Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with respect to the $\{\boldsymbol{I}, \boldsymbol{H}, \boldsymbol{N}\}^n$ Transform

Lars Eirik Danielsen and Matthew G. Parker

The Selmer Center, Department of Informatics, University of Bergen,
PB 7800, N-5020 Bergen, Norway
{larsed,matthew}@ii.uib.no
http://www.ii.uib.no/~{larsed,matthew}

Abstract. We enumerate the inequivalent self-dual additive codes over GF(4) of blocklength n, thereby extending the sequence A090899 in *The On-Line Encyclopedia of Integer Sequences* from $n = 9$ to $n = 12$. These codes have a well-known interpretation as quantum codes. They can also be represented by graphs, where a simple graph operation generates the orbits of equivalent codes. We highlight the regularity and structure of some graphs that correspond to codes with high distance. The codes can also be interpreted as quadratic Boolean functions, where inequivalence takes on a spectral meaning. In this context we define PAR_{IHN}, peak-to-average power ratio with respect to the $\{I, H, N\}^n$ transform set. We prove that PAR_{IHN} of a Boolean function is equivalent to the the size of the maximum independent set over the associated orbit of graphs. Finally we propose a construction technique to generate Boolean functions with low PAR_{IHN} and algebraic degree higher than 2.

1 Self-Dual Additive Codes over GF(4)

A quantum error-correcting code with parameters $[[n, k, d]]$ encodes k qubits in a highly entangled state of n qubits such that any error affecting less than d qubits can be detected, and any error affecting at most $\frac{d-1}{2}$ qubits can be corrected. A quantum code of the stabilizer type corresponds to a code $\mathcal{C} \subset \text{GF}(4)^n$ [1]. We denote $\text{GF}(4) = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$. *Conjugation* in GF(4) is defined by $\overline{x} = x^2$. The *trace map*, $\text{tr} : \text{GF}(4) \mapsto \text{GF}(2)$, is defined by $\text{tr}(x) = x + \overline{x}$. The *trace inner product* of two vectors of length n over GF(4), $\boldsymbol{u}$ and $\boldsymbol{v}$, is given by $\boldsymbol{u} * \boldsymbol{v} = \sum_{i=1}^{n} tr(u_i \overline{v_i})$. Because of the structure of stabilizer codes, the corresponding code over GF(4), $\mathcal{C}$, will be *additive* and satisfy $\boldsymbol{u} * \boldsymbol{v} = 0$ for any two codewords $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$. This is equivalent to saying that the code must be *self-orthogonal* with respect to the trace inner product, i.e., $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, where $\mathcal{C}^{\perp} = \{\boldsymbol{u} \in \text{GF}(4)^n \mid \boldsymbol{u} * \boldsymbol{c} = 0, \forall \boldsymbol{c} \in \mathcal{C}\}$.

We will only consider codes of the special case where the dimension $k = 0$. Zero-dimensional quantum codes can be understood as highly-entangled single quantum states which are robust to error. These codes map to additive codes

In *Sequences and Their Applications – SETA 2004*, edited by T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, *Lecture Notes in Comput. Sci.*, volume 3486, pp. 373–388, Springer-Verlag, Berlin, May 2005.

over GF(4) which are *self-dual* [2], $\mathcal{C} = \mathcal{C}^{\perp}$. The number of inequivalent self-dual additive codes over GF(4) of blocklength n has been classified by Calderbank et al. [1] for $n \leq 5$, by Höhn [3] for $n \leq 7$, by Hein et al. [4] for $n \leq 7$, and by Glynn et al. [5] for $n \leq 9$. Moreover, Glynn has recently posted these results as sequence A090899 in *The On-Line Encyclopedia of Integer Sequences* [6]. We extend this sequence from $n = 9$ to $n = 12$ both for indecomposable and decomposable codes as shown in table 1. Table 2 shows the number of inequivalent indecomposable codes by distance. The distance, d, of a self-dual additive code over GF(4), $\mathcal{C}$, is the smallest weight (i.e., number of nonzero components) of any nonzero codeword in $\mathcal{C}$. A database of orbit representatives with information about orbit size, distance, and weight distribution is also available [7].

Table 1: Number of Inequivalent Indecomposable (i_n) and (Possibly) Decomposable (t_n) Self-Dual Additive Codes Over GF(4)

n	1	2	3	4	5	6	7	8	9	10	11	12
i_n	1	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068
t_n	1	2	3	6	11	26	59	182	675	3,990	45,144	1,323,363

Table 2: Number of Indecomposable Self-Dual Additive Codes Over GF(4) by Distance

$d\backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	1	1	2	3	9	22	85	363	2,436	26,750	611,036
3				1	1	4	11	69	576	11,200	467,513
4					1		5	8	120	2,506	195,455
5										1	63
6											1
Total	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068

2 Graphs, Boolean Functions, and LC-Equivalence

A self-dual additive code over GF(4) corresponds to a *graph state* [4] if its generator matrix, G, can be written as $G = \Gamma + \omega I$, where Γ is a symmetric matrix over GF(2) with zeros on the diagonal. The matrix Γ can be interpreted as the adjacency matrix of a simple undirected graph on n vertices. It has been shown by Schlingemann and Werner [8], Grassl et al. [9], Glynn [10], and Van den Nest et al. [11] that all stabilizer states can be transformed into an equivalent graph state. Thus all self-dual additive codes over GF(4) can be represented by graphs. These codes also have another interpretation as quadratic Boolean functions over n variables. A quadratic function, f, can be represented by an adjacency matrix, Γ, where $\Gamma_{i,j} = \Gamma_{j,i} = 1$ if $x_i x_j$ occurs in f, and $\Gamma_{i,j} = 0$ otherwise.

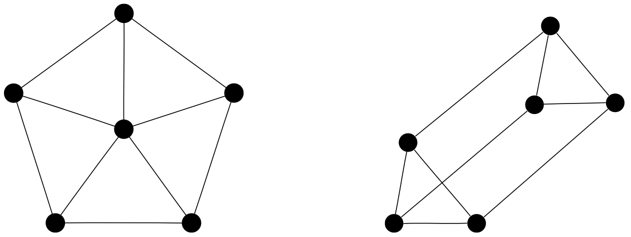
Example 1. A self-dual additive code over GF(4) with parameters $[[6, 0, 4]]$ is generated by the generator matrix

$$\begin{pmatrix} \omega & 0 & 0 & 1 & 1 & 1 \\ 0 & \omega & 0 & \omega^2 & 1 & \omega \\ 0 & 0 & \omega & \omega^2 & \omega & 1 \\ 0 & 1 & 0 & \omega & \omega^2 & 1 \\ 0 & 0 & 1 & \omega & 1 & \omega^2 \\ 1 & \omega^2 & 0 & \omega & 0 & 0 \end{pmatrix}.$$

We can transform the generator matrix into the following generator matrix of an equivalent code corresponding to a graph state,

$$\begin{pmatrix} \omega & 0 & 0 & 1 & 1 & 1 \\ 0 & \omega & 1 & 1 & 0 & 1 \\ 0 & 1 & \omega & 1 & 1 & 0 \\ 1 & 1 & 1 & \omega & 1 & 1 \\ 1 & 0 & 1 & 1 & \omega & 0 \\ 1 & 1 & 0 & 1 & 0 & \omega \end{pmatrix} = \Gamma + \omega I.$$

Γ is the adjacency matrix of the graph shown in fig. 1(a). It can also be represented by the quadratic Boolean function $f(\boldsymbol{x}) = x_0x_3 + x_0x_4 + x_0x_5 + x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5$.



(a) The "Wheel"

(b) The "2-clique of 3-cliques"

Fig. 1: The LC Orbit of the [[6,0,4]] "Hexacode"

Recently, Glynn et al. [5,10] has re-formulated the primitive operations that map equivalent self-dual additive codes over GF(4) to each other as a single, primitive operation on the associated graphs. This symmetry operation is referred to as *Vertex Neighbourhood Complementation* (VNC). It was also discovered independently by Hein et al. [4] and by Van den Nest et al. [11]. The identification of this problem as a question of establishing the *local unitary equivalence* between those quantum states that can be represented as graphs or Boolean functions was presented by Parker and Rijmen at SETA'01 [12]. Graphical representations have also been identified in the context of quantum codes by Schlingemann and Werner [8] and by Grassl et al. [9]. VNC is another name for *Local Complementation* (LC), referred to in the context of *isotropic systems* by Bouchet [13,14]. LC is defined as follows.

Definition 1. *Given a graph $G = (V, E)$ and a vertex $v \in V$. Let $N_v \subset V$ be the neighbourhood of v, i.e., the set of vertices adjacent to v. The subgraph induced by N_v is complemented to obtain the LC image G^v.*

It is easy to verify that $(G^v)^v = G$.

Theorem 1 (Glynn et al. [5,10]). *Two graphs G and H correspond to equivalent self-dual additive codes over* GF(4) *iff there is a finite sequence of vertices $v_1, v_2, \ldots, v_s$, such that $(((G^{v_1})^{v_2})^{\cdots})^{v_s} = H$.*

The symmetry rule can also be described in terms of quadratic Boolean functions.

Definition 2. *If the quadratic monomial $x_i x_j$ occurs in the algebraic normal form of the quadratic Boolean function f, then x_i and x_j are mutual neighbours in the graph represented by f, as described by the $n \times n$ symmetric adjacency matrix, Γ, where $\Gamma_{i,j} = \Gamma_{j,i} = 1$ if $x_i x_j$ occurs in f, and $\Gamma_{i,j} = 0$ otherwise. The quadratic Boolean functions f and f' are* LC equivalent *if*

$$f'(\boldsymbol{x}) = f(\boldsymbol{x}) + \sum_{\substack{j,k \in N_a \\ j<k}} x_j x_k \pmod 2,$$

where $a \in \mathbb{Z}_n$ and N_a comprises the neighbours of x_a in the graph representation of f.

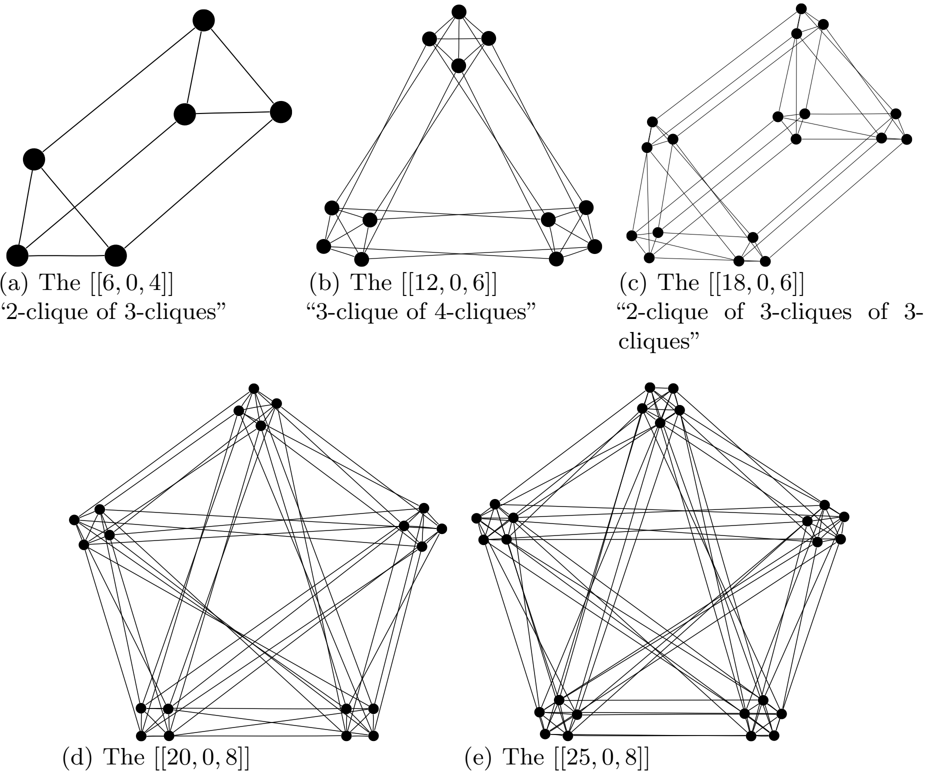
A finite number of repeated applications of the LC operation generates the orbit classes presented in this paper and, therefore, induces an equivalence between quadratic Boolean functions. We henceforth refer to this equivalence as *LC-equivalence* and the associated orbits as *LC orbits.* If the graph representations of two self-dual additive codes over GF(4) are isomorphic, they are also considered to be equivalent. This corresponds to a permutation of the labels of the vertices in the graph or the variables in the Boolean function. We only count members of an LC orbit up to isomorphism. As an example, fig. 1 shows the graph representation of the two only non-isomorphic members in the orbit of the $[[6, 0, 4]]$ "Hexacode".

A recursive algorithm, incorporating the package *nauty* [15] to check for graph isomorphism, was used to generate the LC orbits enumerated in table 1. Only the LC orbits of indecomposable codes (corresponding to connected graphs) were generated, since all decomposable codes (corresponding to unconnected graphs) can easily be constructed by combining indecomposable codes of shorter lengths.

Consider, (a) self-dual additive codes over GF(4) of blocklength n, (b) pure quantum states of n qubits which are joint eigenvectors of a commuting set of operators from the Pauli Group [1], (c) quadratic Boolean functions of n variables, (d) undirected graphs on n vertices. Then, under a suitable interpretation, we consider objects (a), (b), (c), and (d) to be mathematically identical.

3 Regular Graph Structures

Although a number of constructions for self-dual additive codes over GF(4) exist [5,16], it appears that the underlying symmetry of their associated graphs has not been identified or exploited to any great extent. We highlight the regularity and structure of some graphs that correspond to self-dual additive codes over GF(4) with high distance. Of particular interest are the highly regular "nested clique" graphs. Fig. 2 shows a few examples of such graphs. There is an upper bound on the possible distance of self-dual additive codes over GF(4) [2]. Codes that meet this bound are called *extremal*. Other bounds on the distance also exist [1,17]. Of the codes corresponding to graphs shown in fig. 2, the $[[6, 0, 4]]$, $[[12, 0, 6]]$, and $[[20, 0, 8]]$ codes are extremal. To find the "nested clique" graph representations, one may search through the appropriate LC orbits. Also note that all "nested clique" graphs we have identified so far have *circulant* adjacency matrices. An exhaustive search of all graphs with circulant adjacency matrices of up to 30 vertices has been performed.


(a) The $[[6, 0, 4]]$ "2-clique of 3-cliques"

(b) The $[[12, 0, 6]]$ "3-clique of 4-cliques"

(c) The $[[18, 0, 6]]$ "2-clique of 3-cliques of 3-cliques"

(d) The $[[20, 0, 8]]$ "5-clique of 4-cliques"

(e) The $[[25, 0, 8]]$ "5-clique of 5-cliques"

Fig. 2: "Nested Clique" Graphs

If d is the distance of a self-dual additive code over GF(4), then every vertex in the corresponding graph must have a vertex degree of at least $d-1$. This follows from the fact that a vertex with degree δ corresponds to a row in the generator matrix, and therefore a codeword, of weight $\delta+1$. All the graphs shown in fig. 2 satisfy the minimum possible regular vertex degree for the given distance. Some extremal self-dual additive codes over GF(4) do not have any regular graph representation, for example the unique $[[11,0,5]]$ and $[[18,0,8]]$ codes. For codes of length above 25 and distance higher than 8 the graph structures get more complicated. For example, with a non-exhaustive search, we did not find a graph representation of a $[[30,0,12]]$ code with regular vertex degree lower than 15.

4 The $\{I,H,N\}^n$ Transform

LC-equivalence between two graphs can be interpreted as an equivalence between the generalised Fourier spectra of the two associated Boolean functions.

Definition 3. *Let*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix},$$

where $i^2 = -1$, *be the Identity, Hadamard, and Negahadamard kernels, respectively.*

These are *unitary* matrices, i.e., $II^\dagger = HH^\dagger = NN^\dagger = I$, where $\dagger$ means *conjugate transpose*. Let f be a Boolean function on n variables and $\boldsymbol{s} = 2^{-\frac{n}{2}}(-1)^{f(\boldsymbol{x})}$ be a vector of length 2^n. Let s_j, where $j \in \mathbb{Z}_{2^n}$, be the jth coordinate of $\boldsymbol{s}$. Let $U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1}$ where $U_k \in \{I,H,N\}$, and $\otimes$ is the *tensor product* (or *Kronecker product*) defined as

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & a_{11}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}.$$

Let $\boldsymbol{S} = U\boldsymbol{s}$ for any of the 3^n valid choices of the $2^n \times 2^n$ transform U. Then the set of 3^n vectors, $\boldsymbol{S}$, is a multispectra with respect to the transform set, U, with $3^n 2^n$ spectral points. We refer to this multispectra as the spectrum with respect to the $\{I,H,N\}^n$ transform. (Using a similar terminology, the spectrum with respect to the $\{H\}^n$ transform would simply be the well-known Walsh-Hadamard spectrum). It can be shown that the $\{I,H,N\}^n$ spectrum of an LC orbit is invariant to within coefficient permutation. Moreover if, for a specific choice of U, $\boldsymbol{S}$ is flat (i.e., $|S_i| = |S_j|$, $\forall i,j$), then we can write $\boldsymbol{S} = v^{4f'(\boldsymbol{x})+h(\boldsymbol{x})}$, where f' is a Boolean function, h is any function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_8$, and $v^4 = -1$. If the algebraic degree of $h(\boldsymbol{x})$ is ≤ 1, we can always eliminate $h(\boldsymbol{x})$ by post-multiplication by a tensor product of matrices from $\mathcal{D}$, the set of 2×2 diagonal and anti-diagonal unitary matrices [18], an operation that will never change the spectral coefficient magnitudes. Let M be the multiset of f' existing within the

$\{I, H, N\}^n$ spectrum for the subcases where $h(\boldsymbol{x})$ is of algebraic degree ≤ 1. The $\{I, H, N\}^n$*-orbit* of f is then the set of distinct members of M. In particular, if f is quadratic then the $\{I, H, N\}^n$-orbit is the LC orbit [18].

Example 2. We look at the function $f(\boldsymbol{x}) = x_0x_1 + x_0x_2$. The corresponding bipolar vector, ignoring the normalization factor, is

$$\boldsymbol{s} = (-1)^{f(\boldsymbol{x})} = (1, 1, 1, -1, 1, -1, 1, 1)^T.$$

We choose the transform $U = N \otimes I \otimes I$ and get the result

$$\boldsymbol{S} = U\boldsymbol{s} = (v, v^7, v^7, v, v^7, v, v, v^7)^T, \quad v^4 = -1.$$

We observe that $|S_i| = 1$, $\forall i$, which means that $\boldsymbol{S}$ is flat and can be expressed as

$$\boldsymbol{S} = v^{4(x_0x_1+x_0x_2+x_1x_2)+(6x_0+6x_1+6x_2+1)}.$$

We observe that $h(\boldsymbol{x})$, the terms that are not divisible by 4, are all linear or constant. We can therefore eliminate $h(\boldsymbol{x})$, in this case by using the transform

$$D = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \otimes \begin{pmatrix} v^7 & 0 \\ 0 & v \end{pmatrix}.$$

We get the result

$$D\boldsymbol{S} = (-1)^{x_0x_1+x_0x_2+x_1x_2},$$

and thus $f'(\boldsymbol{x}) = x_0x_1 + x_0x_2 + x_1x_2$. The functions f and f' are in the same $\{I, H, N\}^n$ orbit, and since they are quadratic functions, the same LC orbit. This can be verified by applying the LC operation to the vertex corresponding to the variable x_0 in the graph representation of either function.

5 Peak-to-Average Power Ratio w.r.t. $\{I, H, N\}^n$

Definition 4. *The peak-to-average power ratio of a vector,* $\boldsymbol{s}$*, with respect to the* $\{I, H, N\}^n$ *transform [19] is*

$$\mathrm{PAR}_{IHN}(\boldsymbol{s}) = 2^n \max_{\substack{\forall U \in \{I,H,N\}^n \\ \forall k \in \mathbb{Z}_{2^n}}} |S_k|^2, \quad \textit{where } \boldsymbol{S} = U\boldsymbol{s}.$$

If a vector, $\boldsymbol{s}$, has a completely flat $\{I, H, N\}^n$ spectrum (which is impossible) then $\mathrm{PAR}_{IHN}(\boldsymbol{s}) = 1$. If $\boldsymbol{s} = 2^{-\frac{n}{2}}(1, 1, \ldots, 1, 1)$ then $\mathrm{PAR}_{IHN}(\boldsymbol{s}) = 2^n$. A typical vector, $\boldsymbol{s}$, will have a $\mathrm{PAR}_{IHN}(\boldsymbol{s})$ somewhere between these extremes. For quadratic functions, PAR_{IHN} will always be a power of 2. The PAR of $\boldsymbol{s}$ can be alternatively expressed in terms of the *generalised nonlinearity* [19],

$$\gamma(f) = 2^{\frac{n}{2}-1}\left(2^{\frac{n}{2}} - \sqrt{\mathrm{PAR}_{IHN}(\boldsymbol{s})}\right),$$

but in this paper we use the PAR measure. Let $\boldsymbol{s} = 2^{-\frac{n}{2}}(-1)^{f(\boldsymbol{x})}$, as before. When we talk about the PAR_{IHN} of f or its associated graph G, we mean

$\mathrm{PAR}_{IHN}(\boldsymbol{s})$. It is desirable to find Boolean functions with high generalised nonlinearity and therefore low PAR_{IHN} [20]. PAR_{IHN} is an invariant of the $\{I,H,N\}^n$ orbit and, in particular, the LC orbit. We observe that Boolean functions from LC orbits associated with self-dual additive codes over GF(4) with high distance typically have low PAR_{IHN}. This is not surprising as the distance of a quantum code has been shown to be equal to the recently defined *Aperiodic Propagation Criteria distance* (APC distance) [20] of the associated quadratic Boolean function, and APC is derived from the aperiodic autocorrelation which is, in turn, the autocorrelation "dual" of the spectra with respect to $\{I,H,N\}^n$. Table 3 shows PAR_{IHN} values for every LC orbit representative for $n \leq 12$.

Table 3: PAR_{IHN} of LC Orbit Representatives

n	Number of orbits with specified PAR_{IHN}										
	2	4	8	16	32	64	128	256	512	1024	2048
1	1										
2	1										
3		1									
4		1	1								
5		1	2	1							
6		1	5	4	1						
7			6	14	5	1					
8			9	52	32	7	1				
9			2	156	212	60	9	1			
10			1	624	1,753	639	103	11	1		
11				3,184	25,018	10,500	1,578	163	13	1	
12				12,323	834,256	380,722	43,013	3,488	249	16	1

Definition 5. *Let $\alpha(G)$ be the independence number of a graph G, i.e., the size of the maximum independent set in G. Let $[G]$ be the set of all graphs in the LC orbit of G. We then define $\lambda(G) = \max_{H\in[G]} \alpha(H)$, i.e., the size of the maximum independent set over all graphs in the LC orbit of G.*

Consider as an example the Hexacode which has two non-isomorphic graphs in its orbit (see fig. 1). It is evident that the size of the largest independent set of each graph is 2, so $\lambda = 2$. The values of λ for all LC orbits for $n \leq 12$ clearly show that λ and d, the distance of the associated self-dual additive code over GF(4), are related. LC orbits associated with codes with high distance typically have small values for λ. Table 4 summarises this observation by giving the ranges of λ observed for all LC orbits associated with codes of given lengths and distances. For instance, $[[12,0,2]]$ codes exist with any value of λ between 4 and 11, while $[[12,0,5]]$ and $[[12,0,6]]$ codes only exist with $\lambda = 4$.

Definition 6. *Let Λ_n be the minimum value of λ over all LC orbits with n vertices.*

Table 4: Range of Maximum Independent Set Size

d	Range of λ for specified n										
	2	3	4	5	6	7	8	9	10	11	12
2	**1**	**2**	**2**,3	3,4	3–5	3–6	3–7	4–8	4–9	4–10	4–11
3				**2**	3	**3**,4	3,4	3–5	4–6	4–7	4–8
4					**2**		**3**,4	**3**,4	**3**–5	4–6	4–7
5										**4**	4
6											**4**

From table 4 we observe that $\Lambda_n = 2$ for n from 3 to 6, $\Lambda_n = 3$ for n from 7 to 10, and $\Lambda_n = 4$ when n is 11 or 12.

Theorem 2. *$\Lambda_{n+1} \geq \Lambda_n$, i.e., Λ_n is monotonically nondecreasing when the number of vertices is increasing.*

Proof. Consider a graph $G = (V, E)$ with $n + 1$ vertices. Select a vertex v and let G' be the induced subgraph on the n vertices $V \backslash \{v\}$. We generate the LC-orbit of G'. The LC operations may add or remove edges between G' and v, but the presence of v does not affect the LC orbit of G'. The size of the largest independent set in the LC orbit of G' is at least Λ_n. This is also an independent set in the LC orbit of G, so $\Lambda_{n+1} \geq \Lambda_n$. □

A very loose lower bound on Λ_n can also be given. Consider a graph containing a clique of size k. It is easy to see that an LC operation on any vertex in the clique will produce an independent set of size $k - 1$. Thus the maximum clique in an LC orbit, where the largest independent set has size λ, can not be larger than $\lambda + 1$. If r is the *Ramsey number* $R(k, k+1)$ [21], then it is guaranteed that all simple undirected graphs with minimum r vertices will have either an independent set of size k or a clique of size $k + 1$. It follows that all LC orbits with at least r vertices must have $\lambda \geq k$. Thus $\Lambda_n \geq k$ for $n \geq r$. For instance, $R(3, 4) = 9$, so LC orbits with at least 9 vertices can not have λ smaller than 3.

For $n > 12$, we have computed the value of λ for some graphs corresponding to self-dual additive codes over GF(4) with high distance. This gives us upper bounds on the value of Λ_n, as shown in table 5. The bounds on Λ_{13} and Λ_{14} are tight, since $\Lambda_{12} = 4$ and $\Lambda_{n+1} \geq \Lambda_n$.

Table 5: Upper Bounds on Λ_n

n	13	14	15	16	17	18	19	20	21
$\Lambda_n \leq$	4	4	5	5	5	6	6	6	9

For $n = 10$, there is a unique LC orbit that satisfies, optimally, $\lambda = 3$, $\text{PAR}_{IHN} = 8$ and $d = 4$. One of the graphs in this orbit is the *graph complement* of the “double 5-cycle” graph, shown in fig. 3.

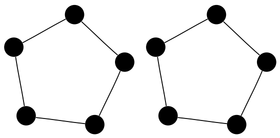


Fig. 3: The “Double 5-Cycle” Graph

Theorem 3 (Parker and Rijmen [12]). *Given a graph $G = (V, E)$ with a maximum independent set $A \subset V$, $|A| = \alpha(G)$. Let $\boldsymbol{s} = (-1)^{f(\boldsymbol{x})}$, where $f(\boldsymbol{x})$ is the boolean function representation of G. Let $U = \bigotimes_{i \in A} H_i \bigotimes_{i \notin A} I_i$, i.e., the transform applying H to variables corresponding to vertices $v \in A$ and I to all other variables. Then* $\max_{\forall k \in \mathbb{Z}_{2^n}} |S_k|^2 = 2^{\alpha(G)}$*, where $\boldsymbol{S} = U\boldsymbol{s}$.*

Arratia et al. [22] introduced the *interlace polynomial* $q(G, z)$ of a graph G. Aigner and van der Holst [23] later introduced the interlace polynomial $Q(G, z)$. Riera and Parker [24] showed that $q(G, z)$ is related to the $\{I, H\}^n$ spectra of the quadratic boolean function corresponding to G, and that $Q(G, z)$ is related to the $\{I, H, N\}^n$ spectra.

Theorem 4 (Riera and Parker [24]). *Let f be a quadratic boolean function and G its associated graph. Then PAR_{IHN} of f is equal to $2^{\deg Q(G,z)}$, where* $\deg Q(G, z)$ *is the degree of the interlace polynomial $Q(G, z)$.*

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

Proof. Let us for brevity define $P(G) = \mathrm{PAR}_{IHN}(\boldsymbol{s})$, where $\boldsymbol{s} = 2^{-\frac{n}{2}}(-1)^{f(\boldsymbol{x})}$, and $f(\boldsymbol{x})$ is the boolean function representation of G. From theorem 3 it follows that $P(G) \geq 2^{\lambda(G)}$. Choose $H = (V, E) \in [G]$ with $\alpha(H) = \lambda(G)$. If $|V| = 1$ or 2, the theorem is true. We will prove the theorem for $n > 2$ by induction on $|V|$. We will show that $P(H) \leq 2^{\alpha(H)}$, which is equivalent to saying that $P(G) \leq 2^{\lambda(G)}$. It follows from theorem 4 and the definition of $Q(H, z)$ by Aigner and van der Holst [23] that $P(H) = \max\{P(H \backslash u), P(H^u \backslash u), P(((H^u)^v)^u \backslash u)\}$. (We recall that H^u denotes the LC operation on vertex u of H.) Assume, by induction hypothesis, that $P(H \backslash u) = 2^{\lambda(H \backslash u)}$. Therefore, $P(H \backslash u) = 2^{\alpha(K \backslash u)}$ for some $K \backslash u \in [H \backslash u]$. Note that $K \backslash u \in [H \backslash u]$ implies $K \in [H]$. It must then be true that $\alpha(K \backslash u) \leq \alpha(K) \leq \alpha(H)$, and it follows that $P(H \backslash u) \leq 2^{\alpha(H)}$. Similar arguments hold for $P(H^u \backslash u)$ and $P(((H^u)^v)^u \backslash u)$, so $P(H) \leq 2^{\alpha(H)}$. □

As an example, the Hexacode has $\lambda = 2$ and therefore $\mathrm{PAR}_{IHN} = 2^2 = 4$.

Corollary 1. *Any quadratic Boolean function on n or more variables must have $PAR_{IHN} \geq 2^{\Lambda_n}$.*

Definition 7. *PAR_{IH} is the peak-to-average power ratio with respect to the transform set $\{I, H\}^n$, otherwise defined in the same way as PAR_{IHN}.*

Definition 8. *PAR_l is the peak-to-average power ratio with respect to the infinite transform set $\{U\}^n$, consisting of matrices of the form*

$$U = \begin{pmatrix} \cos\theta & \sin\theta e^{i\phi} \\ \sin\theta & -\cos\theta e^{i\phi} \end{pmatrix},$$

where $i^2 = -1$, and θ and ϕ can take any real values. $\{U\}$ comprises all 2×2 unitary transforms to within a post-multiplication by a matrix from $\mathcal{D}$, the set of 2×2 diagonal and anti-diagonal unitary matrices.

Theorem 6 (Parker and Rijmen [12]). *If $\boldsymbol{s}$ corresponds to a bipartite graph, then $PAR_l(\boldsymbol{s}) = PAR_{IH}(\boldsymbol{s})$.*

It is obvious that $\{I, H\}^n \subset \{I, H, N\}^n \subset \{U\}^n$, and therefore that $\mathrm{PAR}_{IH} \leq \mathrm{PAR}_{IHN} \leq \mathrm{PAR}_l$. We then get the following corollary of theorems 5 and 6.

Corollary 2. *If an LC orbit, $[G]$, contains a bipartite graph, then all functions corresponding to graphs in the orbit will have $PAR_l = 2^{\lambda(G)}$.*

Thus, all LC orbits with a bipartite member have $\mathrm{PAR}_{IHN} = \mathrm{PAR}_l$. Note that these orbits will always have $\mathrm{PAR}_l \geq 2^{\lceil \frac{n}{2} \rceil}$ [12] and that the fraction of LC orbits which have a bipartite member appears to decrease exponentially as the number of vertices increases. In the general case, PAR_{IHN} is only a lower bound on PAR_l. For example, the Hexacode has $\mathrm{PAR}_{IHN} = 4$, but a tighter lower bound on PAR_l is 4.486 [12]. (This bound has later been improved to 5.103 [25].)

6 Construction for Low PAR_{IHN}

So far we have only considered *quadratic* Boolean functions which correspond to graphs and self-dual additive codes over GF(4). For cryptographic purposes, we are interested in Boolean functions of degree higher than 2. Such functions can be represented by *hypergraphs*, but they do not correspond to quantum stabilizer codes or self-dual additive codes over GF(4). A non-quadratic Boolean function, $f(\boldsymbol{x})$, can, however, be interpreted as a quantum state described by the probability distribution vector $\boldsymbol{s} = 2^{-\frac{n}{2}}(-1)^{f(\boldsymbol{x})}$. A single quantum state corresponds to a quantum code of dimension zero whose distance is the APC distance [20]. The APC distance is the weight of the minimum weight quantum error operator that gives an errored state not orthogonal to the original state and therefore not guaranteed to be detectable.

We are interested in finding Boolean functions of algebraic degree greater than 2 with low PAR_{IHN}, but exhaustive searching becomes infeasible with more than a few variables. We therefore propose a construction technique for nonquadratic Boolean functions with low PAR_{IHN} using the best quadratic functions as building blocks. Before we describe our construction we must first state what we mean by "low PAR_{IHN}". For $n = 6$ to $n = 10$ we computed PAR_{IHN} for samples from the space $\mathbb{Z}_2^{2^n}$, to determine the range of PAR_{IHN} we can expect just by guessing. Table 6 summarises these results. If we can construct Boolean

Table 6: Sampled Range of PAR_{IHN} for $n = 6$ to 10

n # samples	6 50000	7 20000	8 5000	9 2000	10 1000
Range of PAR_{IHN}	6.5–25.0	9.0–28.125	12.25–28.125	14.0625–30.25	18.0–34.03

functions with PAR_{IHN} lower than the sampled minimum, we can consider our construction to be somewhat successful.

Parker and Tellambura [26,27] proposed a generalisation of the Maiorana-McFarland construction for Boolean functions that satisfies a tight upper bound on PAR with respect to the $\{H, N\}^n$ transform (and other transform sets), this being a form of Golay Complementary Set construction and a generalisation of the construction of Rudin and Shapiro and of Davis and Jedwab [28]. Let $p(\boldsymbol{x})$ be a Boolean function on $n = \sum_{j=0}^{L-1} t_j$ variables, where $T = \{t_0, t_1, \ldots, t_{L-1}\}$ is a set of positive integers and $\boldsymbol{x} \in \mathbb{Z}_2^n$. Let $\boldsymbol{y_j} \in \mathbb{Z}_2^{t_j}$, $0 \le j < L$, such that $\boldsymbol{x} = \boldsymbol{y_0} \times \boldsymbol{y_1} \times \cdots \times \boldsymbol{y_{L-1}}$. Construct $p(\boldsymbol{x})$ as follows.

$$p(\boldsymbol{x}) = \sum_{j=0}^{L-2} \theta_j(\boldsymbol{y_j})\gamma_j(\boldsymbol{y_{j+1}}) + \sum_{j=0}^{L-1} g_j(\boldsymbol{y_j}), \tag{1}$$

where θ_j is a permutation: $\mathbb{Z}_2^{t_j} \to \mathbb{Z}_2^{t_{j+1}}$, γ_j is a permutation: $\mathbb{Z}_2^{t_{j+1}} \to \mathbb{Z}_2^{t_j}$, and g_j is any Boolean function on t_j variables. It has been shown [27] that the function $p(\boldsymbol{x})$ will have $\text{PAR}_{HN} \le 2^{t_{\max}}$, where $t_{\max}$ is the largest integer in T. It is helpful to visualise this construction graphically, as in fig. 4. In this example, the size of the largest partition is 3, so $\text{PAR}_{HN} \le 8$, regardless of what choices we make for θ_j, γ_j, and g_j.

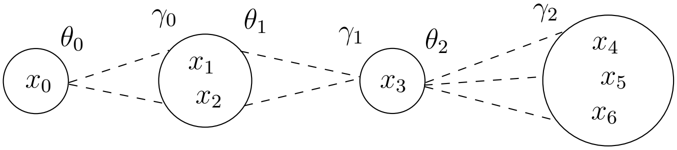


Fig. 4: Example of Construction with $\text{PAR}_{HN} \le 8$

Observe that if we set $L = 2$, $t = t_0 = t_1$, let θ_0 be the identity permutation, and $g_0 = 0$, construction (1) reduces to the Maiorana-McFarland construction over $2t$ variables. Construction (1) can also be viewed as a generalisation of the "path graph", $f(\boldsymbol{x}) = x_0x_1 + x_1x_2 + \cdots + x_{n-2}x_{n-1}$, which has optimal PAR with respect to $\{H, N\}^n$. Unfortunately, the "path graph" is not a particularly good construction for low PAR_{IHN}. But as we have seen, graphs corresponding to self-dual additive codes over GF(4) with high distance do give us Boolean functions with low PAR_{IHN}. We therefore propose the following generalised construction.

$$p(\boldsymbol{x}) = \sum_{i=0}^{L-1} \sum_{j=i+1}^{L-1} \Gamma_{i,j}(\boldsymbol{y_i})\Gamma_{j,i}(\boldsymbol{y_j}) + \sum_{j=0}^{L-1} g_j(\boldsymbol{y_j}), \tag{2}$$

where $\Gamma_{i,j}$ is either a permutation: $\mathbb{Z}_2^{t_i} \rightarrow \mathbb{Z}_2^{t_j}$, or $\Gamma_{i,j} = 0$, and g_j is any Boolean function on t_j variables. It is evident that Γ can be thought of as a "generalised adjacency matrix", where the entries, $\Gamma_{i,j}$, are no longer 0 or 1 but, instead, 0 or permutations from $\mathbb{Z}_2^{t_i}$ to $\mathbb{Z}_2^{t_j}$. Construction (1) then becomes a special case where $\Gamma_{i,j} = 0$ except for when $j = i + 1$ (i.e., the "generalised adjacency matrix" of the "path graph"). In order to minimise PAR_{IHN} we choose the form of the matrix Γ according to the adjacency matrix of a self-dual additive code over GF(4) with high distance. We also choose the "offset" functions, g_j, to be Boolean functions corresponding to self-dual additive codes over GF(4) with high distance. Finally for the non-zero $\Gamma_{i,j}$ entries, we choose selected permutations, preferably nonlinear to increase the overall degree. Here are some initial results which demonstrate that, using (2), we can construct Boolean functions of algebraic degree greater than 2 with low PAR_{IHN}. (We use an abbreviated ANF notation for some many-term Boolean functions, e.g. $012, 12, 0$ is short for $x_0x_1x_2 + x_1x_2 + x_0$.)

Example 3 ($n = 8$). Use the Hexacode graph f = 01, 02, 03, 04, 05, 12, 23, 34, 45, 51 as a template. Let $t_0 = 3$, $t_1 = t_2 = t_3 = t_4 = t_5 = 1$. (See fig. 5.) We use the following matrix Γ.

$$\Gamma = \begin{pmatrix} 0 & 02,1 & 02,1 & 02,1 & 02,1 & 02,1 \\ 3 & 0 & 3 & 0 & 0 & 3 \\ 4 & 4 & 0 & 4 & 0 & 0 \\ 5 & 0 & 5 & 0 & 5 & 0 \\ 6 & 0 & 0 & 6 & 0 & 6 \\ 7 & 7 & 0 & 0 & 7 & 0 \end{pmatrix}$$

Let $g_0(\boldsymbol{y_0})$ = 01, 02, 12 and all other g_j any arbitrary affine functions. Then, using (2) to construct $p(\boldsymbol{x})$ we get $p(\boldsymbol{x})$ = 023, 024, 025, 026, 027, 01, 02, 12, 13, 14, 15, 16, 17, 34, 37, 45, 56, 67. Then $p(\boldsymbol{x})$ has $\mathrm{PAR}_{IHN} = 9.0$.

Example 4 ($n = 8$). Use the Hexacode graph f = 01, 02, 03, 04, 05, 12, 23, 34, 45, 51 as a template. Let $t_0 = 3$, $t_1 = t_2 = t_3 = t_4 = t_5 = 1$. (See fig. 5.) We use the following matrix Γ.

$$\Gamma = \begin{pmatrix} 0 & 02,1 & 12,0,1,2 & 01,02,12,1,2 & 01,02,12 & 02,12,1,2 \\ 3 & 0 & 3 & 0 & 0 & 3 \\ 4 & 4 & 0 & 4 & 0 & 0 \\ 5 & 0 & 5 & 0 & 5 & 0 \\ 6 & 0 & 0 & 6 & 0 & 6 \\ 7 & 7 & 0 & 0 & 7 & 0 \end{pmatrix}$$

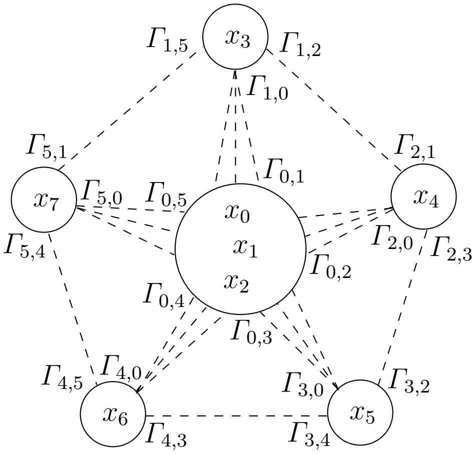


Fig. 5: Example of Construction with low PAR_{IHN}

Let $g_0(\boldsymbol{y_0}) = 01, 12$ and all other g_j any arbitrary affine functions. Then, using (2) to construct $p(\boldsymbol{x})$ we get $p(\boldsymbol{x}) =$ 015, 016, 023, 025, 026, 027, 124, 125, 126, 127, 01, 04, 12, 13, 14, 15, 17, 24, 25, 27, 34, 37, 45, 56, 67. Then $p(\boldsymbol{x})$ has $\text{PAR}_{IHN} = 9.0$.

Example 5 ($n = 9$). Use the triangle graph $f = 01, 02, 12$ as a template. Let $t_0 = t_1 = t_2 = 3$. (See fig. 6.) Assign the permutations

$$\begin{aligned}
\Gamma_{0,1} = \Gamma_{0,2} &= (12, 0, 1, 2)(01, 2)(02, 1, 2),\\
\Gamma_{1,0} &= (34, 5)(35, 4, 5)(45, 3, 4, 5),\\
\Gamma_{1,2} &= (45, 3, 4, 5)(34, 5)(35, 4, 5),\\
\Gamma_{2,0} &= (68, 7, 8)(78, 6, 7, 8)(67, 8),\\
\Gamma_{2,1} &= (78, 6, 7, 8)(67, 8)(68, 7, 8).
\end{aligned}$$

Let $g_0(\boldsymbol{y_0}) = 01, 02, 12$, $g_1(\boldsymbol{y_1}) = 34, 35, 45$, and $g_2(\boldsymbol{y_2}) = 67, 68, 78$. Then, using (2) to construct $p(\boldsymbol{x})$ we get, $p(\boldsymbol{x}) =$ 0135, 0178, 0245, 0267, 1234, 1268, 3467, 3568, 4578, 014, 015, 016, 017, 018, 023, 024, 025, 028, 034, 068, 125, 127, 128, 134, 145, 167, 168, 234, 235, 245, 267, 268, 278, 348, 357, 358, 378, 456, 457, 458, 468, 478, 567, 568, 578, 05, 07, 08, 13, 14, 17, 23, 25, 26, 28, 36, 37, 38, 46, 56, 58, 01, 02, 12, 34, 35, 45, 67, 68, 78. Then $p(\boldsymbol{x})$ has $\text{PAR}_{IHN} = 10.25$.

The examples of our construction satisfy a low PAR_{IHN}. Further work should ascertain the proper choice of permutations. Finally, there is an even more obvious variation of construction (2), suggested by the graphs of fig. 2, where the functions g_j are chosen either to be quadratic cliques or to be further “nested” versions of construction (2). We will report on this variation in a future paper.

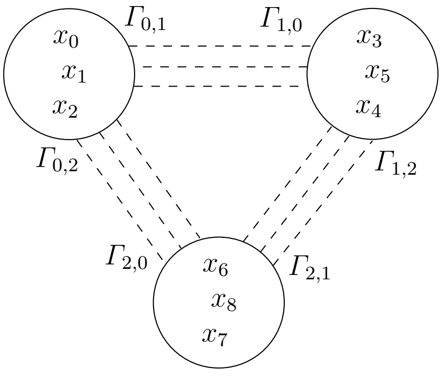


Fig. 6: Example of Construction with low PAR_{IHN}

References

1. Calderbank, A.R., Rains, E.M., Shor, P.M., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44** (1998) pp. 1369–1387 `http://arxiv.org/quant-ph/9608006`.
2. Rains, E.M., Sloane, N.J.A.: Self-dual codes. In Pless, V.S., Huffman, W.C., eds.: Handbook of Coding Theory. Elsevier (1998) 177–294 `http://arxiv.org/math/0208001`.
3. Höhn, G.: Self-dual codes over the Kleinian four group. Mathematische Annalen **327** (2003) pp. 227–255 `http://arxiv.org/math/0005266`.
4. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. Phys. Rev. A **69** (2004) `http://arxiv.org/quant-ph/0307130`.
5. Glynn, D.G., Gulliver, T.A., Maks, J.G., Gupta, M.K.: The geometry of additive quantum codes. Submitted to Springer-Verlag (2004)
6. Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences. Web page (2004) `http://www.research.att.com/~njas/sequences/`.
7. Danielsen, L.E.: Database of self-dual quantum codes. Web page (2004) `http://www.ii.uib.no/~larsed/vncorbits/`.
8. Schlingemann, D., Werner, R.F.: Quantum error-correcting codes associated with graphs. Phys. Rev. A **65** (2002) `http://arxiv.org/quant-ph/0012111`.
9. Grassl, M., Klappenecker, A., Rotteler, M.: Graphs, quadratic forms, and quantum codes. In: Proc. IEEE Int. Symp. Inform. Theory. (2002) p. 45
10. Glynn, D.G.: On self-dual quantum codes and graphs. Submitted to Elect. J. Combinatorics. `http://homepage.mac.com/dglynn/.Public/SD-G3.pdf` (2002)
11. Van den Nest, M., Dehaene, J., De Moor, B.: Graphical description of the action of local Clifford transformations on graph states. Phys. Rev. A **69** (2004) `http://arxiv.org/quant-ph/0308151`.
12. Parker, M.G., Rijmen, V.: The quantum entanglement of binary and bipolar sequences. In Helleseth, T., Kumar, P.V., Yang, K., eds.: Sequences and Their Applications, SETA'01. Discrete Mathematics and Theoretical Computer Science Series, Springer-Verlag (2001) Long version: `http://arxiv.org/quant-ph/0107106`.
13. Bouchet, A.: Isotropic systems. European J. Combin. **8** (1987) pp. 231–244
14. Bouchet, A.: Recognizing locally equivalent graphs. Discrete Math. **114** (1993) pp. 75–86

15. McKay, B.D.: nauty User's Guide. (2004) `http://cs.anu.edu.au/~bdm/nauty/nug.pdf`.
16. Gulliver, T.A., Kim, J.-L.: Circulant based extremal additive self-dual codes over GF(4). IEEE Trans. Inform. Theory **50** (2004) pp. 359–366
17. Grassl, M.: Bounds on d_{min} for additive $[[n, k, d]]$ QECC. Web page (2003) `http://iaks-www.ira.uka.de/home/grassl/QECC/TableIII.html`.
18. Riera, C., Petrides, G., Parker, M.G.: Generalized bent criteria for Boolean functions. Technical Report 285, Dept. of Informatics, University of Bergen, Norway (2004) `http://www.ii.uib.no/publikasjoner/texrap/pdf/2004-285.pdf`.
19. Parker, M.G.: Generalised S-box nonlinearity. NESSIE Public Document, NES/DOC/UIB/WP5/020/A. `https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase2/SBoxLin.pdf` (2003)
20. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic propagation criteria for Boolean functions. Submitted to Inform. Comput. `http://www.ii.uib.no/~matthew/GenDiff4.pdf` (2004)
21. Radziszowski, S.P.: Small Ramsey numbers. Elect. J. Combinatorics (2002) pp. 1–42 Dynamical Survey DS1, `http://www.combinatorics.org/Surveys/ds1.pdf`.
22. Arratia, R., Bollobás, B., Sorkin, G.B.: The interlace polynomial of a graph. J. Combin. Theory Ser. B **92** (2004) pp. 199–233 `http://arxiv.org/math/0209045`.
23. Aigner, M., van der Holst, H.: Interlace polynomials. Linear Algebra and its Applications **377** (2004) pp. 11–30
24. Riera, C., Parker, M.G.: Spectral interpretations of the interlace polynomial. Submitted to WCC2005. `http://www.ii.uib.no/~matthew/WCC4.pdf` (2004)
25. Parker, M.G., Gulliver, T.A.: On graph symmetries and equivalence of the six variable double-clique and wheel. Unpublished (2003)
26. Parker, M.G., Tellambura, C.: A construction for binary sequence sets with low peak-to-average power ratio. In: Proc. IEEE Int. Symp. Inform. Theory. (2002) p. 239 `http://www.ii.uib.no/~matthew/634isit02.pdf`.
27. Parker, M.G., Tellambura, C.: A construction for binary sequence sets with low peak-to-average power ratio. Technical Report 242, Dept. of Informatics, University of Bergen, Norway (2003) `http://www.ii.uib.no/publikasjoner/texrap/pdf/2003-242.pdf`.
28. Davis, J.A., Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. IEEE Trans. Inform. Theory **45** (1999) pp. 2397–2417