitute 0 for 1 in position $[i, i]$
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column unchanged.

We derived simple recursions for the number of flat spectra with respect to $\{I, H, N\}^n$ for certain recursive quadratic Boolean constructions, and we demonstrated that Quantum Error Correcting Codes with optimal distance appear to have the most flat spectra with respect to $\{I, H, N\}^n$, at least for small n. In subsequent work we hope to develop recursive formulae for nested-clique structures of the type highlighted in [29], as we expect that these will have many flat spectra w.r.t. $\{I, H, N\}^n$.

We also showed computationally that, for small n, the number of flat spectra decreases when the algebraic degree of the Boolean function increases. Future work should seek to establish constructions for Boolean functions of degree greater than two that have as large a number of flat spectra as possible w.r.t. $\{I, H, N\}^n$. More generally, it would be of interest to relax the criteria somewhat, and look for those functions which have many spectra with respect to $\{I, H, N\}^n$ with a worst-case spectral power peak less than some low upper bound (see [29]). One would expect, in this case, that many more Boolean functions of degree > 2 would be found that do well for this relaxed criteria. One promising line of inquiry in this context would be to apply and specialise the construction proposed at the end of [29], which takes a global graph structure, where the graph 'nodes' partition the set of Boolean variables, and where the nodes are 'linked' by permutations over these variable subsets, thereby obtaining higher-degree Boolean functions with potentially favourable $\{I, H, N\}^n$ spectra.

We have answered, indirectly, a question posed at the end of [4] as to a simple combinatorial explanation of the (one-variable) interlace polynomial q, and proven that q summarises some of the spectral properties of the graph w.r.t. $\{I, H\}^n$. Similarly the (one-variable) interlace polynomial Q, as defined in [1], summarises some of the spectral properties of the graph w.r.t. $\{I, H, N\}^n$. We also derived (one-variable) interlace polynomials for the clique and clique-line-clique functions. We then defined the (one-variable) HN-interlace polynomial, and derived its form for the clique, the line, and the clique-line-clique functions. We proved some conjectures of [64], and presented other spectral interpretations of the (one-variable) interlace polynomial. Also, we generalised the (one-variable) interlace polynomial to hypergraphs.

We developed a similar interpretation of the two-variable interlace polynomial proposed in [5], and extended the concept to define the polynomials $Q(x, y)$, $Q_{IN}(x, y)$ and

$Q_{HN}(x, y)$. Also, we showed how to derive the weight hierarchy of the binary code associated with a bipartite graph from an extension of its interlace polynomial.

We have characterised the pivot operation using algebraic normal form (ANF), and generalised the concept to hypergraphs, stating the necessary and sufficient condition that a function of degree higher than two must fulfill in order to allow such an operation. Then we show how the pivot operation on a (hyper)graph can be written as a transform on the bipolar vector of the function associated to it. We construct a family of Boolean functions that have a large number of flat spectra w.r.t. $\{I, H\}^n$, and compute this number. We studied the pivot orbit trajectory of structures that include a clique and developed lower bounds on the number of flat spectra of a graph w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$.

Finally, we showed for which cases we can change the degree of a function by pivoting on its associated hypergraph, or reduce or increase the number of high degree terms. We described as well the explicit formula for the result of applying a transform $U \in \{I, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$ (which is a generalisation of the bipolar vector of a Boolean function). This, together with the results of [67], allows to compute the result of the application of a $U \in \{I, H, N\}^n$ to any vector with entries in the set $\{0, \pm 1\}$. Furthermore, we showed how to use these results for computing the result of the application of a $U \in \{I, H, N\}^n$ to i^p for $p : \{0, 1\}^n \to \mathbb{Z}_4$.

9.2 Open Problems

In this section, we propose some open problems, related to the work presented in this thesis.

- In chapter 5, we defined a *generalisation of the interlace polynomial for hypergraphs* (definition 5.29). However, due to the fact that the PAR for Boolean functions of degree higher than two does not summarise much of the information about the power spectra – as opposed to the case of quadratic Boolean functions – it was not entirely satisfactory, and it lacked a proper graph definition. Also, in general it would not be a polynomial, as the PAR for Booleans of degree higher than two is not in general a power of two. The interlace polynomial $q(z)$ for graphs was originally defined in [2, 4] by means of a recursion formula using the pivot operation for graphs. It would

be interesting to construct an interlace polynomial $q(z)$ based on recursive pivots on the hypergraphs, following the generalisation of pivot to hypergraphs proposed in chapter 7, at least for those hypergraphs that allow pivot. The idea would be to define appropriately the interlace polynomial for monomials and construct the interlace polynomial of a hypergraph from them, by using the pivot for hypergraphs to reduce the degree of the function, and/or to reduce the number of terms. Defining the interlace polynomial for these 'basic' terms, we can then define the interlace polynomial for the initial function, based on the PAR of the spectra or on some other property.

- A binary linear code is $\{I, H\}^n$-equivalent to its dual, as seen from [67] (see section 6.7 or section 10.8 in the Appendix). But any $m(\mathbf{x})(-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ affine Boolean and $m(\mathbf{x})$ Boolean, is equivalent (via a diagonal transform of the type we introduced in section 3.3) to a binary indicator of a code. In other words, for any spectrum of the type $s = m(\mathbf{x})(-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ affine Boolean and $m(\mathbf{x})$ Boolean, we can apply a diagonal transform δ such that $\delta \cdot s = m'(\mathbf{x})$, with $m'(\mathbf{x})$ Boolean. m' is the binary indicator for a certain code (linear or non-linear). That is, we define a code C by:

  $$x \in C \Leftrightarrow m_x = 1 \ ,$$

  where m_x is the x^{th} entry of the vector m. Given a Boolean function $p(\mathbf{x})$ of any degree, all spectra in the $\{I, H, N\}^n$ orbit of the type above (i.e. $m(\mathbf{x})(-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ affine Boolean and $m(\mathbf{x})$ Boolean) give $\{I, H, N\}^n$-equivalent codes. Experimentally, we have found some non-linear codes that are equivalent in this sense. It would be interesting to study the properties of these codes. More generally, by taking not only Boolean $m(\mathbf{x})$'s but also generalised Boolean, we can get equivalences between codes whose codewords occur with different probabilities.

- The Kerdock code and the Preparata code are formally dual, i.e. their weight distributions are the same. In [67], it was shown that the Kerdock code is equivalent to a vector $(-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ a cubic Boolean function. It seems likely that the two codes are related by a Local Unitary (LU) transform; that is, with the notation above, let m_K be the indicator of the Kerdock code and m_P be the indicator

of the Preparata code. We are interested in finding a LU transform U such that $m_K = Um_P$. First, we would like to see if such a transform can be found in the set of transforms $\{I, H, N\}^n$, as we have some techniques for the computation of the spectra of functions on a relatively large set of variables. Also, it would be interesting to relate such a transform with an operation on hypergraphs.

- In chapter 8, we showed the result of applying $\{I, N\}^n$ to a state of the form $m(-1)^p$, with m and p Boolean (that is, to a vector with entries in the set $\{0, \pm 1\}$). This result can be combined with the results of Parker and Rijmen in [67] for computing the result of applying $\{I, H, N\}^n$ to $m(-1)^p$. However, it would be nice to have a joint formula for the result of applying a transform $\{I, H, N\}^n$ to $m(-1)^p$.

- Also in chapter 8, we saw how to apply a transform in $\{I, H, N\}^n$ to generalised Boolean functions (that is, mappings $p : \{0, 1\}^n \to \mathbb{Z}_q$). Concretely, we studied the case $q = 4$. It would be interesting to investigate further the spectral properties of those functions for $q = 4$, and more generally for other values of q, and study their symmetries, at least for quadratics. As we saw in section 3.3.3, the case $q = 4$ is highly related to the LC orbit of a Boolean function, so we see that at least in this case some symmetries exist and have a graphical interpretation.

- We are also interested in the graphical interpretation of generalised Boolean functions, with weighted graphs: A *weighted graph* is a graph in which each edge is given a numerical *weight* (that is, a numerical label); we can represent a *quadratic general Boolean function*, that is a mapping $p : \{0, 1\}^n \to \mathbb{Z}_q$ of degree two, with a (simple, undirected) weighted graph with labels in the set $\{0, \ldots, q-1\}$. That is, given the ANF (algebraic normal form) of the function,

$$p = \sum_{0 \le i < j \le n-1} a_{ij} x_i x_j, \quad \text{where } a_{ij} \in \mathbb{Z}_q \ ,$$

  we define as set of vertices the set $\{0, \ldots, n-1\}$; we define an edge between the vertex i and the vertex j iff $a_{ij} \neq 0$. The weight of the edge is then a_{ij}. We are interested in studying this type of graph, as well as the graphical operations connecting graphs and their spectral interpretation.

- In [91], there is a description of the action of H_i on certain APF's via graph operations: let $m(-1)^p$ such that p is a quadratic Boolean function and m is a product of affine functions. Then, the phase p can be represented as a simple undirected graph as shown in this thesis (see for instance the introduction, chapter 1). Also, it is shown there how the magnitude m can be represented by a coloured bipartite graph. Thus, the entire $\{I, H\}^n$ orbit of the state represented by the APF can be represented graphically by graphical transformations on both graphs. This technique can be used to reduce the computing time for the computation of the $\{I, H\}^n$ spectra. It would be interesting to find a generalisation of this graphical description for any transform in $\{I, H, N\}^n$, if this is possible. The main difficulty arises from the fact that, under the transform N_j (that is, the transform $I \otimes \cdots N \otimes \cdots \otimes I$, where the n is on the j^{th} position), in general the result is not of the form $m(-1)^p$, with p and m as described or even Boolean. A possible solution would be the use of weighted graphs as proposed above.

- We are interested in finding recursion formulae for interlace polynomials of some new recursive structures for, as we saw in chapter 5, the interlace polynomials encode most of the information about the power spectra and thus about the quantum properties of the graph state, at least for quadratics.

- As we mentioned in the introduction (see section 1.1), the analysis of spectra w.r.t. $\{I, H, N\}^n$ provides more information about $p(\mathbf{x})$ than is provided by the spectrum w.r.t. the WHT alone; for instance, the analysis of the spectra w.r.t. $\{I, H\}^n$ identifies the linear or affine approximations to a Boolean function after fixing some of the variables, and is thus related to a probabilistic version of the algebraic immunity [56] of the function. We can further generalise this idea, taking the whole spectra w.r.t. $\{I, H, N\}^n$, to include a more general type of linear approximation, concretely linear approximations over any weighted alphabet, as proposed by Parker [69, 28]. In [28], Danielsen, Gulliver and Parker propose a generalised differential cryptanalysis based on the set $\{I, H, N\}^n$. 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, using as in [69] not only binary linear approximations but approximations over more general alphabets (see [28] for more details). It would

be interesting to study further the applications of the generalised bent criteria to classical cryptography, and, more generally, of the results contained in this thesis. For instance, there are more potential applications to Secret Sharing [10, 84], HFE [70] and to the potential cryptanalysis of stream and block ciphers.

- We have seen (lemma 7.3) that the pivot transform applied on bipartite graphs gives as a result a bipartite graph. On the other hand, the results of [67] show that a linear binary code can be obtained from a bipartite graph, via a transform in $\{I, H\}^n$ (see section 6.7, or section 10.8 of the Appendix). Let d_n be the number of binary linear codes isomorphic to their dual. Let c_n be the number of inequivalent binary linear codes. Then it appears that $c_n = 2k_n - d_n$, with k_n the number of pivot-inequivalent bipartite graphs. Is this always true?

Bibliography

[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, 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. Preprint: 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. Preprint: http://arxiv.org/abs/math/0209054, v3, 13 Aug. 2004.

[6] 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.

[7] H. Barnum and N. Linden, "Monotones and Invariants for Multi-Particle Quantum States," *Journal of Physics A: Math. Gen.*, **34**, 6787–6805, 2001. http://xxx.soton.ac.uk/pdf/quant-ph/0103155

[8] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels", Phys. Rev. Lett. vol. 70, pp 1895-1899 (1993) (the original 6-author research article).

[9] S. Bravyi, "Entanglement Entropy of Multipartite Pure State", *Physics Review A*, **67**, 012313, 2003. http://xxx.soton.ac.uk/pdf/quant-ph/0205021

[10] G. R. Blakley, "Safeguarding cryptographic keys", *Proceedings of the National Computer Conference*, **48**, pp. 313–317, 1979.

[11] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Advances in Cryptology Crypto '90, Springer-Verlag*, pp. 2–21, 1991.

[12] E. Biham and A. Shamir, "Differential cryptanalysis of FEAL and N-Hash", *Advances in Cryptology Eurocrypt '91, Springer-Verlag*, pp. 156–171, 1991.

[13] H. J. Briegel and R. Raussendorf, "Persistent Entanglement in Arrays of Interacting Particles", http://xxx.soton.ac.uk/pdf/quant-ph/0004051 v2. 28 Aug 2000.

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

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

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

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

[18] D. Bouwmeester, J-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation", *Nature (London)* **390**, 575, 1997.

[19] 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).

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

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

[22] R. W. Chang, "Synthesis of band-limited orthogonal signals for multi-channel data transmission", *Bell Systems Technical Journal* **46**, 1775–1796, 1966.

[23] R. W. Chang and R. A. Gibbey, "A theoretical study of performance of an orthogonal multiplexing data transmission scheme", *IEEE Transactions on Communications Technology* **16** (4), 529–540, 1968.

[24] D. Coppersmith, "The data encryption standard and its strength against attacks", *IBM Research Report* **RC 18613 (81421)**, T. J. Watson research center, 1992.

[25] B. Courcelle and S. Oum, "Vertex-minors, MS Logic and Seese's Conjecture", *preprint*, 2004.

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

[27] 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.

[28] 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*, Accepted for Inform. Comput., Sept. 2005. http://www.ii.uib.no/∼matthew/GenDiff4.ps.

[29] 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.

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

[31] J. A. Davis and J. Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes", *IEEE Trans. Inform. Theory*, Vol 45, No 7, pp 2397–2417, Nov 1999.

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

[33] P. A. M. Dirac, "Principles of Quantum mechanics", Oxford University Press; 4th edition, 1982.

[34] H. Dobbertin, "Construction of Bent Functions and Balanced Functions with High Nonlinearity", *Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag* No 1008, pp 61-74, 1994.

[35] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.* **47** 777, 1935.

[36] T. Gallai, "Über extreme Punkt- und Kantenmengen." *Ann. Univ. Sci. Budapest, Eotvos Sect. Math.* **2**, 133–138, 1959.

[37] 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.

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

[39] M. J. E. Golay, "Complementary Series", *IRE Trans. Inform. Theory*, **IT-7**, pp. 82–87, Apr. 1961.

[40] D. Gottesman, "An Introduction to Quantum Error Correction". In *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, *Proceedings of Symposia in Applied Mathematics*, 2002. http://arxiv.org/pdf/quant-ph/0004072

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

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

[43] T. A. Gulliver and M. G. Parker, "The Multivariate Merit Factor of a Boolean Function", *Proc. IEEE Information Theory Workshop on Coding and Complexity – ITW 2005*, pp. 58–62 2005.

[44] R. W. Hamming, "Error-detecting and error-correcting codes", *Bell System Technical Journal* **29(2)**, 147–160, 1950.

[45] 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.

[46] T. Helleseth, T. Kløve, J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$", *Discrete Math.* **18**, pp. 179–211, 1977.

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

[48] B. S. Kaliski Jr. and M. J. B. Robshaw, "Linear cryptanalysis using multiple approximations", *Advances in Cryptology - Crypto '94, Springer-Verlag*, pp. 26–39, 1994.

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

[50] L. R. Knudsen, "Practically secure Feistel ciphers", *Proceedings of 1st Workshop on Fast Software Encryption, Springer-Verlag*, pp. 211–221, 1993.

[51] X. Lai, J. L. Massey and S. Murphy, "Markov ciphers and differential cryptanalysis" *Advances in Cryptology - Eurocrypt '91, Springer-Verlag*, pp. 17–38, 1992.

[52] S.K. Langford and M.E. Hellman, "Differential-linear cryptanalysis", *Advances in Cryptology - Crypto '94, Springer-Verlag*, pp. 17–25, 1994.

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

[54] M. Matsui, "Linear cryptanalysis method for DES cipher", *Advances in Cryptology - Eurocrypt '93, Springer-Verlag*, pp. 386–397, 1993.

[55] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher", *Advances in Cryptology - Eurocrypt '92, Springer-Verlag*, pp. 81–91, 1992.

[56] W. Meier, E. Pasalic, C. Carlet, "Algebraic Attacks and Decomposition of Boolean Functions", *Advances in Cryptology - Eurocrypt '04, Springer-Verlag*, pp. 474–491, 2004.

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

[58] J. Monaghan, I. Sarmiento, "Properties of the interlace polynomial via isotropic systems", *preprint*

[59] S. Murphy, "The cryptanalysis of FEAL-4 with 20 chosen plaintexts", *Journal of Cryptology*, **2(3)**, pp. 145–154, 1990.

[60] B. D. McKay, "nauty User's Guide", http://cs.anu.edu.au/∼bdm/nauty/nug.pdf, 2004.

[61] K. Nyberg, "Linear approximation of block ciphers", *Advances in Cryptology - Eurocrypt '94, Springer-Verlag*, pp. 439–44, 1995.

[62] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack", *Journal of Cryptology*, **8(1)**, pp. 27–37, 1995.

[63] L. O'Connor, "A unified markov approach to differential and linear cryptanalysis", *Advances in Cryptology - Asiacrypt '94, Springer-Verlag*, pp. 387–397, 1995.

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

[65] 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.

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

[67] 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.

[68] 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.

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

[70] J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms", *Eurocrypt'96*, Springer Verlag, pp. 33–48, 1996.

[71] S. P. Radziszowski, "Small Ramsey Numbers", *The Electronic Journal of Combinatorics*, Dynamic Survey DS1, 1–42, http://www.combinatorics.org/Surveys/ds1.pdf, 1994.

[72] R. Raussendorf and H. J. Briegel, "Quantum Computing via Measurements Only", http://xxx.soton.ac.uk/abs/quant-ph/0010033, 7 Oct 2000.

[73] R. Raussendorf and H. J. Briegel, "A One-Way Quantum Computer", *Phys. Rev. Lett.* **86**, 910, 2001.

[74] C. Riera and M. G. Parker, "Generalised Bent Criteria for Boolean Functions (I)", *submitted to IEEE Trans Inform. Theory*, Dec. 2004. http://xxx.soton.ac.uk/ps/cs.IT/0502049

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

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

[77] 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/2var3.ps

[78] C. Riera and M. G. Parker, "One and Two-Variable Interlace Polynomials: A Spectral Interpretation", submitted to *Proceedings of WCC2005, Bergen*, Lecture Notes in Computer Science, LNCS, October 2005. http://www.ii.uib.no/∼matthew/paperwcc4.pdf.

[79] C. Rigolin, "Quantum teleportation of an arbitrary two qubit state and its relation to multipartite entanglement", *Phys. Rev. A* **71**, 2005. http://arxiv.org/pdf/quant-ph/0407219

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

[81] W. Rudin, "Some Theorems on Fourier Coefficients", *Proc. Amer. Math. Soc.*, No 10, pp. 855–859, 1959.

[82] 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.

[83] C. E. Shannon, "A mathematical theory of communication", *Bell System Tech. J.* **27**, 1948.

[84] A. Shamir, "How to share a secret", *Communications of the ACM*, **22(1)**, pp. 612–613, 1979.

[85] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM J. Sci. Statist. Comput. 26*, 1997.

[86] P. W. Shor, "Scheme for reducing decoherence in quantum memory", *Phys. Rev. A* **52**, 2493–2496, 1996.

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

[88] A. M. Steane, "Error correcting codes in quantum theory", *Phys. Rev. Lett.* **77**, 793–797, 1996.

[89] A. M. Steane, "Quantum Computing", *Rept. Prog. Phys.* **61**, pp. 117–173, 1998.

[90] A. M. Steane, "Quantum Computing and Error Correction", http://arxiv.org/abs/quant-ph/0304016, 2003.

[91] D. Storøy, "On Boolean Functions, Unitary Transforms, and Recursions", *Master's Thesis, the Selmer Center, Dept. of Informatics, University of Bergen, Norway*, http://rasmus.uib.no/∼dst033/index.html, June, 2005.

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

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

[94] 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. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/?0308151.

[95] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions", *Advances in Cryptology–Eurocrypt 2005, LNCS, Springer-Verlag* (to appear), 2005.

[96] T-C. Wei and P. M. Goldbart, "Geometric Measure of Entanglement and Applications to Bipartite and Multipartite Quantum States", *Physical Review A*, **68**, 042307, 2003. http://xxx.soton.ac.uk/pdf/quant-ph/0307219

[97] T-C. Wei, J. B. Altepeter, P. M. Goldbart and W. J. Munro, "Measures of Entanglement in Multipartite Bound Entangled States", *Physical Review A*, **70**, 022322, 2004. http://xxx.soton.ac.uk/pdf/quant-ph/0308031

[98] T-C. Wei, M. Ericsson, P. M. Goldbart and W. J. Munro, "Connections Between Relative Entropy of Entanglement and Geometric Measure of Entanglement", *quant-ph/0405002 v2*, 3 Jul, 2004. http://xxx.soton.ac.uk/pdf/quant-ph/0405002

[99] V. K. Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. Inform. Theory*, **37 (5)**, pp. 1412–1418, 1991.

[100] S. Wiesner, "Conjugate Coding", *SIGACT News* **15:1**, pp. 78-88, 1983.

[101] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned", *Nature* **299**, pp. 802–803, 1982.

Chapter 10

Appendix: Various Interpretations of Graph States

In this section we summarise the different interpretations of graph states, following [14, 15, 16, 19, 25, 37, 38, 58, 67, 92, 93].

We recall here the definition of a graph state (definition 2.22):

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

$$\begin{aligned} K_i &= \sigma_x^{(i)} \prod_{j \in \mathcal{N}_i} \sigma_z^{(j)} \\ &= \sigma_x^{(i)} \prod_{k=0}^{n-1} (\sigma_z^{(k)})^{\Gamma[k,i]} \ , \end{aligned} \tag{10.1}$$

where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, 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. A *graph state* is defined as:

Definition 10.1 *[45] The* graph state $|G\rangle$*, also known as* cluster state*, is the unique (modulo an overall phase factor) common eigenvector with eigenvalue* 1 *of all operators in the subgroup generated by the K_i operators.*

10.1 Interpretation as a Quadratic Boolean Function

Let $p(\mathbf{x}) : GF(2)^n \rightarrow GF(2)$ be a (homogeneous) quadratic Boolean function, defined by its Algebraic Normal Form (ANF),

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

with $\mathbf{x} = (x_0, \ldots, x_{n-1})$, and the coefficients $a_{ij} \in \{0, 1\}$. We associate to $p(\mathbf{x})$ a graph G, as follows: we take as set of vertices the set $\{0, \ldots, n-1\}$, and as set of edges the set defined by the coefficients of $p(\mathbf{x})$; that is, we define an edge between the index i and the index j if and only if $a_{ij} = 1$ in the ANF. The graph G thus defined will be non-directed and simple (meaning that it has no loops and no multiple edges).

The adjacency matrix, Γ, associated to $p(\mathbf{x})$, is defined as the matrix having as entries $\Gamma(i, j) = \Gamma(j, i) = a_{ij}$, $i < j$, $\Gamma(i, i) = 0$.

From the graph G we can define the graph state $|G\rangle$ as seen at the beginning of the chapter. It can be proven (see Van den Nest's thesis [93]) that

$$|G\rangle = \frac{1}{2^{n/2}} (-1)^{p(\mathbf{x})} \ .$$

We recall here definition 2.2: by $(-1)^{p(\mathbf{x})}$ (the *bipolar vector* of the function $p(\mathbf{x})$) we mean the vector $(-1)^{p(\mathbf{x})} = ((-1)^{p(0,\ldots,0)}, (-1)^{p(0,\ldots,1)}, \ldots, (-1)^{p(1,\ldots,1)})$. Hence, there is an equivalence between homogeneous quadratic Boolean functions and graph states (it is easy to see that from any graph G simple and non-directed we can define a quadratic Boolean function, by defining the ANF from the coefficients of the adjacency matrix).

It will be convenient along the text to consider not only homogeneous quadratic functions, but also functions having an affine offset. However, the graph G is defined depending only on the quadratic terms, and the offset itself will play little role. Then, we shall here consider equivalent functions that vary only in an affine offset.

Theorem 10.2 *[93] (Proposition 2.14). A graph state can be represented by the pure state $s = (-1)^p$, where p is a quadratic Boolean function such that $p = \sum_{j<k} \Gamma_{jk} x_j x_k$.*

Theorem 10.3 *A pure state s of n qubits is an eigenvector of a stabilizer of Hermitian operators K_G iff $s = (-1)^p$, with p Boolean quadratic.*

Proof: To within some normalisation factor, any pure quantum state of n qubits can be approximated to necessary precision by using the following algebraic form,

$$s = m(\mathbf{x})\alpha^{p(\mathbf{x})},$$

where α is a T^{th} complex root of 1, T arbitrary but even, $m : \{0,1\}^n \to \mathbb{Z}$, and p is a generalised Boolean function $p : \{0,1\}^n \to \mathbb{Z}_T$, such that $s_{\mathbf{i}} = m(\mathbf{x} = \mathbf{i})\alpha^{p(\mathbf{x}=\mathbf{i})}$.

We show that no state with non-constant magnitude, m, and/or algebraic degree of p other than two (i.e. with $\deg(p) \neq 2$) can be an eigenvector for K_G.

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

$$s' = m(\mathbf{x})\alpha^{p(\mathbf{x})+\frac{T}{2}\sum_k \Gamma_{vk}x_k}.$$

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,

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

We therefore arrive at our first condition:

- $s'' = \lambda s$ iff $\mathcal{N}_v(\mathbf{x}) = \frac{-T}{2}\sum_k \Gamma_{vk}x_k + c$, where $c \in \mathbb{Z}_T$. Therefore, $\deg(\mathcal{N}_v(\mathbf{x})) \leq 1$.

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 two above 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 $\frac{-T}{2}$ (but for a constant that can be neglected), and so we can write $\alpha^{p(\mathbf{x})} = (-1)^{p_b(\mathbf{x})}$, with p_b 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. ∎

10.2 Interpretation as a Quantum Error Correcting Code

Let E be a $2n$-dimensional binary vector space, whose elements are written as $(a|b)$, where $a,\ b\ \in \mathrm{GF}(2)^n$, 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 10.4 *[19] 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 $< d$ in $S\backslash S^\perp$. Then, there exits 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 GF(4) additive code.

10.3 Interpretation as a GF(4) Additive Code

From [19] we see how to interpret the binary space E as the space $\mathrm{GF}(4)^n$ and thereby how to derive a QECC from an additive (classical) code over $\mathrm{GF}(4)^n$. Let $GF(4) = \{0,1,\omega,\bar{\omega}\}$, 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 $\mathrm{GF}(4)^n$, written $wt(u)$, is the number of non-zero components, and the *Hamming distance* between $u,u'\in \mathrm{GF}(4)^n$ is $\mathrm{dist}(u,u') = wt(u+u')$. Define the *trace function* as: $tr(x) : GF(4)\to GF(2),\ tr(x) = x+\bar{x}$. 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 $\mathrm{GF}(4)^n$ that is closed under addition (defining thus an additive code). The *trace inner product* of $u,v\in$ GF(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

$$C^{\perp} = \{u \in \ \mathrm{GF}(4)^n : u \star v = 0 \ \forall v \in C\} \ .$$

Now one can reformulate Theorem 10.4.

Theorem 10.5 *Let C be an additive self-orthogonal subcode of $GF(4)^n$, containing 2^{n-k} vectors, such that there are no vectors of weight $< d$ in $C \setminus C^{\perp}$. Then any eigenspace*[1] *of $\phi^{-1}(C)$ is a QECC with parameters $[[n, k, d]]$.*

By Glynn (see [37, 38]), we have: Let S be a $(n-k) \times n$ matrix over GF(4), such that its rows are GF(2)-linearly independent. Then we define a QECC with parameters $[[n, k, d]]$ as the set of all GF(2)-linear combinations of the rows of S. The code is *self-dual* when $k = 0$.

10.4 The QECC as a Graph

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 [37], 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 $\mathrm{PG}(m, q)$ be the finite projective space defined from the vector space of rank $m+1$ over the field $\mathrm{GF}(q)$ (that is, the space of one-dimensional vector subspaces of that vector space). Then, we can interprete the *Grassmannian* of lines of $\mathrm{PG}(n-1, 2)$, $G_1(\mathrm{PG}(n-1, 2))$, as a variety immersed in the projective space $\mathrm{PG}(k, 2)$, where $k = \binom{n}{2}$: each line l_i is defined by two points, a_i and b_i. We associate to the set of lines all products $a_i b_j + a_j b_i, \ i \neq j \ (\mathrm{mod}2)$. Define a mapping from a column of an $n \times n$ matrix S over GF(4) to a vector of length $\binom{n}{2}$ with coefficients in GF(2): We write each column over GF(4) as $a + b\omega$, where $a, b \in \mathrm{GF}(2)^n$.

[1] Let A be an $n \times n$ square matrix and λ an eigenvalue of A; then, the *eigenspace* of λ is defined as the union of the zero vector and the set of all eigenvectors corresponding to eigenvalues λ. It is a subspace of $\mathbb{R}^n$.

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

Taking all the 2×2 subdeterminants found when we put the two vectors into a matrix, we get the points of the Grassmannian. A point in $G_1(\mathrm{PG}(n-1,2))$ is equivalent to a line in $\mathrm{PG}(n-1,2)$, which is equivalent to a column of length n over GF(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 $\mathrm{PG}(n-1,2)$. As each line of $\mathrm{PG}(n-1,2)$ corresponds to a (star) kind of graph, the set corresponds to a graph in n vertices.

10.5 Interpretation as a Generator Matrix over GF(2) and GF(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 [92]. 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 $\mathrm{GF}(2)^n$. We can further interpret G_T as a generating matrix of a code over $\mathrm{GF}(4)^n$, as follows [19]:

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

is the generating matrix of an additive code over $\mathrm{GF}(4)^n$. Different graphs may define

the same code, but this relation is 1-1 with respect to LC-equivalence between graphs, as defined in section 3.2.

10.6 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 $\mathrm{GF}(4)^n$. Once again, LC-equivalent graphs define equivalent $\mathbb{Z}_4$ codes.

10.7 Interpretation as an Isotropic System

The graph state can also be viewed as an isotropic system (see [14, 16, 15, 25, 58]).

Let A be a 2-dimensional vector space over GF(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 GF(2)-homomorphisms $A^V : V \to A$. Define in this GF(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 10.6 *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[2] which is a 2-dimensional vector space, and set $K' = K \setminus \{0\}$. Note that $x + y + z = 0$.

Lemma 10.7 *([16]) 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.*

[2]The Klein group is the abstract group (that is, characterized only by its abstract properties and not by the particular representations chosen for elements) corresponding to $C_2 \times C_2$, where C_2 is the group of order 2.

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 10.8 *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 10.9 *([16]) 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 elsewhere referred to as the interlace polynomial of G (see chapter 5).

10.8 Bipartite Quadratics as Binary Linear Codes

The subset of quadratic Boolean functions that can be represented by bipartite graphs, have an interpretation as binary linear codes [67]: Let $\mathbf{T_C}$, $\mathbf{T_{C^\perp}}$ be a bipartite splitting of $\{0, \ldots, n-1\}$, and let us partition the variable set $\mathbf{x} = (x_0, \ldots, x_{n-1})$ as $\mathbf{x} = \mathbf{x_C} \cup \mathbf{x_{C^\perp}}$, where $\mathbf{x_C} = \{x_i : i \in \mathbf{T_C}\}$, and $\mathbf{x_{C^\perp}} = \{x_i : i \in \mathbf{T_{C^\perp}}\}$. For a quadratic bipartite function $p(\mathbf{x})$, we can write $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, with q_k and r_k homogeneous linear Boolean functions (clearly, such a function $p(\mathbf{x})$ 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, C. In other words, for $T = T_C$, $s'(x) = 1$ iff $x \in C$.

Note: There is also an equivalent interpretation of bipartite graphs as *binary matroids* (e.g. [20]).