Aperiodic Correlations of Length 2^m Sequences, Complementarity, and Power Control for OFDM

Timothy Edward Stinchcombe

Thesis submitted to the University of London
for the degree of
Doctor of Philosophy

April 2000

Royal Holloway and Bedford New College
University of London

Abstract

A complementary set of sequences is that for which the sum of the aperiodic auto-correlation functions across all sequences in the set is zero except at the zero shift. They find utility in a wide range of applications, including that of Orthogonal Frequency Division Multiplexing (OFDM), a method of transmitting data simultaneously over a large number of frequencies. Sequences for OFDM have an associated parameter called the 'peak-to-mean envelope power ratio' (PMEPR), and sequences from small complementary sets have low PMEPRs, and so are attractive for engineering reasons.

This thesis follows up aspects of recent results of Davis and Jedwab, and Paterson, who give explicit constructions for complementary sets of sequences of length 2^m over $\mathbb{Z}_q$ (q even). Using techniques deriving from the algebraic normal form of the generalized Boolean functions that represent the sequences, a number of results concerning auto- and cross-correlations are proved, resulting in classes of sequences for which: the auto-correlation functions are the same; pairs of cross-correlation functions sum to zero, or are the same; pairs of cross-correlation functions sum to zero except at one shift; pairs of auto-correlation functions sum to zero except at the zero shift and one other shift. These results are then used to prove a conjecture of Paterson (concerning the maximum PMEPR of certain sets of sequences) for two specific cases, and to show that it is true in many others. A new lower limit on PMEPR is also developed that shows that the conjecture cannot be true in general.

Complementary sets are also manufactured from pairs of sequences given by the construction, thus demonstrating the structure that is inherent within such a pair. By examining the effect of the inverse Gray map on algebraic normal form, it is shown that a complementary pair from the construction over $\mathbb{Z}_2$ remains a complementary pair when mapped to $\mathbb{Z}_4$ by the inverse Gray map.

Acknowledgements

First I would like thank my supervisor and adviser, Professors Fred Piper and Peter Wild, for their help, well-founded advice, and seemingly innate ability to recognize my competence to do this thing, even though I doubted it myself. Next my thanks go to Dr. Kenny Paterson for introducing me to the subject matter, and for guidance and timely comments at critical junctures. Special thanks go to Dr. Karl Brincat for always having an open door and acting as a sounding board for my ideas, and for his endless encouragement and enthusiasm.

The financial assistance provided by the Engineering and Physical Sciences Research Council is gratefully acknowledged.

The staff and my fellow students within the Mathematics Department, by their warmth and friendship, have provided a most pleasant and genial environment during my (nearly five) years of study at Royal Holloway—my thanks go to them all.

Special thanks go to Charles Cunningham, who taught me Transcendental Meditation. Amongst the many things this has given me, the ability to re-take control of the pace of my life, and so to manage my stress levels, has been invaluable—without it I doubt whether I would have made it through my MSc, let alone a PhD.

Lastly, loving thanks go to my family for their unfailing support, and for my neglecting them more than usual during what, as it appears to me, is essentially a self-indulgent activity.

T.E.Stinchcombe
Royal Holloway
April 2000

Dedicated to the memory of my father

RICHARD GEORGE STINCHCOMBE
1927-1988

“Actually, I’ve been thinking it ever since I got here:
‘Why, oh why didn’t I take the *blue* pill?’ ”
The Matrix

Contents

List of Figures

Notation

A^*	Complex conjugate of A	12
$\overline{\mathbf{A}}$	The reverse of vector $\mathbf{A}$	12
$C(\mathbf{A},\mathbf{B})(\ell)$	The aperiodic cross-correlation of $\mathbf{A}$ and $\mathbf{B}$	13
$A(\mathbf{A})(\ell)$	The aperiodic auto-correlation of $\mathbf{A}$	13
$S(\mathbf{A})(t)$	Complex envelope of OFDM signal	16
$P(\mathbf{A})(t)$	Envelope power of OFDM signal	17
PEP	Peak Envelope Power	19
PMEPR	Peak-to-Mean Envelope Power Ratio	19
$f(1-x)$	The reverse of function f, in algebraic normal form	26
$\overline{f}$	Alternative notation for the reverse of function f	26
$G(f)$	The graph of function f	28
$wt_H(\cdot)$	Hamming weight	30
$RM_q(r,m)$	Generalized Reed-Muller code	30
$\mathbf{F}\big\|_{\mathbf{x}=\mathbf{c}}$	A restriction of the vector $\mathbf{F}$	31
$f\big\|_{\mathbf{x}=\mathbf{c}}$	The restricted algebraic normal form of f	32
$i_{\mathbf{c}}$	Index of first non-zero entry in a restricted vector	36
$\overline{i}_{\mathbf{c}}$	Index of last non-zero entry in a restricted vector	36
$n_{\mathbf{x}}$	The span of non-zero entries in a restricted vector	37
$[\mathbf{F}\big\|_{\mathbf{x}=\mathbf{c}}]$	Restricted vector with leading and trailing zeroes truncated	39
$\overline{f\big\|_{\mathbf{x}=\mathbf{c}}}$	The reverse of the restricted function $f\big\|_{\mathbf{x}=\mathbf{c}}$	43
$\widetilde{\mathbf{F}}\big\|_{\mathbf{x}=\mathbf{c}}$	Restricted vector $\mathbf{F}\big\|_{\mathbf{x}=\mathbf{c}}$ with the non-zero entries reversed	44
$\widehat{\mathbf{F}}\big\|_{\mathbf{x}=\mathbf{c}}$	Compressed vector from the restricted vector $\mathbf{F}\big\|_{\mathbf{x}=\mathbf{c}}$	45
$\widehat{f}\big\|_{\mathbf{x}=\mathbf{c}}$	Compressed function equivalent to the vector $\widehat{\mathbf{F}}\big\|_{\mathbf{x}=\mathbf{c}}$	46
$\widehat{\mathbf{f}}\big\|_{\mathbf{x}=\mathbf{c}}$	Vector of values of the compressed function $\widehat{f}\big\|_{\mathbf{x}=\mathbf{c}}$	46

Chapter 1

Introduction and Background

1.1 Introduction and Overview

Orthogonal Frequency Division Multiplexing (OFDM) is a technique for transmitting data simultaneously on a number of sinusoidal waveforms of different, equally spaced frequencies. It has properties that are attractive to a number of different applications, but of course there are inevitably drawbacks. One of these is that the data to be transmitted essentially determine the relative phases of the sinusoids, and when the peaks (or troughs) of the sinusoids line up, so that they add most constructively, it is possible to get peaks in the signal level which are many times that of the average level. A peak in the signal level equates to a peak in the power of the signal, and in order to avoid distortion to the signal the equipment being used has to be able handle these high power levels. This means that for a large percentage of the time the equipment is operating at levels very much below its maximum capacity, which is inefficient. Thus it is very desirable to reduce the gap between the peak and average power levels. Unfortunately the problem of determining the maximum value of the sum of a number of sinusoids of different frequencies is an old and tricky one which so far has defied analytic solution.

For OFDM the problem can be ameliorated by avoiding those combinations of phases which are known to result in large peaks in the power. This implicitly requires some form of coding (which in turn will introduce redundancy), i.e. mapping the source data to some set of data that is more suitable for actual transmission. The problem then shifts to determining which combinations of phases *do* result in large peaks. An exhaustive search through all possibilities to identify suitable combinations, even if this can be achieved in a sensible time frame, is not seen as a very practical solution. However it turns out that if the data to be transmitted is in fact a *Golay complementary sequence*, then the power of the resulting signal is subjected to an upper bound which is sufficiently low to be of practical significance. A Golay complementary sequence is one of a pair for which the sum of the aperiodic auto-correlation functions at all non-zero shifts is zero. That this property leads to the upper bound was published by Popovic in 1991 [36], but even then did not completely resolve the problem because generally such sequences were generated via recursive methods which are not very practical. More recently, however, Davis & Jedwab have devised a deterministic method of constructing Golay complementary sequences of length 2^m over alphabets $\mathbb{Z}_{2^h}$, based on the algebraic normal form representation of certain quadratic generalized Boolean functions, [10, 11]. (As their name suggests, these functions are just a generalization of ordinary Boolean functions, the sequence being all values of the function ordered in a natural way.) The functions so constructed result in a number of schemes for coding the data for OFDM transmission for which the power is tightly bounded, and which additionally allow for error correction. Paterson then developed and extended these ideas for sequences over $\mathbb{Z}_q$ (q even), providing bounds on the power for a wider range of quadratic generalized Boolean functions, [33].

In [33], and in a preliminary version which preceded it, [32], Paterson developed some techniques, most notably including one termed *restriction*, for manipulating the cross- and auto-correlation functions of generalized Boolean functions. These techniques are used effectively to arrive at his results, and a number of open problems are also put forward. This thesis builds upon and expands these techniques, and studies one of the central open problems in [32] in detail, and also presents a number of other results, which are now outlined.

A quadratic Boolean function is usefully represented as a graph, the edge between vertices i and j being present in the graph if the (order 2) term x_ix_j is present in the function. Performing the restriction operation on the function results in vertices in the graph being 'deleted', possibly leaving others disconnected, or 'isolated'. In [32] it is conjectured that an operation that deletes some vertices and leaves others isolated, for a certain class of functions, implies that the power of the sequences corresponding to the functions are limited by a specific upper bound. The only proof offered in [32] was for a special case resulting in a single isolated vertex. This conjecture is studied in detail in Chapters 2, 3 and 4. The conjecture is stated in Chapter 2, and by constructing 2 pairs of functions whose respective cross-correlation functions sum to zero everywhere apart from one shift, it is shown that not only is the conjecture true for some special cases resulting in 1 isolated vertex, but that it is also true for some special cases resulting in 2 isolated vertices. The cross-correlation result is also used to construct simple functions that have the 'near' Golay property in that their out-of-phase auto-correlations sum to zero except at one shift. In Chapter 3 pairs of functions are constructed which share the same auto-correlation function, and repeated application of this result for specific types of quadratic functions leads to a refinement of one of the key results in [32, 33], concerning complementary sets. This result in turn is then used to construct functions with any number of isolated vertices which in fact satisfy the bound of the conjecture. The ideas surrounding the existing lower bounds on power are extended, using the technique of restriction, to provide a new lower bound on power in Chapter 4. Some examples are then manufactured, all having 3 or more isolated vertices, for which this lower bound is greater than the upper bound on the power specified by the conjecture, thus showing that it cannot be true in the general case.

In Chapter 5, by manufacturing pairs of functions whose cross-correlations sum to zero at all shifts, new constructions for complementary sets of functions, derived from the complementary pairs of the Davis & Jedwab construction, are presented. This also results in a non-trivial construction of pairs of functions that share the same cross-correlation function. In Chapter 6 it is shown, somewhat surprisingly, that pairs from the construction over $\mathbb{Z}_2$, under the action of the inverse Gray map, remain as complementary pairs over $\mathbb{Z}_4$.

Conclusions and some thoughts on possible future work are presented at the end of the thesis.

The remainder of this chapter is devoted to a detailed exposition of all the background theory outlined above. In particular the properties and features of the technique of restriction are explored in greater depth than that given in [32, 33], where the technique was introduced. Basic definitions of the various rudimentary aspects of graph theory and coding theory that are used throughout the thesis are recalled where necessary (viz: edges, vertices, degree/valency, paths etc.—see for example [3]; Hamming weight, coset of a code etc.—see for example [21]).

Major references for this thesis are reports [32] (and its successor [33]) and [11]. Papers corresponding to these were submitted to the appropriate journal shortly after their publication, but it was not until the latter stages of preparation of the thesis that these finally appeared as [34] and[12].

1.2 General Notation

This section merely catalogues some notation conventions generally used throughout the thesis. More specialized notation will be established in subsequent sections as and when needed. An index of notation appears after the 'List of Figures' at the end of the preliminary section of the thesis.

A primitive q^{th} root of unity is denoted by ω, e.g. $\omega = e^{2\pi i/q}$.
Bold-faced lower case letters generally represent a $\mathbb{Z}_q$-valued vector, with its coordinates in normal type, e.g.

$$\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}), \quad a_i \in \mathbb{Z}_q, \quad i = 0, 1, \ldots, n-1.$$

Bold-faced upper case letters generally represent a complex-valued vector, e.g.

$$\mathbf{A} = (A_0, A_1, \ldots, A_{n-1}), \quad A_i \in \mathbb{C}, \quad i = 0, 1, \ldots, n-1,$$

where, in particular, $\mathbf{A}$ is the complex-valued equivalent of $\mathbf{a}$ when $A_i = \omega^{a_i}$, $i = 0, 1, \ldots, n-1$.
The complex conjugate of a complex-valued entity A is denoted as A^*, whilst that of an entire vector is

$$\mathbf{A}^* = (A_0^*, A_1^*, \ldots, A_{n-1}^*).$$

The reverse of vector $\mathbf{A}$ is denoted

$$\overline{\mathbf{A}} = (A_{n-1}, A_{n-2}, \ldots, A_0).$$

The '1's complement' of a binary word $\mathbf{c} = c_0 c_1 \cdots c_{k-1} \in \{0, 1\}^k$, i.e. the word with 0's for 1's and vice-versa, will be denoted by $\overline{\mathbf{c}}$, i.e. $\overline{\mathbf{c}} = \overline{c}_0 \overline{c}_1 \cdots \overline{c}_{k-1}$ where

$\overline{c}_i = 1 - c_i \, (\equiv 1 + c_i \mod 2)$ for all i.
For clarity in examples, rather than separate the coordinates of a vector with commas, they may simply be concatenated, e.g. (00110011) may be written instead of $(0, 0, 1, 1, 0, 0, 1, 1)$.
The convention of writing $+$ for 1 and $-$ for -1 may be adopted when writing a real-valued binary vector, i.e. $(1, -1, -1, 1)$ becomes $(+ - -+)$.

Where equations are labelled, they are numbered sequentially within each chapter as $(x.y)$, where x is the chapter number and y is the equation number; theorems, lemmas, corollaries and examples etc. are numbered similarly in a single sequence within each chapter. The end of a proof, definition, example etc. is denoted with a □.

1.3 The Aperiodic Correlation Functions and their Properties

This thesis makes much use of the discrete aperiodic cross- and auto-correlation functions: their definitions and properties are given in this section.

Let $\mathbf{A} = (A_0, A_1, \ldots, A_{n-1})$ and $\mathbf{B} = (B_0, B_1, \ldots, B_{n-1})$ be two length n complex-valued vectors, and let ℓ denote an integer. Then the aperiodic cross-correlation function of $\mathbf{A}$ and $\mathbf{B}$ is defined by:

$$C(\mathbf{A}, \mathbf{B})(\ell) = \begin{cases} \sum\limits_{i=0}^{n-1-\ell} A_i B^*_{i+\ell} & 0 \leqslant \ell < n \\ \sum\limits_{i=0}^{n-1+\ell} A_{i-\ell} B^*_i & -n < \ell < 0 \\ 0 & \text{otherwise.} \end{cases}$$

The complex conjugate of $C(\mathbf{A}, \mathbf{B})(\ell)$ will be written as $C^*(\mathbf{A}, \mathbf{B})(\ell)$.
Putting $\mathbf{B} = \mathbf{A}$, we obtain the aperiodic auto-correlation function of $\mathbf{A}$:

$$A(\mathbf{A})(\ell) = C(\mathbf{A}, \mathbf{A})(\ell).$$

Since $A(\mathbf{A})(-\ell) = A^*(\mathbf{A})(\ell)$ (see the following theorem) it is normal practice to only consider the auto-correlation for $\ell \geqslant 0$.

Swapping and/or reversing the vectors in a cross- or auto-correlation function results in a function that bears a simple relationship to the original. These very useful and well known results are gathered together for convenience in the following theorem:

Theorem 1.1. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be length* n *complex-valued vectors. Then for every integer* ℓ *in the range* $-n < \ell < n$ *we have:*

$$\begin{array}{rr} (i) & C(\mathbf{B}, \mathbf{A})(\ell) = C^*(\mathbf{A}, \mathbf{B})(-\ell) \\ (ii) & C(\overline{\mathbf{A}}, \overline{\mathbf{B}})(\ell) = C(\mathbf{A}, \mathbf{B})(-\ell) \\ (iii) & C(\overline{\mathbf{B}}, \overline{\mathbf{A}})(\ell) = C^*(\mathbf{A}, \mathbf{B})(\ell) \\ (iv) & A(\mathbf{A})(-\ell) = A^*(\mathbf{A})(\ell) \\ (v) & A(\overline{\mathbf{A}})(\ell) = A^*(\mathbf{A})(\ell). \end{array}$$

Proof. (i) For $0 \leqslant \ell < n$

$$C(\mathbf{B},\mathbf{A})(\ell) = \sum_{i=0}^{n-1-\ell} B_i A_{i+\ell}^* = \Big(\sum_{i=0}^{n-1+(-\ell)} A_{i-(-\ell)} B_i^* \Big)^* = C^*(\mathbf{A},\mathbf{B})(-\ell).$$

For $-n < \ell < 0$

$$C(\mathbf{B},\mathbf{A})(\ell) = \sum_{i=0}^{n-1+\ell} B_{i-\ell} A_i^* = \Big(\sum_{i=0}^{n-1-(-\ell)} A_i B_{i+(-\ell)}^* \Big)^* = C^*(\mathbf{A},\mathbf{B})(-\ell).$$

(ii) We have $\overline{A}_i = A_{n-1-i}$ and $\overline{B}_i = B_{n-1-i}$. Then for $0 \leqslant \ell < n$

$$C(\overline{\mathbf{A}},\overline{\mathbf{B}})(\ell) = \sum_{i=0}^{n-1-\ell} \overline{A}_i \overline{B}_{i+\ell}^* = \sum_{i=0}^{n-1-\ell} A_{n-1-i} B_{n-1-(i+\ell)}^*$$

and putting $j = n-1-i-\ell$

$$= \sum_{j=0}^{n-1-\ell} A_{j+\ell} B_j^* = \sum_{j=0}^{n-1+(-\ell)} A_{j-(-\ell)} B_j^* = C(\mathbf{A},\mathbf{B})(-\ell).$$

For $-n < \ell < 0$

$$C(\overline{\mathbf{A}},\overline{\mathbf{B}})(\ell) = \sum_{i=0}^{n-1+\ell} \overline{A}_{i-\ell} \overline{B}_i^* = \sum_{i=0}^{n-1+\ell} A_{n-1-(i-\ell)} B_{n-1-i}^*$$

and putting $j = n-1-i+\ell$

$$= \sum_{j=0}^{n-1+\ell} A_j B_{j-\ell}^* = \sum_{j=0}^{n-1-(-\ell)} A_j B_{j+(-\ell)}^* = C(\mathbf{A},\mathbf{B})(-\ell).$$

(iii)

$$\begin{aligned} C(\overline{\mathbf{B}},\overline{\mathbf{A}})(\ell) &= C^*(\overline{\mathbf{A}},\overline{\mathbf{B}})(-\ell) && \text{by (i)} \\ &= C^*(\mathbf{A},\mathbf{B})(\ell) && \text{by (ii)} \end{aligned}$$

(iv) put $\mathbf{B} = \mathbf{A}$ in (i).
(v) put $\mathbf{B} = \mathbf{A}$ in (iii). □

In addition these relationships are further simplified when both **A** and **B** are real-valued vectors, as any complex conjugation then disappears. In particular this is the case when **A** and **B** are both *binary* vectors, i.e. when there coordinates just take the values +1 or −1.

Generally throughout this thesis the coordinates A_i of the vector **A** will be derived from a $\mathbb{Z}_q$-valued vector **a**, i.e. $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, with $a_i \in \mathbb{Z}_q$ and $A_i = \omega^{a_i}$, $i = 0, 1, \ldots, n-1$, where $\omega = e^{2\pi i/q}$ is a primitive q^{th} root of unity.

There are two consequences of this with respect to the auto-correlation function for such vectors: firstly, at the zero shift we simply get

$$A(\mathbf{A})(0) = \sum_{i=0}^{n-1} \omega^{a_i}(\omega^{a_i})^* = \sum_{i=0}^{n-1} \omega^{a_i}\omega^{-a_i} = \sum_{i=0}^{n-1} 1 = n.$$

Secondly, more generally we have

$$\begin{aligned} |A(\mathbf{A})(\ell)| &= \left| \sum_{i=0}^{n-1-\ell} \omega^{a_i}\omega^{-a_{i+\ell}} \right| \\ &\leqslant \sum_{i=0}^{n-1-\ell} \left|\omega^{a_i}\omega^{-a_{i+\ell}}\right| \\ &= \sum_{i=0}^{n-1-\ell} \left|\omega^{a_i}\right|\left|\omega^{-a_{i+\ell}}\right| \\ &= \sum_{i=0}^{n-1-\ell} 1 \cdot 1 = n - \ell, \end{aligned}$$

so $|A(\mathbf{A})(\ell)| \leqslant n - \ell$ for $1 \leqslant \ell \leqslant n-1$.

1.4 Golay Complementary Sequences

The definition of Golay complementary sequences is now given:

Definition 1.2. A set of N length n complex-valued vectors $\{\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_{N-1}\}$ is said to be a *Golay complementary set* if

$$A(\mathbf{A}_0)(\ell) + A(\mathbf{A}_1)(\ell) + \cdots + A(\mathbf{A}_{N-1})(\ell) = 0, \quad \ell \neq 0.$$

A Golay complementary set of size 2 is called a *Golay complementary pair*, and any sequence in such a pair is called a *Golay complementary sequence*. This terminology is also applied to the $\mathbb{Z}_q$-valued vectors $\{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{N-1}\}$ if the $\mathbf{A}_j$ derive from them, that is if $\mathbf{A}_j = (A_{j,0}, A_{j,1}, \ldots, A_{j,n-1})$ and $\mathbf{a}_j = (a_{j,0}, a_{j,1}, \ldots, a_{j,n-1})$, $j = 0, 1, \ldots, N-1$, with $a_{j,i} \in \mathbb{Z}_q$ and $A_{j,i} = \omega^{a_{j,i}}$, $i = 0, 1, \ldots, n-1$, where $\omega = e^{2\pi i/q}$ is a primitive q^{th} root of unity. As noted above, in this case we have $A(\mathbf{A}_j)(0) = n$ for all j, and so the sum across the set at the zero shift is

$$A(\mathbf{A}_0)(0) + A(\mathbf{A}_1)(0) + \cdots + A(\mathbf{A}_{N-1})(0) = Nn.$$

□

Binary Golay complementary pairs were introduced by Golay in [18] as part of his work on infrared multislit spectrometry; complementary sets were introduced (independently) in [40, 46]. They have application in a diverse range of areas including radar, sonar, navigation etc.: a comprehensive survey of complementary pairs and sets may be found in [14].

1.5 Orthogonal Frequency Division Multiplexing

In this section a brief synopsis of those aspects of OFDM transmission that are relevant to this thesis are given (a detailed treatment being well beyond the scope of this thesis; for further detail see for example [4, 9]). OFDM is sometimes termed Multicarrier Modulation (MCM), or Discrete Multitone (DMT).

OFDM schemes allow for the simultaneous transmission of data on a number of sinusoidal waveforms, or *carriers*, of differing but equally spaced frequencies. The properties they exhibit make them suitable for transmission in multipath and fading channels, and they have been proposed for such uses as mobile land communications, digital audio broadcasting and high speed modems for HF radio [4]. The principal drawback of such schemes is that when the peaks (or troughs) of the sinusoidal carriers line up, so that they add most constructively, the peak signal may be many times the average. The equipment being used has to be able to handle the large peaks when they occur, which may be infrequently, and so for most of the time it may be operating at well below its maximum capacity, which is inefficient. Thus it is desirable to keep the ratio of the peak signal level to the average as low as possible.

Suppose that the data to be transmitted at some particular symbol rate is a codeword $(a_0, a_1, \dots, a_{n-1})$, $a_j \in \mathbb{Z}_q$, and the n carrier frequencies are $f_j = f_0 + jf_s$, $j = 0, 1, \dots, n-1$, where f_0 is the frequency of the first carrier, and f_s is the spacing of the frequencies and which is an integer multiple of the symbol rate. With $\omega = e^{2\pi i/q}$ a primitive q^{th} root of unity, write $A_j = \omega^{a_j}$, and $\mathbf{A} = (A_0, A_1, \dots, A_{n-1})$. Then the transmitted OFDM signal is the real part of the complex signal

$$S(\mathbf{A})(t) = \sum_{j=0}^{n-1} A_j e^{2\pi i(f_0 + jf_s)t}. \tag{1.1}$$

The data a_j determine the relative phases of the sinusoids, as is seen by simply expanding

$$\begin{aligned}\mathrm{Re}\big[A_j e^{2\pi i(f_0+jf_s)t}\big] &= \mathrm{Re}\big[e^{2\pi i a_j/q} e^{2\pi i(f_0+jf_s)t}\big] \\ &= \cos\big(2\pi(f_0 + jf_s)t + 2\pi a_j/q\big),\end{aligned}$$

so in the binary case for example, $q = 2$, $a_j \in \{0, 1\}$, and $2\pi a_j/q$ is simply 0 or π; thus the data merely gives '+' or '−' the cosine wave which is the j^{th} carrier. If $\mathbf{A}$ is the 'all one' vector, $(1, 1, \dots, 1)$, the signal can be seen to consist of cosine waves which are all in phase at time $t = 0$, i.e. all the peaks line up to give the maximum possible signal amplitude of n (and thus the signal from the all one vector has precisely the large peaks that we wish to avoid).

(From an engineering standpoint the transmitted signal is basically the inverse (discrete) Fourier transform of the data $\mathbf{A}$. In practice the data would generally have a length which is a power of 2 (as is the case throughout this thesis) which then allows for the use of Fast Fourier Transforms (FFTs). On receipt of the transmitted signal the reverse operation is performed, i.e. the Fourier transform is taken in order to obtain the data: this effectively 'picks out' each component of the (received) vector $\mathbf{A}$ in turn. This 'orthogonality' aspect, implying the frequencies necessarily be evenly spaced, is what gives this form of frequency division multiplexing its name.)

1.5.1 The power of an OFDM signal

It is the power of the signal $S(\mathbf{A})(t)$ in (1.1) that we are interested in, and that we would like to bound if at all possible. In signal and communications theory the instantaneous power of a signal, $u(t)$ say, is defined as $|u(t)|^2$ (see for example [43]), so over a symbol period such as $0 \leqslant t \leqslant 1/f_s$ for which the a_j are constant, we define the *instantaneous envelope power* of the signal to be

$$P(\mathbf{A})(t) = |S(\mathbf{A})(t)|^2 = S(\mathbf{A})(t)S^*(\mathbf{A})(t). \tag{1.2}$$

It is also possible to consider the power of the real part of the signal, $|\mathrm{Re}[S(\mathbf{A})(t)]|^2$, but since for any complex entity z, $\mathrm{Re}[z]^2 \leqslant |z|^2 = zz^*$, this will always be less than or equal to the envelope power, $P(\mathbf{A})(t)$, and so any upper bound on the envelope power is also an upper bound on the power of the real signal. The key reason for using the envelope power is that it can be expressed in terms of the auto-correlation function of $\mathbf{A}$, as is now shown, which can then be used to give an upper bound on the envelope power. (In some circumstances it is possible that the maximum power of the real signal is markedly less than the maximum of the envelope power—see [16] for more detail—but apart from illustrating the relationship of the signal power to the envelope power in an example to follow, the signal power is not considered further.)

Substitute (1.1) into (1.2) to obtain

$$\begin{aligned}
P(\mathbf{A})(t) &= \sum_{j=0}^{n-1} A_j e^{2\pi i(f_0+jf_s)t} \sum_{k=0}^{n-1} A_k^* e^{-2\pi i(f_0+kf_s)t} \\
&= \sum_{j,k} A_j A_k^* e^{2\pi i(j-k)f_s t} \\
&= \sum_{j=0}^{n-1} A_j A_j^* + \sum_{j<k} A_j A_k^* e^{2\pi i(j-k)f_s t} + \sum_{j>k} A_j A_k^* e^{2\pi i(j-k)f_s t} \\
&= A(\mathbf{A})(0) + \sum_{u=1}^{n-1} \sum_{j=0}^{n-1-u} A_j A_{j+u}^* e^{-2\pi i u f_s t} \\
&\qquad\qquad + \sum_{u=-1}^{1-n} \sum_{k=0}^{n-1+u} A_{k-u} A_k^* e^{-2\pi i u f_s t} \\
&= A(\mathbf{A})(0) + \sum_{u=1}^{n-1} A(\mathbf{A})(u) e^{-2\pi i u f_s t} + \sum_{u=-1}^{1-n} A(\mathbf{A})(u) e^{-2\pi i u f_s t} \\
&= A(\mathbf{A})(0) + \sum_{u=1}^{n-1} A(\mathbf{A})(u) e^{-2\pi i u f_s t} + \sum_{u=1}^{n-1} A^*(\mathbf{A})(u) e^{2\pi i u f_s t}
\end{aligned}$$

finally giving

$$P(\mathbf{A})(t) = n + 2\mathrm{Re}\sum_{u=1}^{n-1} A(\mathbf{A})(u)e^{-2\pi i u f_s t}, \tag{1.3}$$

where the auto-correlation function of $\mathbf{A}$, $A(\mathbf{A})(u)$, has been substituted at the relevant points. Several properties of the envelope power can now be noted. Firstly it is independent of the frequency of the first carrier, f_0, which has dropped out of the expression. (In any experimental computation it can thus be set to an arbitrary value, such as 1.) The expression represents how the envelope power might vary in practice with increasing t, and as $\mathbf{A}$ changes. We are interested in its form within the period $0 \leqslant t \leqslant 1/f_s$ for any particular $\mathbf{A}$, which, by definition, remains unchanged in this period. Re-scale the time-axis by putting $t' = f_s t$, and consider $P'(\mathbf{A})(t') = P(\mathbf{A})(t'/f_s)$. In the period $0 \leqslant t \leqslant 1/f_s$, $\mathbf{A}$ is constant, and so is also constant for $0 \leqslant t' \leqslant 1$, and the envelope power of P' in the period $0 \leqslant t' \leqslant 1$ will be identical to that of P in the period $0 \leqslant t \leqslant 1/f_s$. This has the effect of removing all considerations of the transmission frequencies upon the form of the envelope power—it depends solely on the vector $\mathbf{A}$. Thus we can effectively set $f_s = 1$ and consider the envelope power in the period $0 \leqslant t \leqslant 1$: *all further analysis and computation within this thesis assumes that this re-scaling has taken place*, i.e. that the envelope power is

$$P(\mathbf{A})(t) = n + 2\mathrm{Re}\sum_{u=1}^{n-1} A(\mathbf{A})(u)e^{-2\pi i u t}, \tag{1.4}$$

and that the symbol period is $0 \leqslant t \leqslant 1$.

Further, when $\mathbf{A}$ is a *binary* vector ($a_j \in \mathbb{Z}_2$, and so $A_j \in \{+1, -1\}$), the envelope power is symmetric about $t = \frac{1}{2}$. To see this, move the auto-correlation function outside of the 'Re' operator, since it is real in this case:

$$\begin{aligned} P(\mathbf{A})(t) &= n + 2\mathrm{Re}\left[\sum_{u=1}^{n-1} A(\mathbf{A})(u)e^{-2\pi i u t}\right] \\ &= n + 2\sum_{u=1}^{n-1} A(\mathbf{A})(u)\mathrm{Re}[e^{-2\pi i u t}] \\ &= n + 2\sum_{u=1}^{n-1} A(\mathbf{A})(u)\cos 2\pi u t. \end{aligned}$$

The functions $\cos 2\pi u t$ are even and periodic, of period 1. Any even periodic function of period T, say $f(t)$, is even about $T/2$: take any particular $t \leqslant T/2$, then $f(t) = f(-t)$ since f is even, and $f(-t) = f(T-t)$ since f is periodic, and so $f(t) = f(T-t)$. Put $t' = T/2-t$, then $f(T/2-t') = f(T+t'-T/2) = f(T/2+t')$, i.e. f is even about $T/2$. This property of the envelope power of binary vectors is clearly seen in the example plots.

Example 1.3. Consider first some binary examples of length 8. Figure 1.1 shows the signal and envelope power for $\mathbf{A} = (1, -1, 1, -1, 1, -1, 1, -1)$: note that around $t = 1/2$ the 'larger than average' excursions of the signal from zero produce a large peak in the envelope power. For comparison, plotted to the same scales, Figure 1.2 shows the signal and envelope power for $(1, -1, -1, 1, -1, 1, 1, 1)$: note the much more 'even' variations in the signal and the smaller and flatter envelope power that results. The symmetry of the envelope powers about $t = 1/2$ is also readily apparent.

Figure 1.3 shows the envelope power for a quaternary example, with vector $\mathbf{A} = (1, 1, -i, i, -1, i, i)$. To illustrate how the actual signal power $|\mathrm{Re}[S(\mathbf{A})(t)]|^2$ relates to the envelope power, it is shown dotted (calculated with $f_0 = 5$). Note that the envelope power is now no longer symmetric. □

1.5.2 The Peak-to-Mean Envelope Power Ratio (PMEPR)

We now introduce the measure of power of an OFDM signal that is to be used in this thesis. From (1.4) it is straightforward to see that the average of each of the terms in the summation, over the period $0 \leqslant t \leqslant 1$, is in fact zero, and so the *mean* envelope power of any vector $\mathbf{A}$ over this period is just n. The *peak envelope power* (PEP) of any vector $\mathbf{A}$ is defined to be the supremum of the instantaneous power over the period, i.e.

$$\sup_{0 \leqslant t \leqslant 1} P(\mathbf{A})(t).$$

Then the *peak-to-mean envelope power ratio* (PMEPR) of vector $\mathbf{A}$ is defined as the ratio PEP/n, i.e.

$$\frac{1}{n} \sup_{0 \leqslant t \leqslant 1} P(\mathbf{A})(t).$$

From (1.4) we have that

$$\begin{aligned}
P(\mathbf{A})(t) &= n + 2\mathrm{Re} \sum_{u=1}^{n-1} A(\mathbf{A})(u) e^{-2\pi i u t} \\
&\leqslant n + 2 \left| \sum_{u=1}^{n-1} A(\mathbf{A})(u) e^{-2\pi i u t} \right| \\
&\leqslant n + 2 \sum_{u=1}^{n-1} |A(\mathbf{A})(u) e^{-2\pi i u t}| \\
&\leqslant n + 2 \sum_{u=1}^{n-1} |A(\mathbf{A})(u)| \cdot 1 \\
&\leqslant n + 2 \sum_{u=1}^{n-1} (n-u) \\
&= n^2,
\end{aligned}$$

where the last inequality uses the fact that $|A(\mathbf{A})(u)| \leqslant n - u$ (from the comments after Theorem 1.1). So the PEP of any $\mathbf{A}$ is at most n^2, and the PMEPR at most n. This worst-case value of PMEPR is achieved by the 'all one' vector: it was pointed out earlier that it has maximum amplitude of n, so squaring gives

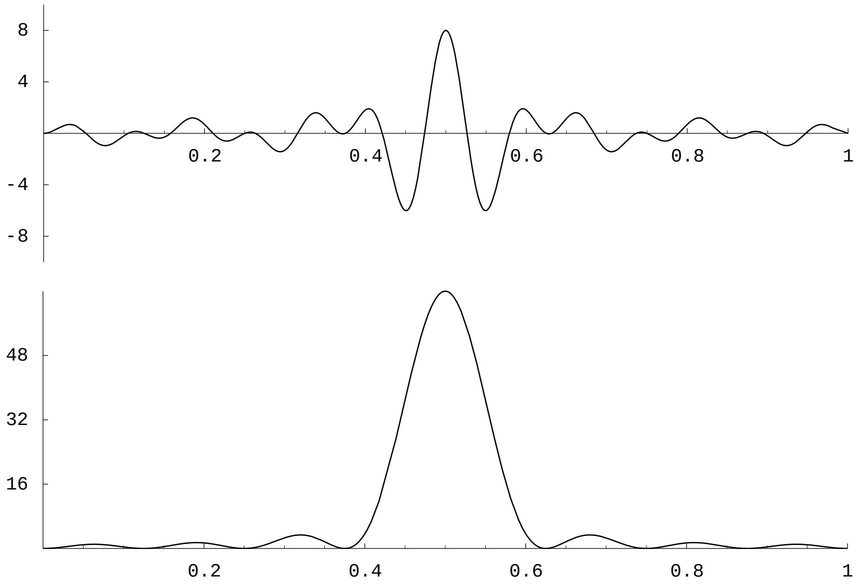

Figure 1.1: The signal (top) and envelope power for $(1, -1, 1, -1, 1, -1, 1, -1)$

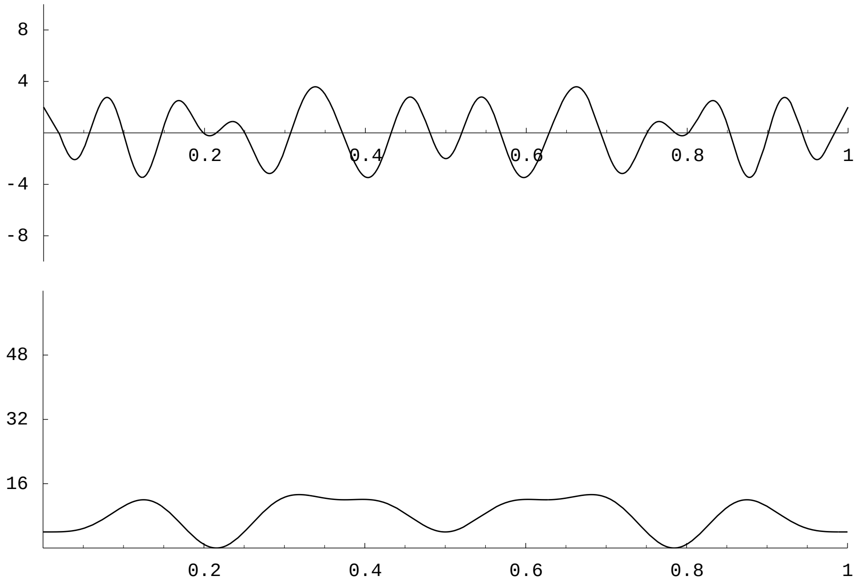

Figure 1.2: The signal (top) and envelope power for $(1, -1, -1, 1, -1, 1, 1, 1)$

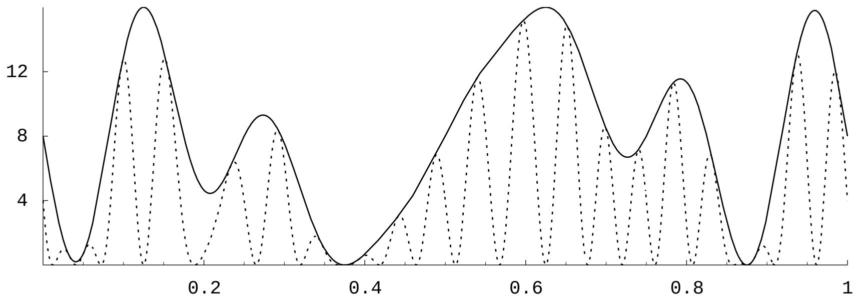

Figure 1.3: Envelope power and signal power (dotted) for $(1, 1, -i, i, -1, i, i)$

its PEP as n^2, and its PMEPR as n. As PMEPR is a ratio of powers it is frequently given in decibels, i.e. a PMEPR of R would be expressed as $10 \log_{10} R$ dB.

(There are a variety of other measures that are in use, and go under such names as 'peak-to-average power ratio', 'peak factor' and 'crest factor': due to the fact that it is possible to base such a measure on either the envelope power or the signal power, some of these are directly equivalent to PMEPR, others not, so care must be exercised when making a comparison. The crest factor, when defined on the envelope power, is the square root of PMEPR—the differences between defining for the signal and the envelope are examined in [16].)

1.5.3 Coding to avoid high peak power

One possible solution to the power control problem for OFDM is then to introduce some form of coding scheme: map the source data into some subset of all the words that could possibly be used for transmission, and only include those words in the subset which are known/can be demonstrated to have low peak power. Many methods have been devised for achieving something along these lines, including [37, 28, 39, 19, 5, 31, 36, 17, 22, 49, 15, 27, 29, 26, 23, 44, 16, 30]: some of these eliminate undesirable codewords by exhaustive search, others use numerical optimization algorithms on the initial phases of the carriers directly, and still others use some form of block coding. However, Popovic [36], who generalized the earlier work of Boyd [5], showed that the maximum PMEPR of a codeword that is a *Golay complementary sequence* is at most 2:

Theorem 1.4. *The PMEPR of any Golay complementary sequence is at most* 2.

Proof. Let $\mathbf{A}$ and $\mathbf{B}$ be a Golay complementary pair, so by definition $A(\mathbf{A})(u) + A(\mathbf{B})(u) = 0$ for any $u \neq 0$. Then the sum of their instantaneous envelope powers, from (1.4), is

$$\begin{aligned} P(\mathbf{A})(t) + P(\mathbf{B})(t) &= 2n + 2\mathrm{Re}\left(\sum_{u=1}^{n-1} A(\mathbf{A})(u)e^{-2\pi iut} + \sum_{u=1}^{n-1} A(\mathbf{B})(u)e^{-2\pi iut}\right) \\ &= 2n + 2\mathrm{Re}\sum_{u=1}^{n-1}\big(A(\mathbf{A})(u) + A(\mathbf{B})(u)\big)e^{-2\pi iut} \\ &= 2n. \end{aligned}$$

From (1.2) it is seen that the power of any vector is non-negative and real valued, hence the above sum implies

$$0 \leqslant P(\mathbf{A})(t) \leqslant 2n$$

and similarly for **B**. Thus the PEP of **A** is at most $2n$, and as PMEPR is PEP/n, then the PMEPR of **A** is at most 2. □

The above argument may be extended to a Golay complementary set. Suppose that the N vectors $\{\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_{N-1}\}$ are such a set. Then the sum of the powers equivalent to the above gives

$$\sum_{i=0}^{N-1} P(\mathbf{A}_i)(t) = Nn,$$

and so

$$0 \leqslant P(\mathbf{A}_i)(t) \leqslant Nn, \quad 0 \leqslant i \leqslant N-1.$$

Thus the instantaneous envelope power of an OFDM signal modulated by a Golay complementary sequence from a set of size N is at most Nn, and the PMEPR is at most N. We associate the PMEPR of the signal with the particular vector **A** concerned, and if vector **A** derives from some $\mathbb{Z}_q$-valued codeword **a**, i.e. if $A_i = \omega^{a_i}$ for all i, then we talk of the PMEPR of the codeword **a**. Thus if **a** is a Golay complementary sequence from a set of size N, it has a PMEPR of at most N.

Convention. The PMEPR of a particular vector **A** may be obtained from a plot of its envelope power by identifying the maximum power on the plot and dividing by the mean power, n. To be able to establish more readily that the PMEPR of **A** is above or below some value, it is convenient to scale envelope power by dividing by the mean power, and plotting this instead. Thus the PMEPR can be read off directly as the maximum value of the plot. This convention is adopted for all the remaining plots of envelope power in this thesis, and such plots will still be regarded as being plots of the envelope power.

Example 1.5. The auto-correlation vectors corresponding to the sequences $(1, 1, 1, -1, 1, 1, -1, 1)$ and $(1, 1, 1, -1, -1, -1, 1, -1)$ are (respectively)

$$\begin{array}{cccccccc} (8, & -1, & 0, & 3, & 0, & 1, & 0, & 1) \\ (8, & 1, & 0, & -3, & 0, & -1, & 0, & -1) \end{array}$$

and which clearly sum to zero at the non-zero shifts, and so the pair are a Golay complementary pair of sequences (in fact they are the first example given in

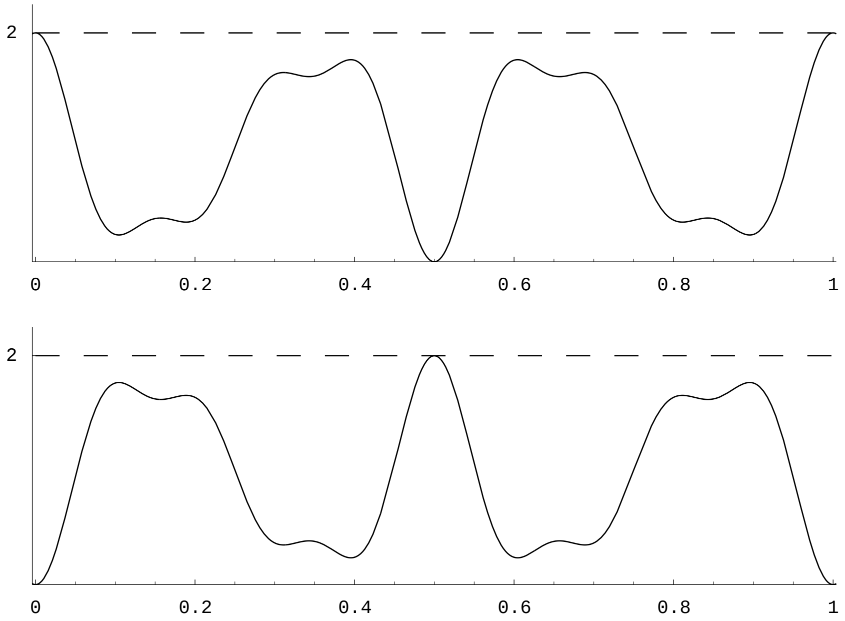

Figure 1.4: The envelope powers for complementary pair $(1, 1, 1, -1, 1, 1, -1, 1)$ (top) and $(1, 1, 1, -1, -1, -1, 1, -1)$

Golay's original paper, [18]). By the above, the PMEPRs of both sequences are thus at most 2, and Figure 1.4 shows that the envelope powers for both sequences are 2 or below everywhere. □

The utility of the above result with respect to practical OFDM schemes relies on the existence of a supply of complementary pairs and sets of sequences of various lengths. Until recently methods for constructing such pairs and sets have generally been of a recursive nature, and thus have not been seen as very practical (for example [6, 42, 46, 40]). This has changed however with the recent publication by Davis & Jedwab of [11], wherein they gave a deterministic method of constructing Golay complementary sequences of length 2^m over alphabets $\mathbb{Z}_{2^h}$, based on certain cosets of an appropriate generalization of the first-order Reed-Muller codes. Paterson then generalized some of their results in [32, 33], also giving a construction for polyphase Golay complementary sets. It is then possible to devise encoding and decoding schemes for OFDM use which utilize these complementary sequences (with their desirably low PMEPRs), along with the error-correcting capabilities of the Reed-Muller codes. A number of such coding schemes may be found in [11, 32, 33], along with an indication of how the schemes and constructions sit in relation to other recent, similar work (these not being a major concern of this thesis). The results from these papers which this thesis relies on are given in sections to follow: the functions, their properties, and the definitions of the codes on which the constructions of the sequences are based are given next; Paterson's generalization of the Davis & Jedwab construction for Golay complementary pairs then appears in Section 1.10, followed by his construction for complementary sets in Section 1.11.

1.6 Boolean and Generalized Boolean Functions

This section defines Boolean functions and their algebraic normal form representation, and their generalization. The definitions of the Reed-Muller codes, in a section to follow, are given in terms of such functions, and many of the techniques used and the results obtained in this thesis are based around the algebraic normal form representation of them. Very informally a Boolean function f is a function whose range is just 0 and 1. There are numerous ways in which to define such a function, depending on the context in which it is to be used: $f : V \to \mathbb{F}_2$, V an m-dimensional vector space over $\mathbb{F}_2$; $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ etc. The definition here follows the tenor of [7], drawing on [25, 2, 41], using the notation adopted in [32, 33].

Let the m variables $x_0, \ldots, x_{m-1}$ each take the values 0 or 1. The set of all binary m-tuples is then given by $\{0,1\}^m = \{(x_0, \ldots, x_{m-1}) : x_i \in \{0,1\}\}$. Let the binary expansion of the integer i be $(i_0, i_1, \ldots, i_{m-1})$, i.e. $i = \sum_{j=0}^{m-1} i_j 2^j$. Then a mapping f from the set of all binary m-tuples to $\mathbb{Z}_2$, $f : \{0,1\}^m \to \mathbb{Z}_2$, defined by a polynomial of the form

$$f(x_0, \ldots, x_{m-1}) = \sum_{i=0}^{2^m-1} c_i x_0^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}, \quad c_i \in \mathbb{Z}_2 \tag{1.5}$$

is a called a *Boolean function*, and this particular representation of a Boolean function is called *algebraic normal form.*

Each Boolean function can be identified with a length 2^m $\mathbb{Z}_2$-valued vector which is a list of its values at all points of $\{0,1\}^m$: denote this vector by $\mathbf{f} = (f_0, f_1, \ldots, f_{2^m-1})$, in which $f_i = f(i_0, i_1, \ldots, i_{m-1})$. There are 2^{2^m} such vectors $\mathbf{f}$, and so there are this many Boolean functions in m variables. Since $x_i^2 = x_i$, for all i, we can obtain *all* monomials in the x_i by forming the 2^m monomials

$$x_0^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}, \quad i_k = 0 \text{ or } 1, \quad k = 0, 1, \ldots m-1,$$

where we write 1 for the constant function $x_0^0 x_1^0 \cdots x_{m-1}^0$. We can thus form 2^{2^m} distinct linear combinations (over $\mathbb{Z}_2$) of these monomials, but this is precisely (1.5) in the definition given above. Thus every Boolean function has a unique representation in this form. The relationship between the values of a Boolean function f and its algebraic normal form is ([25, Theorem 1, p372] and [38]):

$$f(x_0, \ldots, x_{m-1}) = \sum_{i=0}^{2^m-1} g(i) x_0^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}},$$

with coefficients

$$g(i) = \sum_{j \subseteq i} f_j \mod 2,$$

where $j \subseteq i$ means the 1's in the binary expansion of j are a subset of the 1's in the binary expansion of i.

The *order* of a monomial $x_0^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}$ is $\sum_{j=0}^{m-1} i_j$: the non-zero constant term 1 is defined to have 0th order; linear terms are order 1 and quadratic terms are order 2. The order of the Boolean function f is defined to be the maximum order of its monomial terms having a non-zero coefficient.

We also associate a real-valued vector $\mathbf{F} = (F_0, F_1, \ldots, F_{2^m-1})$ with f, where $F_i = (-1)^{f_i}$, $i = 0, 1, \ldots, 2^m - 1$. Of course we may consider each x_i to be the Boolean function $f(x_0, \ldots, x_{m-1}) = x_i$, and we write its vector of values $\mathbf{x}_i$. For example, $\mathbf{x}_1 = (0, 0, 1, 1, 0, 0, 1, 1, \ldots, 0, 0, 1, 1)$. The constant 1, when considered as a Boolean function has vector $\mathbf{1} = (1, 1, \ldots, 1)$. Frequently we write $f(x)$, where it is understood that $x = (x_0, \ldots, x_{m-1})$.

A *generalized Boolean function*, $f : \{0,1\}^m \to \mathbb{Z}_q$, is defined in exactly the same way by (1.5), but where we now allow the c_i to be from $\mathbb{Z}_q$: there are thus q^{2^m} generalized Boolean functions in m variables; $\mathbf{f}$ then becomes a $\mathbb{Z}_q$-valued vector of length 2^m, and the coordinates of $\mathbf{F}$ are now $F_i = \omega^{f_i}$, $i = 0, 1, \ldots, 2^m - 1$, ω a primitive q^{th} root of unity, and so $\mathbf{F}$ is now complex-valued.

We thus work with three entities associated with a generalized Boolean function f: the algebraic normal form representation, the $\mathbb{Z}_q$-valued vector, and the complex-valued vector. In order to minimize confusion with notation yet to be defined, we eschew the normal convention of referring to all three as 'f' and endeavour to maintain some level of distinction between them. The $\mathbb{Z}_q$-valued vector will always be $\mathbf{f}$; the complex-valued vector will always be $\mathbf{F}$; however the algebraic normal form may be $f(x_0, \ldots, x_{m-1})$, $f(x)$ and often merely f.

Example 1.6. For $q = 2$ and $m = 4$, consider the following function, which is in algebraic normal form:

$$f(x_0, x_1, x_2, x_3) = x_0x_1 + x_1x_2 + x_1x_3 + x_0 + x_3.$$

The associated length 16 vector $\mathbf{f}$ of binary values and its real-valued counterpart $\mathbf{F}$ are:

$$\begin{aligned} \mathbf{f} &= (0100011110001011) \\ \mathbf{F} &= (+-+++----+++-+--). \end{aligned}$$

□

We are frequently interested in the algebraic normal form corresponding to a vector which is the *reverse* of the vector for some given function, i.e. given $f(x)$ and $\mathbf{f}$, what is $g(x)$ such that $\mathbf{g} = \overline{\mathbf{f}}$? Now

$$\mathbf{g} = (g_0, g_1, \ldots, g_{2^m-1}) = (f_{2^m-1}, f_{2^m-2}, \ldots, f_0),$$

so $g_i = f_{2^m-1-i}$, $i = 0, 1, \ldots, 2^m - 1$. From the above, the value of $f(x)$ at i is

$$f_i = f(i_0, i_1, \ldots, i_{m-1})$$

where $(i_0, i_1, \ldots, i_{m-1})$ is the binary expansion of i, i.e. $i = \sum_{j=0}^{m-1} i_j 2^j$. The binary expansion of $2^m - 1$ is just $\sum_{j=0}^{m-1} 2^j$, i.e. the all one vector $(1, 1, \ldots, 1)$. Thus the expansion of $2^m - 1 - i$ is $\sum_{j=0}^{m-1} 2^j - \sum_{j=0}^{m-1} i_j 2^j = \sum_{j=0}^{m-1} 2^j(1 - i_j)$, or as a vector, $(1 - i_0, 1 - i_1, \ldots, 1 - i_{m-1})$. So

$$g(i_0, \ldots, i_{m-1}) = g_i = f_{2^m-1-i} = f(1 - i_0, 1 - i_1, \ldots, 1 - i_{m-1}),$$

from which it is clear that

$$g(x_0, \ldots, x_{m-1}) = f(1 - x_0, 1 - x_1, \ldots, 1 - x_{m-1}).$$

Thus given the algebraic normal form for a function, to obtain the algebraic normal form for the function whose vector is the reverse of the given function, merely perform the substitution $x_i \rightarrow 1 - x_i, \quad i = 0, 1, \ldots, m-1$. This may be conveniently written in the abbreviated form $g(x) = f(1-x) \quad (\equiv f(1+x)$ when f is just a Boolean function, since in $\mathbb{Z}_2$, $+1 = -1$). Since the variables that a particular function is of are frequently implicitly assumed, i.e f is written rather than $f(x)$ or $f(x_0, \ldots, x_{m-1})$, the alternative notation $\overline{f}$ is often used to denote the reverse of f (and which of course has commonality with the reversed vector $\overline{\mathbf{f}}$).

Example 1.7. To find $g(x)$, the reverse of the function

$$f(x) = x_0x_1 + x_1x_2 + x_1x_3 + x_0 + x_3$$

used in Example 1.6, substitute $x_i \rightarrow 1 + x_i$ in $f(x)$:

$$\begin{aligned} g(x) &= f(1+x) \\ &= (1+x_0)(1+x_1) + (1+x_1)(1+x_2) \\ &\quad + (1+x_1)(1+x_3) + 1 + x_0 + 1 + x_3 \\ &= 1 + x_0 + x_1 + x_0x_1 + 1 + x_1 + x_2 + x_1x_2 \\ &\quad + 1 + x_1 + x_3 + x_1x_3 + x_0 + x_3 \\ &= 1 + x_0x_1 + x_1x_2 + x_1x_3 + x_1 + x_2. \end{aligned}$$

It is now straightforward to confirm that

$$\begin{aligned} \mathbf{g} &= (1101000111100010) \\ &= \overline{\mathbf{f}}. \end{aligned}$$

□

Of course, depending on the order of the function, such a substitution may be quite complicated. For linear functions such a reversal simply gives the function negated plus the sum of all the coefficients. For certain quadratic functions, this reversal is also particularly straightforward: *path* functions, to be introduced in the next section, are one such case in point, their reversal to be given in Lemma 1.9 of that section.

1.6.1 Correlations of generalized Boolean functions

One of the primary concerns of this thesis is the properties of the correlation functions of the complex-valued vectors associated with generalized Boolean functions. The correlation functions are necessarily actually computed from the complex-valued vectors; if we speak about the correlation function of the generalized Boolean function itself, then it is to be implied that we actually mean that of the vector. Suppose that f and g are two generalized Boolean functions over $\mathbb{Z}_q$, and that their associated complex-valued vectors are $\mathbf{F}$ and $\mathbf{G}$. Theorem 1.1 has already shown the relationships between the correlations of vectors $\mathbf{F}$ and $\mathbf{G}$ and their reverses, $\overline{\mathbf{F}}$ and $\overline{\mathbf{G}}$. There are also some other useful results pertaining to the addition of constants to one or both of the functions f and g, and these now follow.

Theorem 1.8. *Suppose that $f(x)$ and $g(x)$ are two generalized Boolean functions in m variables over $\mathbb{Z}_q$ with associated complex-valued length 2^m vectors $\mathbf{F}$ and $\mathbf{G}$. Let $f'(x) = f(x) + c$ and $g'(x) = g(x) + c$ for some arbitrary $c \in \mathbb{Z}_q$, with corresponding vectors $\mathbf{F}'$ and $\mathbf{G}'$. Let ω be a primitive q^{th} root of unity. Then for every integer ℓ in the range $-2^m < \ell < 2^m$ we have*

$$\begin{array}{llll} (i) & C(\mathbf{F}',\mathbf{G})(\ell) = C(\omega^c\mathbf{F},\mathbf{G})(\ell) & = \omega^c C(\mathbf{F},\mathbf{G})(\ell) \\ (ii) & C(\mathbf{F},\mathbf{G}')(\ell) = C(\mathbf{F},\omega^c\mathbf{G})(\ell) & = \omega^{-c} C(\mathbf{F},\mathbf{G})(\ell) \\ (iii) & C(\mathbf{F}',\mathbf{G}')(\ell) = C(\omega^c\mathbf{F},\omega^c\mathbf{G})(\ell) & = C(\mathbf{F},\mathbf{G})(\ell) \\ (iv) & A(\mathbf{F}')(\ell) = A(\omega^c\mathbf{F})(\ell) & = A(\mathbf{F})(\ell). \end{array}$$

Proof. (i) The coordinates of $\mathbf{F}'$ are

$$F_i' = \omega^{f_i'} = \omega^{(f+c)_i} = \omega^{f_i}\omega^c = \omega^c F_i, \quad i = 0, 1, \ldots, 2^m - 1,$$

and so in fact $\mathbf{F}' = \omega^c\mathbf{F}$, hence the first equality. Put $n = 2^m$ and consider the case $0 \leqslant \ell < n$:

$$\begin{aligned} C(\omega^c\mathbf{F},\mathbf{G})(\ell) &= \sum_{i=0}^{n-1-\ell} \omega^c F_i G_{i+\ell}^* \\ &= \omega^c \sum_{i=0}^{n-1-\ell} F_i G_{i+\ell}^* \\ &= \omega^c C(\mathbf{F},\mathbf{G})(\ell), \end{aligned}$$

and similarly for $-n < \ell < 0$, thus giving the second equality.
(ii) Similar to (i), but the constant c is negated due to the conjugation $(\omega^c G_{i+\ell})^* = \omega^{-c} G_{i+\ell}^*$ in the cross-correlation sum.
(iii) From (i) and (ii):

$$\begin{aligned} C(\mathbf{F}',\mathbf{G}')(\ell) &= C(\omega^c\mathbf{F},\omega^c\mathbf{G})(\ell) \\ &= \omega^c C(\mathbf{F},\omega^c\mathbf{G})(\ell) \\ &= \omega^c\omega^{-c} C(\mathbf{F},\mathbf{G})(\ell) \\ &= C(\mathbf{F},\mathbf{G})(\ell). \end{aligned}$$

(iv) put $\mathbf{G} = \mathbf{F}$ in (iii).

□

Note that in the particular case when $c = q/2$, q even (which includes the only interesting case for binary functions), we have that $\omega^c = \omega^{q/2} = -1$, so adding c to the function is equivalent to negating the complex-valued vector, and the above results become

$$\begin{array}{lr} (i) & C(-\mathbf{F},\mathbf{G})(\ell) = -C(\mathbf{F},\mathbf{G})(\ell) \\ (ii) & C(\mathbf{F},-\mathbf{G})(\ell) = -C(\mathbf{F},\mathbf{G})(\ell) \\ (iii) & C(-\mathbf{F},-\mathbf{G})(\ell) = C(\mathbf{F},\mathbf{G})(\ell) \\ (iv) & A(-\mathbf{F})(\ell) = A(\mathbf{F})(\ell), \end{array}$$

some of which are also usefully employed (sometimes in conjunction with the results of Theorem 1.1).

1.7 The Graph of a Quadratic Function and Paths

For a generalized Boolean function which is quadratic, i.e. whose algebraic normal form monomials are all order 2 or less, it is possible to associate a graph in a simple, natural and very useful way, as is now shown.

First we recall some basic definitions from graph theory. A *graph* $G = (V, E)$ consists of a finite non-empty set V of elements called *vertices* and a set E of unordered pairs of distinct elements of V called *edges*. Graphs have an intuitive pictorial representation with points for the vertices, and with a line joining two points whenever the corresponding pair of vertices is an edge. Vertices u and v are said to be *adjacent* if $\{u, v\}$ is an edge. The *degree* (or *valency*) of a vertex v in the graph is the number of edges of G which contain v. A vertex which is not joined to any other, i.e. for which the degree is zero, is called an *isolated* vertex. If each edge in a graph has some number associated with it, which is conveniently shown on a pictorial representation of the graph by labelling each edge with the corresponding number, then the graph is normally called a *weighted* graph. All graphs in this thesis are assumed to be of this type and so the distinction from an unweighted graph is not made. The graph with n vertices and an edge joining every pair of vertices is called the *complete graph on n vertices*, and is denoted by K_n.

So, let $Q : \{0,1\}^m \to \mathbb{Z}_q$ be the generalized Boolean function defined by

$$Q(x_0, \ldots, x_{m-1}) = \sum_{0 \leqslant i < j \leqslant m-1} q_{ij} x_i x_j, \quad q_{ij} \in \mathbb{Z}_q,$$

so that Q is a quadratic form in m variables over $\mathbb{Z}_q$. The graph associated with Q, $G(Q)$, is formed from m vertices labelled $0, 1, \ldots, m-1$, with edges between vertices i and j, labelled with q_{ij}, for all $q_{ij} \neq 0$ (i.e. for all order two monomials $q_{ij} x_i x_j$ with non-zero coefficient in the algebraic normal form of Q, there is an edge in $G(Q)$ labelled with the coefficient q_{ij}). Of course, from any graph G of this type we can construct an equivalent quadratic form, Q. If f is any quadratic generalized Boolean function, $f : \{0,1\}^m \to \mathbb{Z}_q$, the graph $G(f)$ is defined to be the graph $G(Q)$ where Q is just the quadratic part of f. For the binary case, $q = 2$, all edges in the graph would be labelled by 1, so we omit the labels and take them as read.

This thesis is concerned with functions which have a particular type of graph. When q is *even*, a graph is defined to be a *path* if all its edges are labelled with

$\frac{q}{2}$, and we may start at some vertex and traverse all edges in the graph, from vertex to vertex, such that each vertex is visited only once. Thus a path on the m vertices $\{0, 1, \ldots, m-1\}$, for $m \geqslant 2$, has exactly 2 vertices of degree 1, which we call *end points*, and $m-2$ vertices of degree 2. When $m = 1$, we get a *trivial path* which contains a single vertex and no edges. It is seen that the set of all such paths, for $m \geqslant 2$, corresponds to the set of quadratic forms of the type:

$$\frac{q}{2} \sum_{\alpha=0}^{m-2} x_{\pi(\alpha)} x_{\pi(\alpha+1)},$$

where π is a permutation of $\{0, 1, \ldots, m-1\}$, and where the end points are $\pi(0)$ and $\pi(m-1)$. It is also convenient to refer to functions of this type as paths, and to also refer to the variables $x_{\pi(0)}$ and $x_{\pi(m-1)}$ as end points of the path. For $m = 1$, a trivial path corresponds to any linear term, px_0, $p \in \mathbb{Z}_q$: in this case both 'end points' are equal to the single vertex, i.e. $\pi(0) = \pi(m-1) = 0$. The *length* of a path is defined to be the number of edges in it, viz $m-1$.

A useful property of such path functions is that the algebraic normal form of their reverse is particularly simple to establish, as given by the following lemma:

Lemma 1.9. *Let P, a quadratic generalized Boolean function over $\mathbb{Z}_q$, q even, be*

$$P(x_0, \ldots, x_{m-1}) = \frac{q}{2} \sum_{\alpha=0}^{k-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}},$$

where the x_{i_j}, $j = 0, 1, \ldots, k-1$ are a k-subset of the m variables $x_0, \ldots, x_{m-1}$, $2 \leqslant k \leqslant m$, $0 \leqslant i_0 < i_1 < \cdots < i_{k-1} \leqslant m-1$, and where π is a permutation of $\{0, 1, \ldots, k-1\}$. Then the algebraic normal form of the function whose vector is the reverse of that of P is

$$P + \frac{q}{2}\left(x_{i_{\pi(0)}} + x_{i_{\pi(k-1)}}\right) + \left(\frac{q}{2}(k-1) \mod q\right).$$

Proof. Let the required function be $\overline{P}$. Then from the previous section

$$\begin{aligned}
\overline{P}(x) &= P(1-x) \\
&= \frac{q}{2} \sum_{\alpha=0}^{k-2} (1 - x_{i_{\pi(\alpha)}})(1 - x_{i_{\pi(\alpha+1)}}) \\
&= \frac{q}{2} \sum_{\alpha=0}^{k-2} (1 - x_{i_{\pi(\alpha)}} - x_{i_{\pi(\alpha+1)}} + x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}}) \\
&= \frac{q}{2}(k-1) - \frac{q}{2} x_{i_{\pi(0)}} - q \sum_{\alpha=1}^{k-2} x_{i_{\pi(\alpha)}} - \frac{q}{2} x_{i_{\pi(k-1)}} + \frac{q}{2} \sum_{\alpha=0}^{k-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} \\
&= \frac{q}{2}(k-1) + \frac{q}{2} x_{i_{\pi(0)}} + \frac{q}{2} x_{i_{\pi(k-1)}} + \frac{q}{2} \sum_{\alpha=0}^{k-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} \\
&= P + \frac{q}{2}\left(x_{i_{\pi(0)}} + x_{i_{\pi(k-1)}}\right) + \left(\frac{q}{2}(k-1) \mod q\right),
\end{aligned}$$

since the term $-\frac{q}{2} x_{i_{\pi(j)}}$ from index j in the sum, $1 \leqslant j \leqslant k-2$, combines with $-\frac{q}{2} x_{i_{\pi(j-1+1)}}$ from index $j-1$ to give $-q x_{i_{\pi(j)}} = 0$, and we have also used that since q is even, $-\frac{q}{2} = \frac{q}{2} \mod q$. □

1.8 Reed-Muller Codes and their Generalization

The subject matter of this thesis is not concerned with coding theory *per se*; however it does involve particular cosets of certain generalizations of Reed-Muller codes. This section recalls some basic definitions from coding theory and defines the necessary codes, in terms of generalized Boolean functions described above.

For $q \geqslant 2$, a linear code of length n over $\mathbb{Z}_q$ is defined to be a subset of $\mathbb{Z}_q^n$ such that the sum of any two codewords is also a codeword. Any such code $\mathcal{C}$ can be specified in terms of a generator matrix, such that $\mathcal{C}$ consists of all distinct linear combinations over $\mathbb{Z}_q$ of the rows of the matrix: we say that the rows *generate* the code. For some fixed, length n vector, $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$, over $\mathbb{Z}_q$, the set of the form $\mathbf{a} + \mathcal{C}$ is called a *coset* of the code $\mathcal{C}$, and $\mathbf{a}$ is called the *coset representative* of the coset. The *Hamming weight* of any vector $\mathbf{a}$, denoted $wt_H(\mathbf{a})$, is defined as the number of non-zero a_i, $i = 0, 1, \dots, n-1$. We are frequently interested in the Hamming weight of the vector $\mathbf{f}$ associated with a generalized Boolean function $f(x)$, and so may talk of the Hamming weight *of the function*, this being taken to mean the the weight of the vector, and we may also write $wt_H(f)$.

The following definition generalizes the classical Reed-Muller codes from the binary to the q-ary case. It is from [32, 33], which generalized the 2^h-ary codes of [11], and which were in turn a generalization of the classical binary codes.

Definition 1.10. For $q \geqslant 2$ and $0 \leqslant r \leqslant m$, $RM_q(r, m)$ is defined to be the linear code over $\mathbb{Z}_q$ that is generated by the $\mathbb{Z}_q$-valued vectors corresponding to the monomials in $x_0, \dots, x_{m-1}$ of degree at most r. Alternatively, $RM_q(r, m)$ is the linear code over $\mathbb{Z}_q$ whose generator matrix is formally identical to that of the binary code $RM(r, m)$ but which is interpreted to be over $\mathbb{Z}_q$. □

For $r \geqslant 2$, $RM_q(r, m)$ is a union of cosets of $RM_q(1, m)$; when $r = 2$, the coset representatives may be taken to be quadratic forms in m variables.

Example 1.11. The code $RM_4(2, 3)$ is the linear code over $\mathbb{Z}_4$ generated by the vectors corresponding to the monomials of degree at most 2 in the variables x_0, x_1 and x_2. Its generator matrix, with rows given by the monomials as shown, is:

$$\begin{array}{cc} \begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \\ 00010001 \\ 00000101 \\ 00000011 \end{bmatrix} & \begin{array}{c} 1 \\ x_0 \\ x_1 \\ x_2 \\ x_0x_1 \\ x_0x_2 \\ x_1x_2 \end{array} \end{array}$$

This matrix is thus as that for the standard binary Reed-Muller code, $RM(2, 3)$, but since linear combinations of its rows are taken over $\mathbb{Z}_4$, the code contains codewords such as $3x_0x_2 + 2x_1 \equiv 00220321$. □

It should be noted that these codes are distinct from: the Generalized Reed-Muller code $GRM(r, m)$ [2], which are defined over a field; the quaternary Reed-Muller code $QRM(r, m)$, which generalizes the quaternary representation of the

Kerdock code [48]; and the code $ZRM_q(r,m)$, a subcode of $RM_q(r,m)$ [48], but also further generalized in [11, 32, 33].

Having defined the weight of a vector, the following simple result which gives the weights of particular kinds of Boolean functions is very useful:

Lemma 1.12. *[25, 'The randomisation lemma', p372] Let $g(x_0,\ldots,x_{m-2})$ be an arbitrary Boolean function in the $m-1$ variables $x_0,\ldots,x_{m-2}$. Then the function*

$$f(x_0,\ldots,x_{m-1}) = x_{m-1} + g(x_0,\ldots,x_{m-2})$$

takes the values 0 and 1 equally often, i.e. the weight of the vector $\mathbf{f}$ *is* 2^{m-1}.

Proof. Suppose that g takes the value 0 on θ occasions and 1 on ϕ occasions when it is evaluated over all its inputs, thus $\theta+\phi = 2^{m-1}$. When $x_{m-1}=0$, f will be 0 on θ occasions and 1 on ϕ occasions. When $x_{m-1}=1$, f will be 0 on ϕ occasions and 1 on θ occasions. Thus f is 0 on $\theta+\phi = 2^{m-1}$ occasions and 1 on $\phi+\theta = 2^{m-1}$ occasions. □

In particular this means that all (non-zero) linear Boolean functions are 'balanced' or 'half-weight', i.e. their vectors have weight 2^{m-1}, being half the length of the vector.

1.9 The Restriction of Generalized Boolean Functions and their Vectors

This section establishes the technique of *restriction*, as introduced in [32, 33]. This technique is pivotal in obtaining the results in those papers, and also in this thesis.

Definition 1.13. Let $f:\{0,1\}^m \to \mathbb{Z}_q$ be a generalized Boolean function in the m variables $x_0,\ldots,x_{m-1}$, with associated complex-valued vector $\mathbf{F}$. Let $0 \leqslant j_0 < j_1 \cdots < j_{k-1} \leqslant m-1$ be a list of $k \geqslant 0$ indices, and write $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$. Let $\mathbf{c} = c_0c_1\cdots c_{k-1}$ be a binary word of length k, and let the binary expansion of i be $(i_0,i_1,\ldots,i_{m-1})$, i.e. $i=\sum_{j=0}^{m-1} i_j 2^j$. Then the *restricted vector* $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ is a complex-valued vector with components $(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i$, $i=0,1,\ldots,2^m-1$, defined by

$$(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i = \begin{cases} \omega^{f(i_0,i_1,\ldots,i_{m-1})} & \text{if } i_{j_\alpha} = c_\alpha, \quad 0 \leqslant \alpha \leqslant k-1 \\ 0 & \text{otherwise.} \end{cases}$$

□

Thus component i of $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ is equal to F_i (the i^{th} component of $\mathbf{F}$) when all the coordinates in the binary expansion of i given by the indices j_α are equal to the digits in $\mathbf{c}$, and is zero otherwise. In the special case $k=0$, $\mathbf{x}$ and $\mathbf{c}$ are null, and we simply define $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ to be equal to $\mathbf{F}$. We call $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$ the *restricting variables*, and the j_α, $\alpha = 0,1\ldots,k-1$ the *restricting indices.*

For any given k restricting variables $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$, let the set of restricting indices be denoted by J, i.e.

$$J = \{j_0, j_1, \ldots, j_{k-1}\}.$$

(This could be written $J_{\mathbf{x}}$ to show the dependence on $\mathbf{x}$, but within any given context, $\mathbf{x}$ is generally fixed, so it is omitted for simplicity's sake.) If i has binary expansion $(i_0, i_1, \ldots, i_{m-1})$, then i is the index of a non-zero entry in a restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, where $\mathbf{c} = c_0c_1\cdots c_{k-1}$, if

$$i = \sum_{j=0}^{m-1} i_j 2^j \text{ where } \begin{cases} i_j = c_\alpha & j = j_\alpha \in J \\ i_j = 0 \text{ or } 1 & j \notin J. \end{cases}$$

For a particular $\mathbf{c}$, denote the set of all such indices as $I_{\mathbf{c}}$, which can be written as

$$I_{\mathbf{c}} = \{i : i = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j\notin J} i_j 2^j, \quad i_j = 0 \text{ or } 1\}. \tag{1.6}$$

(Again, the strict dependence on $\mathbf{x}$ is omitted.) Since there are $m-k$ indices j not in J, and a choice of 0 or 1 for each associated i_j, clearly $|I_{\mathbf{c}}| = 2^{m-k}$, i.e. there are 2^{m-k} non-zero entries in a restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$. Also, for $\mathbf{c}_1 \neq \mathbf{c}_2$, it is clear that $I_{\mathbf{c}_1} \cap I_{\mathbf{c}_2} = \varnothing$, and so the $I_{\mathbf{c}}$, across all possible $\mathbf{c}$ for a given $\mathbf{x}$, partition the set $\{0, 1, \ldots, 2^m - 1\}$, giving the simple consequence that

$$\mathbf{F} = \sum_{\mathbf{c}} \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}. \tag{1.7}$$

Depicting $f(i_0, \ldots, i_{m-1})$ as f_i, the value of f at i, the definition of the components in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ may be written

$$(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i = \begin{cases} \omega^{f_i} & i \in I_{\mathbf{c}} \\ 0 & i \notin I_{\mathbf{c}}. \end{cases}$$

The values of f_i for i in $I_{\mathbf{c}}$ can also be obtained by substituting $x_{i_\alpha} = c_\alpha$, for $\alpha = 0, 1, \ldots, k-1$, into the algebraic normal form $f(x)$, and simplifying to obtain a generalized Boolean function in $m-k$ variables, which we denote by $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ (and sometimes just $f\big|_{\mathbf{x}=\mathbf{c}}$). (Note the distinction between the argument x of f, and $\mathbf{x}$, which denotes the restricting variables.) Evaluating $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ over its domain clearly yields the values f_i which establish the restricted vector. This representation is used extensively for manipulating functions and their restrictions in the sequel, but care must be exercised in distinguishing between them:

$\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ is a length 2^m complex-valued vector, incorporating $2^m - 2^{m-k}$ zeroes and 2^{m-k} non-zeroes;

$f(x)\big|_{\mathbf{x}=\mathbf{c}}$ is a $\mathbb{Z}_q$-valued function taking the 2^{m-k} values which define $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$.

Note we use no concept of restricting vector $\mathbf{f}$, the length 2^m vector of values of f.

As a functional analogue to (1.7) above, we can combine all the $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ to re-generate the original function f:

$$f(x) = \sum_{\mathbf{c}} f(x)\big|_{\mathbf{x}=\mathbf{c}} \prod_{c_\alpha=1} x_{j_\alpha} \prod_{c_\alpha=0} (1 - x_{j_\alpha}).$$

(Note that an expression so derived will, in general, not be in algebraic normal form. In fact this representation is very similar to *disjunctive* normal form—see [25, p372].)

Example 1.14. Continuing with the function in Example 1.6:

$$f(x) = x_0x_1 + x_1x_2 + x_1x_3 + x_0 + x_3,$$

restrict with $\mathbf{x} = x_0x_2$ over all four possible values of $\mathbf{c} = c_0c_1$ to get:

$$\begin{aligned}
\mathbf{F}\big|_{x_0x_2=00} &= (+\,0+0\,0\,0\,0\,0-0+0\,0\,0\,0\,0\,) \\
\mathbf{F}\big|_{x_0x_2=10} &= (\,0-0+0\,0\,0\,0\,0+0+0\,0\,0\,0\,) \\
\mathbf{F}\big|_{x_0x_2=01} &= (\,0\,0\,0\,0+0-0\,0\,0\,0\,0-0-0\,) \\
\mathbf{F}\big|_{x_0x_2=11} &= (\,0\,0\,0\,0\,0-0-0\,0\,0\,0\,0+0-) \\
\mathbf{F} &= (+-+++----+++-+--)
\end{aligned}$$

Note that summing down the columns recovers the original vector (equation (1.7)). Substitute $x_0 = c_0$ and $x_2 = c_1$ into $f(x)$ for the four values of $\mathbf{c}$ to get the restricted functions:

$$\begin{aligned}
f(x)\big|_{x_0x_2=00} &= x_1x_3 + x_3 \\
f(x)\big|_{x_0x_2=10} &= x_1 + x_1x_3 + 1 + x_3 \\
f(x)\big|_{x_0x_2=01} &= x_1 + x_1x_3 + x_3 \\
f(x)\big|_{x_0x_2=11} &= x_1x_3 + 1 + x_3.
\end{aligned}$$

It is straightforward to check that

$$\begin{aligned}
f(x)\big|_{x_0x_2=00} \cdot (1-x_0)(1-x_2) &+ f(x)\big|_{x_0x_2=10} \cdot x_0(1-x_2) \\
&+ f(x)\big|_{x_0x_2=01} \cdot (1-x_0)x_2 + f(x)\big|_{x_0x_2=11} \cdot x_0x_2,
\end{aligned}$$

after some manipulation, yields the function $f(x)$. □

It is simple to see from the definition of restriction that the conjugate of a restricted vector is the same as the restriction of the conjugated vector, i.e.

$$\left(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}\right)^* = \mathbf{F}\big|^*_{\mathbf{x}=\mathbf{c}} = \mathbf{F}^*\big|_{\mathbf{x}=\mathbf{c}}.$$

Another simple and important consequence of the definition of restriction is the following. Suppose that the restricted functions $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ and $f'(x)\big|_{\mathbf{x}=\mathbf{c}}$, equivalent to the restricted vectors $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ and $\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}}$, for some particular $\mathbf{x}$ and $\mathbf{c}$, are related by

$$f'(x)\big|_{\mathbf{x}=\mathbf{c}} = f(x)\big|_{\mathbf{x}=\mathbf{c}} + g,$$

where g is an element of $\mathbb{Z}_q$. Then clearly each non-zero entry in $\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}}$ is just ω^g times the corresponding entry in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, i.e. we can write

$$\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}} = \omega^g \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}},$$

and hence from Theorem 1.8 we get that

$$A(\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}})(\ell) = A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) \quad \text{for all } \ell.$$

It is straightforward to see that all the results of Theorem 1.8 apply to restricted vectors in a similar fashion, and these results are used repeatedly in the sequel.

1.9.1 Expanding correlations using restricted vectors

The following two useful results show how auto- and cross-correlations of length 2^m vectors may be expanded in terms of their restricted vectors. They are a slight re-working of Lemmas 7 and 8 of [32, 33], given here with proofs. Let J and L be two disjoint subsets of the set $\{0, 1, \ldots, m-1\}$, of sizes k and k' respectively, i.e.

$$\begin{aligned} J &= \{j_0, j_1, \ldots, j_{k-1}\} \quad \text{where} \quad 0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1, \\ L &= \{l_0, l_1, \ldots, l_{k'-1}\} \quad \text{where} \quad 0 \leqslant l_0 < l_1 < \cdots < l_{k'-1} \leqslant m-1, \\ J \cap L &= \varnothing. \end{aligned}$$

Then we say the restricting variables $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$ and $\mathbf{x}' = x_{l_0}x_{l_1}\cdots x_{l_{k'-1}}$ are also disjoint, and we write $\mathbf{x}\mathbf{x}'$ to represent the restricting variables $x_{j_0}\cdots x_{j_{k-1}}x_{l_0}\cdots x_{l_{k'-1}}$. Similarly if $\mathbf{c} = c_0c_1\cdots c_{k-1}$ and $\mathbf{c}' = c'_0c'_1\cdots c'_{k'-1}$ are two binary words we write $\mathbf{c}\mathbf{c}'$ for the binary word $c_0\cdots c_{k-1}c'_0\cdots c'_{k'-1}$.

Lemma 1.15. *Let f and g be two generalized Boolean functions in m variables over $\mathbb{Z}_q$, and let $\mathbf{x}$ and $\mathbf{x}'$ be disjoint restricting variables as above. Then for all integers ℓ and all binary words $\mathbf{c}$ and $\mathbf{d}$ of length k,*

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})(\ell) = \sum_{\mathbf{c}'_1}\sum_{\mathbf{c}'_2} C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_1}, \mathbf{G}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}'_2})(\ell).$$

Proof. We need only consider ℓ in the range $-2^m < \ell < 2^m$, since otherwise from the definition of cross-correlation both sides of the expression are 0. The proof is by induction on the number of variables k' in $\mathbf{x}'$. When $\mathbf{x}'$ is null, then both $\mathbf{c}'_1$ and $\mathbf{c}'_2$ are null and the result is trivial. For the base case of the induction, when $k' = 1$ and $\mathbf{x}' = x_{l_0}$ is a single variable, we want to show

$$\begin{aligned} C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})(\ell) \\ &= C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}0}, \mathbf{G}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}0})(\ell) + C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}0}, \mathbf{G}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}1})(\ell) \\ &\quad + C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}1}, \mathbf{G}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}0})(\ell) + C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}1}, \mathbf{G}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}1})(\ell). \end{aligned}$$

From equation (1.7) we have

$$\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}} = \mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}0} + \mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}1},$$

so write the coordinates of the restricted vectors on the right side of this expression as $(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}0})_i = F_i^\circ$ and $(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}1})_i = F_i^\bullet$, so that

$$(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i = F_i^\circ + F_i^\bullet$$

and only one of F_i° and $F_i^\bullet$ can be non-zero, for $i = 0, 1, \ldots, 2^m - 1$. Notate for $\mathbf{G}$ similarly. Then for $0 \leqslant \ell < 2^m$, from the definition of cross-correlation,

$$\begin{aligned}
C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})(\ell) &= \sum_{i=0}^{n-1-\ell} (\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i (\mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})^*_{i+\ell} \\
&= \sum_{i=0}^{n-1-\ell} (F_i^\circ + F_i^\bullet)(G_{i+\ell}^{\circ *} + G_{i+\ell}^{\bullet *}) \\
&= \sum_{i=0}^{n-1-\ell} (F_i^\circ G_{i+\ell}^{\circ *} + F_i^\circ G_{i+\ell}^{\bullet *} + F_i^\bullet G_{i+\ell}^{\circ *} + F_i^\bullet G_{i+\ell}^{\bullet *}) \\
&= C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}0}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{d}0})(\ell) + C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}0}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{d}1})(\ell) \\
&\quad + C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}1}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{d}0})(\ell) + C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{c}1}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{d}1})(\ell)
\end{aligned}$$

as desired. The argument for $-2^m < \ell < 0$ is similar. Now suppose the result is true for $k' > 1$ variables in $\mathbf{x}'$, i.e. that

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})(\ell) = \sum_{\mathbf{c}_1'} \sum_{\mathbf{c}_2'} C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}_1'}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{dc}_2'})(\ell).$$

For some new index $l \notin J, L$, we can expand the cross-correlation in the sum on the right-hand side about the new restricting variable x_l, in the same manner as for the base case, giving

$$\begin{aligned}
C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}})(\ell) &= \sum_{\mathbf{c}_1'} \sum_{\mathbf{c}_2'} C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}_1'}, \mathbf{G}\big|_{\mathbf{xx}'=\mathbf{dc}_2'})(\ell) \\
&= \sum_{\mathbf{c}_1'} \sum_{\mathbf{c}_2'} \big(C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'0}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'0})(\ell) + \\
&\qquad\qquad C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'0}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'1})(\ell) + \\
&\qquad\qquad C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'1}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'0})(\ell) + \\
&\qquad\qquad C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'1}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'1})(\ell) \big) \\
&= \sum_{\mathbf{c}_1'} \sum_{\mathbf{c}_2'} \sum_{a} \sum_{b} C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'a}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'b})(\ell) \\
&= \sum_{\mathbf{c}_1'} \sum_{a} \sum_{\mathbf{c}_2'} \sum_{b} C(\mathbf{F}\big|_{\mathbf{xx}'x_l=\mathbf{cc}_1'a}, \mathbf{G}\big|_{\mathbf{xx}'x_l=\mathbf{dc}_2'b})(\ell) \\
&\qquad\qquad\qquad\qquad \text{(on rearranging the sum)} \\
&= \sum_{\mathbf{c}_1''} \sum_{\mathbf{c}_2''} C(\mathbf{F}\big|_{\mathbf{xx}''=\mathbf{cc}_1''}, \mathbf{G}\big|_{\mathbf{xx}''=\mathbf{dc}_2''})(\ell),
\end{aligned}$$

where $\mathbf{x}'' = \mathbf{x}' x_l$ are the $k'+1$ restricting variables $x_{l_0} \cdots x_{l_{k'-1}} x_l$, and $\mathbf{c}_1'' = \mathbf{c}'a$ and $\mathbf{c}_2'' = \mathbf{c}_1' b$ are binary words of length $k'+1$. Thus if the result is true for k' it is true for $k'+1$, and so by induction it is true for all integers $1 \leqslant k' \leqslant m-k$. $\square$

The equivalent result for the expansion of an auto-correlation function is a simple corollary to this:

Corollary 1.16.

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = \sum_{\mathbf{c}'} A(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})(\ell) + \sum_{\mathbf{c}'_1 \neq \mathbf{c}'_2} C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_1}, \mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_2})(\ell).$$

Proof. In the Lemma, put $f = g$ and $\mathbf{c} = \mathbf{d}$ (and so $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}} = \mathbf{G}\big|_{\mathbf{x}=\mathbf{d}}$ etc.). □

1.9.2 The pattern of non-zero entries in a restricted vector

In this section we make some rudimentary observations about the position and pattern of the non-zero entries within a restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$: these are then used in the three immediately following sections to set up some new notation and terms to be used throughout this thesis. It is emphasized that within this section we are *only* concerned about whether a particular entry is non-zero or not, and *not* what its value might be if it is non-zero.

The values in a restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ depend upon the k indices given by $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$, which correspond to the restricting variables $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$, and a binary word of length k, $\mathbf{c} = c_0c_1\cdots c_{k-1}$. Recalling the set $I_{\mathbf{c}}$, equation (1.6), which contains the indices of all the non-zero entries in the restricted vector, then the index of the first non-zero entry in the vector is the smallest value in $I_{\mathbf{c}}$, denote it by $i_{\mathbf{c}}$ say, and is simply given by

$$i_{\mathbf{c}} = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha}. \tag{1.8}$$

Similarly the position of the last non-zero entry is the largest value in $I_{\mathbf{c}}$, denote it by $\bar{i}_{\mathbf{c}}$ say, and is given by

$$\begin{aligned}
\bar{i}_{\mathbf{c}} &= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} 2^j \\
&= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} 2^j + (2^m - 1) - (2^m - 1) \\
&= 2^m - 1 + \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} 2^j - \sum_{j=0}^{m-1} 2^j \\
&= 2^m - 1 + \sum_{\alpha=0}^{k-1} (c_\alpha - 1) 2^{j_\alpha},
\end{aligned}$$

where again from Section 1.9, J is the set of all the restricting indices j_α.

Then the ‘span’ of the non-zeroes entries in a restricted vector, i.e. the length from the first to the last, is

$$\begin{aligned} n_{\mathbf{x}} &= \bar{i}_{\mathbf{c}} - i_{\mathbf{c}} + 1 \\ &= 2^m - 1 + \sum_{\alpha=0}^{k-1} (c_\alpha - 1) 2^{j_\alpha} - \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + 1 \\ &= 2^m - \sum_{\alpha=0}^{k-1} 2^{j_\alpha}, \end{aligned}$$

from which it is seen that the length $n_{\mathbf{x}}$ depends only on $\mathbf{x}$ and not on $\mathbf{c}$.

The *pattern* of the non-zero entries in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ is thus defined as a {0,X}-sequence $\mathbf{p}$ of length $n_{\mathbf{x}}$ with components p_i, $i = 0, 1, \ldots, n_{\mathbf{x}} - 1$ given by

$$p_i = \begin{cases} 0 & \text{if } (\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_{i_{\mathbf{c}}+i} = 0 \\ \mathrm{X} & \text{otherwise,} \end{cases}$$

and we say the pattern is at *position* $i_{\mathbf{c}}$ in the vector. For example, for the restricted vector

$$\mathbf{F}\big|_{x_0 x_2 = 10} = (0 - 0 + 00000 + 0 + 0000)$$

from Example 1.14, the pattern of non-zeroes is X0X00000X0X, at position 1.

For any given restricting variables $\mathbf{x}$, the pattern does not depend on the choice of constant $\mathbf{c}$, as is now shown. Suppose we have two binary words $\mathbf{c}', \mathbf{c}$ for which (when regarded as their decimal equivalents) $\mathbf{c}' > \mathbf{c}$. Define

$$c_{\text{diff}} = \sum_{\alpha=0}^{k-1} (c'_\alpha - c_\alpha) 2^{j_\alpha}$$

(note that in general, due to the j_α values, this is not the difference between the decimal equivalents of $\mathbf{c}'$ and $\mathbf{c}$). Suppose that $i \in I_{\mathbf{c}}$, and evaluate $i' = i + c_{\text{diff}}$:

$$\begin{aligned} i' &= i + c_{\text{diff}} \\ &= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} i_j 2^j + \sum_{\alpha=0}^{k-1} (c'_\alpha - c_\alpha) 2^{j_\alpha} \\ &= \sum_{\alpha=0}^{k-1} c'_\alpha 2^{j_\alpha} + \sum_{j \notin J} i_j 2^j, \end{aligned}$$

i.e. i' is in $I_{\mathbf{c}'}$. Thus if there is a non-zero entry at index i in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, then there is a non-zero entry at index $i + c_{\text{diff}}$ in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}'}$, i.e. the indices of the non-zero entries in the latter vector are just those of the former, shifted by c_{diff}, and indeed

$$I_{\mathbf{c}'} = I_{\mathbf{c}} + c_{\text{diff}}.$$

Thus the pattern of the non-zeroes in a restricted vector does not depend on $\mathbf{c}$, which merely determines the position of the pattern within the vector.

It can also be seen that the pattern of non-zeroes is symmetric. A length n sequence $a_0, a_1, \ldots, a_{n-1}$ is called *symmetric* if $a_i = a_{n-1-i}$ for all i. Thus pattern $\mathbf{p}$ is symmetric if both terms p_i and $p_{n_{\mathbf{x}}-1-i}$, $i = 0, 1, \ldots, n_{\mathbf{x}} - 1$, are either 0 or X, i.e. the corresponding components in the vector are either both zero or both non-zero. Consider the index of a particular non-zero entry in a restricted vector, i.e. $i \in I_{\mathbf{c}}$, $i \geqslant i_{\mathbf{c}}$. Write i as an offset from $i_{\mathbf{c}}$:

$$\begin{aligned} i &= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} i_j 2^j \\ &= i_{\mathbf{c}} + \ell, \text{ say.} \end{aligned}$$

Complement the bits i_j, $j \notin J$ to obtain i':

$$\begin{aligned} i' &= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} (1 - i_j) 2^j \\ &= \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} 2^j - \sum_{j \notin J} i_j 2^j \\ &= \bar{i}_{\mathbf{c}} - \ell. \end{aligned}$$

Clearly i' is also in $I_{\mathbf{c}}$. Thus if there is a non-zero at $i = i_{\mathbf{c}} + \ell$, there is also one at $i' = \bar{i}_{\mathbf{c}} - \ell$. Write i and i' as offsets from the start of the pattern, i.e. by subtracting $i_{\mathbf{c}}$: $i = i_{\mathbf{c}} + \ell \to \ell$, and $i' = \bar{i}_{\mathbf{c}} - \ell \to \bar{i}_{\mathbf{c}} - i_{\mathbf{c}} - \ell = n_{\mathbf{x}} - 1 - \ell$. Thus if there is a non-zero entry (an X) at offset ℓ in the pattern, there is also a non-zero entry at offset $n_{\mathbf{x}} - 1 - \ell$, and so the pattern of non-zeroes is symmetric.

Example 1.17. Again revisit Example 1.14, with $m = 4$ and

$$f(x) = x_0 x_1 + x_1 x_2 + x_1 x_3 + x_0 + x_3.$$

With the restricting variables $\mathbf{x} = x_0 x_2$, then $J = \{0, 2\}$. The pattern of non-zero entries for all four restricted vectors is seen to be X 0 X 0 0 0 0 0 X 0 X, which is clearly symmetric. Taking the particular value $\mathbf{c} = c_0 c_1 = 01$, from the above we get that: the length of the pattern is

$$n_{\mathbf{x}} = 2^m - \sum_{\alpha=0}^{1} 2^{j_\alpha} = 2^4 - (2^0 + 2^2) = 11;$$

$I_{\mathbf{c}}$ is given by

$$\sum_{\alpha=0}^{1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} i_j 2^j = (0.2^0 + 1.2^2) + (i_1 2 + i_3 2^3), \quad i_1, i_3 = 0, 1,$$

and so $I_{\mathbf{c}} = \{4, 6, 12, 14\}$; the first non-zero is at

$$i_{\mathbf{c}} = \sum_{\alpha=0}^{1} c_\alpha 2^{j_\alpha} = 0.2^0 + 1.2^2 = 4;$$

the last non-zero is

$$\bar{i}_{\mathbf{c}} = 2^m - 1 + \sum_{\alpha=0}^{1} (c_\alpha - 1)2^{j_\alpha} = 2^4 - 1 + (-1.2^0 + 0.2^2) = 14,$$

all of which can be verified against the restricted vector itself,

$$\mathbf{F}\big|_{x_0x_2=01} = (0000 + 0 - 00000 - 0 - 0).$$

□

To summarize, the pattern of non-zero entries in a restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ depends only on the choice of restricting variables $\mathbf{x}$, the pattern is symmetric, its length depends only on $\mathbf{x}$, and its position within the vector depends on $\mathbf{c}$.

1.9.3 Truncated restricted vectors

The fact that restricted vectors contain sections of entries which are all zero has a usable impact on the calculation of their cross-correlation function: it is clear that the 'leading' and 'trailing' zeroes in a pair of restricted vectors mean that their cross-correlation will depend only on the respective patterns of non-zero entries within the two vectors. This is given shortly as a lemma, but first some new notation is defined.

Definition 1.18. Let $\mathbf{F} = (F_0, F_1, \ldots, F_{n-1})$ be a complex-valued vector of length n, and $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ be some restriction of it for suitable $\mathbf{x}$ and $\mathbf{c}$. Then with $i_{\mathbf{c}}$ and $\bar{i}_{\mathbf{c}}$ as the indices of the first and last non-zero entries in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ as above, write F'_i for $(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})_i, \quad i = 0, 1, \ldots, n-1$, then

$$F'_i = 0 \text{ for } 0 \leqslant i < i_{\mathbf{c}} \text{ and } \bar{i}_{\mathbf{c}} < i \leqslant n-1,$$

i.e.

$$\begin{aligned}\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}} &= (0, \ldots, 0, F'_{i_{\mathbf{c}}}, F'_{i_{\mathbf{c}}+1}, \ldots, F'_{\bar{i}_{\mathbf{c}}-1}, F'_{\bar{i}_{\mathbf{c}}}, 0, \ldots, 0)\\ &= (0, \ldots, 0, F_{i_{\mathbf{c}}}, F'_{i_{\mathbf{c}}+1}, \ldots, F'_{\bar{i}_{\mathbf{c}}-1}, F_{\bar{i}_{\mathbf{c}}}, 0, \ldots, 0)\end{aligned}$$

as $F'_{i_{\mathbf{c}}} \neq 0$ and $F'_{\bar{i}_{\mathbf{c}}} \neq 0$, and so *are* their respective unrestricted counterparts. The remaining entries, $F'_i, \quad i_{\mathbf{c}} < i < \bar{i}_{\mathbf{c}}$, may or may not be zero, depending on the restricting variables in $\mathbf{x}$. Then the *truncated vector* is obtained by truncating the leading and trailing zeroes of the restricted vector, is of length $n_{\mathbf{x}} = \bar{i}_{\mathbf{c}} - i_{\mathbf{c}} + 1$, and is denoted by square brackets, $[\cdots]$, i.e.

$$[\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}] = (F_{i_{\mathbf{c}}}, F'_{i_{\mathbf{c}}+1}, \ldots, F'_{\bar{i}_{\mathbf{c}}-1}, F_{\bar{i}_{\mathbf{c}}}).$$

□

Example 1.19. Taking one of the restricted vectors from Example 1.14,

$$\mathbf{F}\big|_{x_0x_2=10} = (0 - 0 + 00000 + 0 + 0000),$$

the truncated vector is

$$[\mathbf{F}\big|_{x_0x_2=10}] = (-0 + 00000 + 0+).$$

□

We thus get the following simple lemma:

Lemma 1.20. *Let f and g be two generalized Boolean functions with complex-valued vectors $\mathbf{F}$ and $\mathbf{G}$, and let $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}$ and $\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}$ be corresponding restricted vectors for some suitable restricting variables $\mathbf{x}$ with constants $\mathbf{c}_1$ and $\mathbf{c}_2$. With notation as above, in particular where $i_{\mathbf{c}_j}$ is the index of the first non-zero entry in vector $(\cdot)\big|_{\mathbf{x}=\mathbf{c}_j}$, $j = 1$ or 2, and $n_{\mathbf{x}}$ the length of the non-zero pattern, then the cross-correlation of the restricted vectors is given by the shifted cross-correlation of the truncated vectors:*

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) = \begin{cases} C([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}], [\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}])(\ell - (i_{\mathbf{c}_2} - i_{\mathbf{c}_1})) \\ \qquad (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) - (n_{\mathbf{x}} - 1) \leqslant \ell \leqslant (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) + (n_{\mathbf{x}} - 1) \\ 0 \qquad \textit{otherwise.} \end{cases}$$

In particular, when $f = g$ and $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c}$,

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = \begin{cases} A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}])(\ell) & -(n_{\mathbf{x}} - 1) \leqslant \ell \leqslant n_{\mathbf{x}} - 1 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Visualize two vectors $\mathbf{A}$ and $\mathbf{B}$ shifted by ℓ places with respect to each other:

$$\begin{array}{l} \leftarrow \quad \ell \quad \rightarrow \boxed{A_0\ A_1 \qquad\qquad \cdots \qquad\qquad A_{n-1}} \\ \boxed{B_0^* \qquad\quad \cdots\ B_\ell^*\ B_{\ell+1}^* \quad \cdots \quad B_{n-1}^*} \end{array}$$

Their cross-correlation is now seen to be formed by taking products vertically over the overlapping section and summing:

$$C(\mathbf{A}, \mathbf{B})(\ell) = A_0 B_\ell^* + A_1 B_{1+\ell}^* + \cdots + A_{n-1-\ell} B_{n-1}^*.$$

Consider now the following diagrammatic representation of two restricted vectors:

$$\begin{array}{l} \leftarrow\ \ell\ \rightarrow \boxed{0 \quad \cdots \quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad\quad \cdots \qquad\quad 0} \\ \boxed{0 \qquad\quad \cdots \qquad\quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0\ \cdots\ 0} \end{array}$$

Here the leading and trailing zeroes are shown as '0 ··· 0', and the pattern of non-zeroes as 'X ··· X', where: the index of the first non-zero 'X' is $i_{\mathbf{c}_j}$, $j = 1$ or 2; the index of the last non-zero 'X' is $\bar{i}_{\mathbf{c}_j}$; the length of the pattern is $n_{\mathbf{x}} = \bar{i}_{\mathbf{c}_j} - i_{\mathbf{c}_j} + 1$, and, by the work in the preceding section, is the same for $j = 1$ or 2; and intermediate values may or may not be zero. That the cross-correlation of the restricted vectors is just determined by the cross-correlation of the two patterns of non-zeroes is clear.
When the shift produces no overlap between the non-zero patterns:

$$\begin{array}{l} \leftarrow\ \ell\ \rightarrow \boxed{0\cdots 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad\quad \cdots \qquad\quad 0} \\ \boxed{0 \qquad\quad \cdots \qquad\quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0\cdots 0} \end{array}$$

or

$$\begin{array}{l} \leftarrow\ \ell\ \rightarrow \boxed{0 \qquad \cdots \qquad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \quad \cdots \quad 0} \\ \boxed{0 \quad \cdots \quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad \cdots \qquad 0} \end{array}$$

it is clear that $C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) = 0$ as all the vertical products are zero. The first occurs when

$$\begin{aligned} & \ell + \bar{i}_{\mathbf{c}_1} < i_{\mathbf{c}_2} \\ \text{i.e.}\quad & \ell + i_{\mathbf{c}_1} + n_{\mathbf{x}} - 1 < i_{\mathbf{c}_2} \\ \text{i.e.}\quad & \ell < (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) - (n_{\mathbf{x}} - 1), \end{aligned}$$

the second when

$$\begin{aligned} & \ell + i_{\mathbf{c}_1} > \bar{i}_{\mathbf{c}_2} \\ \text{i.e.}\quad & \ell + i_{\mathbf{c}_1} > i_{\mathbf{c}_2} + n_{\mathbf{x}} - 1 \\ \text{i.e.}\quad & \ell > (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) + (n_{\mathbf{x}} - 1). \end{aligned}$$

For shifts inside this range, i.e. $(i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) - (n_{\mathbf{x}} - 1) \leqslant \ell \leqslant (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) + (n_{\mathbf{x}} - 1)$, which is when the vectors look like

$$\begin{array}{l} \leftarrow\ \ell\ \rightarrow \boxed{0 \qquad \cdots \qquad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad \cdots \qquad 0} \\ \boxed{0 \qquad \cdots \qquad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \quad \cdots \quad 0} \end{array}$$

and the first diagram shown above, the relative shift between the non-zero patterns in the respective vectors is

$$\ell + i_{\mathbf{c}_1} - i_{\mathbf{c}_2} = \ell - (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}),$$

and so the cross-correlation of the whole is given by the cross-correlation of the patterns, that is

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) = C([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}], [\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}])(\ell - (i_{\mathbf{c}_2} - i_{\mathbf{c}_1})).$$

Similarly when ℓ is negative

$$\begin{array}{l} \boxed{0 \quad \cdots \quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad \cdots \qquad 0} \leftarrow -\ell \rightarrow \\ \qquad\qquad \boxed{0 \quad \cdots \quad 0\,\mathrm{X} \quad \cdots \quad \mathrm{X}\,0 \qquad \cdots \qquad 0} \end{array}$$

the cross-correlation $C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell)$ is zero when there is no overlap in the non-zero patterns, which is when

$$\begin{aligned} & \bar{i}_{\mathbf{c}_1} < -\ell + i_{\mathbf{c}_2} \\ \text{i.e.}\quad & i_{\mathbf{c}_1} + n_{\mathbf{x}} - 1 < -\ell + i_{\mathbf{c}_2} \\ \text{i.e.}\quad & \ell < (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) - (n_{\mathbf{x}} - 1), \end{aligned}$$

and when

$$\begin{aligned} & -\ell + \bar{i}_{\mathbf{c}_2} < i_{\mathbf{c}_1} \\ \text{i.e.}\quad & -\ell + i_{\mathbf{c}_2} + n_{\mathbf{x}} - 1 < i_{\mathbf{c}_1} \\ \text{i.e.}\quad & \ell > (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) + (n_{\mathbf{x}} - 1), \end{aligned}$$

giving the same conditions as the positive case.
For shifts inside this range, i.e. $(i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) - (n_{\mathbf{x}} - 1) \leqslant \ell \leqslant (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}) + (n_{\mathbf{x}} - 1)$, again the cross-correlation of the whole is given by that of the non-zero patterns, which are shifted relatively to each other by

$$i_{\mathbf{c}_1} - (-\ell + i_{\mathbf{c}_2}) = \ell - (i_{\mathbf{c}_2} - i_{\mathbf{c}_1}),$$

i.e.

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) = C([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}], [\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}])(\ell - (i_{\mathbf{c}_2} - i_{\mathbf{c}_1})),$$

again as the positive case. This proves the assertion about the cross-correlation. For the auto-correlation, when $f = g$ and $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c}$, then $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1} = \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2} = \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, $[\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}] = [\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}] = [\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}]$ and $i_{\mathbf{c}_1} = i_{\mathbf{c}_2}$. Substituting into the cross-correlation result, and from the definition of auto-correlation we get the required result. □

Since the aperiodic auto-correlation function of any vector is, by definition, zero for any shift whose modulus is greater than or equal to the length of the vector, we have that

$$A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}])(\ell) = 0 \quad \text{for } |\ell| \geqslant n_{\mathbf{x}},$$

for some restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, and so we may simply write

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}])(\ell) \quad \text{for all } \ell.$$

There are then two simple consequences of the above lemma: firstly, if two functions when restricted by the same restricting variables $\mathbf{x}$, but at different values of $\mathbf{c}$, result in the same restricted function, i.e. for functions f and g if

$$f\big|_{\mathbf{x}=\mathbf{c}_1} = g\big|_{\mathbf{x}=\mathbf{c}_2}, \quad \mathbf{c}_1 \neq \mathbf{c}_2,$$

then the restricted vectors have the same auto-correlation function, i.e.

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1})(\ell) = A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) \quad \text{for all } \ell.$$

This is because as the restricted functions are the same, then the non-zero values in the restricted vectors are the same, but all those in one are at a shift relative to those in the other, due to the fact that $\mathbf{c}_1 \neq \mathbf{c}_2$, and so in turn, $i_{\mathbf{c}_1} \neq i_{\mathbf{c}_2}$. The *truncated* vectors, however, are identical, and thus

$$\begin{aligned} A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1})(\ell) &= A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}])(\ell) \\ &= A([\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2}])(\ell) \\ &= A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell). \end{aligned}$$

Secondly, Theorem 1.24, to be given in Section 1.10 below, gives conditions for restricted functions $f\big|_{\mathbf{x}=\mathbf{c}}$ and $g\big|_{\mathbf{x}=\mathbf{c}}$ to form a Golay complementary pair, i.e. when

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell \neq 0,$$

thus immediately giving

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0 \Leftrightarrow A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}])(\ell) + A([\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}}])(\ell) = 0,$$

for $\ell \neq 0$, i.e. $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ and $\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}}$ are a complementary pair if and only if the *truncated* vectors $[\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}]$ and $[\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}}]$ are a complementary pair. Note also that since the non-zero entries are q^{th} roots of unity and thus have modulus 1, if there are k restricting variables $\mathbf{x}$, then there are 2^{m-k} non-zero entries and so this is also the value of the auto-correlation functions for the restricted vectors at the zero shift: hence the sum of the auto-correlations at the zero shift for two restricted functions forming a complementary pair is twice this,

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(0) + A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}})(0) = A([\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}])(0) + A([\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}}])(0) = 2^{m-k+1}.$$

1.9.4 Reversing restricted functions

In Section 1.6 above it was shown that the reverse of a generalized Boolean function $f(x_0, \ldots, x_{m-1})$ is obtained by making the substitution $x_i \to 1 - x_i$ for $i = 0, 1, \ldots, m-1$, and the resulting function was abbreviated to $f(1-x)$ or $\overline{f}$. The same idea extends to the reverse of a restricted function, i.e. that function, which when evaluated over its domain, produces the values of the original restricted function in reverse order. Let $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$ be some k restricting variables and $\mathbf{c}$ be a binary word of length k. The restricted function $f\big|_{\mathbf{x}=\mathbf{c}}$ is thus a function in $m-k$ variables, and the reverse of this is obtained by making the substitutions $x_i \to 1 - x_i$ for just these $m-k$ variables, i.e. for $i = 0, 1, \ldots, m-1$ and $i \notin \{j_0, j_1, \ldots, j_{k-1}\}$. That is, let $x_{\mathbf{x}}$ denote those variables not in $\mathbf{x}$, so the restricted function becomes

$$f\big|_{\mathbf{x}=\mathbf{c}}(x_{\mathbf{x}}) = f(x)\big|_{\mathbf{x}=\mathbf{c}},$$

and then its reverse, also denoted by the $\overline{}$, is

$$\overline{f\big|_{\mathbf{x}=\mathbf{c}}} = f\big|_{\mathbf{x}=\mathbf{c}}(1 - x_{\mathbf{x}}).$$

(Note this is not the same as the restriction of the reversed function, which would be notated as $\overline{f}\big|_{\mathbf{x}=\mathbf{c}}$, but which is not used anywhere in this thesis.)
Now suppose that $g(x)$ is the function, in m variables, defined by

$$g(x) = \overline{f\big|_{\mathbf{x}=\mathbf{c}}} \prod_{c_\alpha=1} x_{j_\alpha} \prod_{c_\alpha=0} (1 - x_{j_\alpha}).$$

Clearly, performing the restriction $\mathbf{x} = \mathbf{c}$ on $g(x)$ merely recovers the function $\overline{f\big|_{\mathbf{x}=\mathbf{c}}}$, i.e.

$$g(x)\big|_{\mathbf{x}=\mathbf{c}} = \overline{f\big|_{\mathbf{x}=\mathbf{c}}}.$$

Thus the restricted vector $\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}}$ is a vector with non-zero entries in the same positions as the vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, but with the values of the non-zero entries reversed. Such a vector will be denoted using a $\widetilde{}$, i.e.

$$\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}} = \widetilde{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}}.$$

It is emphasized that this is *not* the same as reversing the restricted vector, i.e.

$$\widetilde{\mathbf{F}}\Big|_{\mathbf{x}=\mathbf{c}} \neq \overline{\mathbf{F}\Big|_{\mathbf{x}=\mathbf{c}}}.$$

However, if we take the truncation of the vector $\widetilde{\mathbf{F}}\Big|_{\mathbf{x}=\mathbf{c}}$, and then reverse it, it is quite clear that we then get the truncation of the original restricted vector, i.e.

$$\overline{[\widetilde{\mathbf{F}}\Big|_{\mathbf{x}=\mathbf{c}}]} = [\mathbf{F}\Big|_{\mathbf{x}=\mathbf{c}}],$$

and by reversing both sides we do indeed then get the equality

$$[\widetilde{\mathbf{F}}\Big|_{\mathbf{x}=\mathbf{c}}] = \overline{[\mathbf{F}\Big|_{\mathbf{x}=\mathbf{c}}]}.$$

Example 1.21. Continuing on from Example 1.14, with

$$f(x) = x_0x_1 + x_1x_2 + x_1x_3 + x_0 + x_3,$$

and $\mathbf{x} = x_0x_2$ and $\mathbf{c} = 10$, we get the restricted function

$$f(x)\Big|_{x_0x_2=10} = x_1 + x_1x_3 + 1 + x_3$$

which takes the values (1000), and the restricted vector

$$\mathbf{F}\Big|_{x_0x_2=10} = (0 - 0 + 00000 + 0 + 0000).$$

Reversing the restricted function with the substitution $x_1 \to 1 + x_1$ and $x_3 \to 1 + x_3$ gives

$$\begin{aligned} \overline{f\Big|_{x_0x_2=10}} &= (1 + x_1) + (1 + x_1)(1 + x_3) + 1 + (1 + x_3) \\ &= 1 + x_1 + 1 + x_1 + x_3 + x_1x_3 + 1 + 1 + x_3 \\ &= x_1x_3 \end{aligned}$$

which is easily confirmed to have vector (0001). Forming the function

$$\begin{aligned} g(x) &= \overline{f\Big|_{\mathbf{x}=\mathbf{c}}} \prod_{c_\alpha=1} x_{j_\alpha} \prod_{c_\alpha=0} (1 - x_{j_\alpha}) \\ &= x_1x_3x_0(1 + x_2) \\ &= x_0x_1x_3 + x_0x_1x_2x_3, \end{aligned}$$

gives

$$\mathbf{g} = (0000000000010000),$$

from which we get

$$\begin{aligned} \mathbf{G}\Big|_{x_0x_2=10} &= (0 + 0 + 00000 + 0 - 0000) \\ &= \widetilde{\mathbf{F}}\Big|_{x_0x_2=10}, \end{aligned}$$

where the reversal of the non-zero entries compared to the vector $\mathbf{F}\Big|_{x_0x_2=10}$ above may be observed. □

1.9.5 Compressed restricted vectors

It is occasionally convenient to work with the vector consisting of just the non-zero entries of some restricted vector, and also the function corresponding to this vector. Notation for doing this is established in this section.

Suppose $\mathbf{F}$ corresponds to a generalized Boolean function f of m variables, and that we have k restricting variables $\mathbf{x}$, and $\mathbf{c} = c_0 c_1 \ldots c_{k-1}$ is a binary word of length k. After applying the method of restriction, the vector obtained, $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$, consists of a number of zero and non-zero entries, the positions of which are determined by the restricting variables in $\mathbf{x}$ and the value of $\mathbf{c}$, and it is the 2^{m-k} non-zero entries we are interested in. From Section 1.9 we have the set J of the k restricting indices of the restricting variables in $\mathbf{x}$,

$$J = \{j_0, j_1, \ldots, j_{k-1}\} \quad \text{where} \quad 0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1,$$

and (from equation (1.6)) the set $I_{\mathbf{c}}$, the indices of the non-zero entries in the restricted vector, given by

$$i = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{j \notin J} i_j 2^j, \quad i_j = 0 \text{ or } 1.$$

Let the set S be the indices of the non-restricting variables, and label these s_α, $\alpha = 0, 1, \ldots, m-k-1$, with $0 \leqslant s_0 < s_1 < \cdots < s_{m-k-1} \leqslant m-1$, i.e.

$$\begin{aligned} S &= \{0, 1, \ldots, m-1\} \setminus J \\ &= \{s_0, s_1, \ldots, s_{m-k-1}\}. \end{aligned}$$

Then after restriction, the function $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ is just a function of the $m-k$ variables indexed by S, and the indices i of the non-zero entries in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ become

$$i = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{\alpha=0}^{m-k-1} i_{s_\alpha} 2^{s_\alpha}, \quad i_{s_\alpha} = 0 \text{ or } 1, \tag{1.9}$$

and there are 2^{m-k} such i. We now make the following definitions:

Definition 1.22. The length 2^{m-k} *compressed vector*, obtained from $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ by removing or 'compressing' the zero values out, denoted by

$$\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}},$$

has the components

$$\big(\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}}\big)_{\widehat{i}} = \big(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}\big)_i = \omega^{f_i}$$

where

$$\widehat{i} = \sum_{\alpha=0}^{m-k-1} i_{s_\alpha} 2^\alpha, \tag{1.10}$$

where the i are the indices of the non-zero entries in $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ given by (1.9), and where as usual f_i is the i^{th} component of the vector $\mathbf{f}$ of all the 2^m values of f. The *compressed function* equivalent to the compressed vector, denoted by

$$\widehat{f}(x)\big|_{\mathbf{x}=\mathbf{c}},$$

is obtained from $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ by relabelling the variables to run from 0 to $m-k-1$, i.e. by making the transformation $x_{s_\alpha} \to x_\alpha$, $\alpha = 0, 1, \ldots, m-k-1$. □

The $\mathbb{Z}_q$-valued vector of values of $\widehat{f}(x)\big|_{\mathbf{x}=\mathbf{c}}$ is denoted by $\widehat{\mathbf{f}}\big|_{\mathbf{x}=\mathbf{c}}$, and is effectively formed by by evaluating $f(x)\big|_{\mathbf{x}=\mathbf{c}}$ over its domain, and may also be formed by picking out the components of $\mathbf{f}$ in the same manner as the compressed vector, i.e.

$$\big(\widehat{\mathbf{f}}\big|_{\mathbf{x}=\mathbf{c}}\big)_{\widehat{i}} = \big(\mathbf{f}\big)_i = f_i,$$

where again the indices i are those from (1.9). As before, we may drop the '(x)' and just write $\widehat{f}\big|_{\mathbf{x}=\mathbf{c}}$ if the meaning is clear.

Example 1.23. In Example 1.6 we had the function

$$f(x) = x_0x_1 + x_1x_2 + x_1x_3 + x_0 + x_3.$$

Restricting with $\mathbf{x} = x_0x_2$ and $\mathbf{c} = 01$ gives

$$\begin{aligned}\mathbf{F}\big|_{x_0x_2=01} &= (0000+0-00000-0-0)\\ f(x)\big|_{x_0x_2=01} &= x_1 + x_1x_3 + x_3\end{aligned}$$

from which the compressed vectors are

$$\begin{aligned}\widehat{\mathbf{F}}\big|_{x_0x_2=01} &= (+---)\\ \widehat{\mathbf{f}}\big|_{x_0x_2=01} &= (0111)\end{aligned}$$

and mapping the indices in the restricted function as

$$1 \mapsto 0, 3 \mapsto 1,$$

gives the compressed function as

$$\widehat{f}\big|_{x_0x_2=01} = x_0 + x_0x_1 + x_1.$$

□

1.10 A Construction for Golay Complementary Pairs

In this and the following section, those key results from [32, 33] which form the cornerstone of much of the work in this thesis are presented. In Section 1.5.3 it was shown that Golay complementary sequences have PMEPRs which are at most 2, and are thus desirable for use in OFDM schemes. The key result of Davis & Jedwab [11] was to define a simple way to construct such complementary sequences. The following result (Theorem 9 of [32, 33]) gives the conditions under which a pair of *restricted* vectors form a Golay complementary pair of sequences, this being a generalization of the main Davis & Jedwab construction for complementary pairs which follows as a corollary after the theorem.

Throughout the remainder of this thesis, unless stated to the contrary, q will be *even*.

Theorem 1.24. *Let f be a generalized Boolean function over $\mathbb{Z}_q$ in the m variables $x_0, \ldots, x_{m-1}$, let $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$ be some k restricting variables with $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$, and let $\mathbf{c} = c_0c_1\cdots c_{k-1}$ be a binary word of length k. Suppose that the restricted function $f\big|_{\mathbf{x}=\mathbf{c}}$ is a quadratic function and that its graph $G(f\big|_{\mathbf{x}=\mathbf{c}})$ is a path. Then the vector associated with $f\big|_{\mathbf{x}=\mathbf{c}}$ is a Golay complementary sequence, forming a Golay complementary pair with each of the vectors associated with functions the of the form*

$$(f + \frac{q}{2}x_a + r)\big|_{\mathbf{x}=\mathbf{c}},$$

where $r \in \mathbb{Z}_q$ is arbitrary and a is either the single vertex of $G(f\big|_{\mathbf{x}=\mathbf{c}})$ when $k = m-1$, or a vertex of degree 1 in $G(f\big|_{\mathbf{x}=\mathbf{c}})$ when $k < m-1$.

Proof. The proof is by induction on k, where we take as an inductive hypothesis the statement of the theorem. The case $k = m-1$ serves as the base case for the induction. In this case Q, the quadratic part of $f\big|_{\mathbf{x}=\mathbf{c}}$, is identically zero, $G(f\big|_{\mathbf{x}=\mathbf{c}})$ has a single vertex labelled a and $\mathbf{x}$ omits exactly one variable x_a. From (1.6) it can be seen that the restricted vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ will have exactly two non-zero components, at indices $\sum_{\alpha\neq a} c_\alpha 2^\alpha$ and $\sum_{\alpha\neq a} c_\alpha 2^\alpha + 2^a$. Suppose that $f\big|_{\mathbf{x}=\mathbf{c}}$ takes the values f_0 and f_1 as x_a is 0 and 1, and so the corresponding non-zero components in the restricted vector are ω^{f_0} and ω^{f_1} respectively. Since x_a is not in $\mathbf{x}$, the non-zero components in the vector associated with $(f+\frac{q}{2}x_a+r)\big|_{\mathbf{x}=\mathbf{c}}$, where $r \in \mathbb{Z}_q$ is arbitrary, are then ω^{f_0+r} and $\omega^{f_1+\frac{q}{2}+r} = -\omega^{f_1+r}$. Then the only non-zero values of the auto-correlation functions of the vectors associated with

$$f\big|_{\mathbf{x}=\mathbf{c}} \text{ and } (f + \frac{q}{2}x_a + r)\big|_{\mathbf{x}=\mathbf{c}}$$

occur at shift $\ell = 2^a$, where the values are $\omega^{f_0}(\omega^{f_1})^* = \omega^{f_0-f_1}$ and $\omega^{f_0+r}(-\omega^{f_1+r})^* = -\omega^{f_0-f_1}$ respectively, and so the auto-correlations clearly sum to zero for all $\ell \neq 0$, and thus the vectors form a Golay complementary pair. Now suppose the theorem is true in the case when $\mathbf{x}$ contains $k+1 \leqslant m-1$ variables and consider the case of k variables. Now the non-zero components of $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ are determined by the values of the quadratic function $f\big|_{\mathbf{x}=\mathbf{c}}$ in the $m-k$ non-restricted variables $x_{i_0}, \ldots, x_{i_{m-k-1}}$, where the graph $G(f\big|_{\mathbf{x}=\mathbf{c}})$ is a path. So for some permutation π of $\{0, 1, \ldots, m-k-1\}$ and some $g_0, \ldots, g_{m-k-1}, g \in \mathbb{Z}_q$, we can write

$$f\big|_{\mathbf{x}=\mathbf{c}} = Q + L$$

where

$$Q(x_{i_0},\ldots,x_{i_{m-k-1}}) = \frac{q}{2}\sum_{\alpha=0}^{m-k-2} x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}},$$
$$L(x_{i_0},\ldots,x_{i_{m-k-1}}) = \sum_{\alpha=0}^{m-k-1} g_\alpha x_{i_{\pi(\alpha)}} + g.$$

We claim that the vectors associated with the pair of functions

$$f\big|_{\mathbf{x}=\mathbf{c}} \text{ and } (f+\frac{q}{2}x_{i_{\pi(m-k-1)}}+r)\big|_{\mathbf{x}=\mathbf{c}},$$

where $r \in \mathbb{Z}_q$ is arbitrary, form a Golay complementary pair. The argument given to support this claim also applies with minor modifications to the pair

$$f\big|_{\mathbf{x}=\mathbf{c}} \text{ and } (f+\frac{q}{2}x_{i_{\pi(0)}}+r)\big|_{\mathbf{x}=\mathbf{c}}, \quad r\in\mathbb{Z}_q.$$

Note that $i_{\pi(0)}$ and $i_{\pi(m-k-1)}$ are the vertices of degree 1 in the graph $G(f\big|_{\mathbf{x}=\mathbf{c}})$. Write $a = i_{\pi(m-k-1)}$ and $f_a = f + \frac{q}{2}x_a + r$, let $\ell \neq 0$ be fixed, and consider

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell), \tag{1.11}$$

where, as usual, $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ and $\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}}$ are the restricted vectors associated with $f\big|_{\mathbf{x}=\mathbf{c}}$ and $f_a\big|_{\mathbf{x}=\mathbf{c}}$ respectively. Write

$$\begin{aligned}\mathbf{F}_0 &= \mathbf{F}\big|_{\mathbf{x}x_a=\mathbf{c}0},\\ \mathbf{F}_1 &= \mathbf{F}\big|_{\mathbf{x}x_a=\mathbf{c}1},\\ \mathbf{F}_{a0} &= \mathbf{F}_a\big|_{\mathbf{x}x_a=\mathbf{c}0},\\ \mathbf{F}_{a1} &= \mathbf{F}_a\big|_{\mathbf{x}x_a=\mathbf{c}1},\end{aligned}$$

and expand the sum (1.11), using Corollary 1.16, as

$$\begin{aligned}&A(\mathbf{F}_0)(\ell)+A(\mathbf{F}_1)(\ell)+C(\mathbf{F}_0,\mathbf{F}_1)(\ell)+C(\mathbf{F}_1,\mathbf{F}_0)(\ell)+\\ &\qquad A(\mathbf{F}_{a0})(\ell)+A(\mathbf{F}_{a1})(\ell)+C(\mathbf{F}_{a0},\mathbf{F}_{a1})(\ell)+C(\mathbf{F}_{a1},\mathbf{F}_{a0})(\ell).\end{aligned} \tag{1.12}$$

By substituting $x_a = x_{i_{\pi(m-k-1)}} = 0$ into the function $f\big|_{\mathbf{x}=\mathbf{c}}$ above we get

$$f\big|_{\mathbf{x}x_a=\mathbf{c}0} = P' + L' + g \tag{1.13}$$

where

$$P' = \begin{cases} \frac{q}{2}\displaystyle\sum_{\alpha=0}^{m-k-3} x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}} & \text{when } k \leqslant m-3\\ 0 & \text{when } k = m-2\end{cases}$$

$$L' = \begin{cases} \displaystyle\sum_{\alpha=0}^{m-k-2} g_\alpha x_{i_{\pi(\alpha)}} & \text{when } k \leqslant m-3\\ g_0 x_{i_\pi(0)} & \text{when } k = m-2.\end{cases}$$

Similarly putting $x_a = x_{i_{\pi(m-k-1)}} = 1$ gives

$$f\big|_{\mathbf{x}x_a=\mathbf{c}1} = P' + L' + \frac{q}{2}x_{i_{\pi(m-k-2)}} + g + g_{m-k-1}.$$

Now consider the function $f' = f + \frac{q}{2}x_{i_{\pi(m-k-2)}} + g_{m-k-1}$. From this definition and (1.13) it can be seen that

$$f'\big|_{\mathbf{x}x_a=\mathbf{c}0} = P' + L' + \frac{q}{2}x_{i_{\pi(m-k-2)}} + g + g_{m-k-1},$$

but this is precisely $f\big|_{\mathbf{x}x_a=\mathbf{c}1}$ above, i.e.

$$f'\big|_{\mathbf{x}x_a=\mathbf{c}0} = f\big|_{\mathbf{x}x_a=\mathbf{c}1}.$$

From its definition above, the graph of $f\big|_{\mathbf{x}x_a=\mathbf{c}0}$ can be seen to be: either a non-trivial path in the case $k \leqslant m-3$, and the vertex labelled $i_{\pi(m-k-2)}$ is an end point of this path; or a trivial path, in the case when $k = m-2$, consisting of just the single vertex $i_{\pi(m-k-2)} = i_{\pi(0)}$. There are $k+1$ restricting variables in both $f\big|_{\mathbf{x}x_a=\mathbf{c}0}$ and $f'\big|_{\mathbf{x}x_a=\mathbf{c}0}$, and since they differ by a term with an index equivalent to a vertex having the necessary properties, and a constant, they satisfy the inductive hypothesis, and so form a Golay complementary pair, i.e.

$$A(\mathbf{F}_0)(\ell) + A(\mathbf{F}'_0)(\ell) = 0, \quad \ell \neq 0.$$

Since the restricted functions $f\big|_{\mathbf{x}x_a=\mathbf{c}1}$ and $f'\big|_{\mathbf{x}x_a=\mathbf{c}0}$ have the same form, their associated vectors have the same non-zero values, only at positions shifted with respect to one another, and so by the comment after Lemma 1.20 they have the same auto-correlation function, i.e. for all ℓ,

$$A(\mathbf{F}_1)(\ell) = A(\mathbf{F}'_0)(\ell),$$

and thus we have that

$$A(\mathbf{F}_0)(\ell) + A(\mathbf{F}_1)(\ell) = 0 \tag{1.14}$$

for all ℓ. By substituting $x_a = 0$ in $f_a\big|_{\mathbf{x}=\mathbf{c}}$ it is seen that

$$\mathbf{F}_{a0} = \mathbf{F}_a\big|_{\mathbf{x}x_a=\mathbf{c}0} = \omega^r\mathbf{F}\big|_{\mathbf{x}x_a=\mathbf{c}0} = \omega^r\mathbf{F}_0,$$

and similarly

$$\mathbf{F}_{a1} = \mathbf{F}_a\big|_{\mathbf{x}x_a=\mathbf{c}1} = \omega^{r+\frac{q}{2}}\mathbf{F}\big|_{\mathbf{x}x_a=\mathbf{c}1} = -\omega^r\mathbf{F}_1.$$

Then from Theorem 1.8 we get

$$A(\mathbf{F}_{a0})(\ell) = A(\omega^r\mathbf{F}_0)(\ell) = A(\mathbf{F}_0)(\ell)$$

and

$$A(\mathbf{F}_{a1})(\ell) = A(-\omega^r\mathbf{F}_1)(\ell) = A(\mathbf{F}_1)(\ell),$$

for all ℓ, and so

$$A(\mathbf{F}_{a0})(\ell) + A(\mathbf{F}_{a1})(\ell) = 0, \quad \ell \neq 0, \tag{1.15}$$

too. Similarly for the cross-correlations, we have

$$C(\mathbf{F}_{a0}, \mathbf{F}_{a1})(\ell) = C(\omega^r\mathbf{F}_0, -\omega^r\mathbf{F}_1)(\ell) = -C(\mathbf{F}_0, \mathbf{F}_1)(\ell) \tag{1.16}$$

and

$$C(\mathbf{F}_{a1}, \mathbf{F}_{a0})(\ell) = C(-\omega^r \mathbf{F}_1, \omega^r \mathbf{F}_0)(\ell) = -C(\mathbf{F}_1, \mathbf{F}_0)(\ell), \tag{1.17}$$

for all ℓ. Substituting equations (1.14), (1.15), (1.16) and (1.17) into the expanded sum (1.12) shows this to be zero at non-zero shifts, and so the original sum, (1.11), is also zero, i.e.

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell \neq 0,$$

and the functions

$$f\big|_{\mathbf{x}=\mathbf{c}} \text{ and } (f + \frac{q}{2}x_{i_{\pi(m-k-1)}} + r)\big|_{\mathbf{x}=\mathbf{c}} \; (\equiv f_a\big|_{\mathbf{x}=\mathbf{c}})$$

form a Golay complementary pair as claimed. So, if the result is true for $k+1$ restrictions it is true for k; but it is true for $k = m-1$, and hence by induction the result is true for all $k = m-1, m-2, \ldots, 1, 0$. □

Thus after the restriction, the quadratic part of the function $f\big|_{\mathbf{x}=\mathbf{c}}$ in the above theorem is a path function, involving all the unrestricted variables, and any linear terms may only be in these same variables.

Putting $k = 0$ in the above theorem gives a simple method of constructing Golay complementary pairs (this is Corollary 11 of [32, 33], itself a generalization of the main result of [10, 11]):

Corollary 1.25. *Let π be a permutation of $\{0, 1, \ldots, m-1\}$, $m \geqslant 2$, and f a generalized Boolean function over $\mathbb{Z}_q$ be defined by*

$$f(x_0, \ldots, x_{m-1}) = \frac{q}{2}\sum_{\alpha=0}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} + \sum_{\alpha=0}^{m-1} g_\alpha x_\alpha,$$

where $g_0, g_1, \ldots, g_{m-1} \in \mathbb{Z}_q$. Then the vectors associated with the functions

$$\begin{aligned} f_1 &= f + \frac{q}{2}cx_{\pi(0)} + \frac{q}{2}dx_{\pi(m-1)} + g \\ f_2 &= f + \frac{q}{2}(1+c+e)x_{\pi(0)} + \frac{q}{2}(d+e)x_{\pi(m-1)} + g', \end{aligned}$$

where $c, d, e \in \{0, 1\}$ and $g, g' \in \mathbb{Z}_q$, form a Golay complementary pair, i.e.

$$A(\mathbf{F}_1)(\ell) + A(\mathbf{F}_2)(\ell) = 0, \quad \ell \neq 0.$$

□

Whilst for particular values of q this construction produces sequences that are already known, it is notable for its simplicity (other constructions are invariably recursive) and the connection with Reed-Muller codes (allowing for encoding schemes incorporating error-correction)—further detail on both these points may be found in [11, 32, 33]. Since the functions f_1 and f_2 share the same quadratic part, the pair of sequences both belong to the same coset of $RM_q(1, m)$: indeed since there are $m!/2$ ways to choose the path which constitutes the quadratic part, the corollary identifies a total of $(m!/2)q^{m+1}$ Golay complementary sequences, and each thus has a PMEPR of at most 2.

It is not known whether the above corollary accounts for *all* q-ary Golay complementary sequences of length 2^m. The computational evidence of [11, 32, 33] suggests that this is the case: for the shorter lengths, exhaustive searches are readily carried out; additionally, for this thesis, an exhaustive search of all length 64 binary sequences, based on the method of [13] and requiring testing 2^{30} cases, was conducted, but all pairings found corresponded with the above corollary, thus reinforcing this belief.

1.11 A Construction for Golay Complementary Sets

In this section Theorem 12 of [32, 33] is presented, which derives a bound on the PMEPR for the words of an arbitrary second order coset of $RM_q(1, m)$. This is achieved by defining a 'deletion' operation on the graph associated with the quadratic form defining the coset, and constructing a complementary set of size determined by the number of deletion operations: the PMEPRs are then at most the size of the set.

As before consider a typical second order generalized Boolean function in the m variables $x_0, \ldots, x_{m-1}$,

$$f = Q + L$$

where

$$Q(x_0, \ldots, x_{m-1}) = \sum_{0 \leqslant i < j \leqslant m-1} q_{ij} x_i x_j, \quad q_{ij} \in \mathbb{Z}_q$$

is a quadratic form, and

$$L(x_0, \ldots, x_{m-1}) = \sum_{i=0}^{m-1} g_i x_i + g$$

is an affine function. The act of performing a restriction on f has a useful interpretation in terms of its effect on the graph of f. Consider the function $f\big|_{x_j=c}$, obtained by substituting $x_j = c$ in f. In particular, quadratic terms $q_{ij}x_ix_j$ in Q are replaced by linear terms $q_{ij}x_ic$ (and linear terms g_jx_j in L with g_jc), and thus to go from $G(f)$ ($\equiv G(Q)$) to $G(f\big|_{x_j=c})$, the vertex j and all edges connecting to it must be deleted since the second order terms from which they are derived cease to exist. Notice that this graph does not depend on the value of c. Thus this defines a *vertex deletion operation* on the graph $G(Q)$: delete a particular vertex and all its edges. By extension, for a list of k restricting indices $0 \leqslant j_0 < \cdots < j_{k-1} \leqslant m-1$, write $\mathbf{x} = x_{j_0} \cdots x_{j_{k-1}}$ and $\mathbf{c} = c_0 \cdots c_{k-1}$, then the function $f\big|_{\mathbf{x}=\mathbf{c}}$ has a quadratic part which is obtained by applying a sequence of vertex deletion operations on the vertices $j_0, j_1, \ldots, j_{k-1}$ of $G(Q)$. The final graph is independent of the choice of $\mathbf{c}$: so, for any $\mathbf{c}$, the quadratic part of $f\big|_{\mathbf{x}=\mathbf{c}}$ is completely described by the graph obtained from $G(Q)$ by applying vertex deletion operations.

The *deletion index* $d(G)$ of a graph G is then defined to be the minimum integer k for which vertex deletion operations applied to k distinct vertices of G results in a path on $m-k$ vertices.

Before the main result, a lemma is proved. It forms part of the original proof of Theorem 12 in [32, 33], but is proved separately here as it is called upon in a number of places. It establishes the following: for some given restricting variables $\mathbf{x}$, suppose that a function is formed by adding $\frac{q}{2}$ times some linear combination of the restricting variables to some other function. Take the cross-correlation between two restricted vectors of this function, but at different restricting constants. Then the sum across all linear combinations of such cross-correlations is zero at all shifts.

Lemma 1.26. *Let $f(x_0, \ldots, x_{m-1})$ be any generalized Boolean function over $\mathbb{Z}_q$ and let $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$ be some k restricting variables. With $\mathbf{d} = d_0d_1\cdots d_{k-1}$ a length k binary word, form the 2^k functions*

$$f + \frac{q}{2}\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} \equiv f + \frac{q}{2}\mathbf{d}\cdot\mathbf{x}$$

by writing $\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha}$ as $\mathbf{d}\cdot\mathbf{x}$. Denote the vector associated with the restricted function $(f+\frac{q}{2}\mathbf{d}\cdot\mathbf{x})\big|_{\mathbf{x}=\mathbf{c}}$ by $\mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}}$, where $\mathbf{c}$ is a binary word of length k. Then the sum of the cross-correlations

$$\sum_{\mathbf{d}} C(\mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}'})(\ell),$$

for all ℓ and for fixed $\mathbf{c} \neq \mathbf{c}'$, is zero.

Proof. Since the term $\mathbf{d}\cdot\mathbf{x}$ in $(f+\frac{q}{2}\mathbf{d}\cdot\mathbf{x})\big|_{\mathbf{x}=\mathbf{c}}$ involves only the restricting variables, after restriction it is simply the constant $\mathbf{d}\cdot\mathbf{c}$, i.e.

$$(f+\frac{q}{2}\mathbf{d}\cdot\mathbf{x})\big|_{\mathbf{x}=\mathbf{c}} = f\big|_{\mathbf{x}=\mathbf{c}} + \frac{q}{2}\mathbf{d}\cdot\mathbf{c},$$

and thus we have that

$$\mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}} = \omega^{\frac{q}{2}\mathbf{d}\cdot\mathbf{c}}\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}},$$

where $\mathbf{F}$ is the complex-valued vector associated with f. Then using Theorem 1.8 we get, for all ℓ:

$$\begin{aligned}\sum_{\mathbf{d}} C(\mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}'})(\ell) &= \sum_{\mathbf{d}} C(\omega^{\frac{q}{2}\mathbf{d}\cdot\mathbf{c}}\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \omega^{\frac{q}{2}\mathbf{d}\cdot\mathbf{c}'}\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}'})(\ell)\\ &= \sum_{\mathbf{d}} \omega^{\frac{q}{2}\mathbf{d}\cdot(\mathbf{c}-\mathbf{c}')}C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}'})(\ell)\\ &= C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}'})(\ell)\sum_{\mathbf{d}} \omega^{\frac{q}{2}\mathbf{d}\cdot(\mathbf{c}-\mathbf{c}')}\\ &= C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}'})(\ell)\sum_{\mathbf{d}} (-1)^{\mathbf{d}\cdot(\mathbf{c}-\mathbf{c}')}.\end{aligned}$$

By writing the expression $\mathbf{d}\cdot(\mathbf{c}-\mathbf{c}')$ as $\sum_{\alpha=0}^{k-1}(c_\alpha - c'_\alpha)d_\alpha$, and noting that $\mathbf{c}\neq\mathbf{c}'$, it is seen that this expression is just a non-zero linear Boolean function in the d_α, and so by Lemma 1.12 it takes the values 0 and 1 equally often as $\mathbf{d} = d_0 d_1 \cdots d_{k-1}$ runs through all its values, and thus $\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}-\mathbf{c}')} = 0$. Therefore

$$\sum_{\mathbf{d}} C(\mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F_d}\big|_{\mathbf{x}=\mathbf{c}'})(\ell) = 0 \quad \text{for all } \ell,$$

as was to be shown. □

The following theorem (Theorem 12 of [32, 33]) shows how to construct complementary sets of size 2^{k+1} based on an arbitrary second order generalized Boolean function Q: determine those k vertices that are needed to reduce the graph of Q to a path; pick one of the end points to the path; then with L any affine function, the set consists of the 2^{k+1} functions obtained by adding $Q + L$ to $\frac{q}{2}$ times all linear combinations of the delete variables and the end point:

Theorem 1.27. *Suppose $Q : \{0,1\}^m \to \mathbb{Z}_q$ is a quadratic form in variables $x_0, \ldots, x_{m-1}$ with $d(G(Q)) = k$. Then the coset $Q + RM_q(1,m)$ is a union of Golay complementary sets of size 2^{k+1}. Consequently every word of the coset has PMEPR at most 2^{k+1}.*

Proof. Suppose that in the graph $G(Q)$ the deletion of the vertices labelled $j_0, j_1, \ldots, j_{k-1}$ results in a graph which is a path. Let a be either a vertex of degree 1 in this graph, or in the case where $k = m-1$, the single vertex of the graph.

Let $L(x_0, \ldots, x_{m-1})$ be any affine function of $x_0, \ldots, x_{m-1}$. We claim that the 2^{k+1} vectors corresponding to the functions

$$Q(x_0,\ldots,x_{m-1}) + L(x_0,\ldots,x_{m-1}) + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + d x_a\right) \qquad d_\alpha, d \in \{0,1\}$$

form a Golay complementary set. These vectors all lie in the coset of $RM_q(1,m)$ determined by Q.

Let $\mathbf{x} = x_{j_0} x_{j_1} \cdots x_{j_{k-1}}$ and $\mathbf{d} = d_0 d_1 \cdots d_{k-1}$. Write $f = Q + L$ and put $\mathbf{d}\cdot\mathbf{x} = \sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha}$. Then the 2^{k+1} functions are

$$f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + d x_a),$$

and let the vectors equivalent to these be notated as

$$\mathbf{F}_{\mathbf{d}d}\,.$$

Then we need to show that

$$\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell) = 0, \quad \ell \neq 0.$$

Restrict over the variables in $\mathbf{x}$ and expand using Corollary 1.16 to obtain, for all ℓ,

$$\begin{aligned}\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell) &= \sum_{\mathbf{d},d}\sum_{\mathbf{c}} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}})(\ell) \\ &\quad + \sum_{\mathbf{d},d}\sum_{\mathbf{c}_1\neq\mathbf{c}_2} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) \\ &= S_1 + S_2 \text{ say.}\end{aligned}$$

From the discussion at the start of this section, the graph of the restricted function $(f+\frac{q}{2}\mathbf{d}\cdot\mathbf{x})\big|_{\mathbf{x}=\mathbf{c}}$ is the same as the graph $G(Q)$ after applying the k vertex deletions, and by hypothesis, this is a path. Moreover, either a is vertex of degree 1 in this graph, or is the single vertex of the graph when $k=m-1$. So from Theorem 1.24, for every fixed $\mathbf{d}$ and $\mathbf{c}$, the vectors of the functions $(f+\frac{q}{2}\mathbf{d}\cdot\mathbf{x})\big|_{\mathbf{x}=\mathbf{c}}$ and $(f+\frac{q}{2}(\mathbf{d}\cdot\mathbf{x}+x_a))\big|_{\mathbf{x}=\mathbf{c}}$, i.e. for $d=0$ and 1 respectively, form a Golay complementary pair, i.e.

$$\sum_{d} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}})(\ell)=0, \quad \ell\neq 0.$$

Thus, on rearranging the sum S_1, it follows that

$$S_1=\sum_{\mathbf{c}}\sum_{\mathbf{d}}\sum_{d} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}})(\ell)=0, \quad \ell\neq 0.$$

Now consider the rearranged sum S_2:

$$S_2=\sum_{d}\sum_{\mathbf{c}_1\neq\mathbf{c}_2}\sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell).$$

The functions corresponding to the vectors $\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_i}$, $i=1$ or 2, in the inner sum may be written as

$$\left((f+\frac{q}{2}dx_a)+\frac{q}{2}\mathbf{d}\cdot\mathbf{x}\right)\big|_{\mathbf{x}=\mathbf{c}_i},$$

and with fixed d and fixed $\mathbf{c}_1\neq\mathbf{c}_2$, are seen to satisfy the conditions of Lemma 1.26, and so the inner sum

$$\sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell)$$

is zero for all ℓ and hence so also is S_2. Thus

$$\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell)=S_1+S_2=0, \quad \ell\neq 0,$$

and the set is a complementary set as required. □

So, for an arbitrary second order generalized Boolean function Q, the above theorem gives an upper bound of 2^{k+1} on the PMEPR of every word of the coset $Q+RM_q(1,m)$: thus we say that the PMEPR *of the coset* is bounded by 2^{k+1}. Note that the PMEPR of individual words may be considerably lower than this bound, and it may not be tight for *any* word in the coset.

Computational evidence has suggested that, under certain circumstances, not all the deletion operations made to determine the deletion index used in the above theorem may be necessary, leading to Conjecture 1 of [32]. The conjecture is stated here in Chapter 2 and studied in detail in that chapter, and also Chapters 3 and 4. In Chapter 3, for functions having a special form, it is shown that the complementary set of the above theorem is in fact a union of smaller complementary subsets, and the complementary sets constructed in Chapter 5 may sometimes identify a subset of the coset whose words all have PMEPRs less than that given by the theorem.

Chapter 2

Conjecture 1 Proof for the Single and Double Isolated Vertex Cases

2.1 Chapter Overview

In [32] it was noticed that when performing the deletion operations for Theorem 1.27 for certain quadratic functions, if a stage was reached where the graph consisted of a path and other vertices which were disconnected, or 'isolated' from it, then the PMEPR of the associated coset was less than that given by the theorem; this lead to Conjecture 1 of that paper, which suggested that further deletions to remove the isolated vertices to exactly meet the conditions of Theorem 1.27 were unnecessary. At the time, only one special case involving a single isolated vertex could be proved. This chapter examines Conjecture 1 in detail. Section 2.2 introduces the conjecture. The proof for the single isolated vertex case in [32] in fact contained a small fallacy: in Section 2.3 below a lemma concerning cross-correlations is proved, which is then used to provide a correct proof of this single isolated vertex case. This result is then extended in Section 2.4 to provide a proof of a special case involving at most two isolated vertices (the double isolated vertex case). In Section 2.5, the lemma of Section 2.3 is used to construct some simple functions that have the 'near' Golay property in that their out-of-phase auto-correlations sum to zero except at one shift. Some conclusions are drawn in Section 2.6. Note that Chapters 3 and 4 also contain material that relates to specific instances connected with Conjecture 1.

2.2 Introduction

Theorem 1.27 places an upper bound on the PMEPR of all codewords in any general second order coset of $RM_q(1, m)$, this being 2^{k+1} where k is the deletion index for the second order function concerned. In [32] it was noticed from computational data that the PMEPRs of the cosets of $RM_2(1, 4)$ for three specific binary functions were much less than that given by the theorem. The functions are

$$x_0x_1 + x_2x_3, \quad x_0x_2 + x_1x_3, \quad x_0x_3 + x_1x_2,$$

and have a deletion index of $k = 2$ since they all consist of 2 disjoint path 'segments', both vertices in one of the segments needing to be deleted to arrive at the conditions for Theorem 1.27. Thus the theorem gives an upper bound on the PMEPRs of 8, whereas in fact computation shows they have PMEPRs of approximately 3.1. Since applying any single deletion operation on the graphs of these functions results in a graph consisting of a path and a single *isolated* vertex, and that this single deletion appears to give the required bound of 4, it was conjectured in [32] that the second deletion operation was unnecessary. Based on this and further computational evidence, the following more general conjecture was made:

Conjecture 1 *Suppose $Q : \{0,1\}^m \to \mathbb{Z}_q$ is a quadratic form in variables $x_0, \ldots, x_{m-1}$ such that applying $k \geqslant 1$ deletion operations to $G(Q)$ removes all isolated vertices originally in $G(Q)$ and results in a graph that consists of a path and (possibly) new isolated vertices. Then all the words of the coset $Q + RM_q(1,m)$ have PMEPR at most 2^{k+1}.*

The only proof offered for this conjecture in [32] was for a special case where the graph obtained after applying $k \leqslant m-2$ deletion operations consists of a path and a single isolated vertex, and where an additional constraint was imposed over and above the conditions of the hypothesis, namely that every edge in the original graph $G(Q)$ incident with the final isolated vertex must have weight $q/2$ (henceforth this case is known as the *single isolated vertex case*). It is based around the same set used in the proof of Theorem 1.27, and is sufficient to give the lower value of 4 for the upper bound for the PMEPRs of the cosets of the three binary functions above. The proof in fact contained a small fallacy: a correct proof is given in Section 2.3 below, and which also indicates where the error in the proof in [32] occurred. Section 2.4 then gives a proof of a special case where $k \leqslant m-2$ deletions results in a path plus at most two isolated vertices, in what is called the *double isolated vertex case* (and again conditions apply to the weights of certain edges in the graph). This latter proof covers the single isolated vertex case, but uses a different complementary set, thus offering another proof of the single isolated vertex case.

2.3 Proof of Conjecture 1 for the Single Isolated Vertex Case

In this section the first special case proof of Conjecture 1 is given. This case is the single isolated vertex case, when the quadratic generalized Boolean function f, after applying $k \leqslant m-2$ deletion operations yields a graph which consists of a path and a single isolated vertex, and with the additional constraint that every edge in the original graph $G(f)$ incident with the final isolated vertex must have weight $q/2$.

First a lemma is proved, which is used in both the special case proofs and later in Section 2.5 to construct functions with a 'near' Golay property. The lemma establishes the following. Suppose that f is a function meeting the conditions for this case, i.e. after some k restrictions (equivalent to the deletion operations on the graph of f) the function consists of a path (and linear functions involving variables in the path) and a single linear term, equivalent to the isolated vertex. Form the cross-correlation function between the two functions produced by assigning both possible values to the additional restriction on the isolated variable. Then the sum of this cross-correlation, and the similar one for the function f plus one of the end points to the path, is zero everywhere except at one shift—this is because the cross-correlations basically behave as a pair of auto-correlations of a pair of complementary sequences satisfying Theorem 1.24.

Lemma 2.1. *Suppose that f and f', two generalized Boolean function over $\mathbb{Z}_q$ in the m variables $x_0, \ldots, x_{m-1}$, are such that for some $k \leqslant m-2$ restricting variables $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$, $f\big|_{\mathbf{x}=\mathbf{c}}$ and $f'\big|_{\mathbf{x}=\mathbf{c}}$ are given by*

$$\begin{aligned} f\big|_{\mathbf{x}=\mathbf{c}} &= P + L + g_\gamma x_\gamma + g \\ f'\big|_{\mathbf{x}=\mathbf{c}} &= P + \frac{q}{2}x_a + L + g_\gamma x_\gamma + g \end{aligned}$$

where

$$\begin{aligned} P &= \begin{cases} \dfrac{q}{2}\displaystyle\sum_{\alpha=0}^{m-k-3} x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}} & m-k \geqslant 3 \\ p x_{i_0} & m-k = 2 \end{cases} \\ L &= \sum_{\alpha=0}^{m-k-2} g_\alpha x_{i_\alpha}, \end{aligned}$$

and the indices $i_0, i_1, \ldots, i_{m-k-2}$ and γ are distinct, π is a permutation of $\{0, 1, \ldots, m-k-2\}$, and $p, g_\gamma, g, g_\alpha \in \mathbb{Z}_q$, $\alpha = 0, 1, \ldots, m-k-2$ (and in general the constants g_γ, g and the g_α (and hence L) depend on $\mathbf{c}$), and where x_a is either of the end points of the path P, i.e. $a = i_{\pi(0)}$ or $i_{\pi(m-k-2)}$ (and which are equal when the path is trivial). Then with $\mathbf{F}, \mathbf{F}'$ the vectors corresponding to f, f' respectively, and for fixed $\mathbf{c}$ and $d_1 \neq d_2$,

$$\begin{aligned} C(\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}, \mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2})(\ell) &+ C(\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}, \mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2})(\ell) \\ &= \begin{cases} \omega^{(d_1-d_2)g_\gamma}2^{m-k} & \ell = (d_2-d_1)2^\gamma \\ 0 & \textit{otherwise.} \end{cases} \end{aligned}$$

Proof. First note that the graph of $f\big|_{\mathbf{x}=\mathbf{c}}$ contains a path, due to P, and a single isolated vertex, γ: in the non-trivial case, when $m-k \geqslant 3$, the path has $m-k-2$ edges; and in the trivial case, $m-k=2$, the path is just a single vertex, and has no edges. In either case the further restriction on x_γ deletes the isolated vertex, leaving a function whose graph is just a path. Using Lemma 1.20, in terms of the truncated vectors, the sum of cross-correlations of the hypothesis becomes

$$\begin{aligned} &C([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell - (u_2 - u_1)) \\ &\qquad\qquad + C([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell - (u_2 - u_1)), \end{aligned}$$

for $(u_2 - u_1) - (n_{\mathbf{x}} - 1) \leqslant \ell \leqslant (u_2 - u_1) + (n_{\mathbf{x}} - 1)$, where u_1 is the index of the first non-zero entry in the vector $(\cdot)\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}$, u_2 that in $(\cdot)\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}$ and $n_{\mathbf{x}}$ the length of the pattern of non-zeroes in either such vector. For ℓ outside of this range, each cross-correlation is zero by the lemma, so the sum is zero too. For convenience write $\ell' = \ell - (u_2 - u_1)$, and thus we equivalently work with the expression

$$C([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell') + C([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell'), \tag{2.1}$$

for $-(n_{\mathbf{x}} - 1) \leqslant \ell' \leqslant (n_{\mathbf{x}} - 1)$. Next we note that

$$f\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2} = f\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1} + (d_2 - d_1)g_\gamma,$$

which means that the non-zero values in the vector $\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}$ are $\omega^{(d_2-d_1)g_\gamma}$ times those in the vector $\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}$, only shifted relative to each other, but for the truncated vectors we do in fact have

$$[\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}] = \omega^{(d_2-d_1)g_\gamma}[\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}].$$

Substituting this and the equivalent expression for $\mathbf{F}'$ into (2.1), we have, for all ℓ',

$$\begin{aligned}
C([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell') &+ C([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_2}])(\ell') \\
&= C([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], \omega^{(d_2-d_1)g_\gamma}[\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell') \\
&\quad + C([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], \omega^{(d_2-d_1)g_\gamma}[\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell') \\
&= \omega^{-(d_2-d_1)g_\gamma}\big(C([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell') + \\
&\qquad C([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}], [\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell')\big) \\
&= \omega^{(d_1-d_2)g_\gamma}\big(A([\mathbf{F}\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell') + A([\mathbf{F}'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}])(\ell')\big),
\end{aligned}$$

using Theorem 1.8 to factor the constant from the cross-correlations. The auto-correlations are of two truncated restricted vectors, for which the corresponding functions, $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}$ and $f'\big|_{\mathbf{x}x_\gamma=\mathbf{c}d_1}$, by the comments at the start of the proof, have graphs that are paths, and a is either a vertex of degree 1 in the path, or is the single vertex of the graph (in the trivial case when $m - k = 2$). Thus the functions satisfy the conditions of Theorem 1.24 and hence are a Golay complementary pair. Then from the discussion following Lemma 1.20, the truncated vectors are also a Golay complementary pair, and as such the auto-correlations sum to zero everywhere except at the zero shift, $\ell' = 0$, where they equal $2^{m-(k+1)+1} = 2^{m-k}$. Thus the truncated cross-correlations sum to zero everywhere except for shift $\ell' = 0$ where the value is $\omega^{(d_1-d_2)g_\gamma}2^{m-k}$. The untruncated cross-correlations thus sum to zero everywhere except at shift $\ell - (u_2 - u_1) = 0$, i.e. when $\ell = u_2 - u_1$, with the same non-zero value and where u_1 and u_2 are determined by $\mathbf{x}, x_\gamma, \mathbf{c}$ and d_1 or d_2 respectively. From equation (1.8) these are:

$$u_1 = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + d_1 2^\gamma$$
$$u_2 = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + d_2 2^\gamma,$$

where $\mathbf{c} = c_0 c_1 \cdots c_{k-1}$. Hence

$$u_2 - u_1 = (d_2 - d_1)2^\gamma.$$

Therefore the cross-correlation sum is only non-zero at shift $\ell = (d_2 - d_1)2^\gamma$ where the value is $\omega^{(d_1-d_2)g_\gamma}2^{m-k}$, and the lemma is proved. □

The property of this result that is useful in the following proof is that whilst the non-zero value of the sum of the correlations depends on $\mathbf{c}$ (via g_γ), the shift at which it occurs does not.

A proof of Conjecture 1 for the single isolated vertex case is now given—it is essentially that given in [32], but adapted for notational usage in the current context, and also correcting the small fallacy contained therein.

Proof of Conjecture 1 for the single isolated vertex case. Let f be a function satisfying the single isolated vertex case, i.e. the graph obtained after applying $k \leqslant m-2$ deletion operations to the graph of f consists of a path and a single isolated vertex, and where every edge in the original graph incident with the final isolated vertex has weight $q/2$. Write $f = Q + L$ where Q is the quadratic part of f, and L is an affine function of $x_0, \ldots, x_{m-1}$. Let $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$ be the labels of the vertices deleted from $G(f)$, and let G be the resulting graph. When $k < m-2$, G contains a non-trivial path and an isolated vertex: we let a be one of the path end points, and label the isolated vertex j_k. When $k = m-2$, the graph G contains a trivial path and the isolated vertex, and so will just consist of two vertices of degree 0: we label one as a and the other as j_k (consistent with the weight requirements on the edges to j_k in the original graph). As in the proof of Theorem 1.27 we claim that the 2^{k+1} vectors corresponding to the functions

$$f + \frac{q}{2}\Big(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + dx_a\Big), \quad d, d_\alpha \in \{0,1\}$$

form a Golay complementary set. From this it follows that the PMEPR of the coset $Q + RM_q(1,m)$ is at most 2^{k+1}.

Following the proof of Theorem 1.27, the restricting variables equivalent to the deletions are $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$, and let $\mathbf{d} = d_0 d_1 \cdots d_{k-1}$, so that we can write $\mathbf{d}\cdot\mathbf{x} = \sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha}$. Then the 2^{k+1} functions are

$$f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a),$$

and let the vectors equivalent to these be

$$\mathbf{F}_{\mathbf{d}d}\,.$$

Then we need to show that

$$\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell) = 0, \quad \text{for } \ell \neq 0.$$

Restrict over the variables in $\mathbf{x}$ and expand using Corollary 1.16 to obtain

$$\begin{aligned}\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell) &= \sum_{\mathbf{d},d}\sum_{\mathbf{c}} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}})(\ell)\\ &\quad + \sum_{\mathbf{d},d}\sum_{\mathbf{c}_1\neq\mathbf{c}_2} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell)\\ &= S_1 + S_2 \text{ say.}\end{aligned}$$

Re-arrange sum S_2 as

$$S_2 = \sum_{d}\sum_{\mathbf{c}_1\neq\mathbf{c}_2}\sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell).$$

The functions corresponding to the vectors $\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_i}$, $i = 1$ or 2, in the inner sum may be written as

$$\big((f + \frac{q}{2}dx_a) + \frac{q}{2}\mathbf{d}\cdot\mathbf{x}\big)\big|_{\mathbf{x}=\mathbf{c}_i},$$

and with fixed d and fixed $\mathbf{c}_1 \neq \mathbf{c}_2$, are seen to satisfy the conditions of Lemma 1.26, and so the inner sum

$$\sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell)$$

is zero for all ℓ, and hence so also is S_2. For S_1 do a further restriction on the isolated vertex x_{j_k} using Corollary 1.16 to obtain

$$\begin{aligned}S_1 &= \sum_{\mathbf{d},d}\sum_{\mathbf{c}}\sum_{c'} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'})(\ell)\\ &\quad + \sum_{\mathbf{d},d}\sum_{\mathbf{c}}\sum_{c'_1\neq c'_2} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell)\\ &= S_1^* + S_2^* \text{ say.}\end{aligned}$$

Consider the re-arranged sum S_1^*:

$$S_1^* = \sum_{\mathbf{d}}\sum_{\mathbf{c}}\sum_{c'}\sum_{d} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'})(\ell).$$

The functions corresponding to the vectors in the sum are

$$\big(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a)\big)\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'},$$

and have graphs which are paths, since the graph G is a path with an isolated vertex, and the extra restriction removes the isolated vertex, and a is either a vertex of degree 1 in this graph, or is the single vertex of the graph (in the trivial case when $k = m - 2$). Thus by Theorem 1.24, for fixed $\mathbf{c}$ and c', the pair of functions over $d = 0$ and 1, namely

$$\left(f + \frac{q}{2}\mathbf{d}\cdot\mathbf{x}\right)\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'} \text{ and } \left(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + x_a)\right)\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'}$$

form a Golay complementary pair and hence

$$\sum_{d} A(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'})(\ell) = 0, \quad \text{for } \ell \neq 0,$$

thus in turn giving $S_1^* = 0$, $\ell \neq 0$.

Now consider the re-arranged sum S_2^*:

$$S_2^* = \sum_{\mathbf{d},d}\ \sum_{c_1' \neq c_2'}\ \sum_{\mathbf{c}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_1'}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_2'})(\ell).$$

It is here that the fallacy in the original proof in [32] creeps in. Since the vertex j_k is isolated by the deletion operations, in the function f the only second order terms involving variable x_{j_k} are those with the variables of the delete indices, and there may also be a linear term. Thus the only terms in x_{j_k} in f are

$$\sum_{\alpha=0}^{k-1} q_{j_\alpha j_k} x_{j_\alpha} x_{j_k} + g_{j_k} x_{j_k},$$

where $g_{j_k} \in \mathbb{Z}_q$ is the coefficient of x_{j_k} in L, and the $q_{j_\alpha j_k}$ are the weights of the edges between the delete vertices and the isolated vertex, which by assumption are either 0 or $q/2$, and they are not all zero since j_k was not an isolated vertex in the original graph $G(Q)$. For fixed $\mathbf{d}$ and d, by substituting $\mathbf{x} = \mathbf{c}$, where $\mathbf{c} = c_0 c_1 \cdots c_{k-1}$, and $x_{j_k} = c_i'$ into the expression $f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a)$, and gathering together those terms involving just the c_i', we can write the restricted functions $\left(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a)\right)\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'}$, which are equivalent to the vectors $\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'}$ appearing in sum S_2^*, in the following way:

$$\begin{aligned}\left(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a)\right)\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'} &= f'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'} + \left(\sum_{\alpha=0}^{k-1} q_{j_\alpha j_k} c_\alpha + g_{j_k}\right) c_i' \\ &= f'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'} + g_c c_i', \quad \text{say,}\end{aligned}$$

for $i = 1$ or 2, where

$$g_c = \sum_{\alpha=0}^{k-1} q_{j_\alpha j_k} c_\alpha + g_{j_k},$$

and where the restricted function $f'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'}$ consists of the path and linear terms in the path variables, and in particular does not involve c_i' (but for emphasis we leave the restriction notation in). Thus the non-zero values in the vector $\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'}$ are $\omega^{g_c c_i'}$ times those in the vector $\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_i'}$. Using Theorem 1.8

then we get, for all ℓ,

$$\begin{aligned}\sum_{\mathbf{c}} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell) \\ &= \sum_{\mathbf{c}} C(\omega^{g_c c'_1}\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \omega^{g_c c'_2}\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell) \\ &= \sum_{\mathbf{c}} \omega^{g_c(c'_1-c'_2)} C(\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell).\end{aligned}$$

The argument in [32] effectively attempts to factorize this last expression as

$$C(\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell) \sum_{\mathbf{c}} \omega^{g_c(c'_1-c'_2)},$$

and then uses an argument similar to that given below to show that the inner sum, $\sum_{\mathbf{c}} \omega^{g_c(c'_1-c'_2)}$ with $c'_1 \neq c'_2$, is zero. It is the factorization that is incorrect: in general in f there will be second order terms involving delete variables and path variables, and the restriction $\mathbf{x} = \mathbf{c}$ means that these turn into linear terms, with the c_α as coefficients, in the function $f'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_i}$. Hence the correlations $C(\mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}'\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell)$ have a strong dependence on $\mathbf{c}$, and so they cannot be taken through the sum.

This is rectified by using the lemma. For fixed $\mathbf{c}$ and $\mathbf{d}$, and by taking $d = 0$ and 1, the pair of functions

$$\big(f + \frac{q}{2}\mathbf{d}\cdot\mathbf{x}\big)\big|_{\mathbf{x}=\mathbf{c}} \text{ and } \big(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + x_a)\big)\big|_{\mathbf{x}=\mathbf{c}}$$

may be written as

$$f\big|_{\mathbf{x}=\mathbf{c}} + \frac{q}{2}\mathbf{d}\cdot\mathbf{c} \text{ and } f\big|_{\mathbf{x}=\mathbf{c}} + \frac{q}{2}\mathbf{d}\cdot\mathbf{c} + \frac{q}{2}x_a.$$

By the hypothesis, $f\big|_{\mathbf{x}=\mathbf{c}}$ consists of a path and an isolated vertex (index j_k), and the pair of functions thus satisfy the conditions of Lemma 2.1, and so for fixed $\mathbf{c}, \mathbf{d}$ and $c'_1 \neq c'_2$

$$\sum_{d} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell) = \begin{cases} \omega^{(c'_1-c'_2)g_c}2^{m-k} & \ell = (c'_2 - c'_1)2^{j_k} \\ 0 & \text{otherwise,} \end{cases}$$

where, as shown above,

$$g_c = \sum_{\alpha=0}^{k-1} q_{j_\alpha j_k} c_\alpha + g_{j_k}$$

is the coefficient of x_{j_k} in $f\big|_{\mathbf{x}=\mathbf{c}}$. Note that, crucially, the only shift at which the sum is non-zero does not depend on $\mathbf{c}$, and thus we have that

$$\begin{aligned}\sum_{\mathbf{c}}\sum_{d} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c'_2})(\ell) \\ &= \begin{cases} \sum_{\mathbf{c}} \omega^{(c'_1-c'_2)g_c}2^{m-k} = \sum_{\mathbf{c}} \omega_c \quad \text{say,} & \ell = (c'_2 - c'_1)2^{j_k} \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

It is at this point that the additional constraint over the conditions of the hypothesis of the conjecture comes into play, namely that every edge in the original graph of $G(f)$ incident with the final isolated vertex must have weight $q/2$. This means that each $q_{j_\alpha j_k}$ is 0 or $\frac{q}{2}$ and they are not all zero, and thus writing g_c as

$$g_c = \frac{q}{2} \sum_{\alpha : q_{j_\alpha j_k} \neq 0} c_\alpha + g_{j_k}$$

we see that $\sum_{q_{j_\alpha j_k} \neq 0} c_\alpha$ is just a non-zero linear Boolean function in the c_α, which by Lemma 1.12, will take the values 0 and 1 equally often as $\mathbf{c}$ varies. Thus g_c takes the value g_{j_k} or $g_{j_k} + \frac{q}{2}$ equally often as $\mathbf{c}$ varies, and in turn,

$$w_c = \omega^{(c_1'-c_2')g_{j_k}} 2^{m-k} \text{ or } -\omega^{(c_1'-c_2')g_{j_k}} 2^{m-k}$$

equally often, thus giving

$$\sum_{\mathbf{c}} \sum_{d} C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_1'}, \mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{j_k}=\mathbf{c}c_2'})(\ell) = 0 \quad \text{for all } \ell$$

(and note that its the negative terms caused by the $\frac{q}{2}$ values of the $q_{j_\alpha j_k}$ that make the sum zero). Thus reordering the summations in S_2^* gives $S_2^* = 0$ for all ℓ. Therefore

$$\sum_{\mathbf{d},d} A(\mathbf{F}_{\mathbf{d}d})(\ell) = 0, \quad \text{for } \ell \neq 0,$$

and the set of functions is a Golay complementary set as claimed. □

2.4 Proof of Conjecture 1 for the Double Isolated Vertex Case

In this section the second special case proof of Conjecture 1 is given. This case is (nominally) the *double isolated vertex case*, when the quadratic generalized Boolean function f, after applying $k \leqslant m-2$ deletion operations yields a graph which consists of a path and at most two isolated vertices, and where again additional constraints must be imposed over the conditions of the hypothesis of the conjecture: in this case, in the original graph $G(f)$ there must be

(i) a delete vertex with an edge of weight $q/2$ to one of the isolated vertices, and

(ii) any edges from the remaining delete vertices to the other isolated vertex must have weight $q/2$.

The proof also covers the single isolated vertex case, but uses a different complementary set to the proof of that case given above. In this proof, for the single isolated vertex, condition (i) above holds for the single isolated vertex, and condition (ii) is empty. As condition (i) above is less restrictive than the conditions for the first proof, this proof is a better result, covering a more general case. It follows the same idea as that above, i.e. repeatedly expanding a sum of auto-correlation functions using Corollary 1.16 and showing that each component sum is zero, but due to the extra isolated vertex, it requires that this be done more times.

Proof of Conjecture 1 for the double isolated vertex case. Let v be the number of isolated vertices, so $v = 1$ or 2, and let f be a function satisfying this case, i.e. the graph obtained after applying $k \leqslant m - (v+1)$ deletion operations to the graph of f consists of a path and v isolated vertices, and which meets the weight conditions above (which are detailed further below). Write $f = Q + L$ where Q is the quadratic part of f, and L is an affine function of $x_0, \ldots, x_{m-1}$. Let $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$ be the indices of the vertices deleted from $G(f)$, and let G be the resulting graph; let $h_0, \ldots, h_{v-1}$, where $0 \leqslant h_0 < \cdots < h_{v-1} \leqslant m-1$, be the indices of the isolated vertices; and let $i_0, i_1, \ldots i_{m-k-v-1}$, where $0 \leqslant i_0 < i_1 < \cdots < i_{m-k-v-1} \leqslant m-1$ be the indices of the $m-k-v$ remaining variables (which form the path). Then for a single isolated vertex, $v = 1$: when $k \leqslant m-3$, the graph G contains a non-trivial path and an isolated vertex, so we take a to be the index of one of the path end points, and the isolated vertex is labelled h_0; when $k = m-2$, G contains a trivial path and a single isolated vertex, and so just consists of two vertices of degree zero, and we label one as a and the other as h_0. For two isolated vertices, $v = 2$: when $k \leqslant m-4$ the graph G contains a non-trivial path and two isolated vertices, and we take a to be one of the path end points, and the isolated vertices are labelled h_0 and h_1; when $k = m-3$, G contains a trivial path and the two isolated vertices, and so just consists of three vertices of degree 0, and we label one as a, and the others as h_0 and h_1. (Note that labelling of the isolated vertices must be consistent with the weight requirements on the edges in the original graph.)

In the graph $G(f)$, an edge between vertex i and j has weight $q_{ij} \in \mathbb{Z}_q$ if the term $q_{ij}x_ix_j$ appears in Q. To meet the weight conditions on the edges for this special case, it must be possible to select one of the isolated vertices, h_b say, with $b = 0$ or 1, and one of the delete vertices, j_e, $e \in \{0, 1, \ldots, k-1\}$ for which $q_{j_e h_b} = q/2$ and for $\gamma \neq b$, $q_{j_\alpha h_\gamma} = 0$ or $q/2$ for $\alpha = 0, 1, \ldots, k-1$, $\alpha \neq e$. The delete vertex j_e is 'excluded' from the set that follows. Then we claim that the 2^{k+1} vectors corresponding to the functions

$$f + \frac{q}{2}\left(\sum_{\substack{\alpha=0\\ \alpha\neq e}}^{k-1} d_\alpha x_{j_\alpha} + dx_a + d_{h_b}x_{h_b}\right), \text{ where } d_\alpha, d, d_{h_b} \in \{0,1\},$$

form a Golay complementary set: it then follows that all words of the coset $Q + RM_q(1, m)$ have PMEPR at most 2^{k+1}.

Using similar notation to that used previously, let

$$\begin{aligned}\mathbf{x} &= x_{j_0}x_{j_1}\cdots x_{j_{e-1}}x_{j_{e+1}}\cdots x_{j_{k-1}}\\ \mathbf{d} &= d_0d_1\cdots d_{e-1}d_{e+1}\cdots d_{k-1},\end{aligned}$$

i.e. the index of the excluded delete vertex is not included, then put

$$\mathbf{d}\cdot\mathbf{x} = \sum_{\substack{\alpha=0\\ \alpha\neq e}}^{k-1} d_\alpha x_{j_\alpha}.$$

The 2^{k+1} functions are then

$$f + \frac{q}{2}(\mathbf{d} \cdot \mathbf{x} + dx_a + d_{h_b} x_{h_b}), \tag{2.2}$$

and let the vectors equivalent to these be

$$\mathbf{F}_{\mathbf{d}dd_{h_b}}.$$

Thus it is required to show that

$$\sum_{\mathbf{d},d,d_{h_b}} A(\mathbf{F}_{\mathbf{d}dd_{h_b}})(\ell) = 0, \text{ for } \ell \neq 0.$$

Restrict over the variables in $\mathbf{x}$ and use Corollary 1.16 to obtain:

$$\begin{aligned}\sum_{\mathbf{d},d,d_{h_b}} A(\mathbf{F}_{\mathbf{d}dd_{h_b}})(\ell) &= \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}} A(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}})(\ell) \\ &\quad + \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_2})(\ell) \\ &= S_1 + S_2 \text{ say.}\end{aligned}$$

Re-arrange sum S_2 as

$$S_2 = \sum_{d,d_{h_b}} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_2})(\ell).$$

The functions corresponding to the vectors $\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_i}$, $i = 1$ or 2, in the inner sum may be written as

$$\left((f + \frac{q}{2}(dx_a + d_{h_b} x_{h_b})) + \frac{q}{2}\mathbf{d} \cdot \mathbf{x}\right)\Big|_{\mathbf{x}=\mathbf{c}_i},$$

and with fixed d, d_{h_b} and $\mathbf{c}_1 \neq \mathbf{c}_2$, are seen to satisfy the conditions of Lemma 1.26, and so the inner inner sum

$$\sum_{\mathbf{d}} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}=\mathbf{c}_2})(\ell)$$

is zero for all ℓ, and hence so also is S_2. For S_1, do a further restriction on the isolated vertex h_b, i.e. restrict on x_{h_b}. As before using Corollary 1.16:

$$\begin{aligned}S_1 &= \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}} \sum_{c'} A(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}=\mathbf{c}c'})(\ell) \\ &\quad + \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}} \sum_{c'_1 \neq c'_2} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell) \\ &= S_1^* + S_2^* \text{ say.}\end{aligned}$$

Consider the re-arranged sum S_2^* first:

$$S_2^* = \sum_{\mathbf{d},d} \sum_{\mathbf{c}} \sum_{c'_1 \neq c'_2} \sum_{d_{h_b}} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell).$$

In the restricted functions equivalent to the restricted vectors in this sum, separate out the term involving d_{h_b} to get

$$\begin{aligned}\big(f+\frac{q}{2}(\mathbf{d}\cdot\mathbf{x}+dx_a+d_{h_b}x_{h_b})\big)\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_i}&\\ &=\big(f+\frac{q}{2}(\mathbf{d}\cdot\mathbf{x}+dx_a)\big)\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_i}+\frac{q}{2}d_{h_b}c'_i,\end{aligned}$$

for $i = 1$ or 2. Thus for fixed $\mathbf{d}, d, \mathbf{c}$ and c'_i, the values in the vector $\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_i}$ are just $\omega^{\frac{q}{2}d_{h_b}c'_i}$ times those in vector $\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_i}$, the vector associated with the function $\big(f+\frac{q}{2}(\mathbf{d}\cdot\mathbf{x}+dx_a)\big)\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_i}$, which has no dependence on d_{h_b}. Then, using Theorem 1.8, we get for all ℓ,

$$\begin{aligned}\sum_{d_{h_b}}C(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)&\\ &=\sum_{d_{h_b}}C(\omega^{\frac{q}{2}d_{h_b}c'_1}\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\omega^{\frac{q}{2}d_{h_b}c'_2}\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)\\ &=\sum_{d_{h_b}}\omega^{\frac{q}{2}d_{h_b}(c'_1-c'_2)}C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)\\ &=C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)\sum_{d_{h_b}}\omega^{\frac{q}{2}d_{h_b}(c'_1-c'_2)}\\ &=C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)(\omega^0+\omega^{\frac{q}{2}(c'_1-c'_2)})\\ &=C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)(1+\omega^{\pm\frac{q}{2}})\\ &=C(\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_1},\mathbf{F}_{\mathbf{d}d}\big|_{\mathbf{x}x_{h_b}=\mathbf{c}c'_2})(\ell)(1-1)\\ &=0,\end{aligned}$$

using the fact that since the only values for c'_1 and c'_2 are 0 and 1, and they are not equal, $c'_1 - c'_2 = \pm 1$, and so in either case $\omega^{\frac{q}{2}(c'_1-c'_2)} = \omega^{\pm\frac{q}{2}} = -1$. Thus the sum S^*_2 is zero for all ℓ.

Apply Corollary 1.16 again and expand S^*_1 by restricting on the last remaining delete variable, x_{j_e}:

$$\begin{aligned}S^*_1=&\sum_{\mathbf{d},d,d_{h_b}}\sum_{\mathbf{c}}\sum_{c'}\sum_{c''}A(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''})(\ell)\\ &+\sum_{\mathbf{d},d,d_{h_b}}\sum_{\mathbf{c}}\sum_{c'}\sum_{c''_1\neq c''_2}C(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1},\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell)\\ =&\ S^{**}_1+S^{**}_2\text{ say.}\end{aligned}$$

Consider the re-arranged sum S^{**}_2:

$$S^{**}_2=\sum_{\mathbf{d},d,d_{h_b}}\sum_{\mathbf{c}}\sum_{c''_1\neq c''_2}\sum_{c'}C(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1},\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell).$$

Similar to above, for the restricted function associated with the vector in the sum, for any $\mathbf{d}, d, d_{h_b}, \mathbf{c}, c''_i$ and c', gather together all the terms that involve c', i.e. those that emanate from the restriction on the isolated vertex h_b: this may only be connected to the vertices which are deleted in the graph $G(f)$, so Q has terms $q_{j_\alpha h_b} x_{j_\alpha} x_{h_b}$, say, for all α, and let g_{h_b} be the coefficient of x_{h_b} in L, thus giving

$$\begin{aligned}
&\left(f + \frac{q}{2}(\mathbf{d} \cdot \mathbf{x} + dx_a + d_{h_b} x_{h_b})\right)\Big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i} \\
&\qquad = f'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i} + \sum_{\alpha \neq e} q_{j_\alpha h_b} c_\alpha c' + q_{j_e h_b} c' c''_i + g_{h_b} c' + \frac{q}{2} d_{h_b} c' \\
&\qquad = f'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i} + g_{c'} + q_{j_e h_b} c' c''_i,
\end{aligned}$$

for $i = 1$ or 2, where

$$g_{c'} = \sum_{\alpha \neq e} q_{j_\alpha h_b} c_\alpha c' + g_{h_b} c' + \frac{q}{2} d_{h_b} c',$$

and where $f'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i}$ consists of the path and linear terms in the path variables, and includes the $\frac{q}{2}(\mathbf{d} \cdot \mathbf{c} + dx_a)$ term, but specifically does not involve c'. Thus the values of the vector $\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i}$ are just $\omega^{g_{c'} + q_{j_e h_b} c' c''_i}$ times those in the vector $\mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i}$, the vector associated with the function $f'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_i}$. Thus, using Theorem 1.8, for all ℓ,

$$\begin{aligned}
&\sum_{c'} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1}, \mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell) \\
&\qquad = \sum_{c'} C(\omega^{g_{c'} + q_{j_e h_b} c' c''_1} \mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1}, \omega^{g_{c'} + q_{j_e h_b} c' c''_2} \mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell) \\
&\qquad = \sum_{c'} \omega^{q_{j_e h_b} c'(c''_1 - c''_2)} C(\mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1}, \mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell) \\
&\qquad = C(\mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1}, \mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell) \sum_{c'} \omega^{q_{j_e h_b} c'(c''_1 - c''_2)} \\
&\qquad = C(\mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_1}, \mathbf{F}'\big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''_2})(\ell)(\omega^0 + \omega^{\frac{q}{2}(c''_1 - c''_2)}) \\
&\qquad = 0,
\end{aligned}$$

since, by assumption, $q_{j_e h_b}$ is $q/2$, and arguing as before, $c''_1 - c''_2$ is always ± 1 (this is the extra weight condition (i) that was imposed). Thus the sum S_2^{**} is zero for all ℓ.

At this point, if $v = 1$ and we have just a *single* isolated vertex h_b, from the comments at the start of the proof, for any $\mathbf{d}, d_{h_b}, c'$ and c'', we note that the function

$$\left(f + \frac{q}{2}(\mathbf{d} \cdot \mathbf{x} + d_{h_b} x_{h_b})\right)\Big|_{\mathbf{x}x_{h_b}x_{j_e}=\mathbf{c}c'c''}$$

has a graph which is a path, since it was originally a path (either trivial or non-trivial) with an isolated vertex, and the restriction on x_{h_b} has deleted that isolated vertex. The vertex labelled a is either the single vertex of the graph, or a vertex of degree 1 in the path, and in addition, any linear terms only involve the variables in the path. Therefore the conditions of Theorem 1.24 are met, and the functions

$$(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + d_{h_b}x_{h_b}))\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''}$$

and

$$(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + x_a + d_{h_b}x_{h_b}))\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''}$$

form a Golay complementary pair, so

$$\sum_{d} A(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''})(\ell) = 0, \quad \text{for } \ell \neq 0,$$

and thus by reordering the summations in S_1^{**}, it is also zero when $\ell \neq 0$. Thus the original sum,

$$\sum_{\mathbf{d},d,d_{h_b}} A(\mathbf{F}_{\mathbf{d}dd_{h_b}})(\ell) = 0, \text{ for } \ell \neq 0,$$

as required, and the set of 2^{k+1} functions specified forms a complementary set, thus yielding another proof of Conjecture 1 for the special case of the single isolated vertex.

However for the double isolated vertex case, i.e. $v = 2$, we need to make a *further* expansion using Corollary 1.16, by restricting on the second isolated vertex, x_{h_γ}:

$$\begin{aligned}
S_1^{**} = & \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}}\sum_{c'}\sum_{c''}\sum_{c'''} A(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''})(\ell) \\
& + \sum_{\mathbf{d},d,d_{h_b}} \sum_{\mathbf{c}}\sum_{c'}\sum_{c''} \sum_{c_1'''\neq c_2'''} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_1'''}, \\
& \qquad\qquad\qquad\qquad \mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_2'''})(\ell) \\
= & \; S_1^{***} + S_2^{***} \text{ say.}
\end{aligned}$$

Again consider the second sum, S_2^{***}, first. The function $f\big|_{\mathbf{x}x_{je}=\mathbf{c}c''}$ is obtained by performing all the deletion operations on f, and so by hypothesis, has a graph which is a path (either trivial or non-trivial) plus two isolated vertices. The extra restriction on the isolated vertex h_b, gives the function $f\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''}$, which thus has a graph which is a path plus a single isolated vertex. Thus writing the functions

$$(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a + d_{h_b}x_{h_b}))\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''}$$

with $d = 0$ and 1 as

$$f\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''} + \frac{q}{2}(\mathbf{d}\cdot\mathbf{c} + d_{h_b}c')$$

and

$$f\big|_{\mathbf{x}x_{h_b}x_{je}=\mathbf{c}c'c''} + \frac{q}{2}(\mathbf{d}\cdot\mathbf{c} + x_a + d_{h_b}c')$$

gives a pair of functions satisfying the conditions of Lemma 2.1, and so for fixed $\mathbf{d}, d_{h_b}, \mathbf{c}, c', c''$ and $c_1''' \neq c_2'''$

$$\sum_{d} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_1'''}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_2'''})(\ell)$$
$$= \begin{cases} \omega^{(c_1'''-c_2''')g_c}2^{m-k-1} & \ell = (c_2''' - c_1''')2^{h_\gamma} \\ 0 & \text{otherwise,} \end{cases}$$

where g_c is derived from the coefficient of x_{h_γ} in f, as shown below. Since the only shift at which the sum is non-zero does not depend on $\mathbf{c}$, we have that

$$\sum_{\mathbf{c}}\sum_{d} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_1'''}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_2'''})(\ell)$$
$$= \begin{cases} \sum_{\mathbf{c}} \omega^{(c_1'''-c_2''')g_c}2^{m-k-1} = \sum_{\mathbf{c}} \omega_c \quad \text{say,} & \ell = (c_2''' - c_1''')2^{h_\gamma} \\ 0 & \text{otherwise.} \end{cases}$$

To derive g_c, as h_γ is an isolated vertex, it can only make second order terms in f with the delete variables, and there may also be a linear term:

$$\sum_{\substack{\alpha=0 \\ \alpha\neq e}}^{k-1} q_{j_\alpha h_\gamma}x_{j_\alpha}x_{h_\gamma} + q_{j_e h_\gamma}x_{j_e}x_{h_\gamma} + g_{h_\gamma}x_{h_\gamma}.$$

Substituting the appropriate restricting constants gives

$$g_c = \sum_{\substack{\alpha=0 \\ \alpha\neq e}}^{k-1} q_{j_\alpha h_\gamma}c_\alpha + q_{j_e h_\gamma}c'' + g_{h_\gamma}.$$

By assumption each $q_{j_\alpha h_\gamma}$ is 0 or $q/2$ and they are not all zero since h_γ is not isolated in the original graph $G(f)$, and thus writing g_c as

$$g_c = \frac{q}{2} \sum_{\substack{\alpha:\alpha\neq e \\ q_{j_\alpha h_\gamma}\neq 0}} c_\alpha + q_{j_e h_\gamma}c'' + g_{h_\gamma}$$

we see that

$$\sum_{\substack{\alpha:\alpha\neq e \\ q_{j_\alpha h_\gamma}\neq 0}} c_\alpha$$

is just a non-zero linear Boolean function in the c_α, which by Lemma 1.12, will take the values 0 and 1 equally often as $\mathbf{c}$ varies. Thus g_c takes the value $q_{j_e h_\gamma}c'' + g_{h_b}$ or $q_{j_e h_\gamma}c'' + g_{h_b} + q/2$ equally often as $\mathbf{c}$ varies, and in turn,

$$w_c = \omega^{(c_1'''-c_2''')(q_{j_e h_\gamma}c''+g_{h_b})}2^{m-k-1} \text{ or } -\omega^{(c_1'''-c_2''')(q_{j_e h_\gamma}c''+g_{h_b})}2^{m-k-1}$$

equally often, thus giving, for all ℓ,

$$\sum_{\mathbf{c}}\sum_{d} C(\mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_1'''}, \mathbf{F}_{\mathbf{d}dd_{h_b}}|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c_2'''})(\ell) = 0,$$

as the shift at which the non-zero values w_c occur is independent of $\mathbf{c}$. It is at this point that reason for imposition of the extra weight condition (ii) occurs: the coefficients $q_{j_\alpha h_\gamma}$ need to be either 0 or $q/2$ in order for the above argument to work. Thus reordering the summations in S_2^{***} gives $S_2^{***} = 0$ for all ℓ.

Finally to sum S_1^{***}. Further to the discussion for S_2^{***} above, the extra restriction on the other isolated vertex h_γ means that the function $f\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''}$ has a graph which is a path (which may be either trivial or non-trivial), and which involves only linear terms in the variables in the path. Thus for every fixed $\mathbf{d}, d_{h_b}, \mathbf{c}, c', c''$ and c''' writing the functions

$$(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a + d_{h_b}x_{h_b}))\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''}$$

with $d = 0$ and 1 as

$$f\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''} + \frac{q}{2}(\mathbf{d}\cdot\mathbf{c} + d_{h_b}c')$$

and

$$f\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''} + \frac{q}{2}(\mathbf{d}\cdot\mathbf{c} + x_a + d_{h_b}c'))$$

gives a pair of functions satisfying Theorem 1.24, i.e. they form a Golay complementary pair and thus

$$\sum_d A(\mathbf{F}_{\mathbf{d}dd_{h_b}}\big|_{\mathbf{x}x_{h_b}x_{je}x_{h_\gamma}=\mathbf{c}c'c''c'''})(\ell) = 0, \quad \text{for } \ell \neq 0.$$

Thus by reordering the summations within it, the sum S_1^{***} is zero for $\ell \neq 0$. Then the original sum,

$$\sum_{\mathbf{d},d,d_{h_b}} A(\mathbf{F}_{\mathbf{d}dd_{h_b}})(\ell) = 0, \text{ for } \ell \neq 0,$$

as required, and the set of 2^{k+1} functions specified forms a complementary set, thus completing the proof for the double isolated vertex special case. □

Example 2.2. As an example, take the following function f in the 7 variables $x_0, x_1, \ldots, x_6$ over $\mathbb{Z}_6$:

$$\begin{aligned} f = {} & 3(x_0x_1 + x_1x_2) + 2x_3x_6 + 3x_3x_5 + 3x_4x_6 + 5x_4x_5 \\ & + x_0x_6 + 2x_1x_6 + 3x_2x_6 + 2x_5x_6 + 4x_0x_5 + 5x_1x_5 + 4x_2x_5. \end{aligned}$$

The graph of f is shown in Figure 2.1. Choose vertices 5 and 6 to be the delete vertices: this then leaves vertices 3 and 4 isolated, and the path $3(x_0x_1 + x_1x_2)$. Choose 3 to be the isolated vertex in the set $(= h_b)$ and 5 to be the delete vertex excluded from the set $(= j_e)$, so that the other isolated vertex is 4 $(=h_\gamma)$, and the remaining delete vertex is 6. Then the coefficients of x_3x_5 (selected isolate to excluded delete) and x_4x_6 (the remaining delete to the other isolate) are both 3, and so the function satisfies the hypothesis. Choose end point x_2 of the path, then the complementary set is

$$f + 3(ax_6 + bx_2 + cx_3), \quad a, b, c \in \{0, 1\},$$

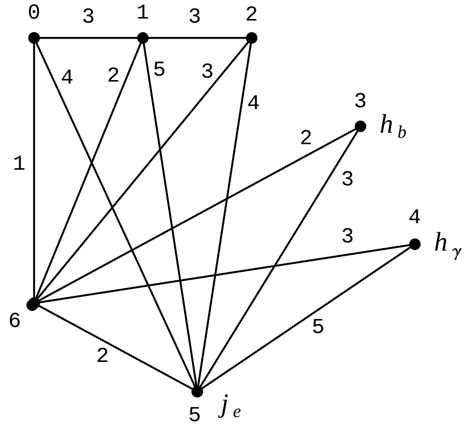

Figure 2.1: The graph for Example 2.2

for all combinations of a, b and c, and direct computation confirms that the sum across the functions of the out of phase auto-correlation functions does indeed yield zero—samples of the auto-correlations at a few shifts are:

$\ell =$	46	47	48	49
$f :$	$3\quad,$	$\frac{1}{2}(-5+5i\sqrt{3}),$	$0,$	$\frac{1}{2}(-13-5i\sqrt{3})$
$f+3x_2 :$	$-1+6i\sqrt{3},$	$\frac{1}{2}(-9+9i\sqrt{3}),$	$0,$	$\frac{1}{2}(-15-3i\sqrt{3})$
$f+3x_6 :$	$-i\sqrt{3},$	$\frac{1}{2}(-1-7i\sqrt{3}),$	$0,$	$\frac{1}{2}(7+3i\sqrt{3})$
$f+3x_3 :$	$6+3i\sqrt{3},$	$\frac{1}{2}(-11+11i\sqrt{3}),$	$0,$	$\frac{1}{2}(-5-i\sqrt{3})$
$f+3(x_2+x_6) :$	$-2-5i\sqrt{3},$	$\frac{1}{2}(15-7i\sqrt{3}),$	$0,$	$\frac{1}{2}(21+5i\sqrt{3})$
$f+3(x_2+x_3) :$	$-4+3i\sqrt{3},$	$\frac{1}{2}(-3+3i\sqrt{3}),$	$0,$	$\frac{1}{2}(-23-7i\sqrt{3})$
$f+3(x_6+x_3) :$	$-9-2i\sqrt{3},$	$\frac{1}{2}(17-9i\sqrt{3}),$	$0,$	$\frac{1}{2}(11+3i\sqrt{3})$
$f+3(x_2+x_6+x_3) :$	$7-4i\sqrt{3},$	$\frac{1}{2}(-3-5i\sqrt{3}),$	$0,$	$\frac{1}{2}(17+5i\sqrt{3})$

Adding down the columns is seen to give zero. Figure 2.2 shows the envelope power of a randomly chosen word in the coset $f + RM_6(1,7)$:

$$f + 3x_0 + 4x_1 + 5x_2 + 5x_4 + 3x_5 + 4x_6,$$

from which it can be seen that the PMEPR is less than $2^{2+1} = 8$, as predicted by the above proof. □

2.5 Pairs of Functions Exhibiting a Near Golay Property

Using Lemma 2.1 from Section 2.3 above it is possible to construct pairs of functions whose out of phase auto-correlation functions sum to zero everywhere *except* for one shift. Such a pair is termed a *near Golay complementary pair.* A pair of pairs is then easily constructed whose auto-correlation sums have opposite values at this particular shift, thus giving a complementary quadruple

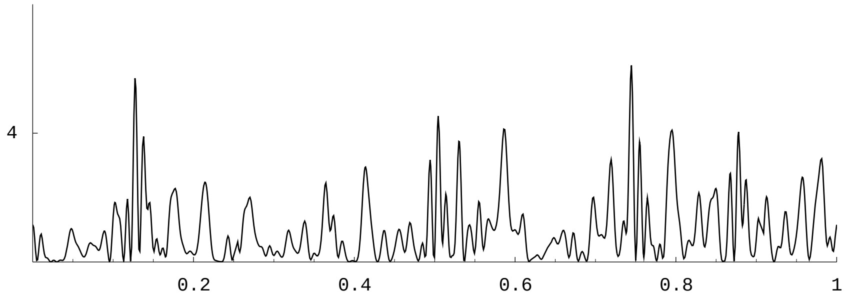

Figure 2.2: Envelope power for Example 2.2

set (this can be shown by Theorem 1.27, but that proof doesn't reveal the near Golay property). (Note that 'except at one shift' is meant within the normal convention of only regarding auto-correlation functions for non-negative shifts. When viewed across all shifts, the sum of the auto-correlations of such a near Golay pair will in fact be non-zero at three shifts: at the zero, 'in phase', shift, as for a normal Golay pair; at one positive shift; and at minus this shift, where the value will be the conjugate of the value at the positive shift, since the values of an auto-correlation function at negative shifts are just the conjugates of the values at the corresponding positive shift, from Theorem 1.1.)

The basic idea is to take a function f in m variables, whose graph is a path on $m-1$ vertices plus an isolated vertex. Pairing this with the function f plus one of the path end points then gives the near Golay pairing. A second pair to which $q/2$ times the isolated variable has been added to both functions is also near Golay, but this pair's non-zero entry in the auto-correlation sum is of the opposite sign to the first pair, and hence together all four form a complementary set. This is given by the following theorem, where the full range of shifts of the auto-correlations are considered for clarity.

Theorem 2.3. *Let f and f', two generalized Boolean functions over $\mathbb{Z}_q$ in the $m \geqslant 3$ variables $x_0, \ldots, x_{m-1}$, be given by*

$$f = P + L + g$$
$$f' = P + \frac{q}{2}x_a + L + g$$

where

$$P = \frac{q}{2}\sum_{\alpha=0}^{m-3} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}}$$
$$L = \sum_{\alpha=0}^{m-1} g_\alpha x_\alpha,$$

and $0 \leqslant i_0 < i_1 < \cdots < i_{m-2} \leqslant m-1$, π is a permutation of $\{0, 1, \ldots, m-2\}$, and $g, g_\alpha \in \mathbb{Z}_q$, $\alpha = 0, 1, \ldots, m-1$, and where a is either $i_{\pi(0)}$ or $i_{\pi(m-2)}$, so that x_a is one of the end points of path P. Let $\{0, 1, \ldots, m-1\} \backslash \{i_0, \ldots, i_{m-2}\} = \{\gamma\}$.

Then the functions f and f' have auto-correlations that sum as

$$A(\mathbf{F})(\ell) + A(\mathbf{F}')(\ell) = \begin{cases} 2^{m+1} & \ell = 0 \\ \omega^{-g_\gamma}2^m & \ell = 2^\gamma \\ \omega^{g_\gamma}2^m & \ell = -2^\gamma \\ 0 & \textit{otherwise}, \end{cases}$$

that is the pair are a near Golay complementary pair.
In addition, the set of the four functions given by

$$f + \frac{q}{2}(dx_a + d_\gamma x_\gamma), \quad d, d_\gamma \in \{0,1\}$$

form a complementary set.

Proof. Perform a restriction on x_γ and expand the sum of the auto-correlations using Corollary 1.16 to get

$$\begin{aligned} &A(\mathbf{F})(\ell) + A(\mathbf{F}')(\ell) \\ &\quad = \sum_c (A(\mathbf{F}\big|_{x_\gamma=c})(\ell) + A(\mathbf{F}'\big|_{x_\gamma=c})(\ell)) \\ &\qquad + \sum_{c_1 \neq c_2} (C(\mathbf{F}\big|_{x_\gamma=c_1}, \mathbf{F}\big|_{x_\gamma=c_2})(\ell) + C(\mathbf{F}'\big|_{x_\gamma=c_1}, \mathbf{F}'\big|_{x_\gamma=c_2})(\ell)). \end{aligned}$$

The graph of $f\big|_{x_\gamma=c}$ is a path (which is non-trivial by the $m \geqslant 3$ condition in the hypothesis), the restriction on x_γ having deleted the isolated vertex, and a is the index of one of the end points of the path. Thus for fixed c, the pair of functions

$$f\big|_{x_\gamma=c} \quad \text{and} \quad (f + \frac{q}{2}x_a)\big|_{x_\gamma=c}$$

form a Golay complementary pair by Theorem 1.24, and so

$$A(\mathbf{F}\big|_{x_\gamma=c})(\ell) + A(\mathbf{F}'\big|_{x_\gamma=c})(\ell)$$

is zero except at $\ell = 0$, where, by the comments after Lemma 1.20, each pair contributes $2^{m-1+1} = 2^m$ to the overall sum, giving a total of 2^{m+1} at the zero shift as usual.
The functions

$$f \quad \text{and} \quad f' = f + \frac{q}{2}x_a$$

are also seen to fit the conditions of Lemma 2.1, for the case of $k = 0$ restrictions, thus, for $c_1 \neq c_2$

$$\begin{aligned} &C(\mathbf{F}\big|_{x_\gamma=c_1}, \mathbf{F}\big|_{x_\gamma=c_2})(\ell) + C(\mathbf{F}'\big|_{x_\gamma=c_1}, \mathbf{F}'\big|_{x_\gamma=c_2})(\ell) \\ &\qquad = \begin{cases} \omega^{(c_1-c_2)g_\gamma}2^m & \ell = (c_2 - c_1)2^\gamma \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Thus the only non-zero contributions made by the cross-correlation sums to the overall sum are $\omega^{g_\gamma}2^m$ at $\ell = -2^\gamma$ when $c_1 = 1, c_2 = 0$, and $\omega^{-g_\gamma}2^m$ at $\ell = 2^\gamma$

when $c_1 = 0, c_2 = 1$. Since the only non-zero values in either the auto- or cross-correlation components of the overall sum occur at distinct shifts ℓ as shown, the first part of the theorem is proved.
To show that the functions

$$f + \frac{q}{2}(dx_a + d_\gamma x_\gamma), \quad d, d_\gamma \in \{0, 1\}$$

form a complementary set, when $d_\gamma = 0$ notate as f and f' above, and when $d_\gamma = 1$ write

$$f_\gamma = f + \frac{q}{2}x_\gamma \quad \text{and} \quad f'_\gamma = f + \frac{q}{2}(x_a + x_\gamma),$$

noting that in the latter cases the overall coefficient on x_γ is now $g_\gamma + \frac{q}{2}$. Then from the first part of the theorem we get

$$A(\mathbf{F})(\ell) + A(\mathbf{F}')(\ell) = \begin{cases} 2^{m+1} & \ell = 0 \\ \omega^{-g_\gamma}2^m & \ell = 2^\gamma \\ \omega^{g_\gamma}2^m & \ell = -2^\gamma \\ 0 & \text{otherwise} \end{cases}$$

and

$$A(\mathbf{F}_\gamma)(\ell) + A(\mathbf{F}'_\gamma)(\ell) = \begin{cases} 2^{m+1} & \ell = 0 \\ \omega^{-(g_\gamma + \frac{q}{2})}2^m = -\omega^{-g_\gamma}2^m & \ell = 2^\gamma \\ \omega^{(g_\gamma + \frac{q}{2})}2^m = -\omega^{g_\gamma}2^m & \ell = -2^\gamma \\ 0 & \text{otherwise,} \end{cases}$$

from which we clearly get

$$A(\mathbf{F})(\ell) + A(\mathbf{F}')(\ell) + A(\mathbf{F}_\gamma)(\ell) + A(\mathbf{F}'_\gamma)(\ell) = 0, \quad \ell \neq 0,$$

which is precisely the condition that the four functions form a complementary set. □

Example 2.4. As a simple example consider the Boolean function in the four variables $x_0, \ldots, x_3$

$$f = x_0x_3 + x_1x_3,$$

so the path is just f and we use end point x_1, $\gamma = 2$ is the isolated vertex, and $g_\gamma = 0$. Then the auto-correlation functions of

$$f, \quad f' = f + x_1, \quad f_\gamma = f + x_2 \quad \text{and} \quad f'_\gamma = f + x_1 + x_2$$

are:

$$\begin{aligned} A(\mathbf{F})(\ell) &= (16, 7, 0, 5, 8, 3, 0, 1, 0, -1, 0, 1, 0, -1, 0, 1) \\ A(\mathbf{F}')(\ell) &= (16, -7, 0, -5, 8, -3, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1) \\ A(\mathbf{F})(\ell) + A(\mathbf{F}')(\ell) &= (32, 0, 0, 0, 16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ A(\mathbf{F}_\gamma)(\ell) &= (16, 1, 0, 3, -8, 1, 0, -5, 0, -3, 0, 3, 0, 1, 0, -1) \\ A(\mathbf{F}'_\gamma)(\ell) &= (16, -1, 0, -3, -8, -1, 0, 5, 0, 3, 0, -3, 0, -1, 0, 1) \\ A(\mathbf{F}_\gamma)(\ell) + A(\mathbf{F}'_\gamma)(\ell) &= (32, 0, 0, 0, -16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), \end{aligned}$$

illustrating the non-zero entries $\pm 2^m = \pm 2^4 = \pm 16$ at shifts $\ell = 2^\gamma = 2^2 = 4$ in the pair of summed auto-correlations, so that adding this pair clearly gives the auto-correlation sum of a complementary set. □

2.6 Conclusions

In this chapter it has been shown that Conjecture 1 (of [32]) is true in some special cases, i.e. when $k \geqslant 1$ deletions in the graph of f results in a graph which is a path and either one or two isolated vertices, and where special constraints on the weights of edges in the original graph of f apply, then the further deletions of the isolated vertices as per Theorem 1.27 are unnecessary: a complementary set of 2^{k+1} functions may be constructed, and all words in the coset $f + RM_q(1, m)$ thus have PMEPR at most 2^{k+1}. In Chapter 3 specific examples of functions are constructed, which satisfy the hypothesis of the conjecture and which have 3 or more isolated vertices following the deletions, the PMEPRs for which also meet the conjectured bound. However, in Chapter 4 several families of (binary) functions are exhibited, which satisfy the hypothesis and have 3 or more isolated vertices following the deletions, and within the cosets of which exist words having PMEPRs greater than 2^{k+1}, and thus the conjecture cannot be true in general.

In the last section pairs of simple functions have been constructed that have the near Golay property in that their out of phase auto-correlations sum to zero except at one shift. Quadruple complementary sets are then easily constructed from a pair of such pairs.

Chapter 3

Generalized Boolean Functions with the same Aperiodic Auto-correlation Function

3.1 Chapter Overview

This chapter looks at generalized Boolean functions which share the same auto-correlation function. The introduction shows some simple ways in which this happens, and gives a necessary condition for this to be so for binary functions. In Section 3.3 a construction is given for pairs of generalized Boolean functions which share the same aperiodic auto-correlation function, and a useful corollary for functions which contain a path segment is obtained. Repeated application of the corollary to a quadratic function consisting solely of path segments culminates in a refinement of Theorem 1.27 in Section 3.4. This result is then applied in Section 3.5 to construct functions meeting the bound of Conjecture 1 and satisfying the hypothesis for an arbitrary number of isolated vertices following the deletions. Some conclusions are drawn in the last section, Section 3.6.

3.2 Introduction

The study of Golay complementary pairs concerns, by definition, sequences whose auto-correlation functions sum to zero, viz

$$A(\mathbf{A})(\ell) + A(\mathbf{B})(\ell) = 0, \quad \ell \neq 0.$$

In this chapter sequences are studied which share the same auto-correlation function, i.e. for which the *difference* of the auto-correlation functions is zero:

$$A(\mathbf{A})(\ell) - A(\mathbf{B})(\ell) = 0 \text{ for all } \ell.$$

In the introductory chapter, two of the theorems listing the properties of correlation functions have already given two simple ways in which this happens. Firstly, from Theorem 1.1,

$$A(\overline{\mathbf{A}})(\ell) = A^*(\mathbf{A})(\ell),$$

where $\overline{\mathbf{A}}$ is the reverse of vector $\mathbf{A}$, so reversing and conjugating the sequence yields the same auto-correlation function:

$$A(\overline{\mathbf{A}}^*)(\ell) = A(\mathbf{A})(\ell).$$

Secondly, Theorem 1.8 gives

$$A(\mathbf{G})(\ell) = A(\mathbf{F})(\ell)$$

where $g(x) = f(x) + c$, c some arbitrary constant in $\mathbb{Z}_q$. Using the notation of Section 1.6 for the algebraic normal form of the reverse of a function, the first of these becomes

$$A(\mathbf{H})(\ell) = A(\mathbf{F})(\ell),$$

where $h(x) = -f(1-x)$, the conjugation being accomplished by the negation of f. Thus for any given generalized Boolean function f in m variables over $\mathbb{Z}_q$, adding a constant to f, or reversing and negating f, or the combination of the two, results in another function that has the same auto-correlation function as f.

For the binary case, for functions of 1,2 or 3 variables, a simple computer search shows that these are the only ways functions may share the same auto-correlation, and so sets of such functions have size at most 4. However when $m = 4$, sets of size 8 in fact exist, i.e. there are functions sharing the same auto-correlation with seven other functions, so there must be other mechanisms at play (the quadratic part of these functions is in fact one of the three 'pathological' functions previously mentioned in Section 2.2: $x_0x_1 + x_2x_3$, $x_0x_3 + x_1x_2$ or $x_0x_2 + x_1x_3$; they are covered by Corollary 3.5 in Section 3.3 which follows). One such mechanism is given by Theorem 3.3 in the next section, but first some observations about the difference between two sequences are made.

Definition 3.1. The length n sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, $a_i \in \mathbb{Z}_q$ for all i and q even, is said to be *symmetric* if

$$a_i = a_{n-1-i}, \quad i = 0, 1, \ldots, n-1.$$

The sequence $\mathbf{a}$ is said to be *antisymmetric* if

$$a_i = a_{n-1-i} + \frac{q}{2} \mod q, \quad i = 0, 1, \ldots, n-1.$$

□

It is well known that for a binary Golay complementary pair of sequences the difference between the sequences is antisymmetric [13, Lemma 1.2], i.e. if

$$A(\mathbf{A})(\ell) + A(\mathbf{B})(\ell) = 0, \quad \ell \neq 0,$$

then

$$\begin{aligned} a_i + b_i + a_{n-1-i} + b_{n-1-i} &= 1 \mod 2 \\ \text{or} \quad \varepsilon_i + \varepsilon_{n-1-i} &= 1 \mod 2, \end{aligned}$$

where $\varepsilon_i = a_i + b_i \mod 2$ is the difference between the sequences. This result is put to good use in [13] for performing exhaustive searches for complementary pairs. The following analogous result shows that the difference between binary sequences sharing the same auto-correlation is in fact symmetric.

Lemma 3.2. *Let* $\mathbf{a}, \mathbf{b}$ *be binary sequences that have the same auto-correlation function, i.e.*

$$A(\mathbf{A})(\ell) - A(\mathbf{B})(\ell) = 0 \textit{ for all } \ell.$$

Then

$$a_i + b_i + a_{n-1-i} + b_{n-1-i} = 0 \mod 2, \quad i = 0, 1, \dots, n-1$$

That is to say, the difference between the two sequences, $\boldsymbol{\varepsilon}$*, given by*

$$\varepsilon_i = a_i + b_i \mod 2$$

is symmetric, i.e.

$$\varepsilon_i + \varepsilon_{n-1-i} = 0 \mod 2, \quad i = 0, 1, \dots, n-1.$$

Proof. The difference in auto-correlation functions gives

$$\sum_{i=0}^{n-1-\ell} \left((-1)^{a_i + a_{i+\ell}} - (-1)^{b_i + b_{i+\ell}} \right) = 0 \text{ for } \ell = 0, \dots, n-1. \tag{3.1}$$

When a_i and $a_{i+\ell}$ 'agree', i.e. $a_i = a_{i+\ell}$, the term $(-1)^{a_i + a_{i+\ell}}$ contributes '+1' to the sum. Likewise when they 'disagree', $a_i \neq a_{i+\ell}$, the term contributes '−1' to the sum. Letting

$$\begin{aligned} \theta_a &= \text{ no. of agreements between } a_i \text{ and } a_{i+\ell} \text{ for } i = 0, \dots n-1-\ell \\ \phi_a &= \text{ no. of disagreements,} \end{aligned}$$

and similarly for b, then clearly

$$\theta_a + \phi_a = n - \ell \tag{3.2}$$

$$\theta_b + \phi_b = n - \ell, \tag{3.3}$$

and (3.1) becomes

$$\theta_a - \phi_a - \theta_b + \phi_b = 0. \tag{3.4}$$

(More formally

$$\begin{aligned} \phi_a &= \sum_{i=0}^{n-1-\ell} (a_i + a_{i+\ell} \mod 2) \\ \theta_a &= (n - \ell) - \phi_a, \end{aligned}$$

and similarly for b.)
Subtracting (3.3) from (3.2) gives

$$\theta_a + \phi_a - \theta_b - \phi_b = 0,$$

which when added to (3.4) gives

$$\begin{aligned} 2\theta_a - 2\theta_b &= 0 \\ \text{which implies} \qquad \theta_a &= \theta_b \\ \text{so that} \qquad \phi_a &= \phi_b \text{ from (3.2) and (3.3).} \end{aligned}$$

Now consider the sum

$$S_\ell = \sum_{i=0}^{n-1-\ell} (a_i + a_{i+\ell} + b_i + b_{i+\ell}) \mod 2, \quad \ell = 0, \ldots, n-1.$$

Agreements between a_i and $a_{i+\ell}$, and similarly for b, do not contribute to the sum, and thus

$$\begin{aligned} S_\ell &= \phi_a + \phi_b \mod 2 \\ &= 2\phi_a \mod 2, \quad \text{as } \phi_a = \phi_b \\ &= 0 \mod 2, \quad \ell = 0, \ldots, n-1. \end{aligned}$$

Now manipulate the sum as

$$\begin{aligned} S_\ell &= \sum_{i=0}^{n-1-\ell} (a_i + a_{i+\ell} + b_i + b_{i+\ell}) \\ &= \sum_{i=0}^{n-1-\ell} (a_i + b_i) + \sum_{i=\ell}^{n-1} (a_i + b_i) \\ &= \sum_{i=0}^{n-2-\ell} (a_i + b_i) + \sum_{i=\ell+1}^{n-1} (a_i + b_i) + a_\ell + b_\ell + a_{n-1-\ell} + b_{n-1-\ell} \\ &= S_{\ell+1} + a_\ell + b_\ell + a_{n-1-\ell} + b_{n-1-\ell} \mod 2 \end{aligned}$$

But, as shown above, $S_\ell = 0 \mod 2$, $\ell = 0, \ldots, n-1$, and $S_n = 0$, and so

$$a_\ell + b_\ell + a_{n-1-\ell} + b_{n-1-\ell} = 0 \mod 2, \quad \ell = 0, \ldots, n-1,$$

that is, the difference ε, between the two sequences is symmetric, as was to be shown. □

Clearly a function is symmetric if the reverse of its vector equals itself. Thus in algebraic normal form terms, a function f is symmetric if the reverse of its algebraic normal form merely equals the function itself, i.e.

$$f(1-x) = f(x)$$

(and likewise, antisymmetric is $f(1-x) = \frac{q}{2} + f(x)$). The difference between two functions over $\mathbb{Z}_q$, $q > 2$, which share the same auto-correlation due to the 'reverse and conjugate' rule above is also symmetric. Suppose $f(x)$ and $g(x) = -f(1-x)$ are such functions, then their difference is

$$f(x) - g(x) = f(x) + f(1-x),$$

the reverse of which, $f(1-x) + f(1-(1-x)) = f(1-x) + f(x)$, is just the same thing. However, over $\mathbb{Z}_q$, $q > 2$, it is also possible to get pairs of functions sharing the same auto-correlation for which the difference is *not* symmetric. For example, over $\mathbb{Z}_4$ with $m = 3$, the functions

$$\begin{aligned} 2(x_0x_1 + x_1x_2) &\equiv (0,0,0,2,0,0,2,0) \quad \text{and} \\ 2(x_1x_2 + x_0x_2) + 3x_1 + x_0 &\equiv (0,1,3,0,0,3,1,0), \end{aligned}$$

both have the auto-correlation (vector)

$$(8, -1, 0, 3, 0, 1, 0, 1),$$

but have the difference

$$(0, 3, 1, 2, 0, 1, 1, 0),$$

which is clearly not symmetric, and thus the above lemma does not generalize to $q > 2$.

With the knowledge of the above lemma, a search, based on that in [13] for complementary pairs but using a symmetric difference, was conducted to look for pairs of functions sharing the same auto-correlation function. The findings generalized to the two results of the next section.

3.3 A Construction for Functions with the same Auto-correlation

The following theorem gives some conditions under which a pair of restricted functions may share the same auto-correlation function. The idea is based around the fact that reversing a function does not affect its auto-correlation function, but in fact not all of the function needs to be reversed in order for this to still be the case. If after restricting it is possible to identify two functions in two distinct sets of variables, then the (restricted) function obtained by reversing and negating the first of these functions and leaving the second untouched will have the same auto-correlation as the original (restricted) function. Note that in the theorem the normal restriction on q being even is removed, i.e. q may be odd or even.

Theorem 3.3. *Let the m variables $x_0, \dots, x_{m-1}$ be partitioned into three sets*

$$\begin{aligned} I &= \{x_{i_0}, \dots, x_{i_{s-1}}\} \text{ where } 0 \leqslant i_0 < i_1 \cdots < i_{s-1} \leqslant m-1 \\ J &= \{x_{j_0}, \dots, x_{j_{t-1}}\} \text{ where } 0 \leqslant j_0 < j_1 \cdots < j_{t-1} \leqslant m-1 \\ K &= \{x_0, \dots, x_{m-1}\} \setminus (I \cup J), \end{aligned}$$

(so the size of K is $m - s - t$). Let f be a generalized Boolean function in the m variables $x_0, \dots, x_{m-1}$, which after restriction on the variables $\mathbf{x}$ in K, is defined as follows:

$$\begin{aligned} f(x_0, \dots, x_{m-1})\big|_{\mathbf{x}=\mathbf{c}} = F_1(x_{i_0}, \dots, x_{i_{s-1}}) + F_2(x_{j_0}, \dots, x_{j_{t-1}}) \\ + L(x_{i_0}, \dots, x_{i_{s-1}}) + h_1, \quad (3.5) \end{aligned}$$

where: $F_1(x_{i_0}, \dots, x_{i_{s-1}})$ is a generalized Boolean function in the s variables in I; $F_2(x_{j_0}, \dots, x_{j_{t-1}})$ is a generalized Boolean function in the t variables in J (and so distinct from those in I); L is any linear function also in the variables in I, namely

$$L(x_{i_0}, \dots, x_{i_{s-1}}) = \sum_{\alpha=0}^{s-1} g_{i_\alpha} x_{i_\alpha}, \quad g_{i_\alpha} \in \mathbb{Z}_q,$$

and h_1 is an arbitrary element of $\mathbb{Z}_q$.
Let $\overline{F}_1$ be the reverse of F_1. Then the functions

$$f\big|_{\mathbf{x}=\mathbf{c}} = F_1 + F_2 + L + h_1$$
$$\textit{and } f'\big|_{\mathbf{x}=\mathbf{c}} = -\overline{F}_1 + F_2 + L + h_2,$$

where h_2 is also an arbitrary element of $\mathbb{Z}_q$, have the same auto-correlation function.

Proof. Consider the difference between the auto-correlations of the corresponding complex-valued vectors:

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) - A(\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}})(\ell),$$

where $\mathbf{x}$ is all the restricting variables in the set K. We need to show that this is zero for all values of $\ell = 0, 1, \dots, 2^m - 1$. Perform a further restriction over all variables *not* in the function F_1, i.e. over the variables in the set J, $\mathbf{x}' = x_{j_0}x_{j_1}\dots x_{j_{t-1}}$, and expand both auto-correlation functions using Corollary 1.16 to obtain

$$\sum_{\mathbf{c}'}\big(A(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})(\ell) - A(\mathbf{F}'\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})(\ell)\big)$$
$$+ \sum_{\mathbf{c}'_1 \neq \mathbf{c}'_2}\big(C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_1}, \mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_2})(\ell) - C(\mathbf{F}'\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_1}, \mathbf{F}'\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'_2})(\ell)\big). \quad (3.6)$$

Consider now the algebraic normal form of $f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}$:

$$f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'} = (F_1 + F_2 + L + h_1)\big|_{\mathbf{x}'=\mathbf{c}'}.$$

Now as F_2 is only in the variables in J, over which we are restricting with $\mathbf{x}'$, it will reduce to an element of $\mathbb{Z}_q$, depending on the value for $\mathbf{c}'$. Denote this by $r(\mathbf{c}')$. The functions F_1 and L will both be unaffected by the restriction because they are not dependent on any of the restriction variables. Thus we have

$$f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'} = F_1 + L + h_1 + r(\mathbf{c}'). \quad (3.7)$$

Similarly, the restriction of f' is

$$f'\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'} = -\overline{F}_1 + L + h_2 + r(\mathbf{c}') \quad (3.8)$$

Now find the reverse of $f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}$, denoted by $\overline{f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}}$, by replacing x_i by $1 - x_i$ for $i = i_0, i_1, \dots, i_{s-1}$ in its constituent functions: F_1 reversed is just $\overline{F}_1$; from Section 1.6, the reverse of a linear function is the sum of the coefficients minus the function, i.e.

$$\overline{L} = \sum_{\alpha=0}^{s-1} g_{i_\alpha} - L.$$

Thus

$$\begin{aligned}\overline{f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}} &= \overline{F}_1 + \overline{L} + h_1 + r(\mathbf{c}') \\ &= \overline{F}_1 + \sum_{\alpha=0}^{s-1} g_{i_\alpha} - L + h_1 + r(\mathbf{c}').\end{aligned}$$

Add this to equation (3.8),

$$
\begin{aligned}
f'\big|_{\mathbf{xx}'=\mathbf{cc}'} + \overline{f\big|_{\mathbf{xx}'=\mathbf{cc}'}} = \\
& - \overline{F}_1 + L + h_2 + r(\mathbf{c}') + \overline{F}_1 + \sum_{\alpha=0}^{s-1} g_{i_\alpha} - L + h_1 + r(\mathbf{c}'),
\end{aligned}
$$

and re-arrange to get

$$
\begin{aligned}
f'\big|_{\mathbf{xx}'=\mathbf{cc}'} &= -\overline{f\big|_{\mathbf{xx}'=\mathbf{cc}'}} + \sum_{\alpha=0}^{s-1} g_{i_\alpha} + h_1 + h_2 + 2r(\mathbf{c}') \\
&= -\overline{f\big|_{\mathbf{xx}'=\mathbf{cc}'}} + \gamma,
\end{aligned}
$$

where $\gamma = \sum_{\alpha=0}^{s-1} g_{i_\alpha} + h_1 + h_2 + 2r(\mathbf{c}')$ is an element of $\mathbb{Z}_q$, dependent on $\mathbf{c}'$. That is, after the restrictions, f' is the negated reverse of f plus a constant. In the associated complex-valued vector, the effect of the negation is to conjugate the entries, and thus recalling the notation from Section 1.9.4 that $\widetilde{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}}$ is vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ with its non-zero entries reversed, and whose non-zero values are given by $\overline{f\big|_{\mathbf{x}=\mathbf{c}}}$, the reverse of $f\big|_{\mathbf{x}=\mathbf{c}}$, we have that

$$
\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'} = \omega^\gamma \widetilde{\mathbf{F}}^*\big|_{\mathbf{xx}'=\mathbf{cc}'}.
$$

Then

$$
\begin{aligned}
A(\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) &= A([\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'}])(\ell) && \text{by Lemma 1.20} \\
&= A(\omega^\gamma[\widetilde{\mathbf{F}}^*\big|_{\mathbf{xx}'=\mathbf{cc}'}])(\ell) \\
&= A([\widetilde{\mathbf{F}}^*\big|_{\mathbf{xx}'=\mathbf{cc}'}])(\ell) && \text{by Theorem 1.8} \\
&= A([\overline{\mathbf{F}^*\big|_{\mathbf{xx}'=\mathbf{cc}'}}])(\ell) && \text{by definition} \\
&= A([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'}])(\ell) && \text{by Theorem 1.1} \\
&= A(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) && \text{by Lemma 1.20,}
\end{aligned}
$$

and for all ℓ. Thus, for $\mathbf{c}'$ fixed, each term in the sum of the auto-correlation functions in expression (3.6) becomes, for all ℓ,

$$
\begin{aligned}
A(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) - A(\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) &= A(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) - A(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'})(\ell) \\
&= 0.
\end{aligned}
$$

Now consider the cross-correlations. From (3.7) it is seen that

$$
\begin{aligned}
f\big|_{\mathbf{xx}'=\mathbf{cc}'_2} &= f\big|_{\mathbf{xx}'=\mathbf{cc}'_1} + r(\mathbf{c}'_2) - r(\mathbf{c}'_1) \\
&= f\big|_{\mathbf{xx}'=\mathbf{cc}'_1} + \delta,
\end{aligned}
$$

where $\delta = r(\mathbf{c}'_2) - r(\mathbf{c}'_1)$ is an element of $\mathbb{Z}_q$, dependent on $\mathbf{c}'_1$ and $\mathbf{c}'_2$. Similarly from (3.8)

$$
\begin{aligned}
f'\big|_{\mathbf{xx}'=\mathbf{cc}'_2} &= f'\big|_{\mathbf{xx}'=\mathbf{cc}'_1} + r(\mathbf{c}'_2) - r(\mathbf{c}'_1) \\
&= f'\big|_{\mathbf{xx}'=\mathbf{cc}'_1} + \delta.
\end{aligned}
$$

Then for fixed $\mathbf{c}'_1$ and $\mathbf{c}'_2$ and for all ℓ, each term in the cross-correlation sum in expression (3.6) becomes

$$
\begin{aligned}
&C(\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}, \mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_2})(\ell) - C(\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}, \mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_2})(\ell) \\
&\quad = C([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], [\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_2}])(\ell') \\
&\qquad - C([\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], [\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_2}])(\ell') && \text{using Lemma 1.20} \\
&\quad = C([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], \omega^{\delta}[\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell') \\
&\qquad - C([\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], \omega^{\delta}[\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell') && \text{by above} \\
&\quad = \omega^{-\delta}\big(C([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], [\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell') \\
&\qquad -C([\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}], [\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell')\big) && \text{by Theorem 1.8} \\
&\quad = \omega^{-\delta}\big(A([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell') - A([\mathbf{F}'\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell')\big) \\
&\quad = \omega^{-\delta}\big(A([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell') - A([\mathbf{F}\big|_{\mathbf{xx}'=\mathbf{cc}'_1}])(\ell')\big) && \text{from above} \\
&\quad = 0
\end{aligned}
$$

where $\ell' = \ell - (u_2 - u_1)$, u_1 is the index of the first non-zero entry in the vector $(\cdot)\big|_{\mathbf{xx}'=\mathbf{cc}'_1}$ and u_2 that of $(\cdot)\big|_{\mathbf{xx}'=\mathbf{cc}'_2}$. Thus all terms in both sums of expression (3.6) are zero for all ℓ, and so

$$
A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) - A(\mathbf{F}'\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell = 0, 1, \ldots, 2^m - 1,
$$

i.e. the two functions have the same auto-correlation function as claimed. □

Example 3.4. As an example, let $m = 8$ and let the functions be over $\mathbb{Z}_4$. Let set $I = \{x_0, x_1, x_2, x_3\}$ and set $J = \{x_4, x_5, x_6, x_7\}$, and so set K is empty and thus there is no restriction. The following functions have been made up more or less at random, but the size of I, being 4, has been specifically picked to be high enough to allow for some order 3 and 4 monomials in F_1, which means its reverse is non-trivial, and in turn the difference between f and g (given below) is far from obvious. So, with

$$
\begin{aligned}
F_1 &= 2x_0x_1x_2x_3 + 3x_0x_1x_3 + x_0x_1 + x_0x_2 + x_0x_3 \\
F_2 &= x_4x_6x_7 + 3x_4x_5 + x_4x_6 + x_4x_7 + 2x_5 \\
L &= 2x_1 + 3x_2 \\
h_1 &= 1 \\
h_2 &= 2,
\end{aligned}
$$

then

$$
\begin{aligned}
-\overline{F}_1 = 2x_0x_1x_2x_3 &+ 2x_0x_1x_2 + x_0x_1x_3 \\
&+ 2x_0x_2x_3 + 2x_1x_2x_3 + 2x_0x_1 + x_0x_2 + 2x_1x_2 \\
&\qquad + 2x_0x_3 + 3x_1x_3 + 2x_2x_3 + 2x_1 + 3x_2 + 2x_3,
\end{aligned}
$$

and so

$$\begin{aligned} f &= F_1 + F_2 + L + h_1 \\ &= 2x_0x_1x_2x_3 + 3x_0x_1x_3 + x_0x_1 + x_0x_2 + x_0x_3 \\ &\qquad + x_4x_6x_7 + 3x_4x_5 + x_4x_6 + x_4x_7 + 2x_5 + 2x_1 + 3x_2 + 1, \\ g &= -\overline{F}_1 + F_2 + L + h_2 \\ &= 2x_0x_1x_2x_3 + 2x_0x_1x_2 + x_0x_1x_3 + 2x_0x_2x_3 + 2x_1x_2x_3 \\ &\qquad + 2x_0x_1 + x_0x_2 + 2x_1x_2 + 2x_0x_3 + 3x_1x_3 + 2x_2x_3 \\ &\qquad + 2x_2 + 2x_3 + x_4x_6x_7 + 3x_4x_5 + x_4x_6 + x_4x_7 + 2x_5 + 2. \end{aligned}$$

Then direct computation shows that indeed

$$A(\mathbf{F})(\ell) = A(\mathbf{G})(\ell), \quad \ell = 0, 1, \ldots, 255.$$

It can also be confirmed that the difference between f and g:

$$\begin{aligned} f - g = {} & 2x_0x_1x_2 + 2x_0x_1x_3 + 2x_0x_2x_3 + 2x_1x_2x_3 \\ & + 3x_0x_1 + 2x_1x_2 + 3x_0x_3 + x_1x_3 + 2x_2x_3 + 2x_1 + x_2 + 2x_3 + 3 \end{aligned}$$

is symmetric. □

The difference between the functions in the theorem is

$$F_1 + \overline{F}_1 + h_1 - h_2.$$

From the discussion in the previous section, since the reverse of this,

$$\overline{F}_1 + F_1 + h_1 - h_2,$$

is just the same thing, the difference is clearly symmetric. The example shows that this is far from obvious when the reverse of F_1 bears little resemblance to F_1 itself. However, when the function F_1 is a path, its reverse is particularly simple, leading to the following corollary which allows for a much easier construction of functions with the same auto-correlation function. Note that now q must be even.

Corollary 3.5. *Using the same notation as the theorem, let f be a generalized Boolean function over $\mathbb{Z}_q$, q even, in the m variables $x_0, \ldots, x_{m-1}$, which after restriction on the variables $\mathbf{x}$ in K, is defined as follows:*

$$\begin{aligned} f(x_0, \ldots, x_{m-1})\big|_{\mathbf{x}=\mathbf{c}} = {} & P(x_{i_0}, \ldots, x_{i_{s-1}}) + F_2(x_{j_0}, \ldots, x_{j_{t-1}}) \\ & + L(x_{i_0}, \ldots, x_{i_{s-1}}) + h_1 \end{aligned} \tag{3.9}$$

where: $P(x_{i_0}, \ldots, x_{i_{s-1}})$ is a path in the $s \geqslant 2$ variables in I, viz:

$$P(x_{i_0}, \ldots, x_{i_{s-1}}) = \frac{q}{2} \sum_{\alpha=0}^{s-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}}$$

where π is a permutation of $\{0,1,\dots,s-1\}$; $F_2(x_{j_0},\dots,x_{j_{t-1}})$ is a generalized Boolean function in the t variables in J (and so distinct from those in I); L is any linear function also in the variables in I, namely

$$L(x_{i_0},\dots,x_{i_{s-1}}) = \sum_{\alpha=0}^{s-1} g_{i_\alpha} x_{i_\alpha}, \quad g_{i_\alpha} \in \mathbb{Z}_q,$$

and h_1 is any element of $\mathbb{Z}_q$.
Then the functions

$$\begin{aligned} f\big|_{\mathbf{x}=\mathbf{c}} &= P + F_2 + L + h_1 \\ \textit{and } f'\big|_{\mathbf{x}=\mathbf{c}} &= P + \frac{q}{2}\big(x_{i_{\pi(0)}} + x_{i_{\pi(s-1)}}\big) + F_2 + L + h_2 \end{aligned}$$

where $x_{i_{\pi(0)}}$ and $x_{i_{\pi(s-1)}}$ are the end points of the path P, and h_2 is any element of $\mathbb{Z}_q$, have the same auto-correlation function.

Proof. In the theorem, put $F_1 = P$. From Lemma 1.9, the negated reverse of P, $-\overline{P}$, is

$$\begin{aligned} -\overline{P} &= -\Big(P + \frac{q}{2}\big(x_{i_{\pi(0)}} + x_{i_{\pi(s-1)}}\big) + \big(\frac{q}{2}(s-1) \mod q\big)\Big) \\ &= P + \frac{q}{2}\big(x_{i_{\pi(0)}} + x_{i_{\pi(s-1)}}\big) + \big(\frac{q}{2}(s-1) \mod q\big) \\ &= -\overline{F}_1, \end{aligned}$$

using the fact that $-\frac{q}{2} = \frac{q}{2} \mod q$, q even. This then gives

$$\begin{aligned} -\overline{F}_1 &+ F_2 + L + h_2' \\ &= P + \frac{q}{2}\big(x_{i_{\pi(0)}} + x_{i_{\pi(s-1)}}\big) + F_2 + L + h_2' + \big(\frac{q}{2}(s-1) \mod q\big) \\ &= P + \frac{q}{2}\big(x_{i_{\pi(0)}} + x_{i_{\pi(s-1)}}\big) + F_2 + L + h_2, \end{aligned}$$

which by the theorem has the same auto-correlation function as $f\big|_{\mathbf{x}=\mathbf{c}}$. □

3.4 Complementary Subsets from Theorem 1.27

In this section it is shown that for quadratic forms consisting of a number of disjoint path segments, the complementary set given by the construction of Theorem 1.27 may be partitioned into subsets which all form complementary sets in their own right. Thus the PMEPR of words in the coset are in fact less than that given by Theorem 1.27. This is due to the fact that within the complementary set there are functions which satisfy Corollary 3.5 above, and which thus share the same auto-correlation function, the effect of which is to reduce the number of distinct auto-correlations that sum to zero across the set.

Suppose that Q is a quadratic form in m variables over $\mathbb{Z}_q$ that satisfies the following construction. Partition the set $\{0,1,\dots,m-1\}$ into the $s+1$ sets I_j of size m_j:

$$\begin{gathered} I_j = \{i_{j,0}, i_{j,1}, \dots, i_{j,m_j-1}\}, \quad j = 0,1,\dots,s, \\ \text{and such that} \quad |I_j| = m_j \geqslant 2, \end{gathered}$$

and so $m = \sum_{j=0}^{s} m_j$. Let each of the π_j, $j = 0, 1, \ldots, s$, be a bijection $\pi_j : \{0, 1, \ldots, m_j - 1\} \to I_j$, and then let Q be given by

$$Q = \frac{q}{2} \sum_{j=0}^{s} \sum_{k=0}^{m_j - 2} x_{\pi_j(k)} x_{\pi_j(k+1)},$$

and thus Q consists of $s + 1$ distinct path segments, each of which has end points $x_{\pi_j(0)}$ and $x_{\pi_j(m_j-1)}$. Choose one of the longest paths to be the path for Theorem 1.27 purposes, i.e. pick $r \in \{0, 1, \ldots, s\}$ such that

$$m_r = |I_r| = \max_{0 \leqslant j \leqslant s} \{|I_j|\},$$

and let a be the index of either of the end points of path r, i.e. $a = \pi_r(0)$ or $\pi_r(m_r - 1)$. Let the sum of the number of indices in all the sets except I_r be K, i.e.

$$K = \sum_{\substack{j=0 \\ j \neq r}}^{s} m_j = m - m_r.$$

Thus deleting the K vertices indexed by sets I_j, $j \neq r$ leaves the path suffix r, and so by Theorem 1.27, the following 2^{K+1} functions form a complementary set:

$$Q + L + \frac{q}{2}\Bigg(\sum_{\substack{j=0 \\ j \neq r}}^{s} \sum_{k \in I_j} d_{jk} x_k + d x_a\Bigg), \quad d_{jk}, d \in \{0, 1\},$$

where as usual L is any affine function of $x_0, \ldots, x_{m-1}$.

Arrange the coefficients d_{jk} into two binary vectors. The first, $\mathbf{d}_{\text{End}}$, of length $2s$, containing the d_{jk} for both end points of the s paths:

$$\begin{aligned}\mathbf{d}_{\text{End}} = (&d_{0\pi_0(0)}, d_{0\pi_0(m_0-1)}, d_{1\pi_1(0)}, d_{1\pi_1(m_1-1)}, \ldots, \\ &d_{r-1\pi_{r-1}(0)}, d_{r-1\pi_{r-1}(m_{r-1}-1)}, d_{r+1\pi_{r+1}(0)}, d_{r+1\pi_{r+1}(m_{r+1}-1)}, \ldots, \\ &d_{s\pi_s(0)}, d_{s\pi_s(m_s-1)}),\end{aligned}$$

and the second, $\mathbf{d}_{\text{Int}}$, of length $m - m_r - 2s (= K - 2s)$, containing the remaining d_{jk} for all the points which are 'internal' to the paths:

$$\begin{aligned}\mathbf{d}_{\text{Int}} = (&d_{0\pi_0(1)}, d_{0\pi_0(2)}, \ldots, d_{0\pi_0(m_0-2)}, d_{1\pi_1(1)}, \ldots, \\ &d_{r-1\pi_{r-1}(m_{r-1}-2)}, d_{r+1\pi_{r+1}(1)}, \ldots, d_{s\pi_s(m_s-2)}).\end{aligned}$$

Thus each of the above 2^{K+1} functions is represented by a particular value of $\mathbf{d}_{\text{End}}$, $\mathbf{d}_{\text{Int}}$ and $d = 0$ or 1. Let f be one of these functions and consider its $\mathbf{d}_{\text{End}}$ vector. Taking the 1's complement of any adjacent pair of coordinates, the first of which has an even index, i.e. adding 1 mod 2 to each coordinate, is equivalent to adding $q/2$ times a pair of end points to f (since in the function the actual coefficients of the x_i are either 0 or $q/2$ added mod q). So if we complement coordinates indexed by $2j$ and $2j + 1$ $(j \neq r)$ we form

$$f + \frac{q}{2}(x_{\pi_j(0)} + x_{\pi_j(m_j-1)}).$$

The path segment to which the appended end points belong appears in f, and thus taking this path as P in Corollary 3.5, this function has the same auto-correlation function as the original function f (and note that no restriction is applied in the corollary). Moreover, complementing other such pairs, by the same mechanism, results in further functions with the same auto-correlation. Thus for a given value of $\mathbf{d}_{\text{End}}$ there are 2^s ways that we can perform this complementation and still have a function with the same auto-correlation as the original, and this is true for all values of $\mathbf{d}_{\text{Int}}$ and d. The set of 2^{K+1} functions thus splits into $2^{K+1} \div 2^s = 2^{K-s+1}$ sets of size 2^s, each consisting of functions sharing the same auto-correlation function. Let $A_i(\ell), i = 1, \ldots, 2^{K+1}$, represent the auto-correlation functions of the 2^{K+1} functions, and that the functions form a complementary set means the auto-correlations sum to zero, i.e.

$$\sum_{i=1}^{2^{K+1}} A_i(\ell) = 0, \quad \ell \neq 0.$$

The preceding argument shows that there are at most 2^{K-s+1} distinct $A_i(\ell)$, each occurring at least 2^s times, and so the sum may be written as

$$2^s \sum_{j=1}^{2^{K-s+1}} A_{i_j}(\ell) = 0, \quad \ell \neq 0,$$

where the i_j are distinct, from which it is seen that the corresponding functions in fact form a Golay complementary set of size 2^{K-s+1}.

The above shows that the function f represented by particular values of $\mathbf{d}_{\text{End}}$, $\mathbf{d}_{\text{Int}}$ and d shares the same auto-correlation function with the following 2^s functions:

$$f + \frac{q}{2} \sum_{\substack{j=0 \\ j \neq r}}^{s} d'_j (x_{\pi_j(0)} + x_{\pi_j(m_j-1)}), \quad d'_j \in \{0, 1\},$$

i.e. the functions obtained by adding a multiple $\frac{q}{2} d'_j$ of both end points of each of the paths, except for suffix r, to f. In order to form the complementary sets of size 2^{K-s+1}, a set of $\mathbf{d}_{\text{End}}$ vectors of size 2^s needs to be established such that complementing any pair of even-indexed coordinates in any $\mathbf{d}_{\text{End}}$ vector does not take it to another vector. One way to achieve this is to set $d_{j\pi_j(m_j-1)} = 0$, $j = 0, 1, \ldots, s$, $j \neq r$, for all 2^s combinations of $d_{j\pi_j(0)} = 0$ or 1, $j = 0, 1, \ldots, s$, $j \neq r$ (thus all pairs of coordinates in all vectors are either '00' or '10', and the complements of these, '11' and '01' do not appear anywhere in any of the vectors). Representing that part of the sum

$$\sum_{\substack{j=0 \\ j \neq r}}^{s} \sum_{k \in I_j} d_{jk} x_k$$

concerning the points internal to the path by

$$\mathbf{d}_{\text{Int}} \cdot \mathbf{x},$$

then the following functions form a complementary set

$$Q + L + \frac{q}{2}(\mathbf{d}_{\text{Int}} \cdot \mathbf{x} + dx_a) + \frac{q}{2}\sum_{\substack{j=0\\ j\neq r}}^{s} d'_j x_{\pi_j(0)}, \quad d'_j \in \{0,1\}.$$

There are 2 choices for d, 2^{K-2s} choices for $\mathbf{d}_{\text{Int}}$, and 2^s choices of the d'_j, giving a total of $2^{1+K-2s+s} = 2^{K-s+1}$ functions in the set as required.

Thus we have proved the following refinement of Theorem 1.27:

Theorem 3.6. *Suppose that Q, a quadratic form in the m variables $x_0, \ldots, x_{m-1}$ over $\mathbb{Z}_q$, is a disjoint union of $s+1$ path segments, and where the number of variables in the longest path is m_r, as detailed above. Then the coset $Q + RM_q(1,m)$ is a union of Golay complementary sets of size 2^{m-m_r-s+1}, and consequently every word of the coset has PMEPR at most 2^{m-m_r-s+1}.* □

3.5 Functions Meeting the Bound of Conjecture 1 for an Arbitrary Number of Isolated Vertices

Using Theorem 3.6 above it is straightforward to construct functions that satisfy the bound of Conjecture 1, and which have an arbitrary number of isolated vertices. Recall from Chapter 2 that Conjecture 1 states that if in the graph of some quadratic form Q some $k \geqslant 1$ vertices are *deleted*, and this results in a graph consisting of a path and *isolated* vertices, then the PMEPR of the coset of Q is at most 2^{k+1}. Thus if the Q from above consists of $s = k$ length 1 path segments, and one path segment of length 1 or more, deleting one end point of each of the length 1 path segments will leave k isolated vertices and a path. By way of example and to keep things simple, take all the bijections π_j to be just the identity, and construct Q as

$$Q = \frac{q}{2}\sum_{i=0}^{k-1} x_{2i}x_{2i+1} + \frac{q}{2}\sum_{i=2k}^{m-2} x_i x_{i+1}, \quad k \leqslant \left\lfloor \frac{m-2}{2} \right\rfloor.$$

Thus the k length 1 path segments are $\frac{q}{2}x_{2i}x_{2i+1}$, $i = 0, \ldots, k-1$, and the path segment of length 1 or more is $\frac{q}{2}\sum_{i=2k}^{m-2} x_i x_{i+1}$. There are $m_r = m - 2k$ variables in the path of length 1 or more, and so from the theorem, every word in the coset of Q has PMEPR less than $2^{m-(m-2k)-k+1} = 2^{k+1}$, and thus Q satisfies the bound of Conjecture 1. It is clear that many such functions can be constructed in this manner.

Example 3.7. For example, the following binary Q in $m = 10$ variables has $k = 3$ paths of length 1 and the longer path has length 3:

$$Q = x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_7x_8 + x_8x_9.$$

The graph for this Q is shown in Figure 3.1, and the deletion of, say, vertices 1, 3 and 5 clearly leaves a length 3 path and 3 isolated vertices (being 0, 2 and 4). Direct computation confirms that the sum of the auto-correlations of the 16

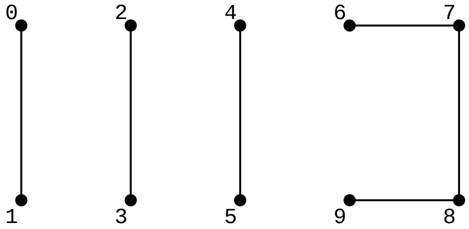

Figure 3.1: The graph of Q in Example 3.7

functions

$$Q + d_0x_0 + d_2x_2 + d_4x_4 + d_6x_6, \quad d_0, d_2, d_4, d_6 \in \{0, 1\}$$

is indeed zero everywhere except at the zero shift, so they form a complementary set, and thus the PMEPR of every codeword in the coset of Q will be less than $2^{3+1} = 16$. □

3.6 Conclusions

In this chapter functions sharing the same auto-correlation function have been investigated. Using the properties of path functions, a useful non-trivial method of constructing such functions has been presented. The result was accomplished by searching for Boolean functions sharing the same auto-correlation, using the fact that their difference must be symmetric. The search of course showed many other functions sharing the same auto-correlation, but it was only the amenable properties of paths that lead to the description of the pairing here. It may be possible to come up with descriptions of other such pairings by further examination of the forms of the functions involved.

For functions which consist solely of a disjoint union of path segments it has been shown in Theorem 3.6 that the complementary set given by Theorem 1.27 in fact consists of a number of smaller complementary subsets. This latter result in fact accounts for the reason the three 'pathological' binary functions

$$x_0x_1 + x_2x_3, \quad x_0x_2 + x_1x_3, \quad x_0x_3 + x_1x_2,$$

have PMEPRs a factor of 2 below that predicted by Theorem 1.27, as noticed in [32] and previously commented on in Section 2.2. Theorem 3.6 has also been used to construct examples of functions which meet the bound of Conjecture 1 and satisfy the hypothesis for an arbitrary number of isolated vertices following the deletions—however in Chapter 4 counterexamples are produced which show that Conjecture 1 cannot be true in general.

Chapter 4

Lower Bounds on PMEPR

4.1 Chapter Overview

This chapter concentrates solely on binary sequences. By utilizing the 'weight structure' of certain sequences it is possible to show that the sequence has large instantaneous power at some particular time, and this may be translated into a lower bound on the PMEPR of the corresponding coset. The existing results and background are given in Section 4.2, and the ideas are extended using the technique of restriction in Section 4.3 to provide a new lower bound on the PMEPR of a coset. This lower bound is then used in Section 4.4 to manufacture some counter-examples (all having three or more isolated vertices) to Conjecture 1 of Chapter 2. The difficulties encountered in extending the technique are given in Section 4.5, and some conclusions are drawn in 4.6.

4.2 Introduction

The main focus of this body of theory has clearly been to develop second-order cosets of the first-order generalized Reed-Muller code whose codewords all have low PMEPRs, i.e. the PMEPRs of the codewords are bounded above. For *binary* Reed-Muller codes however, it is also possible to show that within particular cosets there exist words with high PMEPRs, i.e. that the PMEPR of the coset is subjected to some lower bound. In this section some of the existing lower bounds are stated, along with the techniques used to derive them: these are then extended in Section 4.3 to provide a new bound. The main theoretical tool is the weight distribution of second order cosets of $RM_2(1,m)$ [25, Chapter 15]. The general idea is to show that a word with a particular weight has large instantaneous power at some specific time t: the peak envelope power must then be greater than or equal to this amount; the PMEPR of the word is greater than or equal to this amount divided by the mean power, and thus in turn the PMEPR of the coset is too.

First an expression for the instantaneous power of a binary sequence is derived that is peculiar to the binary case. Let $\mathbf{A} = (A_0, A_1, \ldots, A_{n-1})$ be a real-valued length n binary vector, i.e. $A_j \in \{+1, -1\}$, $j = 0, 1, \ldots, n-1$, and in particular we note that $A_j^* = A_j$ for all j. Referring back to Section 1.5.1, the instantaneous power of the signal, $P(\mathbf{A})(t)$ is obtained by substituting equation

(1.1) into (1.2): from a subsequent discussion in that section we may put $f_s = 1$, and with f_0 the frequency of the first carrier, we get

$$\begin{aligned}
P(\mathbf{A})(t) &= \sum_{j=0}^{n-1} A_j e^{2\pi i(f_0+j)t} \sum_{k=0}^{n-1} A_k e^{-2\pi i(f_0+k)t} \\
&= \Big(\sum_j A_j\big(\cos 2\pi(f_0+j)t + i\sin 2\pi(f_0+j)t\big)\Big) \\
&\qquad \times \Big(\sum_k A_k\big(\cos 2\pi(f_0+k)t - i\sin 2\pi(f_0+k)t\big)\Big) \\
&= \Big(\sum_j A_j \cos 2\pi(f_0+j)t\Big)^2 + \Big(\sum_j A_j \sin 2\pi(f_0+j)t\Big)^2 \\
&= \Big(\cos 2\pi f_0 t \sum_j A_j \cos 2\pi jt - \sin 2\pi f_0 t \sum_j A_j \sin 2\pi jt\Big)^2 \\
&\qquad + \Big(\sin 2\pi f_0 t \sum_j A_j \cos 2\pi jt + \cos 2\pi f_0 t \sum_j A_j \sin 2\pi jt\Big)^2 \\
&= \cos^2 2\pi f_0 t\Big(\sum_j A_j \cos 2\pi jt\Big)^2 + \sin^2 2\pi f_0 t\Big(\sum_j A_j \sin 2\pi jt\Big)^2 \\
&\qquad - 2\cos 2\pi f_0 t \sin 2\pi f_0 t\Big(\sum_j A_j \cos 2\pi jt\Big)\Big(\sum_j A_j \sin 2\pi jt\Big) \\
&\qquad + \sin^2 2\pi f_0 t\Big(\sum_j A_j \cos 2\pi jt\Big)^2 + \cos^2 2\pi f_0 t\Big(\sum_j A_j \sin 2\pi jt\Big)^2 \\
&\qquad + 2\sin 2\pi f_0 t \cos 2\pi f_0 t\Big(\sum_j A_j \cos 2\pi jt\Big)\Big(\sum_j A_j \sin 2\pi jt\Big) \\
&= \left(\sum_{j=0}^{n-1} A_j \cos 2\pi jt\right)^2 + \left(\sum_{j=0}^{n-1} A_j \sin 2\pi jt\right)^2 .
\end{aligned}$$

(Note that, as previously in Section 1.5.1, (i) the frequency of the first carrier, f_0, has vanished from the expression, and (ii) it is straightforward to show that for all $t \geqslant 0$, $P(\cdot)(\frac{1}{2}+t) = P(\cdot)(\frac{1}{2}-t)$, and thus P is symmetric about $t = \frac{1}{2}$ and that $P'(\cdot)(t) = P(\cdot)(\frac{1}{2}+t)$, for all t, is an even function.)

Our primary interest here is when the vector $\mathbf{A}$ derives from some Boolean function f. Thus let f be a Boolean function in m variables, with, as usual, $\mathbf{f} = (f_0, f_1, \ldots, f_{2^m-1})$ the length $n = 2^m$ vector of all its values. Through the real-valued vector $\mathbf{F}$, equivalent to $\mathbf{A}$, where $F_j = (-1)^{f_j}$ for $j = 0, 1, \ldots, 2^m - 1$, we may relate the above expression directly back to the values of f, to get

$$P(\mathbf{f})(t) = \left(\sum_{j=0}^{n-1}(-1)^{f_j} \cos 2\pi jt\right)^2 + \left(\sum_{j=0}^{n-1}(-1)^{f_j} \sin 2\pi jt\right)^2 , \qquad (4.1)$$

taking care not to confuse the f_j to be any frequency!

Suppose that $\mathbf{f}$ is an arbitrary codeword of the coset $Q + RM_2(1, m)$ for some quadratic form Q. Then as first noted in [8], the power at $t = 0$ simply becomes

$$\begin{aligned} P(\mathbf{f})(0) &= \left(\sum_{j=0}^{n-1} (-1)^{f_j} \right)^2 \\ &= \left(2^m - 2 \cdot wt_H(\mathbf{f}) \right)^2, \end{aligned}$$

where $wt_H(\mathbf{f})$ is the Hamming weight of $\mathbf{f}$, and it is also clear that we get $P(\mathbf{f})(1) = P(\mathbf{f})(0)$.

Thus if the weight of $\mathbf{f}$ could be readily determined, then so also could the power at $t = 0$. To this end it is possible to call upon the well-established theory of binary quadratic forms. The main goal in establishing this theory for the current thread is Theorem 4.2 below, which gives the weight distribution of a second order coset of the first order Reed-Muller code, and this relies on a theorem due to Dickson, Theorem 4.1 below, through which the definition of the rank of a quadratic form is given. However, later in Section 4.4, Dickson's theorem is called upon again, along with the results on the weights of certain quadratic forms which lead to the proof of Theorem 4.2, given here as Lemma 4.3. In order to prevent a piecemeal exposition of this theory, all of the required results are now presented, even though not all of them are relevant to the current section.

First the affect that an affine transformation has on the weight of a vector is considered. A very rudimentary (and hence rarely expounded) fact is that applying an invertible affine transformation to a (strictly) Boolean function f does not affect the weight of its associated vector $\mathbf{f}$. This is seen by considering an arbitrary affine transformation of f, say a function g given by

$$g(x) = f(Ax + B),$$

where A is an invertible $m \times m$ binary matrix and B a binary m-tuple. Let $x' = Ax + B$. Since A is invertible there is a one-to-one relationship between x and x': thus the value of g at x is the value of f at x', and so the vector $\mathbf{g}$ associated with g is obtained by permuting the coordinate positions of $\mathbf{f}$, and in particular, the number of 1's in both is the same.

This is extremely useful if f can be transformed into a form for which the weight of the associated vector may be more easily determined. Dickson's Theorem, [25, 35], does exactly that—it states that any Boolean function of degree $\leqslant 2$ can always be transformed such that the quadratic part of the function is placed into a canonical form. Those parts of theorem needed here, and in the current nomenclature, are now stated:

Theorem 4.1 (Dickson's Theorem). *(1) Any Boolean function of degree $\leqslant 2$ in m variables can be transformed via some affine transformation to the form*

$$\sum_{i=0}^{h-1} x_{2i}x_{2i+1} + \sum_{i=0}^{m-1} a_i x_i + \varepsilon$$

for some $1 \leqslant h \leqslant \lfloor m/2 \rfloor$ *and some* $a_i, \varepsilon \in \mathbb{Z}_2$.

(2) Further, if the linear part in (1) is only dependent on $x_0, \ldots, x_{2h-1}$, *i.e.* $a_i = 0, i \geqslant 2h$, *then a further transformation may be made to get*

$$\sum_{i=0}^{h-1} x_{2i}x_{2i+1} + \varepsilon_1, \quad \varepsilon_1 = 0 \text{ or } 1.$$

Proof. See [25]. □

The number of variables, $2h$, in the canonical form $\sum_{i=0}^{h-1} x_{2i}x_{2i+1}$ is termed the *rank* of the original quadratic form, and that any second order Boolean function may be reduced to such a form allows the weight distribution of the corresponding coset to be established, as given by the following theorem.

Theorem 4.2. *[25, Theorem 5, p441] Let* Q *be a quadratic form in the* m *variables* $x_0, \ldots, x_{m-1}$,

$$Q(x_0, \ldots, x_{m-1}) = \sum_{0 \leqslant i < j < m} q_{ij}x_ix_j, \quad q_{ij} \in \mathbb{Z}_2,$$

and suppose Q *has rank* $2h$. *Then the coset* $Q + RM_2(1, m)$ *has the following weight distribution:*

Weight	*Number of words*
$2^{m-1} - 2^{m-h-1}$	2^{2h}
2^{m-1}	$2^{m+1} - 2^{2h+1}$
$2^{m-1} + 2^{m-h-1}$	2^{2h}

This theorem says that codewords in the coset have one of just three possible weights: these are termed, in the obvious way, 'minimum' weight, 'half' weight and 'maximum' weight. The maximum and minimum weights depend on the rank of the quadratic form, but the half weight does not, merely being half the length of the codewords. It is proved by determining the weight of the canonical form, which is readily done, and is shown in the next lemma (which is a distillation of the lemmas used in the proof of Theorem 5 in [25, p441], and the equivalent in [24].)

Lemma 4.3. *(i) Let* $f(x)$, *a Boolean function in the* m *variables* $x_0, \ldots, x_{m-1}$, *be given by*

$$f(x) = \sum_{i=0}^{h-1} x_{2i}x_{2i+1} + \sum_{i=0}^{2h-1} a_ix_i + \varepsilon, \quad \varepsilon = 0 \text{ or } 1,$$

where $1 \leqslant h \leqslant \lfloor m/2 \rfloor$. *Then the weight of vector* $\mathbf{f}$ *is either* $2^{m-1} + 2^{m-h-1}$ *or* $2^{m-1} - 2^{m-h-1}$.

(ii) Let $g(x)$, *a Boolean function in the* m *variables* $x_0, \ldots, x_{m-1}$, *be given by*

$$g(x) = \sum_{i=0}^{h-1} x_{2i}x_{2i+1} + \sum_{i=2h}^{m-1} a_ix_i,$$

where $1 \leqslant h \leqslant \lfloor m/2 \rfloor$, *and where not all the* a_i *are zero. Then the weight of* $\mathbf{g}$ *is* 2^{m-1}.

Proof. (i) By part (2) of Dickson's theorem above, f can be transformed via an invertible affine transformation to the form

$$f'(x) = \sum_{i=0}^{h-1} x_{2i}x_{2i+1} + \varepsilon_1, \ \varepsilon_1 = 0 \text{ or } 1.$$

Consider now the function $\sum_{i=0}^{h-1} x_{2i}x_{2i+1}$ as a function in just the $2h$ variables $x_0, \ldots, x_{2h-1}$: if $x_0 = x_2 = \cdots = x_{2h-2} = 0$ then there are 2^h choices for the values of $x_1, x_3, \ldots, x_{2h-1}$ for which the function is zero. On the other hand if any of $x_0, x_2, \ldots, x_{2h-2}$ are non-zero (which happens in $2^h - 1$ ways), then we have a non-zero linear Boolean function in the h variables $x_1, x_3, \ldots, x_{2h-1}$, which by Lemma 1.12 takes the values 0 and 1 equally often, 2^{h-1} times each, thus giving another $(2^h - 1)2^{h-1}$ zeroes. Therefore the total number of zeroes of $\sum_{i=0}^{h-1} x_{2i}x_{2i+1}$ (regarded as in $2h$ variables) is $2^h + (2^h - 1)2^{h-1} = 2^{2h-1} + 2^{h-1}$, and thus the total number zeroes when regarding it as in the full m variables is $2^{m-2h}(2^{2h-1} + 2^{h-1}) = 2^{m-1} + 2^{m-h-1}$. Thus the weight of f' is:

$$\begin{aligned} 2^m - (2^{m-1} + 2^{m-h-1}) &= 2^{m-1} - 2^{m-h-1} && \text{when } \varepsilon_1 = 0 \\ 2^m - (2^{m-1} - 2^{m-h-1}) &= 2^{m-1} + 2^{m-h-1} && \text{when } \varepsilon_1 = 1. \end{aligned}$$

Applying the inverse transformation to go from f' back to f does not affect these weights (as discussed above), and so f will also have one of these weights.

(ii) Immediate from Lemma 1.12. □

The lemma shows that a function whose quadratic part is the canonical form $\sum_{i=0}^{h-1} x_{2i}x_{2i+1}$, and whose linear terms consist *only* of variables involved in the canonical part, has either maximum or minimum weight, and indeed such functions account for all those having either maximum or minimum weight, since by the second part of the lemma, the involvement of any other linear terms implies the function has half weight. (Repeated use of this fact is made in Section 4.4.)

Proof of Theorem 4.2. Using Theorem 4.1, transform a typical member of the coset to the canonical form, and count the number of each type as given by Lemma 4.3. □

Return now to the expression for the power at $t = 0$:

$$P(\mathbf{f})(0) = \big(2^m - 2 \cdot wt_H(\mathbf{f})\big)^2.$$

Theorem 4.2 gives the weights of $\mathbf{f}$ as f varies over the coset $Q + RM_2(1, m)$: thus at least one codeword $\mathbf{f}$ has weight $2^{m-1} - 2^{m-h-1}$, and for this $\mathbf{f}$,

$$P(\mathbf{f})(0) = \big(2^m - 2(2^{m-1} - 2^{m-h-1})\big)^2 = 2^{2m-2h} = 2^m 2^{m-2h},$$

so that the PMEPR of the coset is at least 2^{m-2h}. A lower bound on the PMEPR for $Q + RM_2(1, m)$ can thus be derived from the rank of Q. A simple application of this leads to a result that first appeared in [8], and subsequently in [32, 33], that shows that the bound on PMEPR from Corollary 1.25 is tight when m is odd:

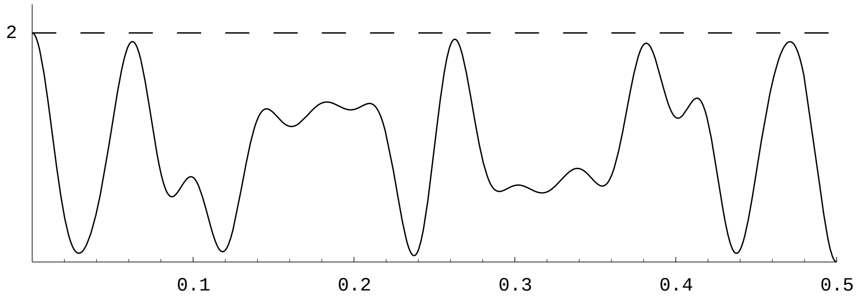

Figure 4.1: Envelope power for Example 4.5

Theorem 4.4. *Suppose m is odd and let*

$$Q(x_0,\dots,x_{m-1})=\sum_{i=0}^{m-2}x_{\pi(i)}x_{\pi(i+1)},$$

where π is a permutation of $\{0,1,\dots,m-1\}$. Then the PMEPR of the coset $Q+RM_2(1,m)$ is equal to 2.

Proof. Since m is odd, the rank of Q is $2h\leqslant m-1$. Then $m-2h\geqslant 1$ and, from the discussion above, the PMEPR of the coset is at least $2^{m-2h}\geqslant 2^1=2$. From Corollary 1.25, it is at most 2. □

Example 4.5. The envelope power for $0\leqslant t\leqslant\frac{1}{2}$ (recall that it is symmetric about $t=\frac{1}{2}$) of the function

$$x_0x_3+x_1x_3+x_1x_2+x_2x_4$$

is shown in Figure 4.1, showing that the peak power occurs exactly at $t=0$, giving a PMEPR of exactly 2. □

4.3 The Instantaneous Power at $t=\frac{1}{2^{u+1}}$

The ideas of the preceding section are now extended to the case when $t=\frac{1}{2^{u+1}}$, $u\geqslant 0$. By adding a specific linear term to the function f and restricting the resulting function in a specific way, it is possible to obtain an expression for the instantaneous power in terms of the weights of the restricted components of f.

Consider first the case of $u=0$, i.e. $t=\frac{1}{2}$. Substituting into (4.1) gives

$$\begin{aligned}P(\mathbf{f})(\frac{1}{2})&=\left(\sum_{j=0}^{n-1}(-1)^{f_j}\cos 2\pi j\frac{1}{2}\right)^2+\left(\sum_{j=0}^{n-1}(-1)^{f_j}\sin 2\pi j\frac{1}{2}\right)^2\\&=\left(\sum_{j=0}^{n-1}(-1)^{j+f_j}\right)^2,\end{aligned}$$

where the second summation has vanished entirely as $\sin\pi j=0$ for all j, and the substitution $\cos\pi j=(-1)^j$ has been made in the first summation. The alternating signs from the cosine terms may be reproduced by adding x_0 to f. Put

$$f' = f + x_0$$

then

$$(-1)^{f'_j} = (-1)^{(f+x_0)_j} = (-1)^{j+f_j}.$$

Thus

$$\begin{aligned} P(\mathbf{f})(\frac{1}{2}) &= \left(\sum_{j=0}^{n-1}(-1)^{f'_j}\right)^2 \\ &= \left(2^m - 2 \cdot wt_H(\mathbf{f}')\right)^2 \\ &= \left(2^m - 2 \cdot wt_H(f + x_0)\right)^2. \end{aligned}$$

So, as with the power at $t = 0$, the power at $t = \frac{1}{2}$ is determined from the Hamming weight of a function: in this case $f + x_0$.

The situation becomes a little more complicated at $t = \frac{1}{4}$, $u = 1$, but examination of this case leads on to the general one. Write F_j for $(-1)^{f_j}$, and expand the sums to see the effects more easily:

$$\begin{aligned} P(\mathbf{f})(\frac{1}{4}) &= \left(\sum_{j=0}^{n-1}(-1)^{f_j}\cos 2\pi j\frac{1}{4}\right)^2 + \left(\sum_{j=0}^{n-1}(-1)^{f_j}\sin 2\pi j\frac{1}{4}\right)^2 \\ &= (F_0 + 0 - F_2 + 0 + F_4 + 0 - F_6 + \cdots - F_{n-2} + 0)^2 \\ &\quad + (0 + F_1 + 0 - F_3 + 0 + F_5 + \cdots + 0 - F_{n-1})^2. \end{aligned}$$

Both summations now contribute to the power. The alternating sign pattern is now different: $\cos\frac{\pi j}{2}$ alternates in sign as $\frac{\pi j}{2}$ takes on values that are π apart, i.e. the sign now changes at every other value of j (and not for every value of j as previously), and the sine terms similarly. As before this effect can be reproduced by adding a linear term to f, this time by adding x_1, so as to change the value of f (from 0 to 1 or vice-versa) at every *fourth* position. Also, only the even terms are to be added in the cosine sum, the odd ones in the sine sum. This can be achieved by restricting the function by x_0 and then using the notion of *compression*, introduced in Section 1.9.5, to regard the function to be only in the $m - 1$ remaining variables $x_1, \ldots, x_{m-1}$. The two summations in the expression for power thus become dependent on the weight of the two restricted, compressed 'halves' of the original function f plus x_1, which using the notation of Section 1.9.5 becomes:

$$P(\mathbf{f})(\frac{1}{4}) = \left(2^{m-1} - 2 \cdot wt_H(\widehat{f + x_1|_{x_0=0}})\right)^2 + \left(2^{m-1} - 2 \cdot wt_H(\widehat{f + x_1|_{x_0=1}})\right)^2.$$

This case is simplified due to the fact that half of the sine and cosine values disappear: in the more general case which now follows, this is no longer so, and a sum across all of the restricting constants appears in both the cosine and sine summations.

For the general case then of $t = \frac{1}{2^{u+1}}$, $u \geqslant 0$, substitute once more into (4.1). The linear term to be added to reproduce the sign changes is now x_u, and the restricting variables to gather the terms appropriate to each trigonometric term are $\mathbf{x} = x_{u-1} \cdots x_0$:

$$
\begin{aligned}
P(\mathbf{f})(\frac{1}{2^{u+1}}) &= \left(\sum_{j=0}^{n-1}(-1)^{f_j}\cos\frac{\pi j}{2^u}\right)^2 + \left(\sum_{j=0}^{n-1}(-1)^{f_j}\sin\frac{\pi j}{2^u}\right)^2 \\
&= \left(\sum_{k=0}^{2^u-1}\sum_{j=0}^{2^{m-u}-1}(-1)^{f_{2^u j+k}}\cos\frac{\pi(2^u j+k)}{2^u}\right)^2 \\
&\quad + \left(\sum_{k=0}^{2^u-1}\sum_{j=0}^{2^{m-u}-1}(-1)^{f_{2^u j+k}}\sin\frac{\pi(2^u j+k)}{2^u}\right)^2 \\
&= \left(\sum_{k=0}^{2^u-1}\cos\frac{\pi k}{2^u}\sum_{j=0}^{2^{m-u}-1}(-1)^{f_{2^u j+k}}(-1)^j\right)^2 \\
&\quad + \left(\sum_{k=0}^{2^u-1}\sin\frac{\pi k}{2^u}\sum_{j=0}^{2^{m-u}-1}(-1)^{f_{2^u j+k}}(-1)^j\right)^2 \\
&= \left(\sum_{k=0}^{2^u-1}\cos\frac{\pi k}{2^u}\sum_{j=0}^{2^{m-u}-1}(-1)^{(f+x_u)_{2^u j+k}}\right)^2 \\
&\quad + \left(\sum_{k=0}^{2^u-1}\sin\frac{\pi k}{2^u}\sum_{j=0}^{2^{m-u}-1}(-1)^{(f+x_u)_{2^u j+k}}\right)^2 \\
&= \left(\sum_{k=0}^{2^u-1}\cos\frac{\pi k}{2^u}(2^{m-u} - 2\cdot wt_H(\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}))\right)^2 \\
&\quad + \left(\sum_{k=0}^{2^u-1}\sin\frac{\pi k}{2^u}(2^{m-u} - 2\cdot wt_H(\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}))\right)^2
\end{aligned}
$$

where use has been made of $\cos\frac{\pi(2^u j+k)}{2^u} = (-1)^j\cos\frac{\pi k}{2^u}$, sine similarly, and in the restriction, $\mathbf{k}$ is the binary expansion of k. (Note that in the case when $u = 0$, $\mathbf{x}$ would be null, so take $(f + x_0)\big|_{\mathbf{x}=\mathbf{c}}$ to be just $f + x_0$, thus giving the same result as derived above.)

To further simplify, let

$$W_k = 2^{m-u} - 2\cdot wt_H(\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}) \text{ for } k = 0, \ldots, 2^u - 1,$$

and expand both factors to get

$$\begin{aligned}
P(\mathbf{f})(\frac{1}{2^{u+1}}) &= \left(\sum_{k=0}^{2^u-1} W_k \cos\frac{\pi k}{2^u}\right)^2 + \left(\sum_{k=0}^{2^u-1} W_k \sin\frac{\pi k}{2^u}\right)^2 \\
&= \sum_{k=0}^{2^u-1} W_k^2 \cos^2\frac{\pi k}{2^u} + 2\sum_{\ell=1}^{2^u-1}\sum_{k=0}^{2^u-1-\ell} W_k W_{k+\ell} \cos\frac{\pi k}{2^u} \cos\frac{\pi(k+\ell)}{2^u} \\
&\quad + \sum_{k=0}^{2^u-1} W_k^2 \sin^2\frac{\pi k}{2^u} + 2\sum_{\ell=1}^{2^u-1}\sum_{k=0}^{2^u-1-\ell} W_k W_{k+\ell} \sin\frac{\pi k}{2^u} \sin\frac{\pi(k+\ell)}{2^u} \\
&= \sum_{k=0}^{2^u-1} W_k^2 + 2\sum_{\ell=1}^{2^u-1}\sum_{k=0}^{2^u-1-\ell} W_k W_{k+\ell} \cos\frac{\pi \ell}{2^u} \\
&= \sum_{k=0}^{2^u-1} W_k^2 + 2\sum_{\ell=1}^{2^u-1} \cos\frac{\pi \ell}{2^u} \sum_{k=0}^{2^u-1-\ell} W_k W_{k+\ell} \\
&= A(\mathbf{W})(0) + 2\sum_{\ell=1}^{2^u-1} A(\mathbf{W})(\ell) \cos\frac{\pi \ell}{2^u},
\end{aligned}$$

where $\mathbf{W} = (W_0, \ldots, W_{2^u-1})$, and in the definition of $A(\mathbf{W})(\ell)$ we have used that $W_k^* = W_k$ since W_k is real. Note the similarity between this expression and (1.4): the difference being that the auto-correlation function in this expression is of a sequence of *sums* of elements of the original sequence. Even though each W_k derives from different components of the vector associated with $f + x_u$, as f is quadratic they can only take on one of the same three values. To see this, consider a Boolean function f of degree $\leqslant 2$ in m variables, as usual consisting of a quadratic part Q and an affine part L, i.e.

$$f = Q + L.$$

As already pointed out in Section 1.11, the graph of the restricted function $f\big|_{\mathbf{x}=\mathbf{c}}$ is independent of the choice of the restricting constant $\mathbf{c}$, or in other words the quadratic part of $f\big|_{\mathbf{x}=\mathbf{c}}$ does not depend on $\mathbf{c}$. This is unaffected by the compression operation, which merely re-labels the variables . Thus for the compressed function appearing above, $\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}$, we may denote the quadratic part by $\bar{Q}$, say, a function in $m-u$ variables, and let its rank be $2\bar{h}$. Then $\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}$ represents a word in the coset $\bar{Q} + RM_2(1, m-u)$, and so has a weight given by Theorem 4.2, i.e.

$$\begin{aligned}
wt_H(\widehat{f+x_u}\big|_{\mathbf{x}=\mathbf{k}}) = \; & 2^{m-u-1} - 2^{m-\bar{h}-u-1}, \quad \text{or} \\
& 2^{m-u-1}, \quad \text{or} \\
& 2^{m-u-1} + 2^{m-\bar{h}-u-1},
\end{aligned}$$

respectively known as minimum weight, half weight and maximum weight, and where $\bar{h} \leqslant \lfloor\frac{m-u}{2}\rfloor$. The three possible values taken by W_k are thus found by substituting each of these into the expression for W_k:

$$\begin{aligned} W_k &= 2^{m-u} - 2 \cdot wt_H(\widehat{f + x_u}\big|_{\mathbf{x}=\mathbf{k}}) \\ &= 2^{m-u} - 2(2^{m-u-1}) \\ &= 0 \quad \text{for half weight words,} \\ W_k &= 2^{m-u} - 2 \cdot wt_H(\widehat{f + x_u}\big|_{\mathbf{x}=\mathbf{k}}) \\ &= 2^{m-u} - 2(2^{m-u-1} \mp 2^{m-\bar{h}-u-1}) \\ &= \pm 2^{m-\bar{h}-u} \quad \text{for min/max weight words.} \end{aligned}$$

Setting

$$W_k = 2^{m-\bar{h}-u} W'_k, \quad W'_k \in \{0, \pm 1\},$$

the power of 2 term can be factored out from the auto-correlations to obtain the final expression for the instantaneous power at $t = \frac{1}{2^{u+1}}$:

$$P(\mathbf{f})(\frac{1}{2^{u+1}}) = 2^{2m-2\bar{h}-2u}\Big(A(\mathbf{W}')(0) + 2\sum_{\ell=1}^{2^u-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u}\Big). \tag{4.2}$$

In order to get a useful lower limit on the power from this expression, the conditions under which it is maximized need to be established. For certain functions f, for which the associated vectors $\mathbf{W}'$ have auto-correlations which are reasonably large and easily determined, this can be achieved, as is shown in the following theorem.

Theorem 4.6. *Let Q be a Boolean quadratic form in m variables, and let $2\bar{h}$ be its rank after restriction on the restricting variables $\mathbf{x} = x_{u-1} \cdots x_0$, where u is an integer, $1 \leqslant u \leqslant m-1$. Let $f = Q + L$ be some codeword in the coset $Q + RM_2(1,m)$. With $\mathbf{k}$ the binary expansion of k, if the weights of the compressed functions $\widehat{f + x_u}\big|_{\mathbf{x}=\mathbf{k}}$, $k = 0, 1, \ldots, 2^u - 1$, fit one of the configurations:*

$\widehat{f + x_u}\big|_{\mathbf{x}=\mathbf{k}}$ *is minimum weight for $k = 0, 1, \ldots, \alpha - 1$, and*
maximum weight for $k = \alpha, \ldots, 2^u - 1$,
with $0 \leqslant \alpha \leqslant 2^u$,

or

$\widehat{f + x_u}\big|_{\mathbf{x}=\mathbf{k}}$ *is minimum weight for $k = 0, 1, \ldots, \alpha - 2$,*
half weight when $k = \alpha - 1$, and
maximum weight for $k = \alpha, \ldots, 2^u - 1$,
with $1 \leqslant \alpha \leqslant 2^u - 1$,

or

either of the above with 'minimum' replaced
with 'maximum' and vice-versa,

then the PMEPR of the coset is greater than $2^{m-2\bar{h}-2}$ *(and where*

$$\begin{aligned} \textit{minimum weight is:} \qquad & wt_H\big(\widehat{f+x_u\big|_{\mathbf{x}=\mathbf{k}}}\big) &= 2^{m-u-1} - 2^{m-\bar{h}-u-1} \\ \textit{half weight is:} \qquad & \dots &= 2^{m-u-1} \\ \textit{maximum weight is:} \qquad & \dots &= 2^{m-u-1} + 2^{m-\bar{h}-u-1}). \end{aligned}$$

Proof. First, since the summation in (4.2) involves terms between 0 and π, we use the symmetry of cosine to reduce the range of the summation by half, so consider the term

$$\sum_{\ell=1}^{2^u-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u} = P_\Sigma, \quad \text{say.}$$

Since $\cos(\pi-\theta) = -\cos\theta$, write this as

$$\begin{aligned} P_\Sigma &= \sum_{\ell=1}^{2^{u-1}-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u} + \cos\frac{\pi}{2} + \sum_{\ell=2^{u-1}+1}^{2^u-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u} \\ &= \sum_{\ell=1}^{2^{u-1}-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u} - \sum_{\ell=2^{u-1}+1}^{2^u-1} A(\mathbf{W}')(\ell)\cos(\pi - \frac{\pi\ell}{2^u}) \\ &= \sum_{\ell=1}^{2^{u-1}-1} A(\mathbf{W}')(\ell)\cos\frac{\pi\ell}{2^u} - \sum_{\ell=1}^{2^{u-1}-1} A(\mathbf{W}')(2^u-\ell)\cos\frac{\pi\ell}{2^u} \\ &= \sum_{\ell=1}^{2^{u-1}-1} \big(A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u-\ell)\big)\cos\frac{\pi\ell}{2^u}, \end{aligned}$$

where a simple substitution to carry out the second summation over $2^u-\ell$ has enabled the two summations to be combined. By establishing expressions for the auto-correlations of the vectors $\mathbf{W}'$, the difference $A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u-\ell)$ can be substantially simplified.

From the work preceding the theorem which equates the weight of the compressed functions deriving from f to the value of the corresponding coordinate of $\mathbf{W}'$, the length 2^u vectors that we are interested in look either like

$$(\underbrace{+1,\dots,+1}_{\alpha \text{ terms}}, -1,\dots,-1),$$

or

$$(\underbrace{+1,\dots,+1,0}_{\alpha \text{ terms}}, -1,\dots,-1),$$

or -1 times these. Note from Theorems 1.1 and 1.8 that reversing such a vector or multiplying it by -1 does not affect its auto-correlation, and so without loss of generality we assume the first α coordinates are $+1$, and that α is restricted to half the length of the vector. Considering the case without the zero entry, we thus have, for $0 \leqslant \alpha \leqslant 2^{u-1}$,

$$\begin{aligned} W_i' &= +1, \quad i = 0,1,\dots,\alpha-1 \\ W_i' &= -1, \quad i = \alpha,\dots,2^u-1. \end{aligned}$$

In the definition of auto-correlation, breaking down the sum into partial sums whose terms are either all $+1$ or all -1 gives

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{2^u-1-\ell} W_i'W_{i+\ell}' \\ &= \sum_{i=0}^{\alpha-\ell-1} W_i'W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i'W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i'W_{i+\ell}'. \end{aligned}$$

Then for $0 \leqslant \ell \leqslant \alpha$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i'W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i'W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i'W_{i+\ell}' \\ &= (\alpha-\ell) + (-\ell) + (2^u-\ell-\alpha) \\ &= 2^u - 3\ell. \end{aligned}$$

For $\alpha < \ell < 2^u - \alpha$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i'W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i'W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i'W_{i+\ell}' \\ &= 0 + \sum_{i=0}^{\alpha-1} W_i'W_{i+\ell}' + (2^u-\ell-\alpha) \\ &= 0 + (-\alpha) + (2^u-\ell-\alpha) \\ &= 2^u - \ell - 2\alpha. \end{aligned}$$

And for $2^u - \alpha \leqslant \ell < 2^u$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i'W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i'W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i'W_{i+\ell}' \\ &= 0 + \sum_{i=0}^{2^u-\ell-1} W_i'W_{i+\ell}' + 0 \\ &= 0 + (-(2^u-\ell)) + 0 \\ &= \ell - 2^u. \end{aligned}$$

Note that for $\ell = 0$ we have

$$A(\mathbf{W}')(0) = 2^u,$$

and that when $\alpha = 0$, i.e. the vector is all of the same sign,

$$A(\mathbf{W}')(\ell) = 2^u - \ell, \quad 0 \leqslant \ell < 2^u,$$

as is well known. Now when $1 \leqslant \ell \leqslant \alpha$ we get $2^u - \alpha \leqslant 2^u - \ell \leqslant 2^u - 1$, giving

$$\begin{aligned} A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u-\ell) &= 2^u - 3\ell - \big((2^u-\ell) - 2^u\big) \\ &= 2^u - 2\ell, \end{aligned}$$

and when $\alpha < \ell < 2^u - \alpha$ we get $\alpha < 2^u - \ell < 2^u - \alpha$, giving

$$\begin{aligned} A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u - \ell) &= 2^u - \ell - 2\alpha - \big(2^u - (2^u - \ell) - 2\alpha\big) \\ &= 2^u - 2\ell. \end{aligned}$$

Thus, since $\alpha \leqslant 2^{u-1}$ means that $2^u - \alpha \geqslant 2^{u-1}$, we have that

$$A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u - \ell) = 2^u - 2\ell, \quad \text{for } 1 \leqslant \ell \leqslant 2^{u-1} - 1.$$

Consider now the case when the $\mathbf{W}'$ contain the single zero entry. So for the case $1 \leqslant \alpha \leqslant 2^{u-1}$,

$$\begin{aligned} W_i' &= +1, \quad i = 0, 1, \ldots, \alpha - 2 \\ W_{\alpha-1}' &= 0 \\ W_i' &= -1, \quad i = \alpha, \ldots, 2^u - 1. \end{aligned}$$

Then for $\ell = 0$:

$$\begin{aligned} A(\mathbf{W}')(0) &= \sum_{i=0}^{2^u-1} W_i' W_i' \\ &= \sum_{i=0}^{\alpha-2} W_i' W_i' + \sum_{i=\alpha}^{2^u-1} W_i' W_i' \\ &= (\alpha - 1) + (2^u - \alpha) \\ &= 2^u - 1. \end{aligned}$$

For $1 \leqslant \ell < \alpha$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i' W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i' W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i' W_{i+\ell}' \\ &= \sum_{i=0}^{\alpha-\ell-2} W_i' W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-2} W_i' W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i' W_{i+\ell}' \\ &= (\alpha - \ell - 1) + (-(\ell - 1)) + (2^u - \ell - \alpha) \\ &= 2^u - 3\ell. \end{aligned}$$

For $\alpha \leqslant \ell \leqslant 2^u - \alpha$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i' W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i' W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i' W_{i+\ell}' \\ &= 0 + \sum_{i=0}^{\alpha-2} W_i' W_{i+\ell}' + (2^u - \ell - \alpha) \\ &= 0 + (-(\alpha - 1)) + (2^u - \ell - \alpha) \\ &= 2^u - \ell - 2\alpha + 1. \end{aligned}$$

And for $2^u - \alpha < \ell < 2^u$:

$$\begin{aligned} A(\mathbf{W}')(\ell) &= \sum_{i=0}^{\alpha-\ell-1} W_i' W_{i+\ell}' + \sum_{i=\alpha-\ell}^{\alpha-1} W_i' W_{i+\ell}' + \sum_{i=\alpha}^{2^u-1-\ell} W_i' W_{i+\ell}' \\ &= 0 + \sum_{i=0}^{2^u-\ell-1} W_i' W_{i+\ell}' + 0 \\ &= 0 + (-(2^u - \ell)) + 0 \\ &= \ell - 2^u. \end{aligned}$$

Again, to establish the difference between the auto-correlations, for $1 \leqslant \ell < \alpha$ we have $2^u - \alpha < 2^u - \ell \leqslant 2^u - 1$, and so

$$\begin{aligned} A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u - \ell) &= 2^u - 3\ell - \big((2^u - \ell) - 2^u\big) \\ &= 2^u - 2\ell, \end{aligned}$$

and for $\alpha \leqslant \ell \leqslant 2^u - \alpha$ we have $\alpha \leqslant 2^u - \ell \leqslant 2^u - \alpha$, giving

$$\begin{aligned} A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u - \ell) &= 2^u - \ell - 2\alpha + 1 - \big(2^u - (2^u - \ell) - 2\alpha + 1\big) \\ &= 2^u - 2\ell. \end{aligned}$$

Thus for either type of vector $\mathbf{W}'$ we get

$$A(\mathbf{W}')(\ell) - A(\mathbf{W}')(2^u - \ell) = 2^u - 2\ell, \quad \text{for } 1 \leqslant \ell \leqslant 2^{u-1} - 1.$$

and so we now have

$$P_\Sigma = \sum_{\ell=1}^{2^{u-1}-1} (2^u - 2\ell) \cos \frac{\pi \ell}{2^u}.$$

Using the standard Taylor series expansion for cosine, we have that $\cos x > 1 - \frac{x^2}{2!}$ and thus we get that

$$\begin{aligned} P_\Sigma &> \sum_{\ell=1}^{2^{u-1}-1} (2^u - 2\ell)\Big(1 - \frac{\pi^2 \ell^2}{2^{2u+1}}\Big) \\ &= \frac{1}{2^{2u}} \sum_{\ell=1}^{2^{u-1}-1} (2^{u-1} - \ell)(2^{2u+1} - \pi^2 \ell^2) \\ &= \frac{1}{2^{2u}} \sum_{\ell=1}^{2^{u-1}-1} (2^{3u} - 2^{2u+1}\ell - 2^{u-1}\pi^2 \ell^2 + \pi^2 \ell^3) \\ &= \frac{1}{2^{2u}} \Big(2^{3u}(2^{u-1} - 1) - \frac{2^{2u+1}}{2}\big((2^{u-1} - 1)2^{u-1}\big) \\ &\quad - \frac{2^{u-1}\pi^2}{6}\big((2^{u-1} - 1)2^{u-1}(2^u - 1)\big) + \frac{\pi^2}{4}\big((2^{u-1} - 1)^2 2^{2u-2}\big)\Big) \\ &\ \vdots \\ &= 2^{2u-2} - 2^{u-1} - \frac{\pi^2}{3} 2^{2u-6} + \frac{\pi^2}{48}, \end{aligned}$$

after some not inconsiderable manipulation. Since

$$A(\mathbf{W}')(0) \geqslant 2^u - 1$$

for both types of vectors, substituting for this and the above expression for P_Σ back into (4.2) gives

$$\begin{aligned}
P(\mathbf{f})(\frac{1}{2^{u+1}}) &> 2^{2m-2\bar{h}-2u}\Big(2^u - 1 + 2\big(2^{2u-2} - 2^{u-1} - \frac{\pi^2}{3}2^{2u-6} + \frac{\pi^2}{48}\big)\Big) \\
&= 2^{2m-2\bar{h}-2u}\Big(2^{2u-1} - \frac{\pi^2}{3}2^{2u-5} + \frac{\pi^2}{24} - 1\Big) \\
&= 2^{2m-2\bar{h}-2u}\Big(2^{2u-1}(1 - \frac{\pi^2}{48}) + \frac{\pi^2}{24} - 1\Big) \\
&= 2^{2m-2\bar{h}-2u}\Big(2^{2u-1}\frac{1}{2} + 2^{2u-1}(1 - \frac{\pi^2}{48} - \frac{1}{2}) + \frac{\pi^2}{24} - 1\Big) \\
&= 2^{2m-2\bar{h}-2u}\Big(2^{2u-1}\frac{1}{2} + 2^{2u-1}(\frac{1}{2} - \frac{\pi^2}{48}) + \frac{\pi^2}{24} - 1\Big) \\
&> 2^{2m-2\bar{h}-2u}\Big(2^{2u-1}\frac{1}{2} + 2(\frac{1}{2} - \frac{\pi^2}{48}) + \frac{\pi^2}{24} - 1\Big) \\
&= 2^{2m-2\bar{h}-2},
\end{aligned}$$

where we have used $u \geqslant 1$ to get the last inequality. Thus the power at $t = \frac{1}{2^{u+1}}$ is certainly greater than $2^{2m-2\bar{h}-2}$, and so the peak power will be too, and on dividing by the mean power, 2^m, we get that the PMEPR will be at least $2^{m-2\bar{h}-2}$. □

For the case $u = 2$, $t = \frac{1}{8}$ it is a straightforward matter to calculate $P(\mathbf{f})(\frac{1}{8})$ for all 3^4 possible $\mathbf{W}'$ vectors. Doing so for the 16 vectors that satisfy the theorem, for example,

$$(+1, -1, -1, -1) \text{ and } (-1, -1, 0, +1),$$

gives the values

$$P(\mathbf{f})(\frac{1}{8}) = (4 + 2\sqrt{2}) \cdot 2^{2m-2\bar{h}-4}$$

and

$$P(\mathbf{f})(\frac{1}{8}) = (3 + 2\sqrt{2}) \cdot 2^{2m-2\bar{h}-4}$$

respectively. Since both $4+2\sqrt{2}$ and $3+2\sqrt{2}$ are greater than 4, and on dividing by 2^m, it is seen that both these power values imply a PMEPR$> 2^{m-2\bar{h}-2}$, thus agreeing with the theorem.

The trick in being able to use this theorem is in finding a quadratic form Q that has a low rank after restriction, and within whose coset there exists an $f = Q + L$ for which the linear terms, after adding x_u and restricting, actually give functions with weights in the right combination, as specified by the theorem. For the $t = \frac{1}{8}$ case this is possible and is explored in the next section. The difficulties encountered in attempting to generalize the method are returned to in Section 4.5.

4.4 Families of Binary Sequences providing Counterexamples to Conjecture 1

Using the theory of the preceding section, for the case of $u = 2$, $t = \frac{1}{8}$, two families of quadratic Boolean functions are now constructed, which satisfy the hypothesis of Conjecture 1 of Chapter 2, but within the cosets of which there exist words whose PMEPRs are bigger than the bound given by the conjecture. The idea is to find an f whose rank, $2\bar{h}$, after restriction using the restricting variables $\mathbf{x} = x_1x_0$, is small, and whose four compressed functions have a weight configuration given by Theorem 4.6, so that the lower bound on the PMEPR from the theorem, $2^{m-\bar{h}-2}$, is greater than the upper bound on the PMEPR from the conjecture, 2^{k+1}, where k is the number of delete vertices.

Recapping from Chapter 2, if in the graph of some quadratic form Q some $k \geqslant 1$ vertices are *deleted*, and this results in a graph consisting of a path and *isolated* vertices, then Conjecture 1 says the PMEPR of the coset of Q is at most 2^{k+1}. Chapter 2 contains proofs of the conjecture for some special cases involving at most two isolated vertices, and where Q is a quadratic form over $\mathbb{Z}_q$. In this section two families of *Boolean* functions are constructed (i.e. Q is over $\mathbb{Z}_2$), each having at least *three* isolated vertices following the deletions, for which the PMEPR of the coset is greater than the upper bound on PMEPR from the conjecture, thus showing that Conjecture 1 cannot be true in general. Here the path that would be left if the deletion operations were to be carried out is called the *residual* path, but note that the restriction which is equivalent to these deletion operations is NOT the same as the restrictions which are applied below. The residual path is measured by the number of edges it has in the graph, and which equals the number of second order terms in its algebraic normal form.

Throughout this section, in determining the weight of the compressed functions for Theorem 4.6, the final re-labelling operation has been omitted in order to keep the notation as simple as possible, but on the understanding that the restricted functions involved are regarded as being in a reduced number of variables, and that the re-labelling could be done if required.

4.4.1 Family 1

Functions in this family have 1 delete vertex, a 1-edge residual path, and $m-3 \geqslant 3$ isolated vertices, and so $m \geqslant 6$, and are given by the quadratic form Q, in m variables:

$$Q = x_0x_1 + \sum_{i=0}^{m-2} x_ix_{m-1}.$$

So the delete vertex is $m-1$, the residual path is x_0x_1, and the isolated vertices are $2, \ldots, m-2$. The graph for Q is shown in Figure 4.2.

Then we claim that there exists a word in the coset $Q + RM_2(1, m)$ which has PMEPR$>$ 4, and thus Conjecture 1, which for the single delete vertex says all words in the coset have PMEPR$\leqslant 2^{1+1} = 4$, is not true for this family.

To prove the claim we find a word in the coset whose power at $t = \frac{1}{8}$ is large, i.e. the PMEPR of the word as given by Theorem 4.6 is greater than the bound

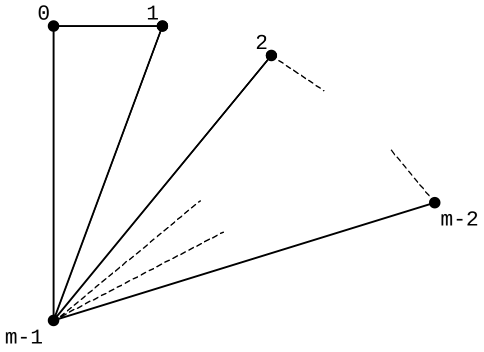

Figure 4.2: The graph for Family 1

given by the conjecture. Restrict $Q+x_2$ using the restricting variables $\mathbf{x}=x_1x_0$ over all values:

$$\begin{aligned}(Q+x_2)\big|_{x_1x_0=00} &= x_2+\sum_{i=2}^{m-2}x_ix_{m-1}=x_2+\bar{Q}\text{ say}\\ (Q+x_2)\big|_{x_1x_0=01} &= x_2+x_{m-1}+\bar{Q}\\ (Q+x_2)\big|_{x_1x_0=10} &= x_2+x_{m-1}+\bar{Q}\\ (Q+x_2)\big|_{x_1x_0=11} &= 1+x_2+\bar{Q},\end{aligned}$$

where we have put

$$\bar{Q}=\sum_{i=2}^{m-2}x_ix_{m-1}.$$

$\bar{Q}$ is a quadratic form in the $m-2$ variables $x_2,\ldots,x_{m-1}$: apply the following transformation to get it into the canonical form of Theorem 4.1, thus determining $\bar{h}$,

$$\begin{aligned}x_2 &= \sum_{i=2}^{m-2}x'_i\\ x_i &= x'_i,\quad 3\leqslant i\leqslant m-1\end{aligned}$$

So

$$\begin{aligned}\bar{Q}=\sum_{i=2}^{m-2}x_ix_{m-1}\Rightarrow\bar{Q}' &= x'_{m-1}\sum_{i=2}^{m-2}x'_i+\sum_{i=3}^{m-2}x'_ix'_{m-1}\\ &= x'_2x'_{m-1},\end{aligned}$$

which (apart from re-labelling) is clearly of the required form with $\bar{h}=1$. Thus, according to Lemma 4.3, the functions

$$\bar{Q}'+a_2x'_2+a_{m-1}x'_{m-1}+\varepsilon,\quad a_2,a_{m-1},\varepsilon\in\mathbb{Z}_2,$$

are maximum or minimum weight words. Applying the inverse transformation

$$\begin{aligned} x_2' &= \sum_{i=2}^{m-2} x_i \\ x_i' &= x_i, \quad 3 \leqslant i \leqslant m-1 \end{aligned}$$

shows that the functions

$$\bar{Q} + a_2 \sum_{i=2}^{m-2} x_i + a_{m-1}x_{m-1} + \varepsilon$$

are also maximum or minimum weight words. Thus a suitable word from within the coset $Q + RM_2(1, m)$ would be

$$f = Q + \sum_{i=3}^{m-2} x_i.$$

Restricting $f + x_2$ using the restricting variables $\mathbf{x} = x_1x_0$ over all values gives:

$$\begin{aligned} (f + x_2)\big|_{x_1x_0=00} &= \bar{Q} + x_2 + \sum_{i=3}^{m-2} x_i = \bar{Q} + \sum_{i=2}^{m-2} x_i \\ (f + x_2)\big|_{x_1x_0=01} &= \bar{Q} + \sum_{i=2}^{m-2} x_i + x_{m-1} \\ (f + x_2)\big|_{x_1x_0=10} &= \bar{Q} + \sum_{i=2}^{m-2} x_i + x_{m-1} \\ (f + x_2)\big|_{x_1x_0=11} &= 1 + \bar{Q} + \sum_{i=2}^{m-2} x_i, \end{aligned}$$

from which it is seen that all four are maximum or minimum weight words: $(f + x_2)\big|_{x_1x_0=01} = (f + x_2)\big|_{x_1x_0=10}$ and so have the same weight, and since $(f+x_2)\big|_{x_1x_0=11} = (f+x_2)\big|_{x_1x_0=00}+1$, if $(f+x_2)\big|_{x_1x_0=00}$ is maximum or minimum weight then $(f+x_2)\big|_{x_1x_0=11}$ is minimum or maximum weight respectively. Thus as the restriction constant varies as

$$\begin{array}{cccc} 00 & 01 & 10 & 11 \end{array}$$

the weights vary as

$$\begin{array}{lllll} \text{min} & \text{min} & \text{min} & \text{max}, & \textit{or} \\ \text{max} & \text{max} & \text{max} & \text{min}, & \textit{or} \\ \text{min} & \text{max} & \text{max} & \text{max}, & \textit{or} \\ \text{max} & \text{min} & \text{min} & \text{min}. & \end{array}$$

These all satisfy the first configuration in Theorem 4.6, and as $\bar{h} = 1$ and $m \geqslant 6$, f thus has PMEPR $> 2^{m-2\bar{h}-2} = 2^{m-4} \geqslant 2^2$, i.e. the PMEPR of the coset is greater than 4, as claimed.

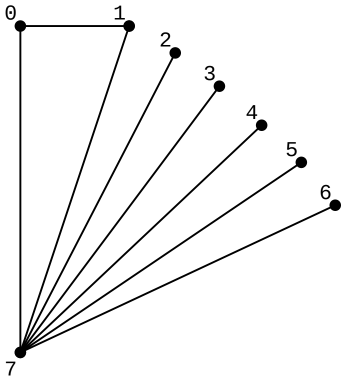

Figure 4.3: The graph for Example 4.7

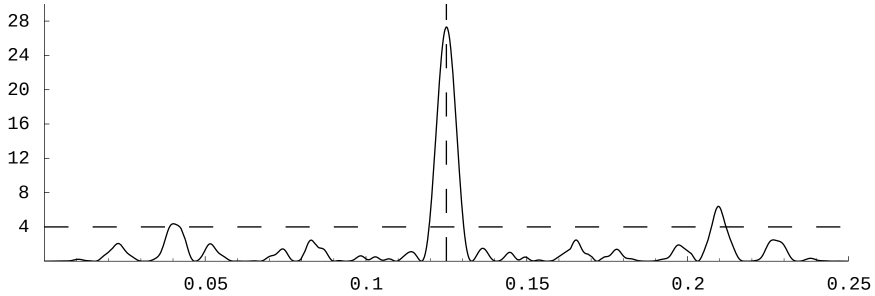

Figure 4.4: Envelope power of $Q + x_3 + x_4 + x_5 + x_6$ for Example 4.7

Example 4.7. As an example, take $m = 8$. Then the quadratic form is

$$Q = x_0x_1 + \sum_{i=0}^{6} x_ix_7,$$

so the delete vertex is 7, the residual path is x_0x_1, and the isolated vertices are $2, 3, 4, 5$ and 6. The graph for Q is shown in Figure 4.3. The lower bound from Theorem 4.6 is $2^{m-4} = 2^4$. Part of the envelope power for the function $Q + x_3 + x_4 + x_5 + x_6$ is shown in Figure 4.4, clearly showing a peak greater than 16 at $t = \frac{1}{8}$, being much larger than the upper bound of 4 predicted by Conjecture 1 (also indicated on the plot). It should be noted that there are many other functions in the coset which do *not* satisfy the conditions of Theorem 4.6, but which nevertheless have large peaks in their power at values of t different from $\frac{1}{8}$, e.g. $Q + x_3 + x_4 + x_5$, part of whose envelope power is shown in Figure 4.5. □

4.4.2 Family 2

Functions in this family have 2 delete vertices, a 1-edge residual path, and $m - 4 \geqslant 3$ isolated vertices, and so $m \geqslant 7$, and are given by the quadratic form

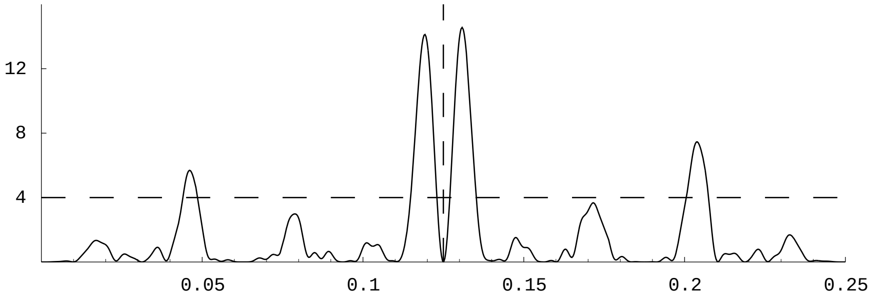

Figure 4.5: Envelope power of $Q + x_3 + x_4 + x_5$ for Example 4.7

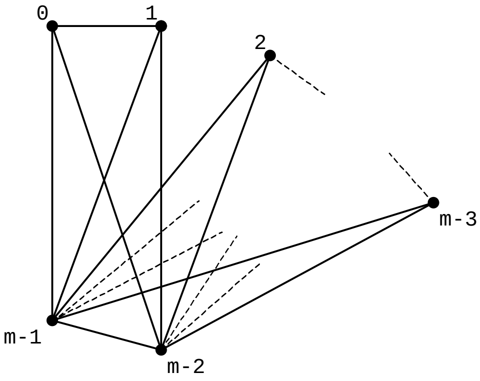

Figure 4.6: The graph for Family 2

Q in m variables:

$$Q = x_0x_1 + \sum_{i=0}^{m-2} x_ix_{m-1} + \sum_{i=0}^{m-3} x_ix_{m-2}.$$

So the delete vertices are $m-1$ and $m-2$, the residual path is x_0x_1, and the isolated vertices are $2, \ldots, m-3$. The graph for this Q is shown in Figure 4.6.

Then we claim that there exists a word in the coset $Q + RM_2(1, m)$ which has PMEPR>8, and thus Conjecture 1, which for the 2 delete vertices, says all words in the coset have PMEPR$\leqslant 2^{2+1} = 8$, is not true for this family also.

The method of proof is as for family 1, thus restrict $Q + x_2$ using the restricting variables $\mathbf{x} = x_1x_0$ over all values:

$$\begin{aligned}
(Q + x_2)\big|_{x_1x_0=00} &= x_2 + \sum_{i=2}^{m-2} x_ix_{m-1} + \sum_{i=2}^{m-3} x_ix_{m-2} = x_2 + \bar{Q} \text{ say} \\
(Q + x_2)\big|_{x_1x_0=01} &= x_2 + x_{m-1} + x_{m-2} + \bar{Q} \\
(Q + x_2)\big|_{x_1x_0=10} &= x_2 + x_{m-1} + x_{m-2} + \bar{Q} \\
(Q + x_2)\big|_{x_1x_0=11} &= 1 + x_2 + \bar{Q}
\end{aligned}$$

where we have put

$$\bar{Q} = \sum_{i=2}^{m-2} x_i x_{m-1} + \sum_{i=2}^{m-3} x_i x_{m-2}. \tag{4.3}$$

Apply the following transformation to $\bar{Q}$:

$$\begin{aligned} x_2 &= \sum_{i=2}^{m-2} x'_i \\ x_i &= x'_i, \quad 3 \leqslant i \leqslant m-2 \\ x_{m-1} &= x'_{m-1} + x'_{m-2}. \end{aligned}$$

So

$$\begin{aligned} \bar{Q} = \sum_{i=2}^{m-2} x_i x_{m-1} + \sum_{i=2}^{m-3} x_i x_{m-2} & \\ \Rightarrow \bar{Q}' &= (x'_{m-1} + x'_{m-2}) \sum_{i=2}^{m-2} x'_i + (x'_{m-1} + x'_{m-2}) \sum_{i=3}^{m-2} x'_i \\ &\quad + \sum_{i=2}^{m-2} x'_i x'_{m-2} + \sum_{i=3}^{m-3} x'_i x'_{m-2} \\ &= x'_2 x'_{m-1} + x'_{m-2}, \end{aligned}$$

which again, apart from re-labelling, is of the form given by Theorem 4.1 with $\bar{h} = 1$. Due to the fact $x_{m-2} = x'_{m-2}$ in the transformation it is readily seen that

$$\bar{Q} + x_{m-2} \leftrightarrow x'_2 x'_{m-1} = \bar{Q}' + x'_{m-2},$$

and thus, according to Lemma 4.3, the functions

$$\bar{Q}' + x'_{m-2} + a_2 x'_2 + a_{m-1} x'_{m-1} + \varepsilon, \quad a_2, a_{m-1}, \varepsilon \in \mathbb{Z}_2,$$

are maximum or minimum weight words. Applying the inverse transformation

$$\begin{aligned} x'_2 &= \sum_{i=2}^{m-2} x_i \\ x'_i &= x_i, \quad 3 \leqslant i \leqslant m-2 \\ x'_{m-1} &= x_{m-1} + x_{m-2}, \end{aligned}$$

thus shows that the functions

$$\begin{aligned} \bar{Q} + x_{m-2} + a_2 \sum_{i=2}^{m-2} x_i + a_{m-1}(x_{m-1} + x_{m-2}) + \varepsilon & \\ = \bar{Q} + a_2 \sum_{i=2}^{m-3} x_i + a_{m-1} x_{m-1} &+ (1 + a_2 + a_{m-1}) x_{m-2} + \varepsilon, \end{aligned}$$

or more explicitly

$$\bar{Q} + x_{m-2}, \quad \bar{Q} + \sum_{i=2}^{m-3} x_i, \quad \bar{Q} + x_{m-1}, \quad \bar{Q} + \sum_{i=2}^{m-1} x_i,$$

are maximum or minimum weight words. Thus a suitable word from within the coset $Q + RM_2(1, m)$ would be

$$f = Q + \sum_{i=3}^{m-3} x_i.$$

Restricting $f + x_2$ using the restricting variables $\mathbf{x} = x_1x_0$ over all values gives:

$$\begin{aligned}
(f + x_2)\big|_{x_1x_0=00} &= \bar{Q} + x_2 + \sum_{i=3}^{m-3} x_i & &= \bar{Q} + \sum_{i=2}^{m-3} x_i \\
(f + x_2)\big|_{x_1x_0=01} &= \bar{Q} + x_2 + x_{m-1} + x_{m-2} + \sum_{i=3}^{m-3} x_i & &= \bar{Q} + \sum_{i=2}^{m-1} x_i \\
(f + x_2)\big|_{x_1x_0=10} &= \bar{Q} + x_2 + x_{m-1} + x_{m-2} + \sum_{i=3}^{m-3} x_i & &= \bar{Q} + \sum_{i=2}^{m-1} x_i \\
(f + x_2)\big|_{x_1x_0=11} &= 1 + \bar{Q} + x_2 + \sum_{i=3}^{m-3} x_i & &= 1 + \bar{Q} + \sum_{i=2}^{m-3} x_i,
\end{aligned}$$

from which it is seen that all four are maximum or minimum weight words, and as before: $(f+x_2)\big|_{x_1x_0=01} = (f+x_2)\big|_{x_1x_0=10}$ and so have the same weight, and since $(f+x_2)\big|_{x_1x_0=11} = (f+x_2)\big|_{x_1x_0=00}+1$, if $(f+x_2)\big|_{x_1x_0=00}$ is maximum or minimum weight then $(f+x_2)\big|_{x_1x_0=11}$ is minimum or maximum weight respectively. This results in the same weight configurations as Family 1, and thus satisfies the first configuration in Theorem 4.6, and as $\bar{h} = 1$ and $m \geqslant 7$, f thus has PMEPR $> 2^{m-2\bar{h}-2} = 2^{m-4} \geqslant 2^3$, i.e. the PMEPR of the coset is greater than 8, as claimed.

Example 4.8. For this example, take $m = 7$. Then the quadratic form is

$$Q = x_0x_1 + \sum_{i=0}^{5} x_ix_6 + \sum_{i=0}^{4} x_ix_5,$$

so the delete vertices are 5 and 6, the residual path is x_0x_1, and the isolated vertices are 2, 3 and 4. The graph for Q is shown in Figure 4.7. The lower bound from Theorem 4.6 is $2^{m-4} = 2^3$. Part of the envelope power for the function $Q + x_3 + x_4$ is shown in Figure 4.8, showing a peak $\geqslant 8$ at $t = \frac{1}{8}$, again greater than the upper bound of 8 predicted by Conjecture 1 (also indicated on the plot). □

4.5 Difficulties in Extending the Technique

The previous section has shown how the results of Section 4.3 may be used to construct some relatively simple quadratic functions within whose cosets there

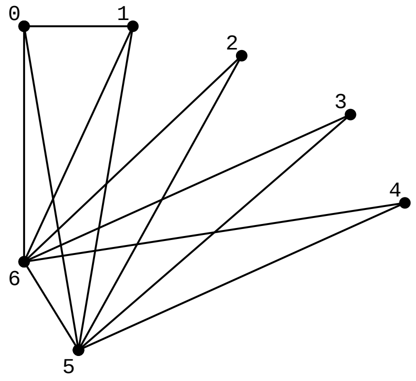

Figure 4.7: The graph for Example 4.8

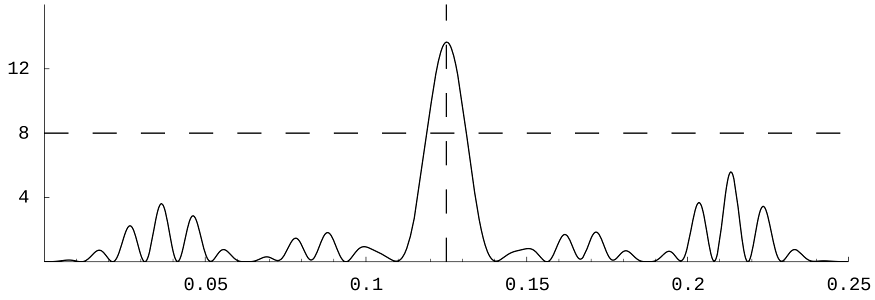

Figure 4.8: Envelope power for Example 4.8

exist words with PMEPRs greater than the upper bound predicted by Conjecture 1, thus showing that the conjecture cannot be true in general. However, attempts to generalize the constructions of the previous section run into a variety of difficulties, and these are explored in this section.

4.5.1 Increasing the number of delete vertices

To make use of Theorem 4.6 to construct a counter-example to Conjecture 1, the PMEPR from the theorem, $2^{m-2\bar{h}-2}$, must be greater than or equal to the PMEPR from the conjecture, 2^{k+1}, where there are k delete vertices, and this imposes an upper limit on $\bar{h}$:

$$\begin{aligned} m - 2\bar{h} - 2 &\geqslant k + 1, \\ \Rightarrow \bar{h} &\leqslant \frac{m-k-3}{2}. \end{aligned}$$

Staying with the $t = \frac{1}{8}$ case, suppose we extended the 2 delete vertex case of Example 4.8 of Family 2 above in the obvious way: add an extra delete vertex, so now $m = 8$, and connect all the delete vertices to all the other vertices, giving

$$Q = x_0x_1 + \sum_{i=0}^{6} x_ix_7 + \sum_{i=0}^{5} x_ix_6 + \sum_{i=0}^{4} x_ix_5,$$

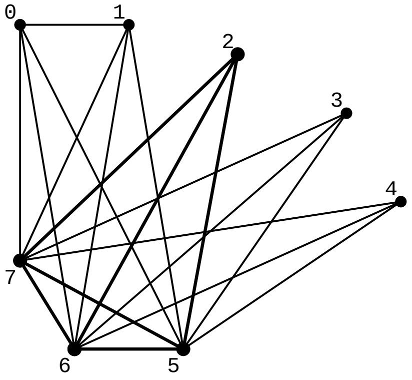

Figure 4.9: Graph for Q of Section 4.5.1

so the delete vertices are 5, 6 and 7, the residual path is x_0x_1, and the isolated vertices are 2, 3 and 4 (see Figure 4.9 for the graph). For this example, $m = 8, k = 3$, and so a PMEPR greater than $2^{3+1} = 16$ is sought: the above limit on $\bar{h}$ implies that $\bar{h}$ needs to be less than or equal to 1. Restricting on the variables $\mathbf{x} = x_1x_0$ gives the quadratic part

$$\bar{Q} = \sum_{i=2}^{6} x_i x_7 + \sum_{i=2}^{5} x_i x_6 + \sum_{i=2}^{4} x_i x_5,$$

which under the transformation

$$\begin{aligned} x_2 &= x_2' + x_3' + x_4' \\ x_i &= x_i', \quad 3 \leqslant i \leqslant 7 \end{aligned}$$

gives

$$\bar{Q}' = x_2'x_7' + x_5'x_7' + x_6'x_7' + x_2'x_6' + x_5'x_6' + x_2'x_5'.$$

The graph of $\bar{Q}'$ is the complete graph on 4 vertices, i.e. K_4 (emphasized in the figure), and $\bar{Q}'$ in fact has full rank [24, p55], i.e. $2\bar{h} = 4$ so that $\bar{h} = 2$. Thus Theorem 4.6 only gives a lower bound of $2^2 = 4$, and so it cannot be guaranteed that there exists a function in the coset whose power at $t = \frac{1}{8}$ would yield a PMEPR greater than 16. (In fact computation shows that there are some words whose powers at $t = \frac{1}{8}$ yield PMEPRs of ≈ 6, but which of course are not big enough to disprove the conjecture. Nevertheless computation also shows that the coset of this Q does contain words with PMEPRs> 16: several exhibit peaks that exceed 16 at values of t either side of $t = \frac{1}{8}$, but not *at* $\frac{1}{8}$. Attempts to explain these cases have been made, but no effective analysis was forthcoming. Plots of some typical words are appended at the end of this chapter in Figures 4.18,4.19 and 4.20.)

4.5.2 Increasing the residual path length

At first sight it may appear that this would give similar problems to increasing the number of delete vertices: the rank of a quadratic form *very* roughly equates

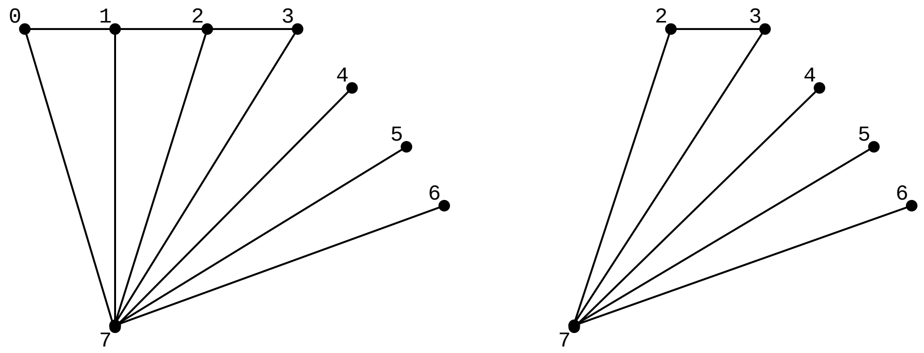

Figure 4.10: Graphs for Q (left) and $\bar{Q}$ of Section 4.5.2

to the number of edges and 'complexity' of its graph (many edges/highly 'connected' tends to imply high rank, whilst few edges/more simply connected implies a lower one), so after the restriction on the variables $\mathbf{x} = x_1 x_0$, any extra edges between the longer path and the delete vertices may contrive to make the rank of $\bar{Q}$ high. However as the number of deletes k is held constant, and the total number of vertices m increases to accommodate the longer path, the difference $m-k$ actually increases, and so does not impose a tighter limit on $\bar{h}$ from the expression $\bar{h} \leqslant \frac{m-k-3}{2}$, as it does in the example of the previous section. In fact it is probable that counter-examples to the conjecture with a longer residual path can be constructed for both the single and double deleted vertices cases for $u = 2$: in both Families 1 and 2 in Section 4.4 if the residual path is increased to length 2 (as $x_0x_1 + x_1x_2$, and now with $m-3-k \geqslant 3$ isolated vertices) and the new path vertex is connected to all delete vertices, after the restriction it is seen that the form of $\bar{Q}$ remains as the length 1 path cases shown, and so the rank of $\bar{Q}$ is the same too. Further increases in length may also be possible: consider that Q with a length 3 residual path and one delete vertex, and whose graph is as shown on the left in Figure 4.10. After the restriction, the graph of $\bar{Q}$ is as on the right in the figure. The expression $\bar{h} \leqslant \frac{m-k-3}{2}$ gives $\bar{h} \leqslant 2$ in this case: the simple transformation

$$\begin{aligned} x_2 &= x_2' + x_3' + x_7' \\ x_3 &= x_3' + x_7' \\ x_4 &= x_4' + x_5' + x_6' \\ x_i &= x_i', \quad i = 5, 6, 7, \end{aligned}$$

leads to the canonical form in four variables, so that $\bar{h} = 2$, and thus it may be possible to find a suitable f, in the coset of Q, which has large power at $t = \frac{1}{8}$. With some persistence in establishing the transformation to get to the canonical form, even longer residual path lengths may be possible. In fact it is even conceivable that two more families, for $k = 1$ or 2 delete vertices, a length $\ell \geqslant 1$ residual path and $m-(\ell+1)-k \geqslant 3$ isolated vertices could be constructed.

4.5.3 Increasing the number of vertices

For a given number of delete vertices, i.e. with k fixed, it is of course possible to increase m, and thus also the number of isolated vertices, until $\frac{m-k-3}{2}$ is greater than or equal to any given $\bar{h}$. This approach may be adopted to circumvent the problem of Section 4.5.1, but a certain amount of generality will have been lost. Working with a larger value of $\bar{h}$ is also not without its disadvantages. Continuing to consider the example of Section 4.5.1, in order to allow $\bar{h} = 2$ requires that m satisfy $2 \leqslant \frac{m-3-3}{2}$, that is $m \geqslant 10$. One is then faced with the task of transforming the function whose graph is K_4 ($\bar{Q}'$ above) to get to the canonical form, and then working backwards to see if an f can be found, all of whose compressed functions fit one of the configurations given in Theorem 4.6. The canonical form now has 4 variables in it, and so there will be a total of 16 functions of maximum or minimum weight which are possible candidates for the four restrictions of $f + x_2$: whether this makes the task easier or just confounds it, either way it is quite an involved one.

4.5.4 Increasing the time parameter, u

Even though Theorem 4.6 is proven for $1 \leqslant u \leqslant m-1$, working with $u > 2$ also presents difficulties. For $u = 2$ the restriction used is on two variables, $\mathbf{x} = x_1x_0$, and the preceding sections have shown that a Q can be devised that has a low rank for both the 1 and 2 delete vertices cases. With $u = 3$, the restriction is now on *three* variables, $\mathbf{x} = x_2x_1x_0$: does this give enough extra scope to be able to more easily manufacture a Q for 3 delete vertices? The extra restriction now gives the ability to remove more edges from the graph, and as, roughly speaking, more edges tend to mean higher rank, this could perhaps lead to a low rank after restriction. However, with 8 restricted functions now to deal with, which can all be either maximum, minimum or half weight, the problems of finding a specific f within the coset which has a suitable combination of linear terms is more acute. For $\bar{h} = 1$ the canonical form arrived at after transformation has just two variables in it, and by Lemma 4.3, combinations of this with the corresponding four linear terms in these two variables are either maximum or minimum weight. Then through the inverse transformation there will be the original (restricted) quadratic form and combinations with two sets of linear terms (being the inverse transformations of the above mentioned variables) which are either maximum or minimum weight. Re-label the vertices of the above example to take advantage of the extra restriction to get

$$Q = x_0x_1 + \sum_{i=0}^{6} x_ix_7 + \sum_{i=0}^{5} x_ix_6 + x_0x_2 + x_1x_2 + \sum_{i=3}^{5} x_ix_2,$$

so now the delete vertices are 2, 6 and 7, the residual path is x_0x_1, and the isolated vertices are 3, 4 and 5 (see Figure 4.11 for the graph). Let

$$f = Q + L$$

$$\text{where} \quad L = \sum_{i=0}^{7} a_ix_i + g, \quad a_i, g \in \mathbb{Z}_2,$$

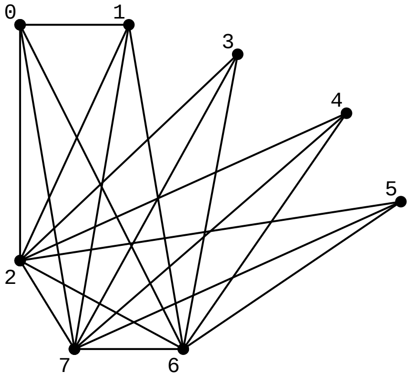

Figure 4.11: Graph for Q of Section 4.5.4

be a typical word in the coset $Q + RM_2(1,8)$. Restricting $f + x_3$ on the variables $\mathbf{x} = x_2x_1x_0$ over all values, and ignoring the constant (which does not affect the categorization as 'max/min' or 'half' weight) gives:

$$\begin{aligned}
(f+x_3)\big|_{x_2x_1x_0=000} &= \sum_{i=3}^{6} x_ix_7 + \sum_{i=3}^{5} x_ix_6 + x_3 + a_3x_3 + a_4x_4 + a_5x_5 \\
&\qquad + a_6x_6 + a_7x_7 \\
&= \bar{Q} + (1+a_3)x_3 + a_4x_4 + a_5x_5 + a_6x_6 + a_7x_7, \quad \text{say} \\
(f+x_3)\big|_{x_2x_1x_0=001} &= \bar{Q} + (1+a_3)x_3 + a_4x_4 + a_5x_5 + (1+a_6)x_6 \\
&\qquad + (1+a_7)x_7 \\
(f+x_3)\big|_{x_2x_1x_0=010} &= (\text{as } 001) \\
(f+x_3)\big|_{x_2x_1x_0=011} &= (\text{as } 000) \\
(f+x_3)\big|_{x_2x_1x_0=100} &= \bar{Q} + a_3x_3 + (1+a_4)x_4 + (1+a_5)x_5 + (1+a_6)x_6 \\
&\qquad + (1+a_7)x_7 \\
(f+x_3)\big|_{x_2x_1x_0=101} &= \bar{Q} + a_3x_3 + (1+a_4)x_4 + (1+a_5)x_5 + a_6x_6 + a_7x_7 \\
(f+x_3)\big|_{x_2x_1x_0=110} &= (\text{as } 101) \\
(f+x_3)\big|_{x_2x_1x_0=111} &= (\text{as } 100).
\end{aligned}$$

$\bar{Q}$ is of the same form as that of Family 2 in Section 4.4 above, equation (4.3), and so in fact $\bar{h} = 1$ as hoped. From the above discussion there are just four functions consisting of $\bar{Q}$ plus linear terms which have either maximum or minimum weight. Are there any combinations of the $a_i = 0$ or 1, $i = 3, \ldots, 7$ for which all eight of the above functions are these maximum or minimum functions and thus satisfy the configurations of Theorem 4.6? Computation shows the answer to be no, and in fact the best that can be managed is that at most 4 of them be either maximum or minimum weight, the rest being half weight. Further computation over all 3^8 possible $\mathbf{W}'$ vectors in (4.2) shows there are 12 values of $x > 16$ in $x \cdot 2^{2m-2\bar{h}-6}$ thus giving $P(\mathbf{f})(\frac{1}{16}) > 2^{2m-2\bar{h}-2}$, which are

$$\begin{aligned}
\approx \{&16.12, 16.22, 16.98, 17.22, 18.16, 18.75, \\
&18.88, 19.16, 21.58, 22.43, 25.27, 26.27\},
\end{aligned}$$

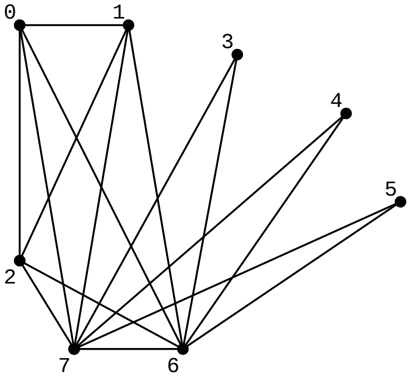

Figure 4.12: Graph for Q' of Section 4.5.4

and which would give a lower bound on the PMEPR of $2^{m-2\bar{h}-2}(=2^{8-2-2}=16$ for the example). They arise from a total of 272 configurations, all of which have $\leqslant 3$ half weight words in them. The above functions therefore cannot be one of these configurations, and again it cannot be guaranteed that there exists an f in the coset of Q which has the power at $t=\frac{1}{16}$ greater than 16.

However, a slight alteration of the coefficients in Q gives

$$Q' = x_0x_1 + \sum_{i=0}^{6} x_ix_7 + \sum_{i=0}^{5} x_ix_6 + x_0x_2 + x_1x_2 + x_6x_2 + x_7x_2,$$

where the terms between delete vertex 2 and the isolated vertices 3, 4 and 5 have been removed (see Figure 4.12 for the graph). With $f = Q' + L$, where L is as before, the restrictions are (again ignoring the constant):

$$\begin{aligned}
(f+x_3)\big|_{x_2x_1x_0=000} &= \sum_{i=3}^{6} x_ix_7 + \sum_{i=3}^{5} x_ix_6 + x_3 + a_3x_3 + a_4x_4 + a_5x_5 \\
&\qquad + a_6x_6 + a_7x_7 \\
&= \bar{Q} + (1+a_3)x_3 + a_4x_4 + a_5x_5 + a_6x_6 + a_7x_7, \quad \text{say} \\
(f+x_3)\big|_{x_2x_1x_0=001} &= \bar{Q} + (1+a_3)x_3 + a_4x_4 + a_5x_5 + (1+a_6)x_6 \\
&\qquad + (1+a_7)x_7 \\
(f+x_3)\big|_{x_2x_1x_0=010} &= (\text{as } 001) \\
(f+x_3)\big|_{x_2x_1x_0=011} &= (\text{as } 000) \\
(f+x_3)\big|_{x_2x_1x_0=100} &= (\text{as } 001) \\
(f+x_3)\big|_{x_2x_1x_0=101} &= (\text{as } 000) \\
(f+x_3)\big|_{x_2x_1x_0=110} &= (\text{as } 000) \\
(f+x_3)\big|_{x_2x_1x_0=111} &= (\text{as } 001),
\end{aligned}$$

noting that $\bar{Q}$ is the same as the previous example, and where it can now been seen that there are just two sets of linear terms, and so a wholly maximum or minimum weight configuration may be possible. Computation shows that indeed $Q' + x_4 + x_5$ has the configuration

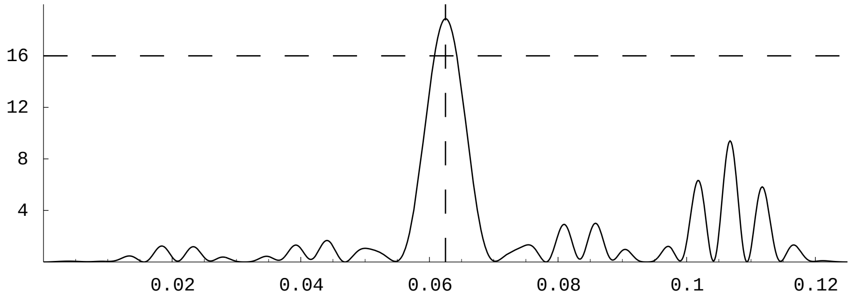

Figure 4.13: Envelope power for $Q' + x_4 + x_5$, of Section 4.5.4, about $t = \frac{1}{16}$

max, min, min, min, min, min, min, max,

which whilst not satisfying Theorem 4.6, is one of the 272 configurations mentioned above, and so the function does have a peak at $t = \frac{1}{16}$, as is shown in the partial plot of its envelope power in Figure 4.13.

4.5.5 Re-labelling the vertices

The order in which the vertices are labelled in the graph of Q has a major effect on the envelope power of codewords in the corresponding coset. In the examples in this chapter the labelling has generally been quite 'structured' in some sense: the vertices forming the residual path come first, then the isolated vertices, followed by the delete vertices. If they are re-labelled by applying a random permutation, then the structure apparently responsible for the usable properties soon disappears. As an example, consider the quadratic form from Example 4.8,

$$Q = x_0x_1 + \sum_{i=0}^{5} x_ix_6 + \sum_{i=0}^{4} x_ix_5,$$

and apply the permutation (013654)(2) to the indices to get

$$\begin{aligned} Q' = x_1x_3 + x_1x_5 + x_3x_5 + x_2x_5 + x_6x_5 + x_0x_5 + x_4x_5 \\ + x_1x_4 + x_3x_4 + x_2x_4 + x_6x_4 + x_0x_4. \end{aligned}$$

(For convenience the graph of Q' is shown in Figure 4.14.) Since the permutation is just an invertible linear transformation, the rank of Q' will be the same as that of Q, and hence via Theorem 4.2, their cosets also share the same weight distribution. It can also be seen from the graph of Q' that after restricting on the variables $\mathbf{x} = x_1x_0$, $\bar{Q}'$ has the same rank $\bar{h}$ as $\bar{Q}$ (the triangular pattern on removing vertices 0 and 1 is the same in both cases). However, in terms of the power $P(\cdot)(t)$, the effect of the permutation is to drastically alter all the phases of the sines and cosines in the signal, and so not surprisingly, the envelope powers of the permuted functions exhibit different patterns from the original. For example, $Q + x_3 + x_4$ was seen (Figure 4.8) to have a large peak at $t = \frac{1}{8}$: the permuted equivalent, $Q' + x_0 + x_6$ does not, and in fact falls below the bound given by Conjecture 1 everywhere, see Figure 4.15. In other instances this is

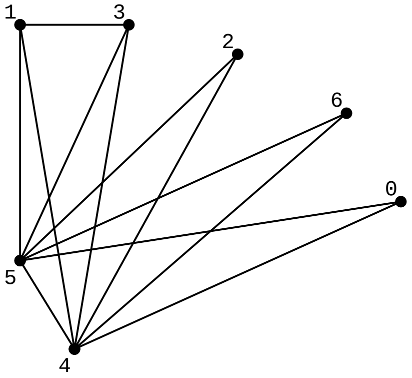

Figure 4.14: Graph for Q' of Section 4.5.5

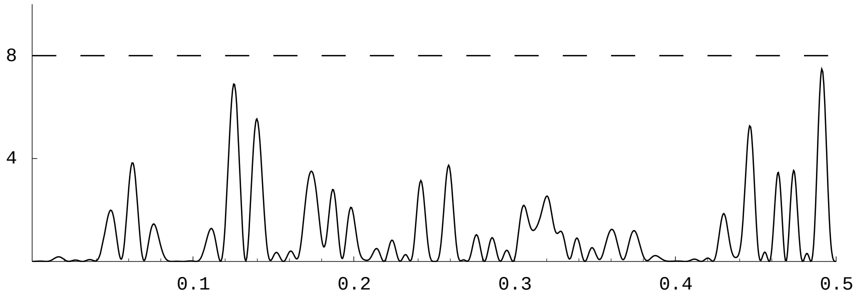

Figure 4.15: Envelope power for $Q' + x_0 + x_6$ of Section 4.5.5

the other way round: for example $Q + x_0 + x_1 + x_2 + x_3 + x_4 + x_6$ is below the bound from the conjecture, see Figure 4.16, whereas its permuted equivalent $Q' + x_0 + x_1 + x_2 + x_3 + x_5 + x_6$ is not, see Figure 4.17. In fact there are about 4 times as many words in the coset of Q' with peaks giving PMEPRs above the bound as there are for Q (some of which do appear to be at t a negative power of 2).

4.6 Conclusions

In this chapter the weights of certain restricted vectors of particular Boolean functions have been used to show that there is a peak in the corresponding envelope power at some particular time. This then leads to a lower bound on the PMEPR of the coset in which the function resides. This has been useful in providing some specific examples, all containing 3 or more isolated vertices, which show that Conjecture 1 cannot be true in general. There is clearly a relationship between the rank of Q and the power for some of the situations examined: the rank needs to be sufficiently high in order to keep the power low, and it appears that it is the omission of this relationship which causes Conjecture 1 to fail.

From the examples in Section 4.5 it is clear that properties of codewords in any particular coset may vary considerably, and it has been shown how altering

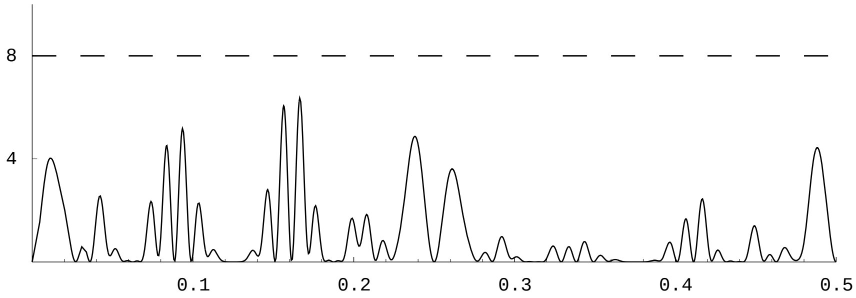

Figure 4.16: Envelope power for the function $Q + x_0 + x_1 + x_2 + x_3 + x_4 + x_6$ of Section 4.5.5

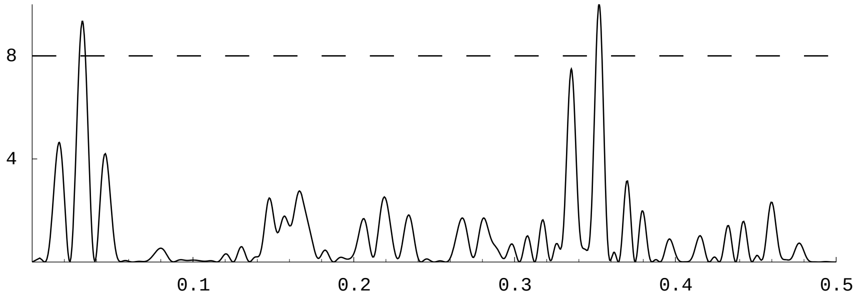

Figure 4.17: Envelope power for the function $Q' + x_0 + x_1 + x_2 + x_3 + x_5 + x_6$ of Section 4.5.5

the parameters concerned (increasing the number of delete vertices, increasing u etc.) can have a major impact on these properties. Thus whilst it has been possible to construct some counter-examples to the conjecture by choosing their structure carefully, picking one at random is unlikely to succeed, and it also seems to be a difficult task to come up with an overall result relating rank, length of residual path, number of isolated vertices and the number of deleted vertices to the PMEPR of the coset of any general Q.

It should also be mentioned that [32, 33], as well as containing the result given here as Theorem 4.4, also contain other results concerning lower bounds on the PMEPR of cosets of quadratic forms Q, where the Q, as the current work, are of very particular constructions. Similar counting techniques are used in [8] to show that the coset $Q + RM_4(1, m)$, where Q is a path over $\mathbb{Z}_4$ and m is even, contains a codeword with the maximum PMEPR as given by Corollary 1.25.

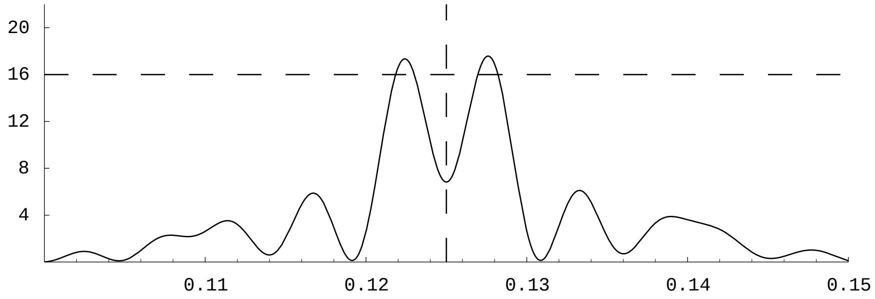

Figure 4.18: Envelope power of $Q + x_2$, for the Q of Section 4.5.1, showing peaks either side of $t = \frac{1}{8}$

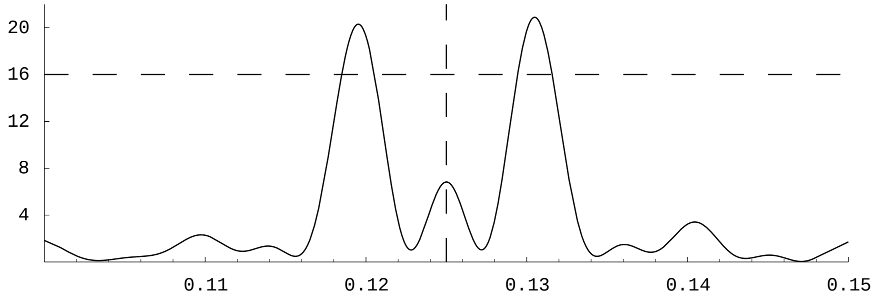

Figure 4.19: Envelope power for $Q + x_2 + x_5 + x_6$ (detail as above)

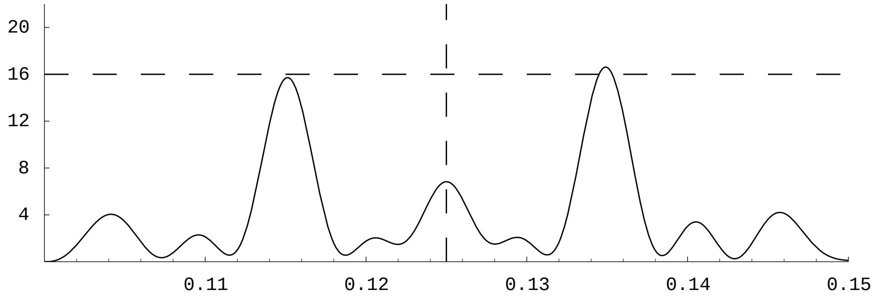

Figure 4.20: Envelope power for $Q + x_2 + x_5 + x_7$ (detail as above)

Chapter 5

Complementary Sets from Pairs

5.1 Chapter Overview

In this chapter some new ways of constructing complementary sets are presented. The introduction recalls what a complementary set is, shows how a simple, well-known method to construct some fits in with the techniques of this thesis, and indicates how the ideas extend to the rest of the chapter. The sets are based around the idea of compressing a restricted vector: how these fit in is also shown in the introduction, and the relationship between the auto-correlations of compressed and restricted vectors is examined. Section 5.3 contains the main result of the chapter, the construction of complementary sets from the compressed vectors of a restricted complementary pair. This is based on a result on pairs of functions whose cross-correlations sum to zero at all shifts. In Section 5.4, using ideas on functions which share the same auto-correlation similar to those in Chapter 3, complementary sets are constructed from a complementary sequence. A non-trivial way of constructing pairs of functions that share the same cross-correlation is given in Section 5.5 (a simple corollary to the result in Section 5.3). Some conclusions are drawn in the final Section 5.6.

5.2 Introduction

Recall from the definition in Chapter 1 that a complementary set of sequences is that for which the sum of the auto-correlation functions across all sequences in the set is zero except at the zero shift. Such sets have been studied by Tseng and Liu in [46, 47] and also independently (but at around the same time) by Schweitzer, [40].

In [46, 47] it is stated that if we form two new sequences from a given sequence (of even length) by taking all the even indexed elements of the sequence as one new sequence, and all the odd indexed elements as the other, and this is done for all members of a complementary set, then the set of all the new sequences is also a complementary set (of twice the number of half-length sequences as the original set). This is a simple consequence of re-ordering the auto-correlation function, at even shifts, of the original sequences. For example, consider some vector $\mathbf{A} = (A_0, A_1, \ldots, A_{n-1})$: define $A'_i = A_{2i+1}$, $i = 0, 1, \ldots, \frac{n}{2}-1$, so $\mathbf{A}' = (A_1, A_3, \ldots, A_{n-1})$ is the half-length vector of odd indices, and $A''_i = A_{2i}$, $i = 0, 1, \ldots, \frac{n}{2} - 1$, so $\mathbf{A}'' = (A_0, A_2, \ldots, A_{n-2})$ is the half-length vector of the even indices. Then the auto-correlation function of $\mathbf{A}$ at even shifts is:

$$\begin{aligned}
A(\mathbf{A})(2\ell) &= \sum_{i=0}^{n-1-2\ell} A_i A^*_{i+2\ell}, \quad \ell = 0, 1, \ldots, \frac{n}{2} - 1 \\
&= \sum_{i=0}^{\frac{n}{2}-1-\ell} A_{2i} A^*_{2i+2\ell} + \sum_{i=0}^{\frac{n}{2}-1-\ell} A_{2i+1} A^*_{2i+1+2\ell} \\
&= \sum_{i=0}^{\frac{n}{2}-1-\ell} A''_i A''^*_{i+\ell} + \sum_{i=0}^{\frac{n}{2}-1-\ell} A'_i A'^*_{i+\ell} \\
&= A(\mathbf{A}')(\ell) + A(\mathbf{A}'')(\ell),
\end{aligned}$$

that is, the auto-correlation of $\mathbf{A}$ at even shifts is just the sum of the auto-correlations of the even and odd 'halves' at half the shift. By definition, the auto-correlation functions of all sequences in a complementary set sum to zero at all shifts except zero: thus by re-ordering the auto-correlations of all sequences at even shifts in this way we see that the auto-correlations of all the even and odd 'halves' will necessarily sum to zero, and hence the new set is a complementary set.

In [46, 47] the above result is really just seen as a special case—the main thrust of that work is to build up complementary sets of longer and longer sequences by recursively concatenating existing complementary sequences in many different ways. However, viewing the above result in the context of restriction suggests a way in that it may be extended, i.e. to take a complementary pair of sequences and split them up into shorter sequences, but in a much more complex manner than just 'every other term' as above, and such that the new sequences do still form a complementary set. Complementary sets are constructed in this manner in this chapter: 'splitting the sequence up' is just the notion of *compression* of a restricted vector, as introduced in Section 1.9.5, that is, of taking a restricted vector and removing all the zeroes. The above result turns out to be a special case obtained by restricting and compressing on the variable x_0, so we examine it first in order to see the possibilities for extending it.

Let $\mathbf{F}$ and $\mathbf{G}$ be a pair of complementary sequences of length $2^m = n$, i.e. for which we have:

$$A(\mathbf{F})(\ell) + A(\mathbf{G})(\ell) = 0, \quad \ell \neq 0. \tag{5.1}$$

Restrict on x_0, and expand the auto-correlation functions using Corollary 1.16 to get, for $\ell \neq 0$,

$$\begin{aligned}
A(\mathbf{F}\big|_{x_0=0})(\ell) + A(\mathbf{F}\big|_{x_0=1})(\ell) + A(\mathbf{G}\big|_{x_0=0})(\ell) + A(\mathbf{G}\big|_{x_0=1})(\ell) \\
+ C(\mathbf{F}\big|_{x_0=0}, \mathbf{F}\big|_{x_0=1})(\ell) + C(\mathbf{F}\big|_{x_0=1}, \mathbf{F}\big|_{x_0=0})(\ell) \\
+ C(\mathbf{G}\big|_{x_0=0}, \mathbf{G}\big|_{x_0=1})(\ell) + C(\mathbf{G}\big|_{x_0=1}, \mathbf{G}\big|_{x_0=0})(\ell) = 0.
\end{aligned} \tag{5.2}$$

In order to clarify the following, let $\mathbf{F}^\circ = \mathbf{F}\big|_{x_0=0}$ and $\mathbf{F}^\bullet = \mathbf{F}\big|_{x_0=1}$. Then from the definition of the restriction by x_0,

$$F_i^\circ = \begin{cases} F_i & i = 0, 2, \ldots, n-2 \\ 0 & i = 1, 3, \ldots, n-1 \end{cases}$$
$$F_i^\bullet = \begin{cases} 0 & i = 0, 2, \ldots, n-2 \\ F_i & i = 1, 3, \ldots, n-1 \end{cases}$$

that is

$$\begin{aligned} \mathbf{F}^\circ &= \mathbf{F}\big|_{x_0=0} = (F_0, 0, F_2, 0, F_4, 0, \ldots, F_{n-2}, 0) \\ \mathbf{F}^\bullet &= \mathbf{F}\big|_{x_0=1} = (0, F_1, 0, F_3, 0, F_5, \ldots, 0, F_{n-1}). \end{aligned} \tag{5.3}$$

Thus the first auto-correlation in (5.2) becomes:

$$\begin{aligned} A(\mathbf{F}\big|_{x_0=0})(\ell) &= A(\mathbf{F}^\circ)(\ell) \\ &= \sum_{i=0}^{n-1-\ell} F_i^\circ F_{i+\ell}^{\circ *} \\ &= \sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\circ *} + \sum_{i=0}^{\frac{n}{2}-1+\lfloor\frac{-\ell}{2}\rfloor} F_{2i+1}^\circ F_{2i+1+\ell}^{\circ *} \\ &= \sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\circ *} + 0 \text{ (odd indexed } F_j^\circ \text{ zero)} \\ &= \begin{cases} \displaystyle\sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\circ *} & \ell \text{ even} \\ 0 & \ell \text{ odd (odd indexed } F_j^\circ \text{ zero).} \end{cases} \end{aligned}$$

Continuing with the even shift case, put $\ell = 2\ell'$:

$$\begin{aligned} A(\mathbf{F}\big|_{x_0=0})(2\ell') &= \sum_{i=0}^{\frac{n}{2}-1-\ell'} F_{2i}^\circ F_{2i+2\ell'}^{\circ *} \\ &= \sum_{i=0}^{\frac{n}{2}-1-\ell'} F_{2i} F_{2i+2\ell'}^{*} \\ &= \sum_{i=0}^{\frac{n}{2}-1-\ell'} F_i'' F_{i+\ell'}''^{*} \\ &= A(\mathbf{F}'')(\ell'), \end{aligned}$$

where, using the notation at the start of the chapter, $F_i'' = F_{2i}$, $i = 0, 1, \ldots, \frac{n}{2}-1$, that is $\mathbf{F}'' = (F_0, F_2, \ldots, F_{n-2})$ is the half-length vector of the even indices. However, from (5.3) this is clearly just the compressed vector, since to form this we remove the zeroes from the restricted vector; that is, using the notation of Section 1.9.5, $\mathbf{F}'' = \widehat{\mathbf{F}}\big|_{x_0=0}$, and so

$$A(\mathbf{F}\big|_{x_0=0})(2\ell') = A(\widehat{\mathbf{F}}\big|_{x_0=0})(\ell'), \quad \ell' = 0, 1, \ldots, \frac{n}{2} - 1.$$

Arguing very similarly for $A(\mathbf{F}\big|_{x_0=1})(\ell) = A(\mathbf{F}^\bullet)(\ell)$, we get that

$$\begin{aligned} A(\mathbf{F}\big|_{x_0=1})(2\ell') &= A(\mathbf{F}')(\ell') \\ &= A(\widehat{\mathbf{F}}\big|_{x_0=1})(\ell'), \end{aligned}$$

where $\mathbf{F}' = (F_1, F_3, \ldots, F_{n-1})$ is the half-length vector of the odd indices, which is the compressed vector $\widehat{\mathbf{F}}\big|_{x_0=1}$.

Next, consider the cross-correlation from (5.2):

$$\begin{aligned} &C(\mathbf{F}\big|_{x_0=0}, \mathbf{F}\big|_{x_0=1})(\ell) \\ &\qquad = C(\mathbf{F}^\circ, \mathbf{F}^\bullet)(\ell) \\ &\qquad = \sum_{i=0}^{n-1-\ell} F_i^\circ F_{i+\ell}^{\bullet *} \\ &\qquad = \sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\bullet *} + \sum_{i=0}^{\frac{n}{2}-1+\lfloor\frac{-\ell}{2}\rfloor} F_{2i+1}^\circ F_{2i+1+\ell}^{\bullet *} \\ &\qquad = \sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\bullet *} + 0 \text{ (odd indexed } F_j^\circ \text{ are zero)} \\ &\qquad = \begin{cases} \displaystyle\sum_{i=0}^{\frac{n}{2}-1-\lfloor\frac{\ell}{2}\rfloor} F_{2i}^\circ F_{2i+\ell}^{\bullet *} & \ell \text{ odd} \\ 0 & \ell \text{ even (even indexed } F_j^\bullet \text{ are zero),} \end{cases} \end{aligned}$$

that is the cross-correlation is always zero at even shifts. Again a very similar argument shows that the cross-correlation $C(\mathbf{F}\big|_{x_0=1}, \mathbf{F}\big|_{x_0=0})(\ell)$ is also zero when ℓ is even, and similar arguments to all the above can of course be applied to $\mathbf{G}$. Thus when ℓ is even, all the cross-correlations in (5.2) are zero, and the auto-correlations can be replaced by the auto-correlations of the compressed vectors at half the shift. So substituting $A(\mathbf{F}\big|_{x_0=0})(2\ell') = A(\widehat{\mathbf{F}}\big|_{x_0=0})(\ell')$ etc., where $\ell = 2\ell', \ell' = 1, 2, \ldots, \frac{n}{2} - 1$, equation (5.2) becomes

$$A(\widehat{\mathbf{F}}\big|_{x_0=0})(\ell') + A(\widehat{\mathbf{F}}\big|_{x_0=1})(\ell') + A(\widehat{\mathbf{G}}\big|_{x_0=0})(\ell') + A(\widehat{\mathbf{G}}\big|_{x_0=1})(\ell') = 0, \quad \ell' \neq 0,$$

that is, as we already know, the four halves of the original sequences form a complementary set. So, what has happened is that the cross-correlations in (5.2) have vanished (albeit in a special way), leaving just the four auto-correlations of the restricted vectors summing to zero, and then we can equate these auto-correlations to those of the compressed vectors. What makes this case special is that the cross-correlations vanish at even shifts due to the alternating pattern of zeroes and non-zeroes in the restricted vectors, and this is also responsible for the direct relationship between the restricted and compressed auto-correlations. Considering the more general case of k restricting variables $\mathbf{x}$, the expansion of (5.1) is, for $\ell \neq 0$,

$$\sum_{\mathbf{c}} \left(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}})(\ell)\right) \\ + \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \left(C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell) + C(\mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_1}, \mathbf{G}\big|_{\mathbf{x}=\mathbf{c}_2})(\ell)\right) = 0, \quad (5.4)$$

and we can use properties of the functions f and g themselves in order to get the cross-correlations to vanish, thus leaving the restricted auto-correlations summing to zero, and then use this fact together with the relationship between the compressed and restricted auto-correlations to show that the sum of the compressed auto-correlations is also zero, rather than direct substitution. The latter relationship is explored now; Theorem 5.3 in the next section shows when the cross-correlations of the functions we are interested in sum to zero.

In calculating the auto-correlations of a restricted vector, $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$, and its compressed counterpart, $\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}$, it is clear that the same non-zero components of vector $\mathbf{A}$ are involved, but that they appear at different shifts relative to each other due to the zeroes in the restricted vector. The calculation of an auto-correlation function for a vector $\mathbf{A}$ at a non-zero shift is seen from its definition,

$$A(\mathbf{A})(\ell) = \sum_{i=0}^{n-1-\ell} A_i A^*_{i+\ell} \quad 1 \leqslant \ell \leqslant n-1,$$

to involve evaluating and summing a number of products formed from the elements of $\mathbf{A}$ with the elements of $\mathbf{A}^*$. It is reasonable to expect, but perhaps is not immediately obvious, that all the non-zero products appearing in the calculation of $A(\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}})(\tau)$ over all τ appear somewhere in the calculation of $A(\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}})(\ell)$ over all ℓ, and this is now shown. For an unrestricted vector (i.e. one with no zero elements in it), at a given shift ℓ, $1 \leqslant \ell \leqslant n-1$, as i varies from 0 to $n-1-\ell$, we get $n-\ell$ products in the sum, and thus the total number of products involved over all the non-zero shifts is $\sum_{\ell=1}^{n-1}(n-\ell) = \sum_{\ell=1}^{n-1} \ell = \frac{n(n-1)}{2}$. This is, not surprisingly, just the number of distinct products that can be formed between pairs of elements of $\mathbf{A}$ and $\mathbf{A}^*$. A compressed vector $\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}$ consists of 2^{m-k} non-zero entries, where k is the number of restricting variables $\mathbf{x}$, and the auto-correlation of $\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}$, for a particular $\mathbf{c}$ and over all non-zero shifts, thus involves $2^{m-k-1}(2^{m-k}-1)$ products (put $n = 2^{m-k}$ in the above). The restricted vector $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$ on the other hand consists of $n = 2^m$ elements, of which only 2^{m-k} are non-zero. Suppose the indices at which these non-zero elements occur are $i_0, \ldots, i_{2^{m-k}-1}$, $0 \leqslant i_0 < i_1 < \cdots < i_{2^{m-k}-1} \leqslant n-1$. Consider i fixed this time. For a particular non-zero entry $i = i_j$, say, in $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$, $0 \leqslant j \leqslant 2^{m-k}-1$, as ℓ varies over $1 \leqslant \ell \leqslant n-1$, this element makes a non-zero product with elements of $\mathbf{A}^*\big|_{\mathbf{x}=\mathbf{c}}$ only when aligned with any of the remaining $2^{m-k}-j-1$ non-zero entries, i.e. when $i_j+\ell=i_{j'}$, $j < j' \leqslant 2^{m-k}-1$. Summing over all such j (i.e. summing over all i for which the elements are non-zero) gives the number of non-zero products involved in the auto-correlation of $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$, for a particular $\mathbf{c}$ and over all non-zero shifts, as $\sum_{j=0}^{2^{m-k}-1}(2^{m-k}-j-1) = \sum_{j=0}^{2^{m-k}-1} j = 2^{m-k-1}(2^{m-k}-1)$. This is the same number as that for the compressed vector, and since the products in both the compressed and restricted auto-correlations involve just the same non-zero elements of $\mathbf{A}$, they are the *same* products. Thus all the non-zero products that appear at a particular shift τ in the auto-correlation of $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$ appear somewhere, at possibly different shifts ℓ, in the auto-correlation of $\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}$, and vice-versa.

Consideration of a simple case shows that products from several shifts τ of the auto-correlation of the restricted vector may appear in a single shift ℓ of the auto-correlation of the compressed vector. For example take $m = 4$, $\mathbf{x} = x_2$ and $\mathbf{c} = 0$. Take an unrestricted vector

$$\mathbf{A} = (A_0, A_1, \ldots, A_{15}),$$

where each A_i is by definition non-zero, with the restricted and compressed vectors

$$\begin{aligned}\mathbf{A}\big|_{x_2=0} &= (A_0, A_1, A_2, A_3, 0, 0, 0, 0, A_8, A_9, A_{10}, A_{11}, 0, 0, 0, 0)\\ \widehat{\mathbf{A}}\big|_{x_2=0} &= (A_0, A_1, A_2, A_3, A_8, A_9, A_{10}, A_{11}).\end{aligned}$$

Then we have, say

$$\begin{aligned}A(\mathbf{A}\big|_{x_2=0})(1) &= A_0A_1^* + A_1A_2^* + A_2A_3^* + A_8A_9^* + A_9A_{10}^* + A_{10}A_{11}^*\\ A(\mathbf{A}\big|_{x_2=0})(5) &= A_3A_8^*\\ A(\widehat{\mathbf{A}}\big|_{x_2=0})(1) &= A_0A_1^* + A_1A_2^* + A_2A_3^* + A_3A_8^* + A_8A_9^* + A_9A_{10}^* + A_{10}A_{11}^*,\end{aligned}$$

and so

$$A(\widehat{\mathbf{A}}\big|_{x_2=0})(1) = A(\mathbf{A}\big|_{x_2=0})(1) + A(\mathbf{A}\big|_{x_2=0})(5).$$

As the number of restricting variables increases the pattern of non-zeroes in the restricted vector may become more complicated, and it becomes less obvious that if one or more products from shift τ of the restricted auto-correlation appear at shift ℓ in the compressed auto-correlation, then they *all* will. This is in fact the case, and the following Lemma gives the precise relationship.

Lemma 5.1. *Let* $\mathbf{A}$ *be a length* 2^m *complex-valued vector, and let* $\mathbf{x}$ *be some particular* k *restricting variables,* $1 \leqslant k \leqslant m$, *and* $\mathbf{c}$ *a binary word of length* k. *Then the auto-correlation function of the compressed vector of* $\mathbf{A}$ *at any given shift is the sum of* 2^k *shifts of the auto-correlation function of the restricted vector, i.e.*

$$A(\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = \sum_{\tau\in I_{\ell,\mathbf{x}}} A(\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}})(\tau), \quad 0 < \ell \leqslant 2^{m-k}-1,$$

where $I_{\ell,\mathbf{x}}$ *is an index set of size* 2^k, *dependent on* ℓ *and* $\mathbf{x}$.

Proof. We first show that if *any* of the non-zero products at shift τ of the auto-correlation of a restricted vector appear at some shift ℓ of the auto-correlation of the compressed vector, then they *all* do. As usual let the k restricting variables be $\mathbf{x} = x_{j_0}x_{j_1}\cdots x_{j_{k-1}}$, where

$$J = \{j_0, j_1, \dots j_{k-1}\}$$

is the set of restricting indices with $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$, and let $\mathbf{c} = c_0c_1\cdots c_{k-1}$ be a binary word of length k. Following Section 1.9.5, let set S be the indices of the non-restricting variables, labelled s_α, $\alpha = 0, 1, \dots, m-k-1$, with $0 \leqslant s_0 < s_1 < \cdots < s_{m-k-1} \leqslant m-1$, i.e.

$$\begin{aligned} S &= \{0, 1, \dots, m-1\} \setminus J \\ &= \{s_0, s_1, \dots, s_{m-k-1}\}. \end{aligned}$$

Then the non-zero components of $\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}$ are indexed by (equation (1.9)):

$$i = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + \sum_{\alpha=0}^{m-k-1} i_{s_\alpha} 2^{s_\alpha}, \quad i_{s_\alpha} = 0 \text{ or } 1,$$

and so the binary expansion of i is

$$i = (i_0, i_1, \dots, i_{m-1}) \text{ where } \begin{cases} i_j = c_\alpha & j = j_\alpha \in J \\ i_j = 0 \text{ or } 1 & j = s_\alpha \in S. \end{cases}$$

Let the components of $\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}$ be $\widehat{A}_{\widehat{i}}$, i.e.

$$\widehat{A}_{\widehat{i}} = \left(\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}}\right)_{\widehat{i}} = \left(\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}}\right)_i$$

where

$$\widehat{i} = \sum_{\alpha=0}^{m-k-1} i_{s_\alpha} 2^\alpha,$$

from equation (1.10), and so the binary expansion of $\widehat{i}$ is $(i_{s_0}, i_{s_1}, \dots, i_{s_{m-k-1}})$. Suppose that u, u', v and v' are the indices of four non-zero components in the restricted vector, such that the products $A_uA^*_{u'}$ and $A_vA^*_{v'}$ are both non-zero and appear at shift $\tau > 0$ in the auto-correlation of the restricted vector, i.e. that $u' - u = v' - v = \tau$. Then we need to show that the corresponding products $\widehat{A}_{\widehat{u}}\widehat{A}^*_{\widehat{u}'}$ and $\widehat{A}_{\widehat{v}}\widehat{A}^*_{\widehat{v}'}$ both appear at the same shift ℓ, say, in the auto-correlation of the compressed vector i.e. that $\widehat{u}' - \widehat{u} = \widehat{v}' - \widehat{v} = \ell$. (So we have

$$\widehat{u} = \sum_{\alpha=0}^{m-k-1} u_{s_\alpha} 2^\alpha,$$

which has binary expansion $(\widehat{u}_0, \widehat{u}_1, \dots, \widehat{u}_{m-k-1}) = (u_{s_0}, u_{s_1}, \dots, u_{s_{m-k-1}})$, and similarly for $\widehat{u}', \widehat{v}$ and $\widehat{v}'$.)

Let the binary expansion of τ be $(\tau_0, \tau_1, \dots, \tau_{m-1})$. From the arithmetic of the subtraction of two binary numbers, the bits of τ are given by

$$\tau_\alpha = u'_\alpha - u_\alpha + a_\alpha 2 - a_{\alpha-1}, \quad \alpha = 0, 1, \dots, m-1,$$

where u'_α and u_α are the bits of u' and u, and the $a_\alpha \in \{0,1\}$ represent any necessary 'borrow' and 'payback' at each stage: if the difference between the u bits minus any payback from the previous stage, $u'_\alpha - u_\alpha - a_{\alpha-1}$, is negative, then we borrow 2 from the next stage by setting $a_\alpha = 1$, i.e. $a_\alpha 2 = 2$, and add this in. The τ_α and a_α may be determined recursively, working from the least significant bit to the most significant bit, as

$$\begin{aligned} a_{-1} &= 0 \\ \tau_\alpha &= u'_\alpha - u_\alpha - a_{\alpha-1} \mod 2 \\ a_\alpha &= \big(\tau_\alpha - (u'_\alpha - u_\alpha - a_{\alpha-1})\big)/2, \end{aligned} \tag{5.5}$$

for $\alpha = 0, 1, \ldots, m-1$, and since we have that $u' > u$, there will be no borrow at the top, i.e. a_{m-1} must be zero. Since $\widehat{u}$ and $\widehat{u}'$ are defined by the bits of u and u' at the positions given by the s_α, we are particularly interested in the bits of τ in these positions. Suppose that at some particular t, $0 \leqslant t \leqslant m-1$, we have $s_t = s_{t-1} + 1$, and define $s_{-1} = -1$ so this includes the case $s_0 = 0$. Then $a_{s_t - 1} = a_{s_{t-1}}$, and so bit τ_{s_t} is given by

$$\begin{aligned} \tau_{s_t} &= u'_{s_t} - u_{s_t} - a_{s_t-1} \mod 2 \\ &= u'_{s_t} - u_{s_t} - a_{s_{t-1}} \mod 2 \\ a_{s_t} &= \big(\tau_{s_t} - (u'_{s_t} - u_{s_t} - a_{s_t-1})\big)/2 \\ &= \big(\tau_{s_t} - (u'_{s_t} - u_{s_t} - a_{s_{t-1}})\big)/2. \end{aligned} \tag{5.6}$$

Now suppose that $s_t > s_{t-1} + 1$ (and again define $s_{-1} = -1$, so this includes the case $s_0 > 0$). At any particular index between s_{t-1} and s_t both bits of u and u' equal some bit c_α, and so for $i = 1, 2, \ldots, s_t - s_{t-1} - 1$ we have

$$u'_{s_{t-1}+i} - u_{s_{t-1}+i} = 0$$

and so

$$\begin{aligned} \tau_{s_{t-1}+i} &= a_{s_{t-1}+i-1}, \\ a_{s_{t-1}+i} &= (\tau_{s_{t-1}+i} + a_{s_{t-1}+i-1})/2 \\ &= (a_{s_{t-1}+i-1} + a_{s_{t-1}+i-1})/2 \\ &= a_{s_{t-1}+i-1}, \end{aligned}$$

and in particular

$$a_{s_{t-1}+(s_t - s_{t-1}-1)} = a_{s_t-1} = a_{s_{t-1}},$$

and so bit τ_{s_t} is once again given by equations (5.6) above. Thus, whether s_t is consecutive or non-consecutive to s_{t-1}, in either case the bits τ_{s_α} are given by

$$\begin{aligned} s_{-1} &= -1, a_{-1} = 0 \\ \tau_{s_\alpha} &= u'_{s_\alpha} - u_{s_\alpha} - a_{s_{\alpha-1}} \mod 2 \\ a_{s_\alpha} &= \big(\tau_{s_\alpha} - (u'_{s_\alpha} - u_{s_\alpha} - a_{s_{\alpha-1}})\big)/2, \end{aligned} \tag{5.7}$$

for $\alpha = 0, 1, \ldots, m-k-1$.

Now equations equivalent to (5.5) can be used to determine the bits $(\ell_0, \ell_1, \ldots, \ell_{m-k-1})$ of $\ell = \widehat{u}' - \widehat{u}$, viz:

$$\begin{aligned} b_{-1} &= 0 \\ \ell_\alpha &= \widehat{u}'_\alpha - \widehat{u}_\alpha - b_{\alpha-1} \mod 2 \\ b_\alpha &= \big(\ell_\alpha - (\widehat{u}'_\alpha - \widehat{u}_\alpha - b_{\alpha-1})\big)/2, \end{aligned}$$

for $\alpha = 0, 1, \ldots, m-k-1$, now with b_α as the borrow bits. Substituting $\widehat{u}'_\alpha - \widehat{u}_\alpha = u'_{s_\alpha} - u_{s_\alpha}$, these become

$$\begin{aligned} b_{-1} &= 0 \\ \ell_\alpha &= u'_{s_\alpha} - u_{s_\alpha} - b_{\alpha-1} \mod 2 \\ b_\alpha &= \big(\ell_\alpha - (u'_{s_\alpha} - u_{s_\alpha} - b_{\alpha-1})\big)/2, \end{aligned}$$

but clearly these are exactly equations (5.7) above, i.e.

$$\begin{aligned} \ell_\alpha &= \tau_{s_\alpha} \\ b_\alpha &= a_{s_\alpha}, \end{aligned}$$

for $\alpha = 0, 1, \ldots, m-k-1$, or in other words, the bits of $\widehat{u}' - \widehat{u}$ at positions α are precisely the bits at positions s_α in $u' - u$. Since the same relationship holds for $\widehat{v}' - \widehat{v}$ and $v' - v$, and $u' - u = v' - v = \tau$, then we must have $\widehat{u}' - \widehat{u} = \widehat{v}' - \widehat{v} = \ell$, as was to be shown (but note that even though $u' - u = v' - v$, and so the binary digits are exactly the same, the borrow bits in both subtractions may be quite different!).

Thus, for any given ℓ, the auto-correlation of the restricted vector at shift τ appears at shift ℓ of the compressed auto-correlation if the bits at positions s_α of τ agree with the bits at positions α in ℓ. Since the s_α are the complement of J in $\{0, 1, \ldots, m-1\}$, they clearly only depend on $\mathbf{x}$, and there are $m-k$ of them. Thus there are 2^k choices for the non-s_α bits in τ, and as the s_α bits depend on ℓ, we may write

$$A(\widehat{\mathbf{A}}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = \sum_{\tau \in I_{\ell,\mathbf{x}}} A(\mathbf{A}\big|_{\mathbf{x}=\mathbf{c}})(\tau), \quad 0 < \ell \leqslant 2^{m-k} - 1,$$

where the index set I_ℓ depends on ℓ and $\mathbf{x}$, and is of size 2^k, and hence the lemma is proved. □

Note that whilst the lemma says that any shift of the auto-correlation of the compressed vector is the sum of 2^k shifts of the auto-correlation of the restricted vector, the number of shifts of the restricted auto-correlation that actually contribute to the compressed auto-correlation may be less than 2^k, since the zeroes in the restricted vector mean that it is entirely possible for some shifts of the restricted auto-correlation to be simply zero.

Using the result of the Lemma, i.e. the fact that the auto-correlation of a compressed vector may be written in terms of a sum of auto-correlations (at a number of shifts) of the restricted vector, the following simple corollary shows that if a set of restricted vectors (under the same restriction) is a complementary set, then so is the set of the compressed vectors.

Corollary 5.2. *Let $\{f_0, f_1, \ldots, f_{N-1}\}$ be a set of N generalized Boolean functions in m variables over $\mathbb{Z}_q$, with corresponding vectors $\mathbf{F}_j$, $j = 0, 1, \ldots, N-1$. Let $\mathbf{x}$ be some particular k restricting variables, $1 \leqslant k \leqslant m$. Then if the sum of the (non-zero shift) auto-correlations of all the restricted vectors across all restrictions is zero,*

$$\sum_{\mathbf{c}} \big(A(\mathbf{F}_0|_{\mathbf{x}=\mathbf{c}})(\tau) + A(\mathbf{F}_1|_{\mathbf{x}=\mathbf{c}})(\tau) + \cdots + A(\mathbf{F}_{N-1}|_{\mathbf{x}=\mathbf{c}})(\tau)\big) = 0,$$
$$0 < \tau \leqslant 2^m - 1,$$

then so is the sum of the auto-correlations of the compressed vectors, i.e.

$$\sum_{\mathbf{c}} \big(A(\widehat{\mathbf{F}}_0|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\widehat{\mathbf{F}}_1|_{\mathbf{x}=\mathbf{c}})(\ell) + \cdots + A(\widehat{\mathbf{F}}_{N-1}|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0,$$
$$0 < \ell \leqslant 2^{m-k} - 1.$$

Proof. From the Lemma, for any given $\mathbf{c}$ and for all j we have

$$A(\widehat{\mathbf{F}}_j|_{\mathbf{x}=\mathbf{c}})(\ell) = \sum_{\tau \in I_{\ell,\mathbf{x}}} A(\mathbf{F}_j|_{\mathbf{x}=\mathbf{c}})(\tau), \quad 0 < \ell \leqslant 2^{m-k} - 1,$$

for some index set $I_{\ell,\mathbf{x}}$ dependent on ℓ and $\mathbf{x}$. In particular we note that there is no dependence of the index set on $\mathbf{c}$, i.e. the same $I_{\ell,\mathbf{x}}$ will apply for all possible $\mathbf{c}$. Thus after summing over j and $\mathbf{c}$ we may interchange the order of the summation, to get

$$\begin{aligned}\sum_{\mathbf{c}} \sum_{j=0}^{N-1} A(\widehat{\mathbf{F}}_j|_{\mathbf{x}=\mathbf{c}})(\ell) &= \sum_{\mathbf{c}} \sum_{j=0}^{N-1} \sum_{\tau \in I_{\ell,\mathbf{x}}} A(\mathbf{F}_j|_{\mathbf{x}=\mathbf{c}})(\tau) \\ &= \sum_{\tau \in I_{\ell,\mathbf{x}}} \sum_{\mathbf{c}} \sum_{j=0}^{N-1} A(\mathbf{F}_j|_{\mathbf{x}=\mathbf{c}})(\tau),\end{aligned}$$

and since the inner sum of this last expression is zero by hypothesis, we have

$$\sum_{\mathbf{c}} \sum_{j=0}^{N-1} A(\widehat{\mathbf{F}}_j|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad 0 < \ell \leqslant 2^{m-k} - 1,$$

as was to be shown. □

5.3 Complementary Sets from a Pair

In this Section we show that the compressed vectors, across all restrictions, for any restriction performed on a Golay complementary pair constructed from Corollary 1.25, form a complementary set. In order to achieve this, we first need the cross-correlations in the expansion of the auto-correlations, equation (5.4), to disappear. The following theorem shows when two pairs of functions, based around the path structure of the construction for complementary pairs, have cross-correlations that indeed sum to zero. Basically it says that if a function, after restriction, consists of a path and a function (of any order) not involving the path variables, then the cross-correlations of

- the function with the function plus an end point, and
- the function plus the other end point with the function plus both end points

sum to zero. The proof once again relies on the useful properties that path functions have, particularly with respect to reversing them.

Theorem 5.3. *Let the m variables $x_0, \dots, x_{m-1}$ be partitioned into three sets*

$$\begin{aligned} I &= \{x_{i_0}, \dots, x_{i_{s-1}}\} \text{ where } 0 \leqslant i_0 < i_1 \cdots < i_{s-1} \leqslant m-1 \\ J &= \{x_{j_0}, \dots, x_{j_{t-1}}\} \text{ where } 0 \leqslant j_0 < j_1 \cdots < j_{t-1} \leqslant m-1 \\ K &= \{x_0, \dots, x_{m-1}\} \setminus (I \cup J), \end{aligned}$$

where $s \geqslant 1$ and the size of the set K is $m-s-t$. Let π be a permutation of $\{0, 1, \dots, s-1\}$, and let $P = P(x_{i_0}, \dots, x_{i_{s-1}})$ be a path on the s variables in I, viz:

$$P = \begin{cases} \dfrac{q}{2} \displaystyle\sum_{\alpha=0}^{s-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} & s \geqslant 2 \\ p x_{i_0}, \quad p \in \mathbb{Z}_q & s = 1. \end{cases}$$

Let $G_1 = G_1(x_{j_0}, \dots, x_{j_{t-1}})$ and $G_2 = G_2(x_{j_0}, \dots, x_{j_{t-1}})$ be two generalized Boolean functions in the t variables in J (and so distinct from those in I), and let $L = L(x_{i_0}, \dots, x_{i_{s-1}})$ be any linear function also in the variables in I, namely

$$L = \sum_{\alpha=0}^{s-1} g_{i_\alpha} x_{i_\alpha}, \quad g_{i_\alpha} \in \mathbb{Z}_q.$$

Denote the end points of P by $x_a = x_{i_{\pi(0)}}$ and $x_b = x_{i_{\pi(s-1)}}$, and let f, f_a, f_b and f_{ab} be four generalized Boolean functions in the m variables $x_0, \dots, x_{m-1}$, which after restriction on the variables $\mathbf{x}$ in K, are defined by

$$\begin{aligned} f\big|_{\mathbf{x}=\mathbf{c}} &= P + L + G_1 + g_1 \\ f_a\big|_{\mathbf{x}=\mathbf{d}} &= P + \frac{q}{2} x_a + L + G_2 + g_2 \\ f_b\big|_{\mathbf{x}=\mathbf{c}} &= P + \frac{q}{2} x_b + L + G_1 + g_1 \\ f_{ab}\big|_{\mathbf{x}=\mathbf{d}} &= P + \frac{q}{2}(x_a + x_b) + L + G_2 + g_2, \end{aligned}$$

where g_1 and g_2 are arbitrary elements of $\mathbb{Z}_q$, and $\mathbf{c}$ and $\mathbf{d}$ are binary words of length $m-s-t$.
Then

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_a\big|_{\mathbf{x}=\mathbf{d}})(\ell) + C(\mathbf{F}_b\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_{ab}\big|_{\mathbf{x}=\mathbf{d}})(\ell) = 0, \qquad -(2^m - 1) \leqslant \ell \leqslant 2^m - 1.$$

Proof. Perform a further restriction over all the variables which are not in the path, i.e. over all variables in set J. So put $\mathbf{x}' = x_{j_0} x_{j_1} \cdots x_{j_{t-1}}$, and expand both cross-correlations in the hypothesis using Lemma 1.15 to obtain, for any ℓ,

$$\sum_{\mathbf{c}_1} \sum_{\mathbf{c}_2} \big(C(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}, \mathbf{F}_a\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2})(\ell) + C(\mathbf{F}_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}, \mathbf{F}_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2})(\ell) \big).$$

Using Lemma 1.20, in terms of the truncated vectors this sum becomes,

$$\sum_{\mathbf{c}_1}\sum_{\mathbf{c}_2}\Big(C([\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}],[\mathbf{F}_a\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}])(\ell-(u_2-u_1)) \\ +C([\mathbf{F}_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}],[\mathbf{F}_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}])(\ell-(u_2-u_1))\Big), \qquad (5.8)$$

for $(u_2-u_1)-(n_\mathbf{x}-1)\leqslant\ell\leqslant(u_2-u_1)+(n_\mathbf{x}-1)$, where u_1 is the index of the first non-zero entry in the vector $(\cdot)\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}$, u_2 that in $(\cdot)\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}$ and $n_\mathbf{x}$ the length of the pattern of non-zeroes in either such vector, and outside of this range each cross-correlation is zero by the lemma, so the sum is zero too. From the standard results on cross-correlation functions, Theorem 1.1, we get, for any ℓ,

$$C(\overline{\mathbf{B}^*},\overline{\mathbf{A}^*})(\ell)=C(\mathbf{A},\mathbf{B})(\ell),$$

so we can manipulate the second cross-correlation term to get

$$\begin{aligned}C([\mathbf{F}_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}],[\mathbf{F}_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}])(\ell-(u_2-u_1))&\\ =C(\overline{[\mathbf{F}_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}]^*},\overline{[\mathbf{F}_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}]^*})(\ell-(u_2-u_1))&\\ =C([\widetilde{\mathbf{F}}^*_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}],[\widetilde{\mathbf{F}}^*_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}])(\ell-(u_2-u_1)),&\end{aligned}$$

where we recall from Section 1.9.4 that $\widetilde{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}}$ is vector $\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}$ with its non-zero entries reversed, the values of which are given by $\overline{f\big|_{\mathbf{x}=\mathbf{c}}}$, obtained by reversing $f\big|_{\mathbf{x}=\mathbf{c}}$ in algebraic normal form, and that the conjugation in the vector is effected by negating the function.

To this end we now consider the forms the four functions take when the restricting variables are replaced by their respective constants. P and L are not affected by the further restriction $\mathbf{x}'$, but G_1 and G_2 boil down to a residual constant that depends on the restricting constant, $\mathbf{c}_1$ or $\mathbf{c}_2$, denoted by $r_{G_i}(\cdot)$, $i=1,2$:

$$\begin{aligned}f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}&=P+L+r_{G_1}(\mathbf{c}_1)+g_1\\ f_a\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}&=P+\frac{q}{2}x_a+L+r_{G_2}(\mathbf{c}_2)+g_2\\ f_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}&=P+\frac{q}{2}x_b+L+r_{G_1}(\mathbf{c}_1)+g_1\\ f_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}&=P+\frac{q}{2}(x_a+x_b)+L+r_{G_2}(\mathbf{c}_2)+g_2.\end{aligned}$$

We now consider $-\overline{f_{ab}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{d}\mathbf{c}_2}}$ and $-\overline{f_b\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}_1}}$, which determine the values of the vectors in the above cross-correlation. The reverse of a path P when P is a non-trivial path, i.e. $s\geqslant 2$, is given by Lemma 1.9, and negating gives

$$\begin{aligned}-\overline{P}&=-(P+\frac{q}{2}(x_a+x_b)+r_p)\\ &=P+\frac{q}{2}(x_a+x_b)+r_p,\end{aligned}$$

since all the coefficients are $\frac{q}{2}=-\frac{q}{2}$ mod q, q even, and where $r_p=\frac{q}{2}(s-1)$ mod q. From Section 1.6, the reverse of a linear function is the sum of the coefficients minus the function, thus

$$\begin{aligned}-\overline{L} &= -\Big(\sum_{\alpha=0}^{s-1} g_{i_\alpha} - L\Big) \\ &= L + r_L, \text{ say.}\end{aligned}$$

Similarly $-\overline{\frac{q}{2}x_a} = \frac{q}{2} + \frac{q}{2}x_a$, and likewise for x_b. Then we get

$$\begin{aligned}
-\overline{f_{ab}\big|_{\mathbf{xx}'=\mathbf{dc}_2}} &= P + \frac{q}{2}(x_a + x_b) + r_p + \frac{q}{2}(x_a + x_b) + L + r_L - r_{G_2}(\mathbf{c}_2) - g_2 \\
&= P + r_p + L + r_L - r_{G_2}(\mathbf{c}_2) - g_2 \\
&= f\big|_{\mathbf{xx}'=\mathbf{cc}_1} - r_{G_1}(\mathbf{c}_1) - g_1 + r_p + r_L - r_{G_2}(\mathbf{c}_2) - g_2 \\
&= f\big|_{\mathbf{xx}'=\mathbf{cc}_1} + \gamma \\
-\overline{f_b\big|_{\mathbf{xx}'=\mathbf{cc}_1}} &= P + \frac{q}{2}(x_a + x_b) + r_p + \frac{q}{2}x_b + \frac{q}{2} + L + r_L - r_{G_1}(\mathbf{c}_1) - g_1 \\
&= P + \frac{q}{2}x_a + r_p + \frac{q}{2} + L + r_L - r_{G_1}(\mathbf{c}_1) - g_1 \\
&= f_a\big|_{\mathbf{xx}'=\mathbf{dc}_2} - r_{G_2}(\mathbf{c}_2) - g_2 + r_p + \frac{q}{2} + r_L - r_{G_1}(\mathbf{c}_1) - g_1 \\
&= f_a\big|_{\mathbf{xx}'=\mathbf{dc}_2} + \gamma + \frac{q}{2},
\end{aligned}$$

where $\gamma = r_p - r_{G_1}(\mathbf{c}_1) - g_1 + r_L - r_{G_2}(\mathbf{c}_2) - g_2$ is an element of $\mathbb{Z}_q$. Thus putting $\ell' = \ell - (u_2 - u_1)$, for fixed $\mathbf{c}_1$ and $\mathbf{c}_2$, the inner term in the sum (5.8) becomes

$$\begin{aligned}
&C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') + C([\mathbf{F}_b|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_{ab}|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad = C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad\quad + C([\widetilde{\mathbf{F}}^*_{ab}|_{\mathbf{xx}'=\mathbf{dc}_2}], [\widetilde{\mathbf{F}}^*_b|_{\mathbf{xx}'=\mathbf{cc}_1}])(\ell') \\
&\qquad = C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad\quad + C(\omega^{\gamma}[\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], \omega^{\gamma+\frac{q}{2}}[\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \qquad \text{by above} \\
&\qquad = C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad\quad + \omega^{\gamma-\gamma-\frac{q}{2}}C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \qquad \text{by Theorem 1.8} \\
&\qquad = C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad\quad - C([\mathbf{F}|_{\mathbf{xx}'=\mathbf{cc}_1}], [\mathbf{F}_a|_{\mathbf{xx}'=\mathbf{dc}_2}])(\ell') \\
&\qquad = 0,
\end{aligned}$$

for $-(n_{\mathbf{x}} - 1) \leqslant \ell' \leqslant (n_{\mathbf{x}} - 1)$, and so by the previous comments, the sum is zero for all ℓ.

In the case of $s = 1$ and $P = px_{i_0}$ is a trivial path, we have that $x_a = x_b = x_{i_0}$, so we get

$$-\overline{P} = -p(1 - x_a) = P - p,$$

and then the negated reverse of the restricted forms of f_a and f_{ab} are

$$\begin{aligned}
-\overline{f_{ab}\big|_{\mathbf{xx'}=\mathbf{dc}_2}} &= P - p + L + r_L - r_{G_2}(\mathbf{c}_2) - g_2 \\
&= f\big|_{\mathbf{xx'}=\mathbf{cc}_1} + \gamma \\
-\overline{f_b\big|_{\mathbf{xx'}=\mathbf{cc}_1}} &= P - p + \frac{q}{2}x_a + \frac{q}{2} + L + r_L - r_{G_1}(\mathbf{c}_1) - g_1 \\
&= f_a\big|_{\mathbf{xx'}=\mathbf{dc}_2} + \gamma + \frac{q}{2},
\end{aligned}$$

where now $\gamma = r_L - p - r_{G_1}(\mathbf{c}_1) - g_1 - r_{G_2}(\mathbf{c}_2) - g_2$, and the rest of the argument above follows exactly.

Thus in either case the expanded sum of the cross-correlations is zero, and so in turn the original sum is too, i.e. we have

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_a\big|_{\mathbf{x}=\mathbf{d}})(\ell) + C(\mathbf{F}_b\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_{ab}\big|_{\mathbf{x}=\mathbf{d}})(\ell) = 0,$$

for all ℓ, and in particular for $-(2^m - 1) \leqslant \ell \leqslant 2^m - 1$, as was to be shown. □

The following theorem is the main result of this chapter. It says that if we take a complementary pair emanating from the construction of Corollary 1.25, then the set of all compressed vectors, from all restrictions for any choice of the restricting variables $\mathbf{x}$, is in fact a complementary set. The effect of the restriction is to cut the original path from the construction into a number of shorter 'path segments', and it is these that the proof is based around.

Theorem 5.4. *Let f and f_a, two generalized Boolean functions over $\mathbb{Z}_q$ in the $m \geqslant 2$ variables $x_0, \ldots, x_{m-1}$, be a Golay complementary pair as constructed by Corollary 1.25, i.e.*

$$\begin{aligned}
f &= P + L \\
f_a &= P + \frac{q}{2}x_a + L,
\end{aligned}$$

where:

$$P = \frac{q}{2}\sum_{\alpha=0}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)}$$

is a path in the m variables for some permutation π of $\{0, 1, \ldots, m-1\}$; x_a is either of the end points of the path, $x_a = x_{\pi(0)}$ or $x_{\pi(m-1)}$; and L is any affine function

$$L = \sum_{i=0}^{m-1} g_{\pi(i)}x_{\pi(i)} + g, \quad g_{\pi(i)}, g \in \mathbb{Z}_q.$$

So, by the corollary, the corresponding vectors of f and f_a form a Golay complementary pair, i.e.

$$A(\mathbf{F})(\ell) + A(\mathbf{F}_a)(\ell) = 0, \quad 1 \leqslant \ell \leqslant 2^m - 1.$$

Let $\mathbf{x} = x_{j_0} \cdots x_{j_{k-1}}$, $0 \leqslant j_0 < j_1 < \cdots < j_{k-1} \leqslant m-1$ be some $k \geqslant 1$ restricting variables, and let $\mathbf{c} = c_0c_1 \cdots c_{k-1}$ be a binary word of length k. Then the set of

2^{k+1} compressed vectors formed by compressing the restricted vectors of both f and f_a over all $\mathbf{c}$ form a complementary set, i.e.

$$\sum_{\mathbf{c}} \left(A(\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\widehat{\mathbf{F}}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\right) = 0, \quad 1 \leqslant \ell \leqslant 2^{m-k} - 1.$$

Proof. Without loss of generality, let the path end point x_a be $x_{\pi(0)}$ (due to the symmetric nature of the path, the following argument is easily modified for the case when x_a is chosen to be the other end point of the path, $x_{\pi(m-1)}$). First we use induction on the number of restricting variables to show that the restricted vectors form a complementary set, i.e.

$$\sum_{\mathbf{c}} \left(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\right) = 0,$$

for $l \neq 0$, and then we invoke Corollary 5.2 to show that the compressed vectors are also a complementary set. For the induction we increase the number of restricting variables being considered, for $t = 1, 2, \ldots, k$, and at each stage expand the sum of the auto-correlations using Corollary 1.16, and then show that the sum of the cross-correlations is zero. We start from the restricting variable which is furthest from $x_{\pi(0)}$ along the path, and then work back down the path toward $x_{\pi(0)}$. Thus re-label the restricting variables to be $x_{\pi(\beta_i)}, i = 1, 2, \ldots, k$ where $m - 1 \geqslant \beta_1 > \beta_2 > \cdots > \beta_k \geqslant 0$. So for the base case of the induction, $t = 1$, we restrict on $x_{\pi(\beta_1)}$ and expand

$$A(\mathbf{F})(\ell) + A(\mathbf{F}_a)(\ell) = 0, \quad \ell \neq 0,$$

using Corollary 1.16 to get, for $\ell \neq 0$,

$$\begin{aligned}\sum_{c} &\left(A(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c})(\ell) + A(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c})(\ell)\right) \\ &\quad + \sum_{c_1 \neq c_2} \Big(C(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}\big|_{x_{\pi(\beta_1)}=c_2})(\ell) \\ &\qquad\qquad + C(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_2})(\ell)\Big) = 0. \quad (5.9)\end{aligned}$$

Substitute $x_{\pi(\beta_1)} = c$ in f to see the general form of the restriction:

$$f\big|_{x_{\pi(\beta_1)}=c} = P' + \frac{q}{2}(cx_{\pi(\beta_1-1)} + cx_{\pi(\beta_1+1)}) + L' + F' + cg_{\pi(\beta_1)} \qquad (5.10)$$

where

$$\begin{aligned} P' &= \frac{q}{2}\sum_{\alpha=0}^{\beta_1-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} \\ L' &= \sum_{i=0}^{\beta_1-1} g_{\pi(i)}x_{\pi(i)} + g \\ F' &= \frac{q}{2}\sum_{\alpha=\beta_1+1}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} + \sum_{i=\beta_1+1}^{m-1} g_{\pi(i)}x_{\pi(i)}. \end{aligned}$$

So here: P' is that part of path P from $x_{\pi(0)}$ to $x_{\pi(\beta_1-1)}$, and so is a path is in its own right; L' contains only those linear terms in the same variables as the path P'; and F' consists of the remaining linear terms and the rest of path P above $x_{\pi(\beta_1+1)}$. The function $f_a\big|_{x_{\pi(\beta_1)}=c}$ is similar, only with the addition of the $\frac{q}{2}x_a = \frac{q}{2}x_{\pi(0)}$ term.
To complete the base case of the induction, three cases are now considered:

(i) the restricting variable is somewhere between the second point in the path and the other end, i.e. $2 \leqslant \beta_1 \leqslant m-1$,

(ii) the restricting variable is next to the end point $x_{\pi(0)}$, i.e. $\beta_1 = 1$,

(iii) the restricting variable is the path end point $x_{\pi(0)}$, i.e. $\beta_1 = 0$ (in which case this is the only restricting variable contained in $\mathbf{x}$).

Base case (i)

This is the most general case, when the restricting variable is somewhere between the second point of the path and the other end point, i.e. $2 \leqslant \beta_1 \leqslant m-1$. Put $c = 0$ and 1 in turn into equation (5.10) to get:

$$\begin{aligned}
f\big|_{x_{\pi(\beta_1)}=0} &= P' + L' + F' \\
f\big|_{x_{\pi(\beta_1)}=1} &= P' + \frac{q}{2}(x_{\pi(\beta_1-1)} + x_{\pi(\beta_1+1)}) + L' + F' + g_{\pi(\beta_1)} \\
f_a\big|_{x_{\pi(\beta_1)}=0} &= P' + L' + F' + \frac{q}{2}x_{\pi(0)} \\
f_a\big|_{x_{\pi(\beta_1)}=1} &= P' + \frac{q}{2}(x_{\pi(\beta_1-1)} + x_{\pi(\beta_1+1)}) + L' + F' + g_{\pi(\beta_1)} + \frac{q}{2}x_{\pi(0)}.
\end{aligned}$$

Re-group the end points of path P', $x_{\pi(0)}$ and $x_{\pi(\beta_1-1)}$, to be with the path to get

$$\begin{aligned}
f\big|_{x_{\pi(\beta_1)}=0} &= P' + L' + F' \\
f\big|_{x_{\pi(\beta_1)}=1} &= \left(P' + \frac{q}{2}x_{\pi(\beta_1-1)}\right) + L' + F' + x_{\pi(\beta_1+1)} + g_{\pi(\beta_1)} \\
f_a\big|_{x_{\pi(\beta_1)}=0} &= \left(P' + \frac{q}{2}x_{\pi(0)}\right) + L' + F' \\
f_a\big|_{x_{\pi(\beta_1)}=1} &= \left(P' + \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(\beta_1-1)}\right) + L' + F' + x_{\pi(\beta_1+1)} + g_{\pi(\beta_1)},
\end{aligned}$$

from which it can be seen these functions satisfy the conditions of Theorem 5.3, and so we get, for $c_1 \neq c_2$ and for all ℓ,

$$C(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}\big|_{x_{\pi(\beta_1)}=c_2})(\ell) + C(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_2})(\ell) = 0.$$

Therefore

$$\sum_{c_1 \neq c_2} \left(C(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}\big|_{x_{\pi(\beta_1)}=c_2})(\ell) + C(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c_2})(\ell)\right) = 0,$$

for all ℓ, and thus (5.9) becomes

$$\sum_{c} \left(A(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c})(\ell) + A(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c})(\ell)\right) = 0, \quad \ell \neq 0,$$

as we required.

Base case (ii)

The restricting variable is next to the end point $x_{\pi(0)}$, i.e. $\beta_1 = 1$. Substituting $c = 0$ or 1 in turn into equation (5.10), now for $x_{\pi(\beta_1)} = x_{\pi(1)}$ gives

$$\begin{aligned}
f\big|_{x_{\pi(1)}=0} &= L' + F' \\
f\big|_{x_{\pi(1)}=1} &= \frac{q}{2}(x_{\pi(0)} + x_{\pi(2)}) + L' + F' + g_{\pi(1)} \\
f_a\big|_{x_{\pi(1)}=0} &= L' + F' + \frac{q}{2}x_{\pi(0)} \\
f_a\big|_{x_{\pi(1)}=1} &= \frac{q}{2}x_{\pi(2)} + L' + F' + g_{\pi(1)},
\end{aligned}$$

where now we note that the path P' is null, and L' is just $g_{\pi(0)}x_{\pi(0)} + g$. Viewing $\frac{q}{2}x_{\pi(0)}$ as a trivial path, both of whose end points are also $\frac{q}{2}x_{\pi(0)}$, and by introducing $0 = \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}$ at appropriate points, we can again group the terms so as to satisfy Theorem 5.3, as indicated:

$$\begin{aligned}
f\big|_{x_{\pi(1)}=0} &= \underbrace{\left(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\right)}_{\text{`}P+\frac{q}{2}x_a\text{'}} + L' + \underbrace{F'}_{\text{`}G_2\text{'}} \\
f\big|_{x_{\pi(1)}=1} &= \underbrace{\left(\frac{q}{2}x_{\pi(0)}\right)}_{\text{`}P\text{'}} + L' + \underbrace{F' + \frac{q}{2}x_{\pi(2)}}_{\text{`}G_1\text{'}} + g_{\pi(1)} \\
f_a\big|_{x_{\pi(1)}=0} &= \underbrace{\left(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\right)}_{\text{`}P+\frac{q}{2}(x_a+x_b)\text{'}} + L' + \underbrace{F'}_{\text{`}G_2\text{'}} \\
f_a\big|_{x_{\pi(1)}=1} &= \underbrace{\left(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\right)}_{\text{`}P+\frac{q}{2}x_b\text{'}} + L' + \underbrace{F' + \frac{q}{2}x_{\pi(2)}}_{\text{`}G_1\text{'}} + g_{\pi(1)}.
\end{aligned}$$

Thus we have, for $c_1 \neq c_2$, that

$$C(\mathbf{F}\big|_{x_{\pi(1)}=c_1}, \mathbf{F}\big|_{x_{\pi(1)}=c_2})(\ell) + C(\mathbf{F}_a\big|_{x_{\pi(1)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(1)}=c_2})(\ell) = 0,$$

for all ℓ, and with $\beta_1 = 1$, as in Base case (i), this again gives

$$\sum_c \left(A(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c})(\ell) + A(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c})(\ell)\right) = 0, \quad \ell \neq 0.$$

Base case (iii)

The restricting variable is the path end point, so $x_{\pi(\beta_1)} = x_{\pi(0)}$. Put $c = 0$ and 1 in expression (5.10) with $x_{\pi(\beta_1)} = x_{\pi(0)}$ to get the four restricted functions:

$$\begin{aligned}
f\big|_{x_{\pi(0)}=0} &= F' \\
f\big|_{x_{\pi(0)}=1} &= F' + \frac{q}{2}x_{\pi(1)} + g_{\pi(0)} \\
f_a\big|_{x_{\pi(0)}=0} &= F' \\
f_a\big|_{x_{\pi(0)}=1} &= F' + \frac{q}{2}x_{\pi(1)} + g_{\pi(0)} + \frac{q}{2},
\end{aligned}$$

where now both P' and L' are null. Thus for fixed $c_1 \neq c_2$, the only difference between the pairings of the restricted functions $f\big|_{x_{\pi(0)}=c_1}, f\big|_{x_{\pi(0)}=c_2}$ and $f_a\big|_{x_{\pi(0)}=c_1}, f_a\big|_{x_{\pi(0)}=c_2}$ is the '$+\frac{q}{2}$' appearing on just one of the latter two functions. Then from Theorem 1.8 we get

$$C(\mathbf{F}_a\big|_{x_{\pi(0)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(0)}=c_2})(\ell) = -C(\mathbf{F}\big|_{x_{\pi(0)}=c_1}, \mathbf{F}\big|_{x_{\pi(0)}=c_2})(\ell),$$

giving

$$\sum_{c_1 \neq c_2} \big(C(\mathbf{F}\big|_{x_{\pi(0)}=c_1}, \mathbf{F}\big|_{x_{\pi(0)}=c_2})(\ell) + C(\mathbf{F}_a\big|_{x_{\pi(0)}=c_1}, \mathbf{F}_a\big|_{x_{\pi(0)}=c_2})(\ell)\big) = 0,$$

for all ℓ. Therefore, with $\beta_1 = 0$, (5.9) once again becomes

$$\sum_c \big(A(\mathbf{F}\big|_{x_{\pi(\beta_1)}=c})(\ell) + A(\mathbf{F}_a\big|_{x_{\pi(\beta_1)}=c})(\ell)\big) = 0, \quad \ell \neq 0,$$

thus completing the base case for the induction.

Now we assume, by the inductive hypothesis, that

$$\sum_{\mathbf{c}} \big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0, \quad \ell \neq 0,$$

where $\mathbf{x} = x_{\pi(\beta_1)} \cdots x_{\pi(\beta_{t-1})}$ consists of $t-1$ restricting variables, and examine the case of t restricting variables. Again we use Corollary 1.16 to expand this by the t^{th} restricting variable, $x_{\pi(\beta_t)}$, to get, for $\ell \neq 0$,

$$\begin{aligned}\sum_{\mathbf{c}} \Big(\sum_{c'} \big(A(\mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell)\big) \\ + \sum_{c'_1 \neq c'_2} \big(C(\mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_1}, \mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_2})(\ell) \\ + C(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_1}, \mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_2})(\ell)\big)\Big) = 0. \qquad (5.11)\end{aligned}$$

The aim is once again to show that the cross-correlation term is always zero. Represent the restricted function $f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'}$ by

$$f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'} = P' + \frac{q}{2}c'x_{\pi(\beta_t-1)} + \Big(\frac{q}{2}c'x_{\pi(\beta_t+1)}\Big)\Big|_{\mathbf{x}=\mathbf{c}} + L' + F'_{\mathbf{c}} + c'g_{\pi(\beta_t)} \qquad (5.12)$$

where

$$P' = \frac{q}{2}\sum_{\alpha=0}^{\beta_t-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)}$$

$$L' = \sum_{i=0}^{\beta_t-1} g_{\pi(i)}x_{\pi(i)} + g$$

$$F'_{\mathbf{c}} = \Big(\frac{q}{2}\sum_{\alpha=\beta_t+1}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} + \sum_{i=\beta_t+1}^{m-1} g_{\pi(i)}x_{\pi(i)} + g\Big)\Big|_{\mathbf{x}=\mathbf{c}}.$$

So here: similar to before, P' and L' are those parts of P and L up to $\beta_t - 1$, and thus are unaffected by the restriction; those parts of P and L above $\beta_t + 1$ are placed in $F'_{\mathbf{c}}$, but since they may be subjected to the restriction, this is shown, and the subscript $\mathbf{c}$ is appended; the variable $x_{\pi(\beta_t+1)}$ could also be part of the restriction, so this is shown in the term $\left(\frac{q}{2}c'x_{\pi(\beta_t+1)}\right)\big|_{\mathbf{x}=\mathbf{c}}$.
There are three cases again, basically as before, but now relative to the previous restricted variable $x_{\pi(\beta_{t-1})}$ rather than the end point $x_{\pi(m-1)}$:

(i) the new restricting variable is somewhere between the second point in the path and the 'lowest' previously restricted variable, i.e. $2 \leqslant \beta_t < \beta_{t-1}$,

(ii) the new restricting variable is next to the end point $x_{\pi(0)}$, i.e. $\beta_t = 1$,

(iii) the new restricting variable is the path end point $x_{\pi(0)}$, i.e. $\beta_t = 0$ (and thus is the last restricting variable).

Case (i)

This is the most general case again, where the new restricting variable is somewhere between the second point of the path and the lowest previously restricted variable ($x_{\pi(\beta_{t-1})}$), i.e. $2 \leqslant \beta_t < \beta_{t-1}$. Substitute $c' = 0$ and 1 into equation 5.12 to get

$$\begin{aligned}
f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}0} &= P' + L' + F'_{\mathbf{c}} \\
f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}1} &= P' + \frac{q}{2}x_{\pi(\beta_t-1)} + \left(\frac{q}{2}x_{\pi(\beta_t+1)}\right)\big|_{\mathbf{x}=\mathbf{c}} + L' + F'_{\mathbf{c}} + g_{\pi(\beta_t)} \\
f_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}0} &= P' + L' + F'_{\mathbf{c}} + \frac{q}{2}x_{\pi(0)} \\
f_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}1} &= P' + \frac{q}{2}x_{\pi(\beta_t-1)} + \left(\frac{q}{2}x_{\pi(\beta_t+1)}\right)\big|_{\mathbf{x}=\mathbf{c}} \\
&\quad + L' + F'_{\mathbf{c}} + g_{\pi(\beta_t)} + \frac{q}{2}x_{\pi(0)}.
\end{aligned}$$

As before, group the ends of the path P', $x_{\pi(0)}$ and $x_{\pi(\beta_t-1)}$, with the path to get

$$\begin{aligned}
f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}0} &= P' + L' + F'_{\mathbf{c}} \\
f\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}1} &= \left(P' + \frac{q}{2}x_{\pi(\beta_t-1)}\right) + L' + F'_{\mathbf{c}} + \left(\frac{q}{2}x_{\pi(\beta_t+1)}\right)\big|_{\mathbf{x}=\mathbf{c}} + g_{\pi(\beta_t)} \\
f_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}0} &= \left(P' + \frac{q}{2}x_{\pi(0)}\right) + L' + F'_{\mathbf{c}} \\
f_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}1} &= \left(P' + \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(\beta_t-1)}\right) \\
&\quad + L' + F'_{\mathbf{c}} + \left(\frac{q}{2}x_{\pi(\beta_t+1)}\right)\big|_{\mathbf{x}=\mathbf{c}} + g_{\pi(\beta_t)},
\end{aligned}$$

from which it can be seen these functions again satisfy the conditions of Theorem 5.3, and so we get, for fixed $\mathbf{c}$ and $c'_1 \neq c'_2$ and for all ℓ,

$$C(\mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_1}, \mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_2})(\ell) + C(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_1}, \mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'_2})(\ell) = 0.$$

Therefore

$$\sum_{\mathbf{c}}\sum_{c_1'\neq c_2'}\big(C(\mathbf{F}|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c_1'},\mathbf{F}|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c_2'})(\ell) \\ + C(\mathbf{F}_a|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c_1'},\mathbf{F}_a|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c_2'})(\ell)\big) = 0,$$

for all ℓ, and thus (5.11) becomes

$$\sum_{\mathbf{c}}\sum_{c'}\big(A(\mathbf{F}|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell) + A(\mathbf{F}_a|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell)\big) = 0, \quad \ell\neq 0.$$

So if we subsume $x_{\pi(\beta_t)}$ into $\mathbf{x}$, so that it now represents the t restricting variables $x_{\pi(\beta_1)}\cdots x_{\pi(\beta_t)}$, and likewise put c' into $\mathbf{c}$, we get

$$\sum_{\mathbf{c}}\big(A(\mathbf{F}|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0, \quad \ell\neq 0,$$

as required.

Case (ii)

The new restricting variable is next to the end point $x_{\pi(0)}$, i.e. $\beta_t = 1$. Substituting $c' = 0$ or 1 in turn into equation (5.12), now for $x_{\pi(\beta_t)} = x_{\pi(1)}$ gives

$$\begin{aligned} f|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}0} &= L' + F'_{\mathbf{c}} \\ f|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}1} &= \frac{q}{2}x_{\pi(0)} + \Big(\frac{q}{2}x_{\pi(2)}\Big)|_{\mathbf{x}=\mathbf{c}} + L' + F'_{\mathbf{c}} + g_{\pi(1)} \\ f_a|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}0} &= L' + F'_{\mathbf{c}} + \frac{q}{2}x_{\pi(0)} \\ f_a|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}1} &= \Big(\frac{q}{2}x_{\pi(2)}\Big)|_{\mathbf{x}=\mathbf{c}} + L' + F'_{\mathbf{c}} + g_{\pi(1)}. \end{aligned}$$

where again we note that the path P' is null, and L' is just $g_{\pi(0)}x_{\pi(0)} + g$. As in the base case, viewing $\frac{q}{2}x_{\pi(0)}$ as a trivial path, both of whose end points are also $\frac{q}{2}x_{\pi(0)}$, and by introducing $0 = \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}$ at appropriate points, we can group the terms so as to satisfy Theorem 5.3, as indicated:

$$\begin{aligned} f|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}0} &= \underbrace{\Big(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\Big)}_{`P+\frac{q}{2}x_a\text{'}} + L' + \underbrace{F'_{\mathbf{c}}}_{`G_2\text{'}} \\ f|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}1} &= \underbrace{\Big(\frac{q}{2}x_{\pi(0)}\Big)}_{`P\text{'}} + L' + \underbrace{F'_{\mathbf{c}} + \Big(\frac{q}{2}x_{\pi(2)}\Big)|_{\mathbf{x}=\mathbf{c}}}_{`G_1\text{'}} + g_{\pi(1)} \\ f_a|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}0} &= \underbrace{\Big(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\Big)}_{`P+\frac{q}{2}(x_a+x_b)\text{'}} + L' + \underbrace{F'_{\mathbf{c}}}_{`G_2\text{'}} \\ f_a|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}1} &= \underbrace{\Big(\frac{q}{2}x_{\pi(0)} + \frac{q}{2}x_{\pi(0)}\Big)}_{`P+\frac{q}{2}x_b\text{'}} + L' + \underbrace{F'_{\mathbf{c}} + \Big(\frac{q}{2}x_{\pi(2)}\Big)|_{\mathbf{x}=\mathbf{c}}}_{`G_1\text{'}} + g_{\pi(1)}. \end{aligned}$$

Thus we have, for fixed $\mathbf{c}$ and $c'_1 \neq c'_2$ and for all ℓ,

$$C(\mathbf{F}\big|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}c'_1}, \mathbf{F}\big|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}c'_2})(\ell) + C(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}c'_1}, \mathbf{F}_a\big|_{\mathbf{x}x_{\pi(1)}=\mathbf{c}c'_2})(\ell) = 0,$$

and with $\beta_t = 1$, as in Case (i), this again gives

$$\begin{aligned}\sum_{\mathbf{c}}\sum_{c'}\big(A(\mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell)\big)& \\ &= \sum_{\mathbf{c}}\big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) \\ &= 0, \quad \ell \neq 0.\end{aligned}$$

Case (iii)

The new restricting variable is the path end point, so $x_{\pi(\beta_t)} = x_{\pi(0)}$. Put $c' = 0$ and 1 and $x_{\pi(\beta_t)} = x_{\pi(0)}$ into expression (5.12) to get

$$\begin{aligned} f\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}0} &= F'_{\mathbf{c}} \\ f\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}1} &= F'_{\mathbf{c}} + \Big(\frac{q}{2}x_{\pi(1)}\Big)\big|_{\mathbf{x}=\mathbf{c}} + g_{\pi(0)} \\ f_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}0} &= F'_{\mathbf{c}} \\ f_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}1} &= F'_{\mathbf{c}} + \Big(\frac{q}{2}x_{\pi(1)}\Big)\big|_{\mathbf{x}=\mathbf{c}} + g_{\pi(0)} + \frac{q}{2}, \end{aligned}$$

where again both P' and L' are null. Thus for fixed $c'_1 \neq c'_2$, the only difference between the pairings of the restricted functions $f\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_1}, f\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_2}$ and $f_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_1}, f_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_2}$ is the '$+\frac{q}{2}$' appearing on just one of the latter two functions. Then from Theorem 1.8 we get, for all ℓ,

$$C(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_1}, \mathbf{F}_a\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_2})(\ell) = -C(\mathbf{F}\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_1}, \mathbf{F}\big|_{\mathbf{x}x_{\pi(0)}=\mathbf{c}c'_2})(\ell),$$

so again the sum of the cross-correlations is zero, and therefore, with $\beta_t = 0$, (5.11) once again becomes

$$\begin{aligned}\sum_{\mathbf{c}}\sum_{c'}\big(A(\mathbf{F}\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}x_{\pi(\beta_t)}=\mathbf{c}c'})(\ell)\big)& \\ &= \sum_{\mathbf{c}}\big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) \\ &= 0, \quad \ell \neq 0.\end{aligned}$$

Thus in each case, if the auto-correlations sum to zero, i.e.

$$\sum_{\mathbf{c}}\big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0, \quad \ell \neq 0,$$

when $\mathbf{x}$ contains $t-1$ variables, then they also sum to zero when $\mathbf{x}$ contains t variables, and hence by induction they sum to zero for $t = 1, 2, \ldots, k$ restricting variables. Then from Corollary 5.2, since the sum across $\mathbf{c}$ of the restricted vectors is zero, then so also is the sum of the compressed vectors, i.e.

$$\sum_{\mathbf{c}} \big(A(\widehat{\mathbf{F}}|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\widehat{\mathbf{F}}_a|_{\mathbf{x}=\mathbf{c}})(\ell) \big) = 0, \quad 1 \leqslant \ell \leqslant 2^{m-k} - 1,$$

and the theorem is proved. □

Since the set identified by the theorem is of size 2^{k+1}, then all words in the set have a PMEPR$\leqslant 2^{k+1}$. If we denote the quadratic part of f after restriction by $\bar{Q}$, and the compressed version of this as $\widehat{\bar{Q}}$, then the set of the theorem is a subset of the coset $\widehat{\bar{Q}} + RM_q(1, m-k)$. This coset of course has a PMEPR determined by Theorem 1.27, and this will depend on how many deletions are necessary in order to reduce $\widehat{\bar{Q}}$ to the longest path segment that remains after the original restriction. It is quite possible that the PMEPR given by the above theorem is less than that given by Theorem 1.27, as is illustrated in the following example.

Example 5.5. Consider the following binary case for $m = 11$. Let f be

$$\begin{aligned} f = {} & x_6x_3 + x_3x_{10} + x_{10}x_1 + x_1x_4 + x_4x_7 \\ & + x_7x_2 + x_2x_0 + x_0x_9 + x_9x_5 + x_5x_8, \end{aligned}$$

and pick end point $x_a = x_6$, so that f and $f_a = f + x_6$ are a Golay complementary pair. Restrict using the variables $\mathbf{x} = x_2x_{10}$, and let

$$\bar{Q} = x_6x_3 + x_1x_4 + x_4x_7 + x_0x_9 + x_9x_5 + x_5x_8$$

be the quadratic part left following any restriction for the given $\mathbf{x}$. Then vectors of the eight restricted functions

$$\begin{aligned} f|_{x_2x_{10}=c_0c_1} &= \bar{Q} + c_0(x_0 + x_7) + c_1(x_1 + x_3) \\ f_a|_{x_2x_{10}=c_0c_1} &= \bar{Q} + c_0(x_0 + x_7) + c_1(x_1 + x_3) + x_6, \end{aligned}$$

$c_0, c_1 \in \{0, 1\}$, form a complementary set. Map the indices using

$$0 \mapsto 0, 1 \mapsto 1, 3 \mapsto 2, 4 \mapsto 3, 5 \mapsto 4, 6 \mapsto 5, 7 \mapsto 6, 8 \mapsto 7, 9 \mapsto 8,$$

to get the compressed $\bar{Q}$,

$$\widehat{\bar{Q}} = x_5x_2 + x_1x_3 + x_3x_6 + x_0x_8 + x_8x_4 + x_4x_7,$$

and the eight compressed functions,

$$\begin{aligned} \widehat{f}|_{x_2x_{10}=c_0c_1} &= \widehat{\bar{Q}} + c_0(x_0 + x_6) + c_1(x_1 + x_2) \\ \widehat{f_a}|_{x_2x_{10}=c_0c_1} &= \widehat{\bar{Q}} + c_0(x_0 + x_6) + c_1(x_1 + x_2) + x_5, \end{aligned}$$

$c_0, c_1 \in \{0, 1\}$, the vectors of which also form a complementary set. Each of the vectors in the set thus has a PMEPR$\leqslant 2^{2+1} = 8$; from Theorem 1.27, we would need to delete vertices 1,2,3,5 and 6 from $\widehat{\bar{Q}}$, to leave just path $x_0x_8 + x_8x_4 + x_4x_7$, and so this gives the PMEPR of the coset as being at most $2^{5+1} = 64$. Thus the above theorem has identified words in the coset $\widehat{\bar{Q}} + RM(1, 9)$ which have a considerably lower PMEPR than is generally the case. □

5.4 Complementary Sets from a Sequence

The functions in the set specified by Theorem 5.4 in the previous section have a quadratic part that is a number of disjoint path segments. In Section 3.3 of Chapter 3 we saw how it was possible, using functions with such path segments, to construct functions that share the same auto-correlation function, and then in Section 3.4, by grouping together such functions, how it was possible to split up a complementary set into smaller complementary subsets. The same idea is used in this section: it is shown that for particularly choices of restricting variables, the complementary set generated from a complementary pair in Theorem 5.4 may be split in two, thus generating a complementary set from a single complementary sequence.

The following theorem shows that if two restricted functions essentially consist of a number of (the same) disjoint path segments, but the linear terms representing the end points of the paths are 'opposite' to each other, i.e. if the end point '$+\frac{q}{2}x_a$' appears in one it doesn't in the other, then the functions share the same auto-correlation function. Additionally, any further restriction, which generally splits one path segment into two new ones, results in functions that may be paired in exactly the same way.

Theorem 5.6. *Let the m indices $\{0, 1, 2, \ldots, m-1\}$ be partitioned into three sets: the set I, further partitioned into the subsets I_j, $j = 0, 1, \ldots, \ell - 1$, containing indices on which ℓ paths are to be defined; J containing indices for a generalized function; and K, the indices of any restricting variables $\mathbf{x}$, viz*

$$\begin{aligned}
I &= \bigcup_{j=0}^{\ell-1} I_j \textit{ where } I_j = \{i_{j,0}, i_{j,1}, \ldots, i_{j,s_j-1}\}, \quad s_j \geqslant 2,\ j = 0, 1, \ldots, \ell-1,\\
J &= \{j_0, j_1, \ldots, j_{t-1}\},\\
K &= \{0, 1, \ldots, m-1\} \setminus (I \cup J),
\end{aligned}$$

where

$$\begin{aligned}
I_i \cap I_j &= \varnothing \qquad \textit{for } i \neq j,\\
I \cap J &= \varnothing.
\end{aligned}$$

Let the size of set I be $s = \sum_{j=0}^{\ell-1} s_j$, and so the set K is of size $m - s - t$. Let the ℓ bijective functions $\pi_j : \{0, 1, \ldots, s_j - 1\} \to I_j$ define the path segments

$$P_j = \frac{q}{2} \sum_{\alpha=0}^{s_j-2} x_{\pi_j(\alpha)} x_{\pi_j(\alpha+1)},$$

which have end points $x_{\pi_j(0)}$ and $x_{\pi_j(s_j-1)}$. Let F be a generalized Boolean function in the variables indexed by J, namely $F = F(x_{j_0}, x_{j_1}, \ldots, x_{j_{t-1}})$, and let L be a linear function in the same variables as the paths, i.e. whose indices are taken from I, so $L = \sum_{i \in I} g_i x_i$, $g_i \in \mathbb{Z}_q$. Let f and g be two generalized Boolean functions in the m variables $x_0, \ldots, x_{m-1}$, which after restriction by the *variables indexed by K are defined as:*

$$f\big|_{\mathbf{x}=\mathbf{c}} = \sum_{j=0}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + F + L + h_1$$

$$g\big|_{\mathbf{x}=\mathbf{c}} = \sum_{j=0}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j) x_{\pi_j(0)} + (1-e_j) x_{\pi_j(s_j-1)}\big)\Big) + F + L + h_2$$

where $d_j, e_j \in \{0,1\}, h_1, h_2 \in \mathbb{Z}_q$. Then the restricted functions $f\big|_{\mathbf{x}=\mathbf{c}}$ and $g\big|_{\mathbf{x}=\mathbf{c}}$ have the same auto-correlation function. Further, for each $\delta \in \{0,1\}$, the pair of functions resulting from an additional restriction on any variable indexed in $I \cup J$,

$$f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} \text{ and } g\big|_{\mathbf{x}x_\gamma=\mathbf{c}d}$$

where

$$d = \begin{cases} \delta & \gamma \in J \\ \overline{\delta} = 1-\delta & \gamma \in I, \end{cases}$$

have the same form as given above, and thus also share the same auto-correlation function.

Proof. First we show that the two functions have the same auto-correlation function. Using the fact that we are working mod q (q even), so that $-\frac{q}{2} = \frac{q}{2}$, and re-grouping the terms we get

$$f\big|_{\mathbf{x}=\mathbf{c}} = \sum_{j=0}^{\ell-1} P_j + F + \Big(\sum_{j=0}^{\ell-1}\frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big) + L\Big) + h_1$$

$$g\big|_{\mathbf{x}=\mathbf{c}} = \sum_{j=0}^{\ell-1}\Big(P_j + \frac{q}{2}(x_{\pi_j(0)} + x_{\pi_j(s_j-1)})\Big) + F$$
$$+ \Big(\sum_{j=0}^{\ell-1}\frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big) + L\Big) + h_2.$$

For each of the ℓ paths P_j in $f\big|_{\mathbf{x}=\mathbf{c}}$, the path along with both of its end points, $P_j + \frac{q}{2}(x_{\pi_j(0)} + x_{\pi_j(s_j-1)})$, appears in $g\big|_{\mathbf{x}=\mathbf{c}}$, and thus by applying Corollary 3.5 sequentially to each of these paths we obtain a succession of functions with the same auto-correlation as $f\big|_{\mathbf{x}=\mathbf{c}}$, ending with $g\big|_{\mathbf{x}=\mathbf{c}}$. Thus the two functions have the same auto-correlation function.

Next we show that a further restriction where the new restricting variable is one in F, i.e. whose index is in J, still leads to a similar pairing of two functions with the same auto-correlation function. Suppose that the new restriction is x_γ, where $\gamma \in J$, and that δ is the equivalent constant. Since $J \cap I_j = \varnothing$ for all j, the index γ does not occur in any of the paths, and so on applying the new restriction, we simply get

$$\begin{aligned} f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{j=0}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + F\big|_{x_\gamma=\delta} + L + h_1 \\ g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{j=0}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big) \\ &\qquad + F\big|_{x_\gamma=\delta} + L + h_2. \end{aligned}$$

It is clear that the new restriction could be subsumed into $\mathbf{x}$, and we are left with expressions of precisely the same type that we started with. Thus by repeating the first argument given above we have, for $\gamma \in J$, that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ and $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ have the same auto-correlation function. A special instance of this case is when x_γ appears only as a linear term in F, as may occur from a previous invocation of the theorem which resulted in Cases (ii), (iii) and (iv) below, whereby new linear terms are introduced. The variable x_γ is no longer a path variable, i.e. $\gamma \notin I$, and so does belong to F, as in the above expressions, but now the restriction $F\big|_{x_\gamma=\delta}$ becomes

$$F\big|_{x_\gamma=\delta} = (F' + g'_\gamma x_\gamma)\big|_{x_\gamma=\delta} = F' + g'_\gamma\delta,$$

where F' does not depend on x_γ, and the constant g'_γ depends on the coefficients of the terms involving x_γ from the previous invocation. Thus even though $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ and $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ have the same auto-correlation, since the value of a constant added in such a way to a function does not affect the auto-correlation, we choose to pair them as $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ and $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$, where $\overline{\delta} = 1-\delta$ is the 1's complement of δ, and these two functions will also have the same auto-correlation. This maintains the pairing established for the cases below when the new restriction occurs in one of the paths (which x_γ once was).

Now we consider a further restriction where the new restricting variable is one of the path variables, i.e. x_γ, say, where the index γ is an element of one of the sets $I_j, j = 0, 1, \ldots, \ell-1$. There are five cases to consider, depending on the length of the path segment which contains x_γ, and whereabouts within the path it appears. The first is the most general case, where the path is split into two new ones; the rest are special cases where one or both of the new paths is null:

(i) the new restriction is more than two vertices in from each end of a path with four or more edges—this leaves two new shorter paths,

(ii) it is the second vertex in a path of three or more edges—this leaves a shorter path and new linear terms,

(iii) it is the mid-point of a double-edge path—this introduces just new linear terms,

(iv) it is the end point of a single-edge path—this also just introduces new linear terms, and

(v) it is the end point of a path with two or more edges—this leaves just a shorter path.

The working for each of the special cases is very similar to that for the general case, and therefore is unfortunately somewhat repetitious. However for simplicity's sake it seems more appropriate to repeat the working rather than complicate the general case by trying to make allowance for the special cases where they arise.

For each of these cases we now pair the new restriction $x_\gamma = \delta$ in one function with the 1's complement of the restriction, i.e. $x_\gamma = \overline{\delta}$ $(= 1 - \delta)$ in the other. Suppose that γ is in I_k, i.e. x_γ is in path P_k. The different cases arise from x_γ being a certain distance from one of the end points of the path P_k, and from the length of the path, s_k. For convenience we shall work with end $x_{\pi_k(0)}$, but due to the symmetric nature of a path, the arguments apply equally well should the other end point, $x_{\pi_k(s_k-1)}$, be chosen.

Case (i)

This is the most general case: the new restriction is more than two vertices in from each end of a path. So the path P_k has at least four edges, thus $s_k \geqslant 5$, and the index of the new restriction is at least two vertices in from either end point of the path, i.e. let $\gamma = \pi_k(\beta)$, where β is such that $2 \leqslant \beta \leqslant s_k - 3$. The new restriction causes path P_k to be split into two new paths:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} = {} & \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}\sum_{\alpha=0}^{\beta-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} \\
& + \frac{q}{2}\big(\delta x_{\pi_k(\beta-1)} + \delta x_{\pi_k(\beta+1)}\big) + \frac{q}{2}\sum_{\alpha=\beta+1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} \\
& + \frac{q}{2}\big(d_k x_{\pi_k(0)} + e_k x_{\pi_k(s_k-1)}\big) + F + L\big|_{x_\gamma=\delta} + h_1 \\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} = {} & \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big) \\
& + \frac{q}{2}\sum_{\alpha=0}^{\beta-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} + \frac{q}{2}\big((1-\delta)x_{\pi_k(\beta-1)} + (1-\delta)x_{\pi_k(\beta+1)}\big) \\
& + \frac{q}{2}\sum_{\alpha=\beta+1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} + \frac{q}{2}\big((1-d_k)x_{\pi_k(0)} + (1-e_k)x_{\pi_k(s_k-1)}\big) \\
& + F + L\big|_{x_\gamma=\overline{\delta}} + h_2.
\end{aligned}$$

Re-group the terms in each expression:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j+\frac{q}{2}\big(d_j x_{\pi_j(0)}+e_j x_{\pi_j(s_j-1)}\big)\Big)\\
&\quad+\Big(P'_k+\frac{q}{2}\big(d_k x_{\pi_k(0)}+\delta x_{\pi_k(\beta-1)}\big)\Big)\\
&\quad+\Big(P''_k+\frac{q}{2}\big(\delta x_{\pi_k(\beta+1)}+e_k x_{\pi_k(s_k-1)}\big)\Big)+F+L\big|_{x_\gamma=\delta}+h_1\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j+\frac{q}{2}\big((1-d_j)x_{\pi_j(0)}+(1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&\quad+\Big(P'_k+\frac{q}{2}\big((1-d_k)x_{\pi_k(0)}+(1-\delta)x_{\pi_k(\beta-1)}\big)\Big)\\
&\quad+\Big(P''_k+\frac{q}{2}\big((1-\delta)x_{\pi_k(\beta+1)}+(1-e_k)x_{\pi_k(s_k-1)}\big)\Big)\\
&\quad+F+L\big|_{x_\gamma=\delta}+h'_2,
\end{aligned}$$

where

$$\begin{aligned}
P'_k &= \frac{q}{2}\sum_{\alpha=0}^{\beta-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)}\\
P''_k &= \frac{q}{2}\sum_{\alpha=\beta+1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)}\\
h'_2 &= h_2+g_\gamma(1-2\delta)
\end{aligned}$$

and where we have substituted

$$L\big|_{x_\gamma=\overline{\delta}} = L\big|_{x_\gamma=\delta}+g_\gamma(1-2\delta)$$

since

$$L\big|_{x_\gamma=\delta}=\sum_{\substack{i\in I\\ i\neq\gamma}} g_i x_i+g_\gamma\delta \quad\text{and}\quad L\big|_{x_\gamma=\overline{\delta}}=\sum_{\substack{i\in I\\ i\neq\gamma}} g_i x_i+g_\gamma(1-\delta).$$

Examination of the expression for $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ above shows that it consists of: $\ell+1$ path segments (path P_k has been split into two new paths) in the variables indexed by $I'=I\setminus\{\gamma\}$, plus some combination of their end points; the generalized Boolean function F (still in those variables indexed by J); a linear function $L\big|_{x_\gamma=\delta}$ also in the variables indexed by I', i.e. the path variables; and some constant in $\mathbb{Z}_q$, h_1. The function $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$ consists of: the same $\ell+1$ paths, but with the opposite end points; the same function F; the same linear function $L\big|_{x_\gamma=\delta}$; and some different constant h'_2. Group the new restriction on x_γ in with $\mathbf{x}$ and call it $\mathbf{x}'$ (i.e. $K'=K\cup\{\gamma\}$), and similarly put δ in with $\mathbf{c}$ to get $\mathbf{c}'$, then we can regard $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ as $f\big|_{\mathbf{x}'=\mathbf{c}'}$. For g, put

$$g'(x_0,\ldots,x_\gamma,\ldots,x_{m-1})=g(x_0,\ldots,1-x_\gamma,\ldots,x_{m-1}),$$

so that $g'\big|_{\mathbf{x}'=\mathbf{c}'} = g'\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} = g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}}$, and thus we see that $f\big|_{\mathbf{x}'=\mathbf{c}'}$ and $g'\big|_{\mathbf{x}'=\mathbf{c}'}$ are a pair of functions fitting the conditions of the theorem, and which additionally, by the first argument given in the proof, share the same auto-correlation function. Thus, for $\gamma \in I$, we have that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ and $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}}$ have the same auto-correlation function.

Case (ii)

The new restriction is the second vertex in a path which has three or more edges. So take the path P_k to have 3 or more edges, thus $s_k \geqslant 4$, and take the index of the new restriction to be the next index from the end point of the path, i.e. $\beta = 1$, so $\gamma = \pi_k(1)$. The new restriction causes the path P_k to become a path with two less edges than it started with, plus new linear terms:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} = &\sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}\big(\delta x_{\pi_k(0)} + \delta x_{\pi_k(2)}\big)\\
&+ \frac{q}{2}\sum_{\alpha=2}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} + \frac{q}{2}\big(d_k x_{\pi_k(0)} + e_k x_{\pi_k(s_k-1)}\big)\\
&+ F + L\big|_{x_\gamma=\delta} + h_1\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}} = &\sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&+ \frac{q}{2}\big((1-\delta)x_{\pi_k(0)} + (1-\delta)x_{\pi_k(2)}\big) + \frac{q}{2}\sum_{\alpha=2}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)}\\
&+ \frac{q}{2}\big((1-d_k)x_{\pi_k(0)} + (1-e_k)x_{\pi_k(s_k-1)}\big) + F + L\big|_{x_\gamma=\bar{\delta}} + h_2.
\end{aligned}$$

Re-group terms as:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} = &\sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big)\\
&+ \Big(P_k' + \frac{q}{2}\big(\delta x_{\pi_k(2)} + e_k x_{\pi_k(s_k-1)}\big)\Big)\\
&+ F' + L'\big|_{x_\gamma=\delta} + h_1\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}} = &\sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&+ \Big(P_k' + \frac{q}{2}\big((1-\delta)x_{\pi_k(2)} + (1-e_k)x_{\pi_k(s_k-1)}\big)\Big)\\
&+ F' + L'\big|_{x_\gamma=\delta} + h_2',
\end{aligned}$$

where now

$$\begin{aligned}
P_k' &= \frac{q}{2}\sum_{\alpha=2}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} \\
F' &= F + \frac{q}{2}(\delta + d_k)x_{\pi_k(0)} + g_{\pi_k(0)}x_{\pi_k(0)} \\
L'\big|_{x_\gamma=\delta} &= \Big(\sum_{\substack{i\in I \\ i\neq\pi_k(0)}} g_i x_i\Big)\big|_{x_\gamma=\delta} \\
h_2' &= h_2 + g_\gamma(1-2\delta),
\end{aligned}$$

so the linear terms in $x_{\pi_k(0)}$, which is no longer a path variable, have been grouped in with F, and a similar substitution as Case (i) above has been made for $L'\big|_{x_\gamma=\overline{\delta}}$. Thus in this case we see that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ consists of: ℓ paths plus some combination of end points (path P_k has been shortened); the function F', involving variables not in any of the paths; the linear function $L'\big|_{x_\gamma=\delta}$, in the path variables; and a constant. The function $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$ consists of: the same ℓ paths, but with the opposite end points; F' again; the same linear function; and a different constant. Then making the same notational adjustments as Case (i), we again see that this pairing of functions satisfies the condition of the theorem, and thus we again have that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ and $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$ have the same auto-correlation function when $\gamma \in I$.

Case (iii)

The new restriction is the mid-point of a double-edge path. In this case we take path P_k to have just two edges, i.e. $s_k = 3$:

$$P_k = \frac{q}{2}(x_{\pi_k(0)}x_{\pi_k(1)} + x_{\pi_k(1)}x_{\pi_k(2)}),$$

and the new restriction is the mid-point of the path, i.e. $\gamma = \pi_k(1)$. This causes path P_k to cease to exist, reducing it to just linear terms:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0 \\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}\big(\delta x_{\pi_k(0)} + \delta x_{\pi_k(2)}\big) \\
&\quad + \frac{q}{2}\big(d_k x_{\pi_k(0)} + e_k x_{\pi_k(2)}\big) + F + L\big|_{x_\gamma=\delta} + h_1 \\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0 \\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big) \\
&\quad + \frac{q}{2}\big((1-\delta)x_{\pi_k(0)} + (1-\delta)x_{\pi_k(2)}\big) \\
&\quad + \frac{q}{2}\big((1-d_k)x_{\pi_k(0)} + (1-e_k)x_{\pi_k(2)}\big) + F + L\big|_{x_\gamma=\overline{\delta}} + h_2.
\end{aligned}$$

Re-grouping terms:

$$
\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big)\\
&\qquad + F' + L'\big|_{x_\gamma=\delta} + h_1\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&\qquad + F' + L'\big|_{x_\gamma=\delta} + h_2',
\end{aligned}
$$

where

$$
\begin{aligned}
F' &= F + \frac{q}{2}\big((\delta+d_k)x_{\pi_k(0)} + (\delta+e_k)x_{\pi_k(2)}\big) + g_{\pi_k(0)}x_{\pi_k(0)} + g_{\pi_k(2)}x_{\pi_k(2)}\\
L'\big|_{x_\gamma=\delta} &= \Bigg(\sum_{\substack{i\in I\\ i\neq\pi_k(0)\\ i\neq\pi_k(2)}} g_i x_i\Bigg)\Big|_{x_\gamma=\delta}\\
h_2' &= h_2 + g_\gamma(1-2\delta),
\end{aligned}
$$

gathering the remaining linear terms of path P_k with F, and with the same substitution for $L'\big|_{x_\gamma=\bar{\delta}}$ as before. Here we see that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ consists of: $\ell-1$ paths plus some combination of end points (the original paths minus path P_k); the function F', involving non-path variables; the linear function $L'\big|_{x_\gamma=\delta}$, in the path variables; and a constant. The function $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\bar{\delta}}$ consists of: the same $\ell-1$ paths, but with the opposite end points; F' again; the same linear function; and a different constant. Again, making the same notational adjustments as Case (i), we see that this pairing of functions also satisfies the condition of the theorem, and thus they share the same auto-correlation function.

Case (iv)

The new restriction is the end point of a single-edge path. In this case we take the path P_k to have just one edge, i.e. $s_k = 2$:

$$P_k = \frac{q}{2}x_{\pi_k(0)}x_{\pi_k(1)}.$$

The new restriction is on the end point of the path, i.e. $\gamma = \pi_k(0)$. Again this causes path P_k to cease to exist, reducing it to just linear terms:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}\delta x_{\pi_k(1)} \\
&\quad + \frac{q}{2}\big(d_k\delta + e_k x_{\pi_k(1)}\big) + F + L\big|_{x_\gamma=\delta} + h_1 \\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}(1-\delta)x_{\pi_k(1)} \\
&\quad + \frac{q}{2}\big((1-d_k)(1-\delta) + (1-e_k)x_{\pi_k(1)}\big) + F + L\big|_{x_\gamma=\overline{\delta}} + h_2.
\end{aligned}$$

Re-grouping the terms gives

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) \\
&\quad + F' + L'\big|_{x_\gamma=\delta} + h_1' \\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big) \\
&\quad + F' + L'\big|_{x_\gamma=\delta} + h_2',
\end{aligned}$$

where

$$\begin{aligned}
F' &= F + \frac{q}{2}(\delta + e_k)x_{\pi_k(1)} + g_{\pi_k(1)}x_{\pi_k(1)} \\
L'\big|_{x_\gamma=\delta} &= \Big(\sum_{\substack{i\in I\\ i\neq\pi_k(1)}} g_i x_i\Big)\big|_{x_\gamma=\delta} \\
h_1' &= h_1 + \frac{q}{2}d_k\delta \\
h_2' &= h_2 + \frac{q}{2}(1-d_k)(1-\delta) + g_\gamma(1-2\delta),
\end{aligned}$$

again gathering the remaining linear term of the path P_k with F, and using the same substitution for $L'\big|_{x_\gamma=\overline{\delta}}$. This time we have that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ consists of: $\ell-1$ paths plus some combination of end points (the original paths minus path P_k); the function F' in non-path variables; the linear function $L'\big|_{x_\gamma=\delta}$, in just the path variables; and a constant. The function $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$ consists of: the same $\ell-1$ paths, but with the opposite end points; F' again; the same linear function; and a different constant. Once more it is seen that this pairing of functions also satisfies the condition of the theorem, and that they therefore share the same auto-correlation.

Case (v)

The new restriction is the end point of a path with two or more edges. In this last case, the path P_k has at least two edges, i.e. $s_k \geqslant 3$, and again the new restriction is on the end point of the path, i.e. $\gamma = \pi_k(0)$. This just shortens the path P_k:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big) + \frac{q}{2}\sum_{\alpha=1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)}\\
&\quad + \frac{q}{2}\delta x_{\pi_k(1)} + \frac{q}{2}\big(d_k\delta + e_k x_{\pi_k(s_k-1)}\big) + F + L\big|_{x_\gamma=\delta} + h_1\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&\quad + \frac{q}{2}\sum_{\alpha=1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)} + \frac{q}{2}(1-\delta)x_{\pi_k(1)}\\
&\quad + \frac{q}{2}\big((1-d_k)(1-\delta) + (1-e_k)x_{\pi_k(s_k-1)}\big) + F + L\big|_{x_\gamma=\overline{\delta}} + h_2.
\end{aligned}$$

Re-grouping terms:

$$\begin{aligned}
f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big(d_j x_{\pi_j(0)} + e_j x_{\pi_j(s_j-1)}\big)\Big)\\
&\quad + \Big(P_k' + \frac{q}{2}\big(\delta x_{\pi_k(1)} + e_k x_{\pi_k(s_k-1)}\big)\Big) + F + L\big|_{x_\gamma=\delta} + h_1'\\
g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}} &= \sum_{\substack{j=0\\ j\neq k}}^{\ell-1}\Big(P_j + \frac{q}{2}\big((1-d_j)x_{\pi_j(0)} + (1-e_j)x_{\pi_j(s_j-1)}\big)\Big)\\
&\quad + \Big(P_k' + \frac{q}{2}\big((1-\delta)x_{\pi_k(1)} + (1-e_k)x_{\pi_k(s_k-1)}\big)\Big)\\
&\quad + F + L\big|_{x_\gamma=\delta} + h_2',
\end{aligned}$$

where

$$\begin{aligned}
P_k' &= \frac{q}{2}\sum_{\alpha=1}^{s_k-2} x_{\pi_k(\alpha)}x_{\pi_k(\alpha+1)}\\
h_1' &= h_1 + \frac{q}{2}d_k\delta\\
h_2' &= h_2 + \frac{q}{2}(1-d_k)(1-\delta) + g_\gamma(1-2\delta),
\end{aligned}$$

and once more the same substitution for $L\big|_{x_\gamma=\overline{\delta}}$ has been made. For this last case we have that $f\big|_{\mathbf{x}x_\gamma=\mathbf{c}\delta}$ consists of: ℓ paths plus some combination of end points (path P_k has been shortened); the function F; the linear function is just $L\big|_{x_\gamma=\delta}$, in just the path variables; and a constant. The function $g\big|_{\mathbf{x}x_\gamma=\mathbf{c}\overline{\delta}}$

consists of: the same ℓ paths, but with the opposite end points; F again; the same linear function; and a different constant. This pairing of functions is again seen to satisfy the condition of the theorem, and so again they share the same auto-correlation function.

We have shown that a pair of functions satisfying the conditions of the the theorem *do* have the same auto-correlation function, and also that (by examining all the cases) suitably pairing the functions following a further restriction on any variable results in pairs of functions that *still* satisfy the conditions of the theorem, and therefore also have the same auto-correlation function, and thus the theorem is proved. □

When the restricting variables contain either of the end points of the path, or a pair of indices which are adjacent in the path, the following theorem shows that, by pairing up functions with the same auto-correlation function according to the above theorem, the complementary set from Theorem 5.4 of the previous section may be halved in size i.e. the compressed vectors formed from just one of the sequences in the original pairing form a complementary set in their own right.

Theorem 5.7. *Let f be a generalized Boolean function over $\mathbb{Z}_q$ in the $m \geqslant 2$ variables $x_0, \ldots, x_{m-1}$ whose vector is a Golay complementary sequence as constructed by Corollary 1.25. That is, f is an element of the coset $P + RM_q(1, m)$ where P is the path*

$$P = \frac{q}{2} \sum_{\alpha=0}^{m-2} x_{\pi(\alpha)} x_{\pi(\alpha+1)},$$

for some permutation π of $\{0, 1, \ldots, m-1\}$. Let $J = \{j_0, j_1, \ldots, j_{k-1}\}$ be the set of indices of the $k \geqslant 1$ restricting variables $\mathbf{x} = x_{j_0} x_{j_1} \cdots x_{j_{k-1}}$, and let $\mathbf{c}$ be a binary word of length k.
If $\mathbf{x}$ contains either end point of the path, or a pair of indices adjacent in the path, i.e. $\pi(0) \in J$, or $\pi(m-1) \in J$, or $\pi(\beta) \in J$ and $\pi(\beta+1) \in J$ for some β, $0 \leqslant \beta \leqslant m-2$, then the set of 2^k compressed vectors $\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}}$, over all $\mathbf{c}$, form a complementary set, i.e.

$$\sum_{\mathbf{c}} A(\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad 1 \leqslant \ell \leqslant 2^{m-k} - 1.$$

Proof. Construct a Golay complementary pair according to Corollary 1.25 as

$$\begin{aligned} f &= P + L \\ f_a &= P + \frac{q}{2} x_a + L, \end{aligned} \tag{5.13}$$

where

$$L = \sum_{i=0}^{m-1} g_{\pi(i)} x_{\pi(i)} + g, \quad g_{\pi(i)}, g \in \mathbb{Z}_q$$

is any affine function, P is per the hypothesis, and x_a is either of the end points of the path, i.e. $x_a = x_{\pi(0)}$ or $x_{\pi(m-1)}$. From the proof of Theorem 5.4 we get that the set, over all $\mathbf{c}$, of *restricted* vectors is a complementary set, i.e.

$$\sum_{\mathbf{c}} \big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0, \quad \ell \neq 0.$$

We now show that when the restricting variables $\mathbf{x}$ satisfy the hypothesis it is possible to arrange the vectors into pairs sharing the same auto-correlation function, i.e. to get

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_1})(\ell) = A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}_2})(\ell), \quad \text{for all } \ell,$$

and for some $\mathbf{c}_1$ and $\mathbf{c}_2$, which halves both the number of distinct auto-correlations in the sum and thus also the size of the complementary set. Corollary 5.2 then completes the proof.

First consider the case when either of the path end points is one of the restricting variables, i.e. $\pi(0) \in J$ or $\pi(m-1) \in J$. Put $a = \pi(0)$ or $\pi(m-1)$, whichever one is being restricted on. Let the digit in $\mathbf{c}$ corresponding to x_a be labelled c_a, let $\mathbf{x}'$ be all restricting variables apart from x_a, and $\mathbf{c}'$ similarly. Thus by considering the restriction $\mathbf{x} = \mathbf{c}$ as $\mathbf{x}'x_a = \mathbf{c}'c_a$, and actually substituting c_a for x_a in f and f_a, we get

$$\begin{aligned} f\big|_{\mathbf{x}=\mathbf{c}} &= f\big|_{\mathbf{x}'x_a=\mathbf{c}'c_a} = \big(\tfrac{q}{2}c_a x_d + P_1 + L_1\big)\big|_{\mathbf{x}'=\mathbf{c}'} + g_a c_a + g \\ f_a\big|_{\mathbf{x}=\mathbf{c}} &= f_a\big|_{\mathbf{x}'x_a=\mathbf{c}'c_a} = \big(\tfrac{q}{2}c_a x_d + P_1 + L_1\big)\big|_{\mathbf{x}'=\mathbf{c}'} + g_a c_a + \frac{q}{2}c_a + g \end{aligned}$$

where

$$\left.\begin{aligned} x_d &= x_{\pi(1)} \\ P_1 &= \frac{q}{2}\sum_{\alpha=1}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} \\ L_1 &= \sum_{\alpha=1}^{m-1} g_{\pi(\alpha)}x_{\pi(\alpha)} \end{aligned}\right\} \text{ when } a = \pi(0),$$

$$\left.\begin{aligned} x_d &= x_{\pi(m-2)} \\ P_1 &= \frac{q}{2}\sum_{\alpha=0}^{m-3} x_{\pi(\alpha)}x_{\pi(\alpha+1)} \\ L_1 &= \sum_{\alpha=0}^{m-2} g_{\pi(\alpha)}x_{\pi(\alpha)}. \end{aligned}\right\} \text{ when } a = \pi(m-1).$$

Since the only difference between these two functions is the constant $\frac{q}{2}c_a$, by Theorem 1.8 the restricted functions $f\big|_{\mathbf{x}=\mathbf{c}}$ and $f_a\big|_{\mathbf{x}=\mathbf{c}}$ have the same auto-correlation function, i.e. for any given $\mathbf{c}$ and for all ℓ,

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell).$$

Now we consider the case when the restricting variables include a pair which are adjacent in the path, i.e. for some β, $0 \leqslant \beta \leqslant m-2$, $\pi(\beta)$ and $\pi(\beta+1)$ are both restricting indices (so $\pi(\beta) \in J$ and $\pi(\beta+1) \in J$). (We may assume that $m \geqslant 4$ and $1 \leqslant \beta \leqslant m-3$, since otherwise the case above applies.) Suppose $x_a = x_{\pi(0)}$, and take β to be the lowest value possible, i.e. pick the adjacent pair which are closest to the path end point $x_{\pi(0)}$ (with minor adjustments the following argument is also seen to be true when x_a is chosen to be $x_{\pi(m-1)}$). There are two cases to consider: first the most general case when $\beta \geqslant 2$, so that after restriction on $x_{\pi(\beta)}$ a non-trivial path is obtained. The case when $\beta = 1$, which results in a trivial path after restriction, is dealt with below. Let $\overline{e}$ denote the 1's complement of the constant e, i.e. $\overline{e} = 1 - e$, and examine the form of the restriction of f by $x_{\pi(\beta)}x_{\pi(\beta+1)} = e\varepsilon$, and f_a by $x_{\pi(\beta)}x_{\pi(\beta+1)} = \overline{e}\varepsilon$, by substituting into equations (5.13):

$$\begin{aligned} f\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon} &= P_1 + L_1 + \frac{q}{2}ex_{\pi(\beta-1)} + \frac{q}{2}e\varepsilon + \frac{q}{2}\varepsilon x_{\pi(\beta+2)} + P_2 + L_2 \\ &\quad + g + g_{\pi(\beta)}e + g_{\pi(\beta+1)}\varepsilon \\ f_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=\overline{e}\varepsilon} &= P_1 + L_1 + \frac{q}{2}(1-e)x_{\pi(\beta-1)} + \frac{q}{2}(1-e)\varepsilon + \frac{q}{2}\varepsilon x_{\pi(\beta+2)} \\ &\quad + P_2 + L_2 + \frac{q}{2}x_{\pi(0)} + g + g_{\pi(\beta)}(1-e) + g_{\pi(\beta+1)}\varepsilon, \end{aligned} \tag{5.14}$$

where

$$\begin{aligned} P_1 &= \frac{q}{2}\sum_{\alpha=0}^{\beta-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} \\ L_1 &= \sum_{\alpha=0}^{\beta-1} g_{\pi(\alpha)}x_{\pi(\alpha)} \\ P_2 &= \frac{q}{2}\sum_{\alpha=\beta+2}^{m-2} x_{\pi(\alpha)}x_{\pi(\alpha+1)} \\ L_2 &= \sum_{\alpha=\beta+2}^{m-1} g_{\pi(\alpha)}x_{\pi(\alpha)}. \end{aligned}$$

Gather together terms in variables indexed by $\beta + 2$ or greater (as F), gather together the constants in each expression, and let $d = 0$ and introduce the term $\frac{q}{2}dx_{\pi(0)} = 0$ into the first expression and write $\frac{q}{2}x_{\pi(0)}$ as $\frac{q}{2}(1-d)x_{\pi(0)}$ in the second, to get

$$\begin{aligned} f\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon} &= P_1 + \frac{q}{2}dx_{\pi(0)} + \frac{q}{2}ex_{\pi(\beta-1)} + F + L_1 + g_1 \\ f_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=\overline{e}\varepsilon} &= P_1 + \frac{q}{2}(1-d)x_{\pi(0)} + \frac{q}{2}(1-e)x_{\pi(\beta-1)} + F + L_1 + g_2, \end{aligned}$$

where

$$\begin{aligned} F &= P_2 + L_2 + \frac{q}{2}\varepsilon x_{\pi(\beta+2)} \\ g_1 &= \frac{q}{2}e\varepsilon + g + g_{\pi(\beta)}e + g_{\pi(\beta+1)}\varepsilon \\ g_2 &= \frac{q}{2}(1-e)\varepsilon + g + g_{\pi(\beta)}(1-e) + g_{\pi(\beta+1)}\varepsilon. \end{aligned}$$

If we put $f'_a(x_0,\ldots,x_{\pi(\beta)},\ldots,x_{m-1}) = f_a(x_0,\ldots,1-x_{\pi(\beta)},\ldots,x_{m-1})$, then we get $f'_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon} = f_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=\bar{e}\varepsilon}$, and it can be seen that, for the given value of d, $f\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon}$ and $f'_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon}$ satisfy the conditions of Theorem 5.6, and thus $f\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=e\varepsilon}$ and $f_a\big|_{x_{\pi(\beta)}x_{\pi(\beta+1)}=\bar{e}\varepsilon}$ have the same auto-correlation function. Furthermore, the theorem also tells us how we may pair the functions if further restrictions are made: if a new restricting variable is not one of the path variables, i.e. is one of the variables in F, then f and f_a both take the same restricting constant in the new pairing; if the new restricting variable is one of the path variables, i.e. in P_1, then the restricting constant in f_a is the 1's complement of that in f. Thus denote all the restricting variables with an index in the path P which is less than or equal to β, by $\mathbf{x}$ (so these variables appear in P_1), and denote all restricting variables with index $\beta+1$ or above by $\mathbf{x}'$ (these all appear in F). Then let $\mathbf{c}$ be a binary word of length compatible with $\mathbf{x}$, $\mathbf{c}'$ similarly for $\mathbf{x}'$, and denote the 1's complement of $\mathbf{c}$ by $\overline{\mathbf{c}}$, i.e. if $\mathbf{c}$ has digits c_α, then $\overline{\mathbf{c}}$ has digits $1-c_\alpha$. Then from the theorem we get that $f\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}$ and $f_a\big|_{\mathbf{x}\mathbf{x}'=\overline{\mathbf{c}}\mathbf{c}'}$ have the same auto-correlation, i.e.

$$A(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})(\ell) = A(\mathbf{F}_a\big|_{\mathbf{x}\mathbf{x}'=\overline{\mathbf{c}}\mathbf{c}'})(\ell) \quad \text{for all } \ell.$$

The last case to consider is that of a pair of adjacent restricting variables when $\beta = 1$. Substituting $\beta = 1$ into equations (5.14) above, and noting that now path P_1 is null, we get

$$\begin{aligned} f\big|_{x_{\pi(1)}x_{\pi(2)}=e\varepsilon} &= L_1 + \frac{q}{2}ex_{\pi(0)} + \frac{q}{2}e\varepsilon + \frac{q}{2}\varepsilon x_{\pi(3)} + P_2 + L_2 \\ &\quad + g + g_{\pi(1)}e + g_{\pi(2)}\varepsilon \\ f_a\big|_{x_{\pi(1)}x_{\pi(2)}=\bar{e}\varepsilon} &= L_1 + \frac{q}{2}(1-e)x_{\pi(0)} + \frac{q}{2}(1-e)\varepsilon + \frac{q}{2}\varepsilon x_{\pi(3)} \\ &\quad + P_2 + L_2 + \frac{q}{2}x_{\pi(0)} + g + g_{\pi(1)}(1-e) + g_{\pi(2)}\varepsilon. \end{aligned}$$

Gathering terms, and noting that $-\frac{q}{2} = \frac{q}{2} \mod q$, q even, these become

$$\begin{aligned} f\big|_{x_{\pi(1)}x_{\pi(2)}=e\varepsilon} &= L_1 + \frac{q}{2}ex_{\pi(0)} + \frac{q}{2}\varepsilon x_{\pi(3)} + P_2 + L_2 \\ &\quad + g + g_{\pi(2)}\varepsilon + g_{\pi(1)}e + \frac{q}{2}e\varepsilon \\ f_a\big|_{x_{\pi(1)}x_{\pi(2)}=\bar{e}\varepsilon} &= L_1 + \frac{q}{2}ex_{\pi(0)} + \frac{q}{2}\varepsilon x_{\pi(3)} + P_2 + L_2 \\ &\quad + g + g_{\pi(2)}\varepsilon + g_{\pi(1)}(1-e) + \frac{q}{2}(1-e)\varepsilon, \end{aligned}$$

which only differ in the constant term, and so by Theorem 1.8 they have the same auto-correlation. In addition, any further restriction can only be on the variables in P_2 (we disallowed restriction on $x_{\pi(0)}$ in this case), and this clearly also gives functions with the same auto-correlation. Thus in this case we also have

$$A(\mathbf{F}\big|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})(\ell) = A(\mathbf{F}_a\big|_{\mathbf{x}\mathbf{x}'=\overline{\mathbf{c}}\mathbf{c}'})(\ell) \quad \text{for all } \ell,$$

but where now $\mathbf{x}$ is just $x_{\pi(1)}$.

So, in all the above cases we have shown that there is a one-to-one correspondence between the auto-correlations of the restrictions of f and f_a, i.e.

$$A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}_i})(\ell) = A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}_j})(\ell)$$

for all ℓ and for some $\mathbf{c}_i$ and $\mathbf{c}_j$. Thus the sum

$$\sum_{\mathbf{c}} \big(A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) + A(\mathbf{F}_a\big|_{\mathbf{x}=\mathbf{c}})(\ell)\big) = 0, \quad \ell \neq 0$$

becomes

$$2\sum_{\mathbf{c}} A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell \neq 0,$$

and hence

$$\sum_{\mathbf{c}} A(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell \neq 0,$$

so that the set of restricted vectors of f form a complementary set. Then by invoking Corollary 5.2 we get that

$$\sum_{\mathbf{c}} A(\widehat{\mathbf{F}}\big|_{\mathbf{x}=\mathbf{c}})(\ell) = 0, \quad \ell \neq 0,$$

as was to be shown. □

Example 5.8. Let $m = 7$ and let f be the generalized Boolean function over $\mathbb{Z}_4$

$$f = 2(x_5x_3 + x_3x_4 + x_4x_2 + x_2x_1 + x_1x_0 + x_0x_6) + x_0 + 3x_5,$$

so that f is a Golay complementary pair with, for example, $f_a = f + 2x_6$. For the restriction, pick two adjacent indices on the path, for instance let $\mathbf{x} = x_2x_4$. Let

$$\bar{Q} = 2(x_5x_3 + x_1x_0 + x_0x_6)$$

be the quadratic part left following any restriction for the given $\mathbf{x}$. Then vectors of the four restricted functions

$$f\big|_{x_2x_4=c_0c_1} = \bar{Q} + 2(c_0x_1 + c_1x_3 + c_0c_1) + x_0 + 3x_5, \quad c_0, c_1 \in \{0,1\},$$

form a complementary set. Map the indices using

$$0 \mapsto 0, 1 \mapsto 1, 3 \mapsto 2, 5 \mapsto 3, 6 \mapsto 4,$$

to get the compressed $\bar{Q}$,

$$\widehat{\bar{Q}} = 2(x_3x_2 + x_1x_0 + x_0x_4),$$

and the compressed functions,

$$\widehat{f}\big|_{x_2x_4=c_0c_1} = \widehat{\bar{Q}} + 2(c_0x_1 + c_1x_2 + c_0c_1) + x_0 + 3x_3 \quad c_0, c_1 \in \{0,1\},$$

the vectors of which also form a complementary set. Each of the vectors in the set thus has a PMEPR$\leqslant 2^{1+1} = 4$. Theorem 1.27 says that words in the coset $\widehat{\bar{Q}} + RM_4(1,5)$ have PMEPR at most $2^{2+1} = 8$, since vertices 2 and 3 need to be deleted in $\widehat{\bar{Q}}$ to leave the path $2(x_1x_0 + x_0x_4)$. Thus, as the example in the previous section, words in the set identified by the theorem have lower PMEPRs than general words in the coset. □

5.5 Pairs of Functions with the same Cross-correlation

A simple modification to the functions in Theorem 5.3 produces two pairs of functions that share the same cross-correlation, but in a non-trivial way:

Corollary 5.9. *With the notation as Theorem 5.3, let four functions be defined as*

$$\begin{aligned} f\big|_{\mathbf{x}=\mathbf{c}} &= P + L + G_1 + g_1 + \frac{q}{2}d_1 \\ f_a\big|_{\mathbf{x}=\mathbf{d}} &= P + \frac{q}{2}x_a + L + G_2 + g_2 + \frac{q}{2}d_2 \\ f_b\big|_{\mathbf{x}=\mathbf{c}} &= P + \frac{q}{2}x_b + L + G_1 + g_1 + \frac{q}{2}d_3 \\ f_{ab}\big|_{\mathbf{x}=\mathbf{d}} &= P + \frac{q}{2}(x_a + x_b) + L + G_2 + g_2 + \frac{q}{2}d_4 \end{aligned}$$

where

$$d_1 + d_2 + d_3 + d_4 = 1 \mod 2.$$

Then the cross-correlations of the pairs are the same at all shifts, i.e.

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_a\big|_{\mathbf{x}=\mathbf{d}})(\ell) - C(\mathbf{F}_b\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_{ab}\big|_{\mathbf{x}=\mathbf{d}})(\ell) = 0, \qquad -(2^m - 1) \leqslant \ell \leqslant 2^m - 1.$$

Proof. By the theorem, if $d_i = 0$ for $i = 1, 2, 3, 4$, then

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_a\big|_{\mathbf{x}=\mathbf{d}})(\ell) = -C(\mathbf{F}_b\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_{ab}\big|_{\mathbf{x}=\mathbf{d}})(\ell) \quad \text{for all } \ell.$$

From Theorem 1.8, setting one of the d_i to 1 introduces an extraneous '$+\frac{q}{2}$' on one side of the corresponding cross-correlation, causing that cross-correlation to be negated. Since an odd number of the d_i are 1, one or other of the cross-correlations will always be negated, so the minus sign in the above equality disappears, giving,

$$C(\mathbf{F}\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_a\big|_{\mathbf{x}=\mathbf{d}})(\ell) = C(\mathbf{F}_b\big|_{\mathbf{x}=\mathbf{c}}, \mathbf{F}_{ab}\big|_{\mathbf{x}=\mathbf{d}})(\ell),$$

for all ℓ, and in particular for $-(2^m - 1) \leqslant \ell \leqslant 2^m - 1$. □

Example 5.10. Consider a simple unrestricted binary case for $m = 7$, and take the following two pairs of functions:

$$\begin{aligned} f &= x_0x_1 + x_1x_2 + x_1 + x_3x_4x_6 + x_3x_5 \\ f_a &= x_0x_1 + x_1x_2 + x_2 + x_1 + x_4x_5x_6 + x_5x_6 + 1 \\ f_b &= x_0x_1 + x_1x_2 + x_0 + x_1 + x_3x_4x_6 + x_3x_5 \\ f_{ab} &= x_0x_1 + x_1x_2 + x_2 + x_0 + x_1 + x_4x_5x_6 + x_5x_6 \end{aligned}$$

where $x_a = x_2$ and $x_b = x_0$. Straightforward computation shows that $C(\mathbf{F}, \mathbf{F}_a)(\ell) = C(\mathbf{F}_b, \mathbf{F}_{ab})(\ell)$. Note that the cross-correlation $C(\overline{\mathbf{F}_a}, \overline{\mathbf{F}})(\ell)$, obtained by simply reversing and swapping the vectors of f and f_a, is the same as $C(\mathbf{F}, \mathbf{F}_a)(\ell)$ by Theorem 1.1, but the equivalent functions are now considerably more complicated (due to the fact that the 'non-path' functions G_1 and G_2 also get reversed):

$$\begin{aligned}\overline{f_a} &= x_0x_1 + x_1x_2 + x_0 + x_1 + x_4x_5x_6 + x_4x_5 + x_4x_6 + x_4 + 1\\ \overline{f} &= x_0x_1 + x_1x_2 + x_2 + x_0 + x_1 + x_3x_4x_6 + x_3x_4 + x_3x_5\\ &\qquad + x_3x_6 + x_4x_6 + x_4 + x_5 + x_6 + 1.\end{aligned}$$

□

5.6 Conclusions

In this chapter it has been shown that 'splitting up' a pair of complementary sequences (constructed by Corollary 1.25) into a number of shorter sequences results in complementary sets of sequences. Under certain circumstances, doing this to just a single sequence of a pair also results in a complementary set. In showing why this works, much use has again been made of the inherent structure of the path functions that are at the root of the construction of the complementary pair. It is not known how these sets may be related to those of [46, 47, 40], but since the sets in the latter are generally constructed by iteratively interleaving shorter sequences to make longer ones, it seems likely that there may be a connection, since the restriction and compression techniques used here can be seen in some respects to be just the reverse of such a process. It would be an interesting exercise to investigate if there is a connection, for even if there is one, the description and construction given here could possibly be simpler and more concise.

Chapter 6

Binary Golay Sequences under the Inverse Gray Map

6.1 Chapter Overview

The main result of this chapter is to show that a binary Golay sequence (emanating from the construction of Corollary 1.25) remains a complementary sequence when mapped to $\mathbb{Z}_4$ under the inverse Gray map (Section 6.4). The subset of all complementary sequences over $\mathbb{Z}_4$ (from the construction) which are the images of a binary complementary sequence is also identified. Section 6.2 defines the Gray map, its inverse, and some of their properties; their effects on the algebraic normal form representations of generalized Boolean and Boolean functions, over $\mathbb{Z}_4$ and $\mathbb{Z}_2$ respectively, are deduced in Section 6.3. A few conclusions are drawn in the final Section, 6.5.

6.2 Introduction

The *Gray map* is a mapping from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$, is usually denoted by ϕ, and is defined as:

$$\begin{aligned} \phi : \mathbb{Z}_4 &\to \mathbb{Z}_2^2 \\ 0 &\mapsto 00 \\ 1 &\mapsto 01 \\ 2 &\mapsto 11 \\ 3 &\mapsto 10, \end{aligned}$$

and is clearly a bijection. It finds utility in a variety of situations where a connection between quaternary and binary objects is desirable (e.g. within communications and, more recently, coding theory [20, 48]). (Much of the initial material in this section is taken from [48, Ch. 3].)

It is useful to define the following three maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$:

$\mathbb{Z}_4$	α	β	γ
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

The maps α and β give the binary expansion of any element of $\mathbb{Z}_4$, i.e. for each $x \in \mathbb{Z}_4$,

$$x = \alpha(x) + 2\beta(x) \tag{6.1}$$

(this is normally called the '2-adic expansion' of x). Note also that

$$\alpha(x) + \beta(x) + \gamma(x) = 0 \text{ for all } x \in \mathbb{Z}_4. \tag{6.2}$$

The Gray map ϕ can then be expressed in terms of β and γ as:

$$\begin{aligned} \phi(x) &= \big(\beta(x), \gamma(x)\big) \text{ for all } x \in \mathbb{Z}_4 \\ &\big(\equiv \big(\beta(x), \beta(x) + \alpha(x)\big)\big). \end{aligned}$$

The maps α, β, γ and ϕ can be extended to operate on vectors in an obvious way, as is shown below. We are interested in cases when the vector over $\mathbb{Z}_4$ is that associated with a generalized Boolean function. It is seen that under the action of the Gray map, the length of the resulting vector over $\mathbb{Z}_2$ is twice that of the original vector over $\mathbb{Z}_4$, and thus the number of variables representing the associated Boolean function of the image vector is one more than the number of variables of the generalized Boolean function over $\mathbb{Z}_4$. We shall use $n' = 2^{m'}$ as the length of a vector over $\mathbb{Z}_4$ from the associated function in m' variables, and $n = 2^m$ as the length of the resulting vector over $\mathbb{Z}_2$ from the associated function in m variables, where $n = 2n'$ and $m = m' + 1$.

Letting $\mathbf{a}$ be a vector over $\mathbb{Z}_4$, i.e. $\mathbf{a} = (a_0, a_1, \ldots, a_{n'-1}) \in \mathbb{Z}_4^{n'}$, we can extend the maps α, β, γ to $\mathbb{Z}_4^{n'}$ by defining

$$\begin{aligned} \alpha(\mathbf{a}) &= \big(\alpha(a_0), \alpha(a_1) \ldots, \alpha(a_{n'-1})\big) \\ \beta(\mathbf{a}) &= \big(\beta(a_0), \beta(a_1) \ldots, \beta(a_{n'-1})\big) \\ \gamma(\mathbf{a}) &= \big(\gamma(a_0), \gamma(a_1) \ldots, \gamma(a_{n'-1})\big), \end{aligned}$$

and then extend ϕ as

$$\phi(\mathbf{a}) = \big((\beta(\mathbf{a}), \gamma(\mathbf{a})\big) \text{ for all } \mathbf{a} \in \mathbb{Z}_4^{n'}, \tag{6.3}$$

and this extended ϕ is also a bijection, from $\mathbb{Z}_4^{n'}$ to $\mathbb{Z}_2^{n}$ (where $n = 2n'$).

Since the Gray map is a bijection, it has as inverse the *inverse Gray map*, $\phi^{-1}(x, y)$, from $\mathbb{Z}_2^2$ to $\mathbb{Z}_4$. From the definition of ϕ, and (6.1) and (6.2), it can be seen that ϕ^{-1} is given by

$$\phi^{-1}(x, y) = (x + y \mod 2) + 2x. \tag{6.4}$$

For n even, and now letting $\mathbf{a}$ be over $\mathbb{Z}_2$, i.e. $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}_2^n$, and denoting the left and right halves of the vector $\mathbf{a}$ as

$$\begin{aligned} \mathbf{a}_L &= (a_0, \ldots, a_{n/2-1}) \\ \mathbf{a}_R &= (a_{n/2}, \ldots, a_{n-1}), \end{aligned}$$

the extension of ϕ^{-1} to a map from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4^{n'}$ $(n' = \frac{n}{2})$, i.e. the inverse of (6.3), is:

$$\begin{aligned} \phi^{-1}(\mathbf{a}) &= \big(\phi^{-1}(a_0, a_{n/2}), \phi^{-1}(a_1, a_{n/2+1}), \ldots, \phi^{-1}(a_{n/2-1}, a_{n-1})\big) \\ &= \big((a_0 + a_{n/2} \mod 2) + 2a_0, (a_1 + a_{n/2+1} \mod 2) + 2a_1, \cdots, \\ &\qquad\qquad (a_{n/2-1} + a_{n-1} \mod 2) + 2a_{n/2-1}\big) \\ &= (\mathbf{a}_L + \mathbf{a}_R \mod 2) + 2\mathbf{a}_L. \end{aligned} \tag{6.5}$$

Only the map α is actually an additive group homomorphism: β and γ, and hence ϕ, are not. The following lemma shows what the image of the sum of two vectors under the Gray map is in terms of their individual images and the map α. Denoting the componentwise multiplication of two vectors $\mathbf{a}$ and $\mathbf{b}$ by

$$(a_0, \ldots, a_{n'-1}) * (b_0, \ldots, b_{n'-1}) = (a_0 b_0, \ldots, a_{n'-1} b_{n'-1}),$$

then we have

Lemma 6.1. *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_4^{n'}$,

$$\phi(\mathbf{a} + \mathbf{b}) = \phi(\mathbf{a}) + \phi(\mathbf{b}) + \phi\big(2\alpha(\mathbf{a}) * \alpha(\mathbf{b})\big),$$

where the product $2\alpha(\mathbf{a}) * \alpha(\mathbf{b})$ *is taken in* $\mathbb{Z}_4$.

Proof. It suffices to show that the left and right hand sides of the identity are the same for all combinations of input values when $n' = 1$. The following truth table shows this for all distinct pairings of the input values:

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{a}+\mathbf{b}$	LHS	$\phi(\mathbf{a})$	$\phi(\mathbf{b})$	$\phi(2\alpha(\mathbf{a}) * \alpha(\mathbf{b}))$	RHS
0	0	0	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
0	1	1	(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
0	2	2	(1,1)	(0,0)	(1,1)	(0,0)	(1,1)
0	3	3	(1,0)	(0,0)	(1,0)	(0,0)	(1,0)
1	1	2	(1,1)	(0,1)	(0,1)	(1,1)	(1,1)
1	2	3	(1,0)	(0,1)	(1,1)	(0,0)	(1,0)
1	3	0	(0,0)	(0,1)	(1,0)	(1,1)	(0,0)
2	2	0	(0,0)	(1,1)	(1,1)	(0,0)	(0,0)
2	3	1	(0,1)	(1,1)	(1,0)	(0,0)	(0,1)
3	3	2	(1,1)	(1,0)	(1,0)	(1,1)	(1,1)

(Note that in [48] this is deduced as a corollary to some other results, but for completeness is proved directly here.) □

In the current setting we are also interested in the equivalent result for ϕ^{-1}, and this is given in the following lemma.

Lemma 6.2. *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$*, n even,*

$$\phi^{-1}(\mathbf{a}+\mathbf{b}) = \phi^{-1}(\mathbf{a}) + \phi^{-1}(\mathbf{b}) + 2\big((\mathbf{a}_L + \mathbf{a}_R) * (\mathbf{b}_L + \mathbf{b}_R)\big)$$

where the additions $\mathbf{a}_L + \mathbf{a}_R$ *and* $\mathbf{b}_L + \mathbf{b}_R$ *are performed* mod 2.

Proof. It suffices to show that the left and right hand sides of the identity are the same for all combinations of input values when $n = 2$. The following truth table shows this for all distinct pairings of the input values:

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{a}+\mathbf{b}$	LHS	$\phi^{-1}(\mathbf{a})$	$\phi^{-1}(\mathbf{b})$	$2((\cdot) * (\cdot))$	RHS
$(0,0)$	$(0,0)$	$(0,0)$	0	0	0	0	0
$(0,1)$	$(0,0)$	$(0,1)$	1	1	0	0	1
$(0,1)$	$(0,1)$	$(0,0)$	0	1	1	2	0
$(1,1)$	$(0,0)$	$(1,1)$	2	2	0	0	2
$(1,1)$	$(0,1)$	$(1,0)$	3	2	1	0	3
$(1,1)$	$(1,1)$	$(0,0)$	0	2	2	0	0
$(1,0)$	$(0,0)$	$(1,0)$	3	3	0	0	3
$(1,0)$	$(0,1)$	$(1,1)$	2	3	1	2	2
$(1,0)$	$(1,1)$	$(0,1)$	1	3	2	0	1
$(1,0)$	$(1,0)$	$(0,0)$	0	3	3	2	0

□

6.3 The Effect of the Gray Map and Its Inverse on Algebraic Normal Form

In the next section we require the effect of the inverse Gray map on a Boolean function which is a path: thus in this section the action of the inverse Gray map on the algebraic normal form of a Boolean function is established. It is also useful to know the effect of the Gray map on a generalized Boolean function over $\mathbb{Z}_4$, so both these cases are now considered in turn.

6.3.1 The inverse Gray map and algebraic normal form

Let $f = f(x_0, \dots, x_{m-1})$ be a Boolean function, in algebraic normal form, of the m variables $x_0, \dots, x_{m-1}$, and let $\mathbf{f} = (f_0, f_1, \dots, f_{2^m-1})$ be the associated vector of all its values, with $f_i = f(i_0, i_1, \dots, i_{m-1})$ where $(i_0, i_1, \dots, i_{m-1})$ is the binary expansion of $i = 0, 1, \dots, 2^m - 1$. From (6.4) we can take the inverse Gray map of the pairing $f_i, f_{i+n/2}$ as

$$\phi^{-1}(f_i, f_{i+n/2}) = (f_i + f_{i+n/2} \mod 2) + 2f_i \tag{6.6}$$

for $i = 0, 1, \dots, n/2-1$. The values f_i, $i = 0, 1, \dots, n/2-1$, may be obtained from the algebraic normal form of f by setting $x_{m-1} = 0$ and evaluating the resulting function over all 2^{m-1} combinations of the remaining $m' = m-1$ variables. Similarly the values $f_{i+n/2}$, $i = 0, 1, \dots, n/2-1$, may be obtained by setting $x_{m-1} = 1$ in f and evaluating over the same combinations of the remaining variables. But these values are none other than those of the compressed functions of f following its restriction by $x_{m-1} = 0$ and $x_{m-1} = 1$ respectively, as defined in Section 1.9.5. Thus using the notation established in that section, viz $\widehat{f}\big|_{\mathbf{x}=\mathbf{c}}$, we can extend the notion of the inverse Gray map acting on pairs of elements and vectors over $\mathbb{Z}_2$ to that of acting directly on the algebraic normal form of a function f, and thus equation (6.6) becomes

$$\phi^{-1}(f) = \big(\widehat{f}\big|_{x_{m-1}=0} + \widehat{f}\big|_{x_{m-1}=1} \mod 2\big) + 2\widehat{f}\big|_{x_{m-1}=0},$$

which is readily seen to be the functional analogue of equation (6.5) since

$$\begin{aligned}\mathbf{f}_L &\equiv \widehat{\mathbf{f}}\big|_{x_{m-1}=0}\\ \mathbf{f}_R &\equiv \widehat{\mathbf{f}}\big|_{x_{m-1}=1}.\end{aligned}$$

In fact since in this case the relabelling of indices in the compression operation '$\widehat{\ }$' after the restriction on x_{m-1} is always just an 'identity' operation, it is rather superfluous, and so is dropped on the understanding that functions so obtained are implicitly just functions in the $m-1$ variables $x_0, \ldots, x_{m-2}$. The above is then

$$\phi^{-1}(f) = \big(f\big|_{x_{m-1}=0} + f\big|_{x_{m-1}=1} \mod 2\big) + 2f\big|_{x_{m-1}=0}.$$

Note that since the algebraic normal form of a function over $\mathbb{Z}_4$ is implicitly taken mod 4, and in general for $a, b \in \{0,1\}$, $a+b \mod 2 \neq a+b \mod 4$, the right-hand side of this expression is not very helpful in establishing the algebraic normal form of a function over $\mathbb{Z}_4$. However, in the case when a function, h say, is just a monomial, simple expressions for the algebraic normal form of $\phi^{-1}(h)$ in terms of h can be established: if h is a monomial not containing x_{m-1}, i.e.

$$h(x_0, \ldots, x_{m-1}) = x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}},$$

where $i_k = 0$ or 1, $k = 0, 1, \ldots m-2$, then we get

$$\begin{aligned}\phi^{-1}(h) &= \phi^{-1}\big(x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\big)\\ &= \big(x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\big|_{x_{m-1}=0} + x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\big|_{x_{m-1}=1} \mod 2\big)\\ &\qquad + 2x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\big|_{x_{m-1}=0}\\ &= \big(x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}} + x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}} \mod 2\big) + 2x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\\ &= 2x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}}\\ &= 2\big(h\big|_{x_{m-1}=0}\big)\\ &= 2h,\end{aligned}$$

again on the understanding that we are now regarding the monomial as just a function of the $m-1$ variables $x_0, \ldots, x_{m-2}$.

If h does contain x_{m-1}, i.e.

$$h(x_0, \ldots, x_{m-1}) = x_0^{i_0} \cdots x_{m-2}^{i_{m-2}} x_{m-1},$$

we get

$$\begin{aligned}
\phi^{-1}(h) &= \phi^{-1}\big(x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}x_{m-1}\big)\\
&= \big(x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}x_{m-1}\big|_{x_{m-1}=0} + x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}x_{m-1}\big|_{x_{m-1}=1} \mod 2\big)\\
&\qquad + 2x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}x_{m-1}\big|_{x_{m-1}=0}\\
&= \big(0 + x_0^{i_0}\cdots x_{m-2}^{i_{m-2}} \mod 2\big) + 0\\
&= x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\\
&= h\big|_{x_{m-1}=1}
\end{aligned}$$

where now since $h\big|_{x_{m-1}=1}$ is just 0 or 1, the expression $\big(h\big|_{x_{m-1}=1} \mod 2\big)$ *does* equal $\big(h\big|_{x_{m-1}=1} \mod 4\big)$.

For example with $m = 4$, $\phi^{-1}(x_0x_2) = 2x_0x_2$, which is easily verified directly from the operations on the vectors, for

$$\mathbf{x}_0 * \mathbf{x}_2 = (0000010100000101),$$

which when paired as (6.5) gives

$$\begin{aligned}
\phi^{-1}(\mathbf{x}_0 * \mathbf{x}_2) &= \phi^{-1}\big((0,0),(0,0),(0,0),(0,0),(0,0),(1,1),(0,0),(1,1)\big)\\
&= (00000202)\\
&= 2\mathbf{x}_0 * \mathbf{x}_2.
\end{aligned}$$

Using similar reasoning we can form the algebraic normal form equivalent of Lemma 6.2 for the functions f and g:

$$\begin{aligned}
\phi^{-1}(f+g) = \phi^{-1}(f) + \phi^{-1}(g) + 2\big((f\big|_{x_{m-1}=0} + f\big|_{x_{m-1}=1} &\mod 2)\\
\times (g\big|_{x_{m-1}=0} + g\big|_{x_{m-1}=1} &\mod 2)\big).
\end{aligned}$$

It is easy to verify that for $a, b, c, d \in \{0, 1\}$,

$$2(a+b \mod 2)(c+d \mod 2) = 2(a+b)(c+d) \mod 4,$$

and so in this case it is possible to drop the 'mod 2's from the expression and obtain a valid expression for algebraic normal form over $\mathbb{Z}_4$, and so this, with the above results for monomials, can be used to deduce the most general case.

When f does not involve x_{m-1}, then $f\big|_{x_{m-1}=0} = f\big|_{x_{m-1}=1}$, and so if either f or g does not involve x_{m-1} then the last term is identically zero, giving in this case

$$\phi^{-1}(f+g) = \phi^{-1}(f) + \phi^{-1}(g). \tag{6.7}$$

Thus for an f consisting entirely of monomials not dependent on x_{m-1}, repeated application of this and the above rules clearly gives

$$\phi^{-1}(f) = 2f,$$

where once again the right-hand side is now considered to be over $\mathbb{Z}_4$ and only in the $m-1$ variables $x_0, x_1, \ldots, x_{m-2}$. Repeated application of these rules also leads to the most general case, when f consists of a mixture of monomials that include and exclude the variable x_{m-1}:

Theorem 6.3. *Let f be a Boolean function in the m variables $x_0, \ldots, x_{m-1}$. Partition the algebraic normal form of f into those monomials involving x_{m-1} and those not, i.e. if $(i_0, i_1, \ldots, i_{m-1})$ is the binary expansion of integer i, let set I_0 be the set of those indices i for which $i_{m-1} = 0$ and for which monomial $x_0^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}$ has a non-zero coefficient in the algebraic normal form of f, and similarly let set I_1 be those indices for which $i_{m-1} = 1$ and the corresponding monomial has non-zero coefficient, so write*

$$\begin{aligned} f &= f^0 + f^1 \\ &= \sum_{i \in I_0} x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}} + \sum_{i \in I_1} x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}} x_{m-1}. \end{aligned}$$

Then the algebraic normal form (over $\mathbb{Z}_4$) of the image of f under the inverse Gray map is

$$\begin{aligned} \phi^{-1}(f) &= 2f^0\big|_{x_{m-1}=0} + \left(f^1\big|_{x_{m-1}=1}\right)^2 \\ &= 2f^0 + \left(f^1\big|_{x_{m-1}=1}\right)^2. \end{aligned}$$

Proof. First note that since each x_i takes just the values 0 or 1, then $x_i = (x_i)^2$ for all i. Now use induction on the number of terms in f involving x_{m-1}, i.e. on $|I_1|$. First suppose that I_1 contains only one index, i.e $|I_1| = 1$. Then

$$\begin{aligned} \phi^{-1}(f) &= \phi^{-1}(f^0 + f^1) \\ &= \phi^{-1}(f^0) + \phi^{-1}(f^1) \\ &\qquad + 2\left(f^0\big|_{x_{m-1}=0} + f^0\big|_{x_{m-1}=1}\right)\left(f^1\big|_{x_{m-1}=0} + f^1\big|_{x_{m-1}=1}\right) \\ &= 2f^0 + f^1\big|_{x_{m-1}=1} \\ &= 2f^0 + \left(f^1\big|_{x_{m-1}=1}\right)^2, \end{aligned}$$

by the results preceding the theorem for f^0 and the monomial f^1, and since $f^0\big|_{x_{m-1}=0} = f^0\big|_{x_{m-1}=1}$. Now suppose the result is true when the cardinality of I_1 is k for some integer $k > 1$, and consider the case $|I_1| = k+1$. Split one index $i' \in I_1$ away from the rest, i.e. write

$$\begin{aligned} f &= f^0 + f^1 \\ &= f^0 + \sum_{\substack{i \in I_1 \\ i \neq i'}} x_0^{i_0} x_1^{i_1} \cdots x_{m-2}^{i_{m-2}} x_{m-1} + x_0^{i'_0} x_1^{i'_1} \cdots x_{m-2}^{i'_{m-2}} x_{m-1} \\ &= f^0 + f^{1''} + f^{1'}, \text{ say,} \end{aligned}$$

where $f^{1''}$ contains k terms. Then

$$\begin{aligned} \phi^{-1}(f) &= \phi^{-1}(f^0 + f^{1''} + f^{1'}) \\ &= \phi^{-1}(f^0 + f^{1''}) + \phi^{-1}(f^{1'}) \\ &\qquad +2\left((f^0 + f^{1''})\big|_{x_{m-1}=0} + (f^0 + f^{1''})\big|_{x_{m-1}=1}\right) \\ &\qquad\qquad \times\left(f^{1'}\big|_{x_{m-1}=0} + f^{1'}\big|_{x_{m-1}=1}\right) \\ &= 2f^0 + \left(f^{1''}\big|_{x_{m-1}=1}\right)^2 + f^{1'}\big|_{x_{m-1}=1} + 2\left(f^{1''}\big|_{x_{m-1}=1}\right)\left(f^{1'}\big|_{x_{m-1}=1}\right) \end{aligned}$$

(using the induction hypothesis)

$$
\begin{aligned}
&= 2f^0 + \Big(\sum_{\substack{i\in I_1\\ i\neq i'}} x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\Big)^2 + x_0^{i'_0}\cdots x_{m-2}^{i'_{m-2}}\\
&\quad + 2\Big(\sum_{\substack{i\in I_1\\ i\neq i'}} x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\Big)\Big(x_0^{i'_0}\cdots x_{m-2}^{i'_{m-2}}\Big)\\
&= 2f^0 + \Big(\sum_{\substack{i\in I_1\\ i\neq i'}} \big(x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\big)^2 + 2\sum_{\substack{i\neq j\in I_1\\ i,j\neq i'}} x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\cdot x_0^{j_0}\cdots x_{m-2}^{j_{m-2}}\Big)\\
&\quad + \big(x_0^{i'_0}\cdots x_{m-2}^{i'_{m-2}}\big)^2 + 2\Big(\sum_{\substack{i\in I_1\\ i\neq i'}} x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\Big)\Big(x_0^{i'_0}\cdots x_{m-2}^{i'_{m-2}}\Big)\\
&= 2f^0 + \Big(\sum_{i\in I_1} \big(x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\big)^2 + 2\sum_{i\neq j\in I_1} x_0^{i_0}\cdots x_{m-2}^{i_{m-2}}\cdot x_0^{j_0}\cdots x_{m-2}^{j_{m-2}}\Big)\\
&= 2f^0 + \big(f^1\big|_{x_{m-1}=1}\big)^2,
\end{aligned}
$$

which is the result for $k+1$, and hence by induction the result is true for all integers $k \geqslant 1$. □

Example 6.4. Let $m = 4$ and take the function

$$f(x) = x_0 + x_1x_2 + x_2x_3 + x_0x_2x_3.$$

Then the algebraic normal form of the image of f under the inverse Gray map is, by the theorem

$$
\begin{aligned}
f'(x) = \phi^{-1}(f(x)) &= \phi^{-1}\big((x_0 + x_1x_2) + (x_2x_3 + x_0x_2x_3)\big)\\
&= 2(x_0 + x_1x_2) + \big((x_2x_3 + x_0x_2x_3)\big|_{x_3=1}\big)^2\\
&= 2x_0 + 2x_1x_2 + (x_2 + x_0x_2)^2\\
&= 2x_0 + 2x_1x_2 + (x_2)^2 + 2x_2\cdot x_0x_2 + (x_0x_2)^2\\
&= 2x_0 + 2x_1x_2 + x_2 + 2x_0x_2 + x_0x_2\\
&= 2x_0 + 2x_1x_2 + x_2 + 3x_0x_2.
\end{aligned}
$$

Evaluate f at all its points by adding the equivalent vectors:

$$
\begin{aligned}
\mathbf{x}_0 &= (0101010101010101)\\
\mathbf{x}_1 * \mathbf{x}_2 &= (0000001100000011)\\
\mathbf{x}_2 * \mathbf{x}_3 &= (0000000000001111)\\
\mathbf{x}_0 * \mathbf{x}_2 * \mathbf{x}_3 &= (0000000000000101)\\
\mathbf{f} = \ \text{sum mod } 2 &= (0101011001011100),
\end{aligned}
$$

which pairing as (6.5) and applying ϕ^{-1} gives

$$\phi^{-1}\big((0,0),(1,1),(0,0),(1,1),(0,1),(1,1),(1,0),(0,0)\big) = (02021230).$$

Further, direct calculation from f', via the equivalent vectors, gives

$$\begin{aligned} 2\mathbf{x}_0 &= (02020202)\\ 2\mathbf{x}_1 * \mathbf{x}_2 &= (00000022)\\ \mathbf{x}_2 &= (00001111)\\ 3\mathbf{x}_0 * \mathbf{x}_2 &= (00000303)\\ \mathbf{f}' = \text{ sum mod } 4 &= (02021230), \end{aligned}$$

this being in agreement with the previous vector, thus confirming that the derivation of the algebraic normal form is correct. □

6.3.2 The Gray map and algebraic normal form

Let $f = f(x_0, \dots, x_{m'-1})$ be a generalized Boolean function over $\mathbb{Z}_4$, and in algebraic normal form, of the $m' = m - 1$ variables $x_0, \dots, x_{m'-1}$, and let $\mathbf{f}$ be the associated vector of all its values. From (6.3), the image of the Gray map of $\mathbf{f}$ is

$$\phi(\mathbf{f}) = (\beta(\mathbf{f}), \gamma(\mathbf{f})),$$

which will be viewed as a $2^{m'+1} = 2^m$ dimensional vector over $\mathbb{Z}_2$. We require the algebraic normal form, over $\mathbb{Z}_2$, of the Boolean function f' associated with this vector, in terms of the original function f over $\mathbb{Z}_4$. Since the vector is of length $2^{m'+1} = 2^m$, the function f' will necessarily be of $m = m' + 1$ variables, so we expect any algebraic normal form over $\mathbb{Z}_2$ to involve the variable x_{m-1}, in addition to those used over $\mathbb{Z}_4$. Extend the notation for β and γ so that $\beta(f)$ and $\gamma(f)$ are the algebraic normal forms, over $\mathbb{Z}_2$, of the vectors $\beta(\mathbf{f})$ and $\gamma(\mathbf{f})$ respectively. Then examination of the vector $(\beta(\mathbf{f}), \gamma(\mathbf{f}))$ shows that the function f' must give the values $\beta(\mathbf{f})$ when $x_{m-1} = 0$, and the values $\gamma(\mathbf{f})$ when $x_{m-1} = 1$, and thus f' is given by

$$f' = \beta(f)(1 + x_{m-1}) + \gamma(f)x_{m-1}. \qquad (6.8)$$

The relationships between the algebraic normal forms for $\beta(f)$ and $\gamma(f)$ over $\mathbb{Z}_2$ and that for f over $\mathbb{Z}_4$ are simple enough to establish when f is merely a monomial, but unfortunately, since neither β nor γ are homomorphisms, the relationship for the general case is less straightforward.

So let $h(x_0, \dots, x_{m'-1}) = x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}}$ and consider the monomial $c{\cdot}h$, $c \in \mathbb{Z}_4$, as a typical term in the algebraic normal form of f. Then since h only takes the values 0 and 1, from the definitions of the maps α, β and γ, it is clear that

$$\begin{aligned} \alpha(c \cdot h) &= \alpha(c)h\\ \beta(c \cdot h) &= \beta(c)h \qquad (6.9)\\ \gamma(c \cdot h) &= \gamma(c)h. \end{aligned}$$

Substituting into equation (6.8) and evaluating for all values of c gives:

$$\begin{aligned}
\phi(c\cdot h) &= \beta(c\cdot h)(1+x_{m-1})+\gamma(c\cdot h)x_{m-1}\\
&= \beta(c)h(1+x_{m-1})+\gamma(c)h\cdot x_{m-1}.\\
\phi(0\cdot h) &= \beta(0)h(1+x_{m-1})+\gamma(0)h\cdot x_{m-1}\\
&= 0\cdot h(1+x_{m-1})+0\cdot h\cdot x_{m-1}=0\\
\phi(h) &= \beta(1)h(1+x_{m-1})+\gamma(1)h\cdot x_{m-1}\\
&= 0\cdot h(1+x_{m-1})+1\cdot h\cdot x_{m-1}=h\cdot x_{m-1}\\
\phi(2h) &= \beta(2)h(1+x_{m-1})+\gamma(2)h\cdot x_{m-1}\\
&= 1\cdot h(1+x_{m-1})+1\cdot h\cdot x_{m-1}=h\\
\phi(3h) &= \beta(3)h(1+x_{m-1})+\gamma(3)h\cdot x_{m-1}\\
&= 1\cdot h(1+x_{m-1})+0\cdot h\cdot x_{m-1}=h(1+x_{m-1}).
\end{aligned}$$

In summary, the algebraic normal form of the images of the monomials $c\cdot h$ under the Gray map, where $c\in\mathbb{Z}_4$ and $h=x_0^{i_0}x_1^{i_1}\cdots x_{m'-1}^{i_{m'-1}}$, are

$$\begin{aligned}
\phi(0) &= 0\\
\phi(h) &= h\cdot x_{m-1}\\
\phi(2h) &= h\\
\phi(3h) &= h(1+x_{m-1}).
\end{aligned}$$

For example, for $m'=3$ and with $c=3$ and $h=1$, $\phi(3)=1+x_{m-1}$ (note the '3' here represents a function in algebraic normal form, and not just the constant 3!). This is easily verified from the vectors, for

$$\begin{aligned}
\phi(3)\equiv\phi(\mathbf{3}) &= \phi(3,3,3,3,3,3,3,3)\\
&= \big(\beta(3,3,3,3,3,3,3,3),\gamma(3,3,3,3,3,3,3,3)\big)\\
&= (1111111100000000)\\
&= \mathbf{1}+\mathbf{x}_{m-1}.
\end{aligned}$$

The functional equivalent of Lemma 6.1 is then

$$\phi(f+g)=\phi(f)+\phi(g)+\phi\big(2\alpha(f)\alpha(g)\big),$$

where the product $2\alpha(f)\alpha(g)$ is over $\mathbb{Z}_4$. If either f or g consists entirely of monomials having coefficient 2, so its values are all either 0 or 2, then since $\alpha(0)=\alpha(2)=0$, then the last term is identically zero, giving in this case

$$\phi(f+g)=\phi(f)+\phi(g).$$

Thus for an f consisting entirely of monomials with coefficient 2, repeated application of this and the above rules clearly gives

$$\phi(f)=f,$$

but where now the right-hand side is regarded as a function in $m=m'+1$ variables (cf equation (6.7) in the previous section). Repeated application of all these rules then gives the most general case when f consists of monomials with all possible coefficients:

Theorem 6.5. *Let f be a generalized Boolean function over $\mathbb{Z}_4$ in the m' variables $x_0, \ldots, x_{m'-1}$. Partition the algebraic normal form of f into monomials with coefficients $1, 2$ or 3, i.e. if $(i_0, i_1, \ldots, i_{m'-1})$ is the binary expansion of integer i, let set I_1 be the set of those indices i for which the monomials $x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}}$ have the coefficient 1, let I_2 be the set of indices for which the corresponding monomials have coefficient 2, and I_3 for monomials with coefficient 3, so write*

$$\begin{aligned} f &= 2 \cdot f^2 + 1 \cdot f^1 + 3 \cdot f^3 \\ &= 2 \sum_{i \in I_2} x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}} + \sum_{i \in I_1} x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}} + 3 \sum_{i \in I_3} x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}} \end{aligned}$$

(and noting that the superscripts on f are not powers). Representing the monomial $x_0^{i_0} x_1^{i_1} \cdots x_{m'-1}^{i_{m'-1}}$ by x^i, then the algebraic normal form (over $\mathbb{Z}_2$) of the image of f under the Gray map is

$$\phi(f) = f^2 + f^1 \cdot x_{m-1} + f^3(1 + x_{m-1}) + \sum_{\substack{i,j \in I_1 \cup I_3 \\ i \neq j}} x^i \cdot x^j.$$

Proof. Use induction on the number of monomials with coefficient either 1 or 3, i.e. on $|I_1 \cup I_3|$. First suppose that there is just a single monomial with coefficient 1, i.e. that f^1 consists of a single monomial, and that f^3 is identically zero (the argument will work equally well if the roles of f^1 and f^3 are reversed). Then

$$\begin{aligned} \phi(f) &= \phi(2f^2 + f^1 + 3f^3) = \phi(2f^2 + f^1) \\ &= \phi(2f^2) + \phi(f^1) + \phi\big(2\alpha(2f^2)\alpha(f^1)\big) \\ &= f^2 + f^1 \cdot x_{m-1} \\ &= f^2 + f^1 \cdot x_{m-1} + 0 + 0 \\ &= f^2 + f^1 \cdot x_{m-1} + f^3(1 + x_{m-1}) + \sum_{\substack{i,j \in I_1 \cup I_3 \\ i \neq j}} x^i \cdot x^j. \end{aligned}$$

using the statements and rules preceding the theorem, and that f^3 is zero and the sum is necessarily empty when $|I_1 \cup I_3| = 1$. Now suppose that the result is true when the cardinality of $I_1 \cup I_3$ is k for some integer $k > 1$, and consider the case $|I_1 \cup I_3| = k + 1$. Split one index $i' \in I_1$ away from the rest, i.e. write

$$\begin{aligned} f &= 2f^2 + f^1 + 3f^3 \\ &= 2f^2 + \sum_{\substack{i \in I_1 \\ i \neq i'}} x^i + x^{i'} + 3f^3 \\ &= 2f^2 + f^{1''} + f^{1'} + 3f^3, \text{ say,} \end{aligned}$$

so ${f^1}'' + 3f^3$ contain a total of k terms. Then

$$\begin{aligned}\phi(f) &= \phi(2f^2 + {f^1}'' + {f^1}' + 3f^3)\\ &= \phi(2f^2 + {f^1}'' + 3f^3) + \phi({f^1}') + \phi\big(2\alpha(2f^2 + {f^1}'' + 3f^3)\alpha({f^1}')\big)\\ &= f^2 + {f^1}'' \cdot x_{m-1} + f^3(1 + x_{m-1}) + \sum_{\substack{i,j \in I_1 \cup I_3\\ i,j \neq i'\\ i \neq j}} x^i \cdot x^j\\ &\qquad + {f^1}' \cdot x_{m-1} + \phi\big(2\alpha(2f^2 + {f^1}'' + 3f^3)\alpha({f^1}')\big)\end{aligned}$$

by the induction hypothesis, and we now need to consider the last term in this expression, the term $\phi\big(2\alpha(2f^2 + {f^1}'' + 3f^3)\alpha({f^1}')\big)$. Let g and h be generalized Boolean functions whose algebraic normal forms are

$$\begin{aligned} g &= \sum g_i x^i\\ h &= \sum h_i x^i,\end{aligned}$$

where the coefficients g_i, h_i are in $\mathbb{Z}_4$, and x^i represents a monomial as above. Then

$$\begin{aligned}\phi\big(2\alpha(g)\alpha(h)\big) &= \phi\big(2\alpha\big(\textstyle\sum g_i x^i\big)\alpha\big(\sum h_i x^i\big)\big)\\ &= \phi\big(2\textstyle\sum\alpha(g_i x^i)\sum\alpha(h_i x^i)\big) && (\alpha \text{ is a homomorphism})\\ &= \phi\big(2\textstyle\sum\alpha(g_i)x^i \cdot \sum\alpha(h_i)x^i\big) && (\text{by (6.9) above})\\ &= \textstyle\sum\alpha(g_i)x^i \cdot \sum\alpha(h_i)x^i,\end{aligned}$$

since all the coefficients in the polynomial $2\sum\alpha(g_i)x^i \cdot \sum\alpha(h_i)x^i$ are 2. Thus we have

$$\begin{aligned}\phi\big(2\alpha(2f^2 + {f^1}'' + 3f^3)\alpha({f^1}')\big) &= \phi\big(2\big(\alpha(2f^2) + \alpha({f^1}'' + 3f^3)\big)\alpha({f^1}')\big)\\ &= \phi\big(2\alpha({f^1}'' + 3f^3)\alpha({f^1}')\big)\\ &= \sum_{\substack{i \in I_1 \cup I_3\\ i \neq i'}} x^i \cdot x^{i'},\end{aligned}$$

since we know that α of all the coefficients in ${f^1}''$, $3f^3$ and ${f^1}'$ will be 1. Thus, in this case,

$$\begin{aligned}\phi(f) &= f^2 + {f^1}'' \cdot x_{m-1} + {f^1}' \cdot x_{m-1} + f^3(1 + x_{m-1})\\ &\qquad + \sum_{\substack{i,j \in I_1 \cup I_3\\ i,j \neq i'\\ i \neq j}} x^i \cdot x^j + \sum_{\substack{i \in I_1 \cup I_3\\ i \neq i'}} x^i \cdot x^{i'}\\ &= f^2 + f^1 \cdot x_{m-1} + f^3(1 + x_{m-1}) + \sum_{\substack{i,j \in I_1 \cup I_3\\ i \neq j}} x^i \cdot x^j,\end{aligned}$$

which is the result for $k + 1$, and hence by induction the result is true for all integers $k \geqslant 1$. □

Example 6.6. Let $m' = 3$ and take the function

$$f(x) = 2x_2 + 2x_0x_1 + x_0 + x_1 + 3x_0x_2.$$

Then the algebraic normal form of the image of f under the Gray map is, by the theorem

$$\begin{aligned} f'(x) = \phi\big(f(x)\big) &= \phi\big((2x_2 + 2x_0x_1) + (x_0 + x_1 + 3x_0x_2)\big) \\ &= (x_2 + x_0x_1) + (x_0 + x_1)x_3 + x_0x_2(1 + x_3) \\ &\quad + (x_0 \cdot x_1 + x_0 \cdot x_0x_2 + x_1 \cdot x_0x_2) \\ &= x_2 + x_0x_1 + x_0x_3 + x_1x_3 + x_0x_2 \\ &\quad + x_0x_2x_3 + x_0x_1 + x_0x_2 + x_0x_1x_2 \\ &= x_2 + x_0x_3 + x_1x_3 + x_0x_2x_3 + x_0x_1x_2. \end{aligned}$$

Evaluate f at all its points by adding the equivalent vectors:

$$\begin{aligned} 2\mathbf{x}_2 &= (00002222) \\ 2\mathbf{x}_0 * \mathbf{x}_1 &= (00020002) \\ \mathbf{x}_0 &= (01010101) \\ \mathbf{x}_1 &= (00110011) \\ 3\mathbf{x}_0 * \mathbf{x}_2 &= (00000303) \\ \mathbf{f} = \text{ sum mod } 4 &= (01102231), \end{aligned}$$

and then applying ϕ to this gives

$$\begin{aligned} \phi(0,1,1,0,2,2,3,1) &= \big(\beta(0,1,1,0,2,2,3,1), \gamma(0,1,1,0,2,2,3,1)\big) \\ &= (00001110\,01101101). \end{aligned}$$

Calculating all the values of f' from its vectors gives

$$\begin{aligned} \mathbf{x}_2 &= (0000111100001111) \\ \mathbf{x}_0 * \mathbf{x}_3 &= (0000000001010101) \\ \mathbf{x}_1 * \mathbf{x}_3 &= (0000000000110011) \\ \mathbf{x}_0 * \mathbf{x}_2 * \mathbf{x}_3 &= (0000000000000101) \\ \mathbf{x}_0 * \mathbf{x}_1 * \mathbf{x}_2 &= (0000000100000001) \\ \mathbf{f}' = \text{ sum mod } 2 &= (0000111001101101), \end{aligned}$$

which agrees with the previous vector, thus confirming the derivation of the algebraic normal form. □

6.4 The Effect of the Inverse Gray Map on a Path

In this section it is shown that a Boolean function which is a path, under the action of the inverse Gray map, maps to a generalized Boolean function over $\mathbb{Z}_4$ that is also a path. That is, a Golay complementary sequence constructed by Corollary 1.25 remains a complementary sequence when mapped to $\mathbb{Z}_4$ by the inverse Gray map.

Let f, a function in $m \geqslant 2$ variables, represent a binary Golay sequence constructed by Corollary 1.25:

$$f = \sum_{i=0}^{m-2} x_{\pi(i)}x_{\pi(i+1)} + \sum_{i=0}^{m-1} g_{\pi(i)}x_{\pi(i)} + c, \quad c, g_{\pi(i)} \in \mathbb{Z}_2,$$

and where π is some permutation of $\{0, 1, \ldots, m-1\}$. The effect of the inverse Gray map on f varies according to the terms in f involving x_{m-1}. This must occur somewhere in the path, so consider the two cases, firstly when x_{m-1} is internal to the path, and then when it is an end point.

Suppose first then that $x_{m-1} = x_{\pi(j)}$, for some j, $1 \leqslant j \leqslant m-2$ (and so $m \geqslant 3$), and write f as

$$f = (P_1 + P_2 + L + c) + (x_{\pi(j-1)}x_{m-1} + x_{\pi(j+1)}x_{m-1} + g_{m-1}x_{m-1})$$

where

$$\begin{aligned} P_1 &= \sum_{i=0}^{j-2} x_{\pi(i)}x_{\pi(i+1)} \\ P_2 &= \sum_{i=j+1}^{m-2} x_{\pi(i)}x_{\pi(i+1)} \\ L &= \sum_{\substack{i=0 \\ i \neq j}}^{m-1} g_{\pi(i)}x_{\pi(i)}, \end{aligned}$$

and where the bracketting has been used to gather terms not involving/involving x_{m-1}. (Note that P_1 is null when $j = 1$, and P_2 is null when $j = m-2$, so both are null when $m = 3$, but this does not affect the following argument.) Then, by Theorem 6.3,

$$\begin{aligned} \phi^{-1}(f) &= \phi^{-1}\big((P_1 + P_2 + L + c) + (x_{\pi(j-1)}x_{m-1} + x_{\pi(j+1)}x_{m-1} + g_{m-1}x_{m-1})\big) \\ &= 2P_1 + 2P_2 + 2L + 2c + (x_{\pi(j-1)} + x_{\pi(j+1)} + g_{m-1})^2 \\ &= 2P_1 + 2P_2 + 2L + 2c + x_{\pi(j-1)} + x_{\pi(j+1)} + g_{m-1} \\ &\qquad + 2x_{\pi(j-1)}x_{\pi(j+1)} + 2x_{\pi(j-1)}g_{m-1} + 2x_{\pi(j+1)}g_{m-1} \\ &= P' + 2L + 2c + (1 + 2g_{m-1})x_{\pi(j-1)} + (1 + 2g_{m-1})x_{\pi(j+1)} + g_{m-1}, \end{aligned}$$

where

$$\begin{aligned} P' &= 2P_1 + 2x_{\pi(j-1)}x_{\pi(j+1)} + 2P_2 \\ &= 2\sum_{i=0}^{j-2} x_{\pi(i)}x_{\pi(i+1)} + 2x_{\pi(j-1)}x_{\pi(j+1)} + 2\sum_{i=j+1}^{m-2} x_{\pi(i)}x_{\pi(i+1)}, \end{aligned}$$

and it can be seen that this is a function satisfying Corollary 1.25 over $\mathbb{Z}_4$. Thus even though the loss of the variable x_{m-1} creates a 'gap' in the original path, the inverse Gray map has the effect of joining the two remaining path segments back together again.

Now suppose that x_{m-1} is an end point, so let $x_{\pi(m-1)} = x_{m-1}$ (the argument is similar if the other end point is chosen), and write

$$f = (P + L + c) + (x_{\pi(m-2)}x_{m-1} + g_{m-1}x_{m-1}),$$

where

$$\begin{aligned} P &= \sum_{i=0}^{m-3} x_{\pi(i)}x_{\pi(i+1)} \\ L &= \sum_{i=0}^{m-2} g_{\pi(i)}x_{\pi(i)}, \end{aligned}$$

noting that P is null when $m = 2$. Then, again by Theorem 6.3,

$$\begin{aligned} \phi^{-1}(f) &= \phi^{-1}((P + L + c) + (x_{\pi(m-2)}x_{m-1} + g_{m-1}x_{m-1})) \\ &= 2P + 2L + 2c + (x_{\pi(m-2)} + g_{m-1})^2 \\ &= 2P + 2L + 2c + x_{\pi(m-2)} + g_{m-1} + 2x_{\pi(m-2)}g_{m-1} \\ &= 2P + 2L + 2c + (1 + 2g_{m-1})x_{\pi(m-2)} + g_{m-1}, \end{aligned}$$

which, for $m > 2$, is again seen to satisfy Corollary 1.25—since x_{m-1} was an end point, in this case the path has merely been shortened. When $m = 2$ and so P is null, we are left with just a linear term, which being a trivial path means we must appeal directly to Theorem 1.24 to see that it is in fact a complementary sequence.

Thus in either case, a binary complementary sequence constructed according to Corollary 1.25 remains a complementary sequence when mapped up to $\mathbb{Z}_4$ by the inverse Gray map.

Example 6.7. Let $m = 4$ and take the function

$$f = x_0x_3 + x_1x_3 + x_1x_2.$$

The sequence (vector) associated with this, and the vector of auto-correlation values are

$$(0000001101100101), \quad (16, 1, 0, 5, 0, -5, 0, -1, 0, 1, 0, 1, 0, -1, 0, -1).$$

It is complementary to (for example), $f + x_0$, with sequence and auto-correlation

$$(0101011000110000), \quad (16, -1, 0, -5, 0, 5, 0, 1, 0, -1, 0, -1, 0, 1, 0, 1).$$

Mapping to $\mathbb{Z}_4$ via the inverse Gray map:

$$\begin{aligned} f' = \phi^{-1}(f) &= 2x_1x_2 + (x_0 + x_1)^2 \\ &= 2x_1x_2 + x_0 + x_1 + 2x_0x_1 \\ &= 2(x_0x_1 + x_1x_2) + x_0 + x_1, \end{aligned}$$

with associated sequence and auto-correlation

$$(01100132), \quad (8, 1, 0, 1 + 2i, 0, -1 - 2i, 0, -1).$$

The function f' is complementary with (for example), $f' + 2x_2$, with sequence and auto-correlation

$$(01102310), \quad (8, -1, 0, -1 - 2i, 0, 1 + 2i, 0, 1).$$

□

From Corollary 1.25, there are $\frac{m!}{2}2^{m+1}$ complementary sequences of length 2^m over $\mathbb{Z}_2$, and there are $\frac{(m-1)!}{2}4^m$ complementary sequences of length 2^{m-1} over $\mathbb{Z}_4$. Thus there are

$$\begin{aligned}\frac{(m-1)!}{2}4^m - \frac{m!}{2}2^{m+1} &= \frac{(m-1)!}{2}2^m(2^m - 2m)\\ &= (m-1)!2^m(2^{m-1} - m)\end{aligned}$$

sequences in $\mathbb{Z}_4$ which are not the image under the inverse Gray map of a binary complementary sequence. The two cases examined above suggest the form of those sequences over $\mathbb{Z}_4$ which are the image of a binary sequence. However since the mapping generates linear terms of variables which also appear in the functions 'L', it is perhaps easier to identify, and count, those $\mathbb{Z}_4$ sequences which are the image of a binary sequence by constructing sequences over $\mathbb{Z}_4$ and checking that the Gray map takes them to binary complementary sequences. So let the number of variables over $\mathbb{Z}_4$ be $m' = m - 1$, $m' \geqslant 2$. Then a function over $\mathbb{Z}_4$ representing the first case above is

$$f = 2P + 2L + g + g_{\pi(j)}x_{\pi(j)} + g_{\pi(j+1)}x_{\pi(j+1)}, \tag{6.10}$$

where

$$\begin{aligned}P &= \sum_{i=0}^{m'-2} x_{\pi(i)}x_{\pi(i+1)}\\ L &= \sum_{\substack{i=0\\ i\neq j,j+1}}^{m'-1} g_{\pi(i)}x_{\pi(i)} \quad g_{\pi(i)} \in \{0, 1\},\end{aligned}$$

and where $g \in \mathbb{Z}_4$, $0 \leqslant j \leqslant m' - 2$, and $g_{\pi(j)}, g_{\pi(j+1)} \in \{1, 3\}$. This is thus a path, plus a pair of linear terms with coefficients either 1 or 3 and corresponding to a pair of adjacent indices in the path, and the remaining linear terms all have coefficient 2, and a constant. Then from Theorem 6.5, the effect of the Gray map on the components of this f are: $2P + 2L$ simply becomes $P + L$; since $g_{\pi(j)}$ and $g_{\pi(j+1)}$ are either 1 or 3, the cross-term $x_{\pi(j)}x_{\pi(j+1)}$ is always present; when $g_{\pi(j)} = 1$ we get $x_{\pi(j)}x_{m-1}$, and $g_{\pi(j)} = 3$ gives $x_{\pi(j)}(1 + x_{m-1})$, which can be represented as $\beta(g_{\pi(j)})x_{\pi(j)} + x_{\pi(j)}x_{m-1}$, and similarly for $g_{\pi(j+1)}$; $g = 1$ gives $1 \cdot x_{m-1}$, $g = 2$ gives just 1, and $g = 3$ gives $1 \cdot (1 + x_{m-1})$, which can be represented as $\beta(g) + \alpha(g)x_{m-1}$; in addition when $g = 1$ or 3, we get the cross-term $1 \cdot x_{\pi(j)}$, represented as $\alpha(g)x_{\pi(j)}$, and similarly for $x_{\pi(j+1)}$. Thus the binary image is

$$\begin{aligned}\phi(f) &= P + L + \beta(g) + \alpha(g)x_{m-1} + \alpha(g)x_{\pi(j)} + \alpha(g)x_{\pi(j+1)} \\ &\quad + x_{\pi(j)}x_{\pi(j+1)} + \beta(g_{\pi(j)})x_{\pi(j)} + x_{\pi(j)}x_{m-1} \\ &\quad + \beta(g_{\pi(j+1)})x_{\pi(j+1)} + x_{\pi(j+1)}x_{m-1} \\ &= P' + L + \beta(g) + \alpha(g)x_{m-1} + \big(\alpha(g) + \beta(g_{\pi(j)})\big)x_{\pi(j)} \\ &\quad + \big(\alpha(g) + \beta(g_{\pi(j+1)})\big)x_{\pi(j+1)},\end{aligned}$$

where

$$P' = \sum_{\substack{i=0 \\ i\neq j}}^{m'-2} x_{\pi(i)}x_{\pi(i+1)} + x_{\pi(j)}x_{m-1} + x_{\pi(j+1)}x_{m-1}.$$

Note the effect of the '1 or 3' coefficients on the linear terms is to elongate the path by removing the $x_{\pi(j)}x_{\pi(j+1)}$ term and replace it with $x_{\pi(j)}x_{m-1}$ and $x_{\pi(j+1)}x_{m-1}$, thus giving a function which does satisfy Corollary 1.25. Also note that this is reason that we cannot tolerate any other linear terms with a 1 or 3 coefficient, as they would generate unwanted extraneous second order terms in the binary function. Since there are $\frac{m'!}{2}$ distinct paths of m' variables, 2^2 ways to pick g, $2^{m'-2}$ ways to construct L, $m'-1$ values for j, and 2^2 ways to pick either 1 or 3 for the linear terms, there are a total of

$$\frac{m'!}{2}2^2.2^{m'-2}(m'-1)2^2 = \frac{m'!}{2}(m'-1)2^{m'+2}$$

ways to construct functions over $\mathbb{Z}_4$ given by (6.10).

A function over $\mathbb{Z}_4$ representing the second case above (when x_{m-1} was an end point in the binary path) is

$$f = 2P + 2L + g + g_{\pi(j)}x_{\pi(j)}, \tag{6.11}$$

where

$$\begin{aligned}P &= \sum_{i=0}^{m'-2} x_{\pi(i)}x_{\pi(i+1)} \\ L &= \sum_{\substack{i=0 \\ i\neq j}}^{m'-1} g_{\pi(i)}x_{\pi(i)} \quad g_{\pi(i)} \in \{0,1\},\end{aligned}$$

and where $g \in \mathbb{Z}_4$, $j = 0$ or $m'-1$, and $g_{\pi(j)} \in \{1,3\}$. This is thus a path, plus one of the end points with coefficient 1 or 3, and the remaining linear terms all have coefficient 2, and a constant. Then from Theorem 6.5 the binary image of this is

$$\begin{aligned}\phi(f) &= P + L + \beta(g) + \alpha(g)x_{m-1} + \alpha(g)x_{\pi(j)} + x_{\pi(j)}x_{m-1} + \beta(g_{\pi(j)})x_{\pi(j)} \\ &= P' + L + \beta(g) + \alpha(g)x_{m-1} + \big(\alpha(g) + \beta(g_{\pi(j)})\big)x_{\pi(j)},\end{aligned}$$

where

$$P' = \sum_{i=0}^{m'-2} x_{\pi(i)}x_{\pi(i+1)} + x_{\pi(j)}x_{m-1}.$$

This time the path is elongated by the addition of $x_{\pi(j)}x_{m-1}$, and again we get a function which satisfies Corollary 1.25. Again, there are $\frac{m'!}{2}$ distinct paths of m' variables, 2^2 ways to pick g, $2^{m'-1}$ ways to construct L, 2 values for j, and 2 ways to pick either 1 or 3 for the end point, and so there are a total of

$$\frac{m'!}{2}2^2.2^{m'-1}.2.2 = \frac{m'!}{2}2^{m'+3}$$

ways to construct functions over $\mathbb{Z}_4$ given by (6.11). Thus the total of both these kinds of function is

$$\begin{aligned}\frac{m'!}{2}(m'-1)2^{m'+2} + \frac{m'!}{2}2^{m'+3} &= (m'-1+2)\frac{m'!}{2}2^{m'+2} \\ &= \frac{(m'+1)!}{2}2^{m'+2} \\ &= \frac{m!}{2}2^{m+1},\end{aligned}$$

where $m = m' + 1$, and this total is the number of complementary binary sequences, and thus those sequences over $\mathbb{Z}_4$ that are the image under the inverse Gray map of a binary complementary sequence are precisely the functions constructed in (6.10) and (6.11).

6.5 Conclusions

Given the algebraic normal form of a Boolean function f over $\mathbb{Z}_2$, some simple rules have been deduced which show how to establish the algebraic normal form of the function that results when f is mapped up to $\mathbb{Z}_4$ using the inverse Gray map. Then using the very specific form for a binary complementary sequence given by Corollary 1.25, it has been shown that this sequence remains a complementary sequence when it is mapped to $\mathbb{Z}_4$ by the inverse Gray map. In addition to the results given here, a variety of attempts were made to try and show that *any* binary complementary sequence (i.e without using the construction of the corollary) might always map to a complementary sequence over $\mathbb{Z}_4$, but unfortunately these were not successful. However it is still thought that it may be possible to show this.

The ways in which complementary sequences constructed by Corollary 1.25 share the same auto-correlation function is due to those given by either of Theorems 1.1 or 1.8 (namely reversing the sequence or adding a constant, or both). For sequences over $\mathbb{Z}_{2^h}$, as h increases, and along with it the order of the root of unity involved in the calculation of auto-correlation, the possible mechanisms which cause two sequences to share the same auto-correlation function also increase. Thus it is possible to form complementary pairs in ways other than the 'standard' ones given by Corollary 1.25: this was noted in [11, p5], and they gave an example over $\mathbb{Z}_4$. It is not too hard to show, using Theorem 6.3, that two binary functions forming a complementary pair in a standard way given by the corollary, when mapped to $\mathbb{Z}_4$, still form a standard complementary pair. Thus any 'non-standard' pairing over $\mathbb{Z}_4$ cannot be between sequences which are the images of binary complementary sequences. The example given in [11] was the following:

Any of the 8 sequences from the functions in set A form a complementary pair with those in B; similarly for A' and B'; in addition, sequences in A and A' share the same auto-correlation function, and similarly for B and B':

$$\begin{aligned}
A &= \{2(x_0x_1 + x_1x_2) + c_1, 2(x_0x_1 + x_1x_2) + 2x_0 + 2x_2 + c_1 : c_1 \in \mathbb{Z}_4\} \\
B &= \{2(x_0x_1 + x_1x_2) + 2x_0 + c_2, 2(x_0x_1 + x_1x_2) + 2x_2 + c_2 : c_2 \in \mathbb{Z}_4\} \\
A' &= \{2(x_1x_2 + x_0x_2) + 3x_1 + x_0 + c_3, \\
&\qquad\qquad 2(x_1x_2 + x_0x_2) + x_1 + 3x_0 + c_3 : c_3 \in \mathbb{Z}_4\} \\
B' &= \{2(x_1x_2 + x_0x_2) + x_1 + x_0 + c_4, \\
&\qquad\qquad 2(x_1x_2 + x_0x_2) + 3x_1 + 3x_0 + c_4 : c_4 \in \mathbb{Z}_4\}
\end{aligned}$$

Clearly none of these functions is of the form (6.10) or (6.11). (Note: in [11], the indices run from 1 to m, and also the example there contained an error—the sequences in the set A' did not in fact have the auto-correlation stated.) The results in this chapter may be of potential use in analysing what causes such new pairings, particularly by examining the behaviour of the corresponding two pairs of binary sequences when mapped down to $\mathbb{Z}_2$ by the Gray map.

Summary and Conclusion

In this thesis the properties and features of the technique of restriction, introduced in [32, 33], have been expanded and exploited, their usefulness having been demonstrated by successfully combining them throughout the thesis with the algebraic normal form representation of generalized Boolean functions, to produce simple descriptions of functions whose cross- and auto-correlations are of the same, or opposite, sense. These results have then been used to:

- prove that Conjecture 1 (of [32]) is true in some special cases involving at most 2 isolated vertices,
- produce an improvement in the size of (i.e. reduce) the complementary sets given by Theorem 1.27 for functions which consist of path segments, and which enable the construction of functions which satisfy the bound of Conjecture 1 for an arbitrary number of isolated vertices,
- produce a new lower limit on the PMEPR of the coset of certain binary functions, from which examples with 3 or more isolated vertices have been constructed which exceed the bound of Conjecture 1, thus showing that it cannot be true in general,
- construct complementary sets based on complementary sequences and pairs, which may often identify a subset of the coset of the function concerned, words within which have lower PMEPRs than that given by Theorem 1.27,
- show that binary complementary pairs (given by the construction of Corollary 1.25) remain complementary pairs when mapped to $\mathbb{Z}_4$ by the inverse Gray map.

Much of this comes about as a direct result of the structure of the path functions which are at the root of the construction of the complementary pairs given by Corollary 1.25, thus emphasizing the contribution made by such a simple description.

Some possible avenues for further work could be:

- could the rank of the quadratic form, for the binary case, be incorporated into Conjecture 1 in some way so as to improve it?
- can the methods of Chapter 4 be extended to account for the peaks in the power seen either side of $t = \frac{1}{8}$ (and other values of t)? (As illustrated in the figures at the end of that chapter.)

- do the complementary sets constructed in Chapter 5 tie in with any of the constructions of [46, 47] or [40]?

- is it possible to show that a complementary pair over $\mathbb{Z}_2$ remains a complementary pair over $\mathbb{Z}_4$ under the inverse Gray map *without* recourse to the specific construction of Corollary 1.25?

- can a simple description be found for those functions over $\mathbb{Z}_4$, mentioned in Section 6.5, which share the same auto-correlation function in a 'non-standard' way ? (Indeed the same comment applies to those binary functions mentioned in Section 3.6.)

(Reference [34] also contains a list of problems connected with this subject area.)

Bibliography

[1] T.H.Andres and R.G.Stanton, Golay Sequences, In *Combinatorial Maths - Proc. of* 5^{th} *Australian Conf.*, Melbourne, 1976. Lecture Notes in Maths vol 622 1977 pp44–54

[2] E.F.Assmus and J.D.Key, *Designs and their Codes*, Cambridge University Press, 1992

[3] N.L.Biggs, *Discrete Mathematics*, Oxford University Press, Revised Edition, 1989

[4] J.A.C.Bingham, Multicarrier Modulation for Data Transmission: An Idea Whose Time Has Come, *IEEE Comms. Magazine*, vol 28, pp5–14, May 1990

[5] S.Boyd, Multitone Signals with Low Crest Factor, *IEEE Trans. Circuits and Systems*, CAS-33(1), pp1018–1022, Oct 1986

[6] S.Z.Budisin, New Complementary Pairs of Sequences, *Electronics Letters*, 26(13), pp881–883 Jun 1990

[7] P.J.Cameron and J.H.van Lint, *Designs ,Graphs, Codes and their Links*, Cambridge University Press, 1991

[8] M.W.Cammarano and M.L.Walker, Integer Maxima in Power Envelopes of Golay Codewords, Technical report, University of Richmond, VA, USA, 1997

[9] L.J.Cimini, Analysis and Simulation of a Digital Mobile Channel Using Orthogonal Frequency Division Multiplexing, *IEEE Trans. Comms.* COM-33(7), pp665–675, Jul 1985

[10] J.A.Davis and J.Jedwab, Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes, *Electronics Letters*, 33(4), pp267–268 Feb 1997

[11] J.A.Davis and J.Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes, HP Laboratories Technical Report HPL-97-158, Bristol, Dec 1997

[12] J.A.Davis and J.Jedwab, Peak-to-Mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes, *IEEE Trans. Info. Theory* IT-45(7), pp2397–2417, Nov 1999

[13] S.Eliahou, M.Kervaire and B.Saffari, On Golay Polynomial Pairs, *Advances in Applied Mathematics* 12, pp235–292, 1991

[14] P.Fan and M.Darnell, *Sequence Design for Communications Applications*, Research Studies Press Ltd., 1996

[15] M.Friese, Multicarrier modulation with low peak-to-average power ratio, *Electronics Letters* 32, pp713–714, Apr 1996

[16] M.Friese, Multitone Signals with Low Crest Factor, *IEEE Trans. Comms.* 45(10) pp1338–1344, Oct 1997

[17] D.R.Gimlin and C.R.Patisaul, On Minimizing the Peak-to-Average Power Ration for the Sum of N Sinusoids, *IEEE Trans. Comms.* 41(4), pp631–635, Apr 1993

[18] M.J.E.Golay, Complementary Series, *IRE Trans. Info. Theory* IT-7, pp82–87, Apr 1961

[19] L.J.Greenstein and P.J.Fitzgerald, Phasing Multitone Signals to Minimize Peak Factors, *IEEE Trans. Comms.* COM-29(7), pp1072–1074, Jul 1981

[20] A.R.Hammons, P.V.Kumar, A.R.Calderbank, N.J.A.Sloane and P.Sole, The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes, *IEEE Trans. Info. Theory* IT-40(2), pp301–319, Mar 1994

[21] R.Hill, *A First Course in Coding Theory*, Oxford University Press, 1986

[22] A.E.Jones, T.A.Wilkinson and S.K.Barton, Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes, *Electronics Letters*, 30, pp2098–2099, Dec 1994

[23] X.Li and J.A.Ritcey, M-sequences for OFDM peak-to-average power ratio reduction and error correction, *Electronics Letters* 33, pp554–555, Mar 1997

[24] J.H.van Lint, *Introduction to Coding Theory*, Springer Verlag, Second Edition 1992

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

[26] S.Narahashi and T.Nojima, A New Phasing Scheme for Multitone Signal Systems to Reduce Peak-to-Average Power Ratio, *Electronics and Comms. in Japan*, part 1, vol 80, No. 1, pp89–99, 1997

[27] R.D.J.van Nee, OFDM Codes for Peak-to-Average Power Reduction and Error Correction, In *Proc. IEEE Globecomm 1996*, London, pp740–744, Nov 1996

[28] D.J.Newman, An L^1 Extremal Problem for Polynomials, *Proc. Amer. Math. Soc* vol 16, pp1287–1290, 1965

[29] J.E.M.Nilsson, Spectrum and Waveform Relations of Multicarrier Communications, In *Proc. IEEE MILCOM 1996*, McLean, Virginia 1996

[30] H.Ochiai and H.Imai, Block Coding Scheme Based on Complementary Sequences for Multicarrier Signals, *IEICE Trans. Fundamentals* vol E80-A, No. 11, pp2136–2143, Nov 1997

[31] E.van der Ouderaa, J.Schoukens and J.Renneboog, Comments on "Multitone Signals with Low Crest Factor", *IEEE Trans. Circuits and Systems* CAS-34(9), pp1125–1127, Sep 1987

[32] K.G.Paterson, Generalised Reed-Muller Codes and Power Control in OFDM, HP Laboratories Technical Report HPL-98-21, Bristol, Feb 1998

[33] K.G.Paterson, Generalised Reed-Muller Codes and Power Control in OFDM Modulation, HP Laboratories Technical Report HPL-98-57, Bristol, Mar 1998

[34] K.G.Paterson, Generalised Reed-Muller Codes and Power Control in OFDM Modulation, *IEEE Trans. Info. Theory* IT-46(1), pp104–120, Jan 2000

[35] V.S.Pless and W.C.Huffman (eds.), *Handbook of Coding Theory*, Elsevier,1998

[36] B.M.Popovic, Synthesis of Power Efficient Multitone Signals with Flat Amplitude Spectrum, *IEEE Trans. Comms.* 39(7), pp1031–1033, July 1991

[37] W.Rudin, Some Theorems on Fourier Coefficients, *Proc. Amer. Math. Soc.*, vol 10, pp855–859, 1959

[38] R.A.Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986

[39] M.R.Schroeder, Synthesis of Low-Peak-Factor Signals and Binary Sequences With Low Autocorrelation, *IEEE Trans. Info. Theory* IT-16, pp85–89, 1970

[40] B.P.Schweitzer, *Generalised Complementary Code Sets*, PhD Thesis, University of California, Los Angeles, California, 1971

[41] G.J.Simmons (ed.) *Contemporary Cryptology: The Science of Information Integrity* IEEE Press, 1992

[42] R.Sivaswamy, Multiphase Complementary Codes, *IEEE Trans. Info. Theory* IT-24(5), pp546–552, Sept 1978

[43] F.G.Stremler, *Introduction to Communication Systems*, Addison-Wesley, Second Edition, 1982

[44] C.Tellambura, Use of m-sequences for OFDM peak-to-average power ratio reduction, *Electronics Letters* 33, pp1300–1301, Jul 1997

[45] C.Tellambura, Upper bound on peak factor of N-multiple carriers, *Electronics Letters* 33, pp1608–1609, Sep 1997

[46] C-C.Tseng and C.L.Liu, Complementary Sets of Sequences, *IEEE Trans. Info. Theory* IT-18(5), pp644–652, Sept 1972

[47] C-C.Tseng and C.L.Liu, Complementary Sets of Sequences, IBM Thomas J. Watson Research Center, Yorktown Heights, N.Y., Report RC 3397, Apr 20, 1971

[48] Z-X. Wan, *Quaternary Codes*, World Scientific, 1997

[49] D.Wulich, Reduction of peak to mean ratio of multicarrier modulation using cyclic coding, *Electronics Letters* 32, pp432–433, Feb 1996