Univariate and Multivariate Merit Factors

Matthew G. Parker

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

Abstract. Merit factor of a binary sequence is reviewed, and constructions are described that appear to satisfy an asymptotic merit factor of 6.3421... Multivariate merit factor is characterised and recursive Boolean constructions are presented which satisfy a non-vanishing asymptote in multivariate merit factor. Clifford merit factor is characterised as a generalisation of multivariate merit factor and as a type of quantum merit factor. Recursive Boolean constructions are presented which, however, only satisfy an asymptotic Clifford merit factor of zero. It is demonstrated that Boolean functions obtained via quantum error correcting codes tend to maximise Clifford merit factor. Results are presented as to the distribution of the above merit factors over the set of binary sequences and Boolean functions.

1 Introduction

This paper reviews spectral properties of binary sequences and Boolean functions. It deals with aperiodic and continuous spectral properties of the sequence or function, as quantified by *merit factor* and aperiodic *sum-of-squares*, from which merit factor is derived. The *sum-of-squares* can be computed in two ways, firstly by the sum-of-squares of the autocorrelation coefficients and, secondly, by the sum of the fourth powers of the magnitudes of the spectral values. Merit factor quantifies the continuous mean-square deviation from the average power spectrum of the sequence or Boolean function. Therefore it quantifies the degree of uniformity of spectral energy distribution for the sequence or Boolean function. It is an attractive metric because it computes a continuous (infinite) property of the sequence or function by using a relatively small amount of discrete finite computation. We demonstrate constructions for binary sequences and for Boolean functions such that the associated merit factors asymptote to constant values for large sizes. These asymptotes result from convenient number-theoretic relationships for the sum-of-squares of the associated aperiodic autocorrelation coefficients.

The univariate merit factor ($\mathcal{MF}$) of a $(1,-1)$ binary sequence has been relatively well-studied [1–9] resulting in a few well-known constructions based on quadratic residues which have tried to maximise *asymptotic merit factor* $\mathcal{F}$ [6–8, 10]. Until recently there was a longstanding conjecture [6, 10] that the maximum $\mathcal{F}$ achievable by an infinite binary construction is 6.0. In Section 2 we report on a recent construction by Kristiansen and Parker [11,12], independently obtained by Borwein, Choi, and Jedwab [13], that satisfies $\mathcal{F} > 6.3$. This result is discussed in detail elsewhere in this proceedings [14]. We also report on a variant of this construction which appears to achieve the same asymptote.

In comparison to the univariate case, merit factor for the multivariate case remains largely unstudied, apart from some activity with respect to aperiodic binary (two-dimensional) arrays (e.g. see [15]), and with respect to the periodic sum-of-squares metric for a Boolean function [16]. In Section 3 we consider the extreme multivariate case where each dimension is of size 2 and the alphabet is $(1, -1)$ binary. These multivariate 'arrays' are conveniently specified by Boolean functions. We are, therefore, interested here in merit factors of sequences described by Boolean functions [11, 17]. We demonstrate that, as with the one-dimensional case, the *multivariate merit factor* ($\mathcal{MMF}$) for infinite constructions often asymptotes to a constant value, at least for recursive quadratic constructions. These constructions exhibit linear recursive formulae for both univariate and multivariate sum-of-squares and, in these cases, asymptotic merit factors are easily computed. This research was initially inspired by a previous result by Høholdt, Jensen, and Justesen [5] who proved the recursion $\gamma_n = 2\gamma_{n-1} + 8\gamma_{n-2}$ for the univariate sum-of-squares of the *Golay-Rudin-Shapiro sequence* of length 2^n [18–20].

In Section 4 we discuss our aim to characterise and evaluate *quantum merit factor* ($\mathcal{QMF}$) of a Boolean function where, in this context, the Boolean function of n binary variables is actually interpreted as a pure quantum multipartite state of n quantum bits (qubits) [21, 22]. $\mathcal{QMF}$ quantifies the degree of uniformity of energy distribution for the state with respect to the set of transform spectra resulting from the infinite set of transforms comprising all n-fold tensor products of 2×2 unitary matrices. High $\mathcal{QMF}$ indicates a high degree of uncertainty as to the joint value obtained by observing the n qubits in any local measurement basis and is a measure of entanglement of the n qubits [23–25]. Using brute-force algorithms on classical computers, it is not possible to compute $\mathcal{QMF}$ beyond about $n = 4$ qubits to any reasonable accuracy. It is therefore desirable to find faster algorithms to evaluate $\mathcal{QMF}$, and to recursively construct 'graphical' quantum states (*quantum graphs*) [21, 26–30] such that their $\mathcal{QMF}$ is computed precisely via simple recursive relationships for their quantum sum-of-squares. This paper achieves both these goals. The second goal is motivated, in part, by the recent proposal for *measurement-driven quantum computation* based on the idea of pre-entangling an array of qubits, where quantum computation is then undertaken by a series of well-chosen quantum measurements [23, 24, 26, 31]. The form of inter-qubit pre-entanglement chosen for the array can be modelled, precisely, by a quadratic Boolean function of n variables, as shown by Parker and Rijmen at SETA01 [21]. Moreover, *stabilizer quantum error-correcting codes* (QECCs) are exactly described using quadratic Boolean functions [27–30]. So the metric of $\mathcal{QMF}$ can be used to evaluate *entanglement* of a graph-based multipartite quantum state (QECC), where large $\mathcal{QMF}$ indicates high entanglement [1] .

In Section 5 we back off somewhat from the problem of $\mathcal{QMF}$ to consider the evaluation of something we call *Clifford merit factor* ($\mathcal{CMF}$). Instead of computing merit factor with respect to the infinite set of transforms formed from tensor products of all 2×2 unitary transforms we, instead, compute merit factor with respect to the finite set of transforms formed from tensor products of members of the *Local Clifford Group* [30, 33–35]. $\mathcal{CMF}$ is a natural generalisation of $\mathcal{MMF}$ as it is computed via a collection of *fixed-multivariate* aperiodic autocorrelations over the set of all possible fixings [36], and gives a good indication of the quantum energy distribution for the associated quantum state. We further show that $\mathcal{CMF}$ is a measure of quantum entanglement of the associated multipartite state as it remains invariant with respect to local unitary transform of the state. We also, quite unexpectedly [2], arrive at the conclusion that $\mathcal{CMF}$ is precisely equal to $\mathcal{QMF}$. We also find that, for recursively constructed graphs, $\mathcal{CMF}$ can, once again, be exactly computed via sum-of-squares recursions. $\mathcal{CMF}$ is typically maximised over quadratic Boolean functions which describe zero-dimension QECCs with maximum distance [22, 33, 35–39]. Graphs constructed from adjacency matrices of a bordered-quadratic residue form tend to maximise $\mathcal{CMF}$ [30]. This nicely mirrors the univariate situation where quadratic residue constructions are central to the optimisation of $\mathcal{MF}$.

We conclude by listing some interesting open problems that this research suggests.

1.1 Key To Notation

We introduce some of the notation and fundamental spectral concepts that we use. All of the metrics discussed can be viewed as arising from the output spectra with respect to unitary transforms over complex space (i.e. the result of a set of matrix-vector products).

Consider matrix-vector products, Ts, in complex space, where T is a $2^n \times 2^n$ unitary matrix, and s is a $2^n \times 1$ vector, where both matrix and vector have entries from $\mathbb{C}$. 'Unitary' means that $TT^\dagger = I$, where '$\dagger$' means conjugate-transpose and I is the identity matrix. Transform T is constructed using the following unitary primitives:

$$U(\theta, \phi) = \begin{pmatrix} \cos\theta & \sin\theta e^{i\phi} \\ \sin\theta & -\cos\theta e^{i\phi} \end{pmatrix}, \qquad 0 \le \theta < \frac{\pi}{2}, \quad 0 \le \phi < \pi, \tag{1}$$

where $i^2 = -1$.

Define $I, H, N \in \{U\}$, where
$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$.

[1] QMF satisfies the requirement for an entanglement metric that it is invariant with respect to local unitary transform of the associated state [21, 32].

[2] It was not the author's original intention to establish the equivalence of $\mathcal{CMF}$ and $\mathcal{QMF}$ but it appears that they are equivalent.

Define the *tensor product* (or *Kronecker product*) as:

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

We introduce the notion of a set of identically-dimensioned unitary matrices, $\{A_0, A_1, \ldots, A_{k-1}\}$, such that an associated set, $\{A_0, A_1, \ldots, A_{k-1}\}^n$, comprises all n-fold tensor products of members of $\{A_0, A_1, \ldots, A_{k-1}\}$, giving a total of k^n unitary matrices, each of size $2^n \times 2^n$.

Example: $\{H\}^n = H \otimes H \otimes \ldots \otimes H$ defines a set of one $2^n \times 2^n$ unitary matrix, which implements the *Walsh-Hadamard* transform.

Example: $\{I, H\}^n = \{I \otimes \ldots \otimes I \otimes I, \quad I \otimes \ldots \otimes I \otimes H, \quad I \otimes \ldots \otimes H \otimes I, \quad I \otimes \ldots \otimes H \otimes H, \quad \ldots \quad H \otimes \ldots \otimes H \otimes H\}$ defines a set of 2^n distinct unitary matrices of size $2^n \times 2^n$ which implement the so-called $\{I, H\}^n$*-transform*.

Let $\mathcal{D}$ be the set of all diagonal and antidiagonal 2×2 unitary matrices. Thus

$$\mathcal{D} = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}, \} \tag{2}$$

$\forall a, b, c, d$ such that $|a| = |b| = |c| = |d| = 1$.

We use '$\simeq$' to indicate that two $2^n \times 2^n$ matrices A and B are $\mathcal{D}$*-equivalent*, where,

$$A \simeq B \quad \Rightarrow \quad A = \Delta B \qquad \text{for some } \Delta \in \mathcal{D}^n. \tag{3}$$

Then $\mathcal{D}^n\{U\}^n$ comprises all $2^n \times 2^n$ local unitary transforms.

We further define $\{V\} = \{U\}_{\theta=\pi/4}$, i.e. V is the subset of U where all matrix entries have the same magnitude. We also define the infinite transform sets $\{W\} \simeq \{V\}N$ and $\{X\} \simeq \{W\}N$. We can partition $\{V\}$ into matrix pairs, F_α and F'_α, where,

$$\{V\} = \{F_\alpha, F'_\alpha \quad | \quad \forall \alpha \in \mathcal{C}, |\alpha| = 1, \quad 0 \le \angle\alpha < \frac{\pi}{2}\}, \tag{4}$$

where $F_\alpha = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \alpha \\ 1 & -\alpha \end{pmatrix}$, and $F'_\alpha = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i\alpha \\ 1 & -i\alpha \end{pmatrix}$. The rows of F_α relate to the residue system, mod $(x-\alpha)(x+\alpha) = (x^2-\alpha^2)$, as left-multiplication of a vector, s, by F_α can be interpreted as evaluating the residues of $s(x) = s_0 + s_1 x$ mod $(x - \alpha)$ and mod $(x + \alpha)$. Similarly, the rows of F'_α relate to a residue system, mod $(x - i\alpha)(x + i\alpha) = (x^2 + \alpha^2)$. The combined rows of F_α and F'_α therefore relate to a residue system, mod $(x^4 - \alpha^4)$.

1.2 Useful Example

Here is an example of the spectral computations underlying $\mathcal{MF}$, $\mathcal{MMF}$, and $\mathcal{CMF}$. Let $p(\mathbf{x}) : Z_2^n \to Z_2$ be the Boolean function $p(\mathbf{x}) = x_0 x_1$, where $n = 2$. From p we create a 4×1 bipolar vector, $s = (s_{00}, s_{01}, s_{10}, s_{11})^T$, where

$s_{ab} = (-1)^{p(x_0=a,x_1=b)}$. Thus $s = (-1)^{p(\mathbf{x})} = (1,1,1,-1)^T$. One computes the merit factor by first computing the *sum-of-squares* metric. This, in turn, can be computed directly by computing the sum-of-squares of the out-of-phase autocorrelation coefficient magnitudes, but here we, equivalently, sum the fourth powers of spectral magnitudes, whilst retaining the nomenclature 'sum-of-squares' for the resultant *sum-of-squares* metric.

To compute $\mathcal{MF}$ for p we proceed as follows, where $N = 2^n = 4$:

– $S = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} s = (1, i, 1, -i)^T$.
– $S' = \frac{1}{2}\begin{pmatrix} 1 & \omega & i & \omega^3 \\ 1 & \omega^3 & -i & \omega \\ 1 & \omega^5 & i & \omega^7 \\ 1 & \omega^7 & -i & \omega^5 \end{pmatrix} s = \frac{1}{\sqrt{2}}(1+\omega, -1+\omega^7, -1+\omega, 1+\omega^7)^T$,
where $\omega = \sqrt{i}$.
– The univariate sum-of-squares, γ, is
$\gamma = \frac{1}{2}(\frac{N}{2}(\sum_k |S_k|^4 + \sum_k |S'_k|^4) - N^2) = \frac{1}{2}(\frac{4}{2}(4+6) - 16) = 2$.
– $\mathcal{MF} = \frac{N^2}{2\gamma} = 4.0$.

To compute $\mathcal{MMF}$ for p we proceed as follows, where $n = 2$:

– $S^{00} = (H \otimes H)s = (1,1,1,-1)^T$.
– $S^{01} = (H \otimes N)s = (1,1,i,-i)^T$.
– $S^{10} = (N \otimes H)s = (1,i,1,-i)^T$.
– $S^{11} = (N \otimes N)s = (1+i,0,0,1-i)^T$.
– The multivariate sum-of-squares, σ, is
$\sigma = \frac{1}{2}((\sum_{\mathbf{r}\in\{0,1\}^n} \sum_{\mathbf{k}\in\{0,1\}^n} |S^{\mathbf{r}}_{\mathbf{k}}|^4) - 4^n) = \frac{1}{2}(4+4+4+8-16) = 2$.
– $\mathcal{MMF} = \frac{4^n}{2\sigma} = 4.0$.

To compute $\mathcal{CMF}$ for p we proceed as follows, where $n = 2$:

– $S^{00} = (I \otimes I)s = (1,1,1,-1)^T$.
– $S^{01} = (I \otimes H)s = (\sqrt{2},0,0,\sqrt{2})^T$.
– $S^{02} = (I \otimes N)s = (\omega,\omega^7,\omega^7,\omega)^T$.
– $S^{10} = (H \otimes I)s = (\sqrt{2},0,0,\sqrt{2})^T$.
– $S^{11} = (H \otimes H)s = (1,1,1,-1)^T$.
– $S^{12} = (H \otimes N)s = (1,1,i,-i)^T$.
– $S^{20} = (N \otimes I)s = (\omega,\omega^7,\omega^7,\omega)^T$.
– $S^{21} = (N \otimes H)s = (1,i,1,-i)^T$.
– $S^{22} = (N \otimes N)s = (1+i,0,0,1-i)^T$.
– The fixed-multivariate sum-of-squares, $\mathcal{E}$, is
$\mathcal{E} = \frac{1}{2}((\sum_{\mathbf{r}\in\{0,1,2\}^n} \sum_{\mathbf{k}\in\{0,1\}^n} |S^{\mathbf{r}}_{\mathbf{k}}|^4) - 6^n) = \frac{1}{2}(4+8+4+8+4+4+4+4+8-36) = 6$.
– $\mathcal{CMF} = \frac{6^n}{2\mathcal{E}} = 3.0$.

1.3 The Rough Guide to Transform Spectra

We also provide a "map" (Fig. 1) that indicates the types of spectra we will be dealing with and how they relate to each other. For simplicity, the map only deals with input sequences, s, of length 2^n. The map represents sets of spectral outputs, S, by their associated transforms, T, from which S is computed where $S = Ts$, and the different forms of T are indicated on the map. All three metrics, $\mathcal{MF}$, $\mathcal{MMF}$, and $\mathcal{CMF}$, describe a property of an infinite spectral set - indicated on the map by an infinite set of transforms - but, as just shown in the example, each of the three metrics can be computed using only a finite set of spectral points. For sequences of length $N = 2^n$, the spectral outputs with respect to (w.r.t.) the univariate continuous Fourier transform occur as a strict subset of the spectral set $\{S\} = \{V\}^n s$ [40]. For example the univariate spectral points generated by rows of the matrix:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

can be found as a subset of the rows of the matrices $H \otimes H$ and $N \otimes H$. The matrix multisets $\{V^I\}$, $\{W^N\}$, and $\{X^H\}$, are defined in definitions 9 and 16.

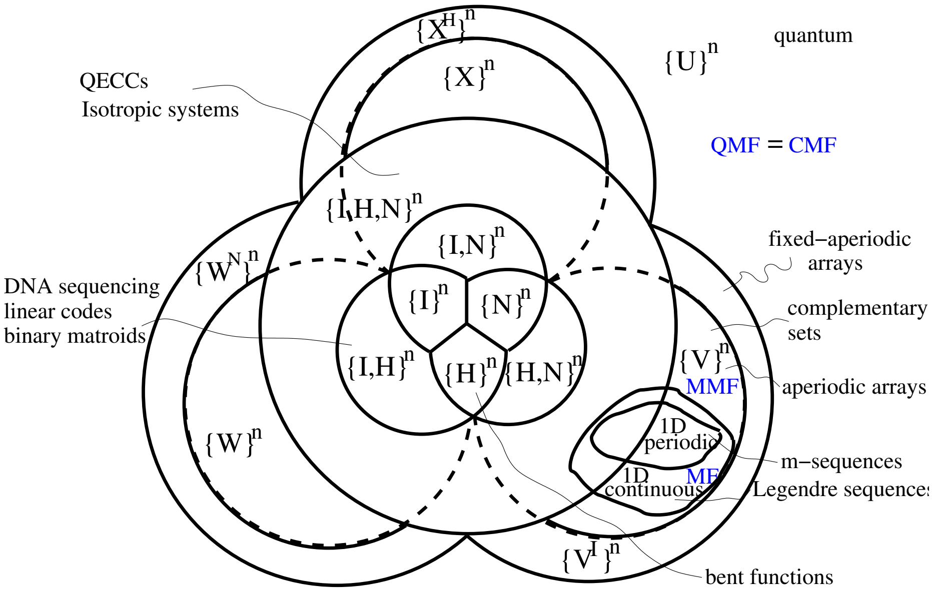


Fig. 1. Map of spectral outputs described by their associated transforms

2 Univariate merit factor

The univariate aperiodic autocorrelation of s is given by,

$$u_k = \sum_{j=0}^{N-1} s_j s_{j+k}^*, \qquad -N < k < N, \tag{5}$$

where $s_j = 0$, $N \geq j < 0$.

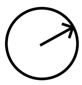
Alternatively, by representing s as a polynomial $s(z) = s_0 + s_1 z + \ldots + s_{N-1}z^{N-1}$, we can express u as $u(z) = u_{1-N}z^{1-N} + u_{2-N}z^{2-N} + \ldots + u_{N-2}z^{N-2} + u_{N-1}z^{N-1}$, where

$$u(z) = s(z)s(z^{-1})^*. \tag{6}$$

Using the polynomial form for s, define the *univariate continuous fourier transform* of s by,

$$S_k(L,c) = \frac{1}{\sqrt{N}} s(e^{\frac{\pi i(2tk+c)}{L}}), \qquad 0 \leq k < N, \tag{7}$$

where $L = tN$, $t \in \{1,2,\ldots,\infty\}$, with $c \in \{\{1,2,\ldots,2t-1\} | \gcd(c,2t) = 1\} + \{0,t\} \bmod 2t$ if t odd, and $c \in \{\{1,2,\ldots,2t-1\} | \gcd(c,2t) = 1\}$ if t even. Each (L,c) pair defines a different $N \times N$ unitary transform, $T(L,c)$, such that $S(L,c) = T(L,c)s$, where $T_{kj}(L,c) = \frac{1}{\sqrt{N}} e^{\frac{\pi ij(2tk+c)}{L}}$ and the infinite set of spectral points, $\{S_k(L,c)\}$, for valid triples (k,L,c) approximates the continuous univariate Fourier transform spectra infinitely closely. Therefore (7) evaluates $s(z)$ at all points on the unit circle. We symbolically represent this evaluation as


.

Definition 1 *The* sum-of-squares, γ, *of the sequence,* s, *is given by,*

$$\gamma = \frac{1}{2}((\sum_{k=1-N}^{N-1} |u_k|^2) - N^2) = \sum_{k=1}^{N-1} |u_k|^2. \tag{8}$$

Definition 2 *The* merit factor, $\mathcal{MF}$, *of the sequence,* s, *is given by,*

$$\mathcal{MF} = \frac{N^2}{2\gamma}. \tag{9}$$

Definition 3 *Let* $s_{\mathcal{A}}$ *be a length* N *sequence generated by construction* $\mathcal{A}$. *Then the* asymptotic merit factor *of* $s_{\mathcal{A}}$ *is given by,*

$$\mathcal{F} = \lim_{N \to \infty} \mathcal{MF}(s_{\mathcal{A}}).$$

2.1 Transform $\Leftrightarrow$ Autocorrelation Duality

The *Wiener-Kinchine theorem* states that (5) and (7) are related by

$$\sum_{k=1-N}^{N-1} |u_k|^2 = \frac{N}{2}\left(\sum_{k=0}^{N-1} |S_k(L,c)|^4 + |S_k(L,c')|^4\right), \tag{10}$$

where $c' = c + t \bmod 2t$, $c = 0$ if $t = 1$, $c \in \{\{1, 2, \ldots, 2t-1\} | \gcd(c, 2t) = 1\}$ if t odd, and $c \in \{\{1, 2, \ldots, t-1\} | \gcd(c, 2t) = 1\}$ if t even. The reason for the choice of pairings (c, c') becomes clear when we consider an embedding of the non-modular polynomial multiplication (6) in a polynomial modulus (i.e. we realise an aperiodic autocorrelation using a constaperiodic autocorrelation). Specifically, let

$$u'(z) = s(z)s(z^{-1})^* \bmod (z^{2N} - \epsilon), \tag{11}$$

where ϵ is a complex root of one of order t, $t \in \{1, 2, \ldots, \infty\}$. Then,

$$\begin{array}{ll} u'_k = u_k, & 0 \le k < N, \\ u'_k = \epsilon^{-1} u_{k-2N}, & N < k < 2N, \\ u'_k = u'_N = 0 & \text{otherwise.} \end{array}$$

In particular,

$$\sum_{k=0}^{2N-1} |u'_k|^v = \sum_{k=1-N}^{N-1} |u_k|^v, \qquad \forall v. \tag{12}$$

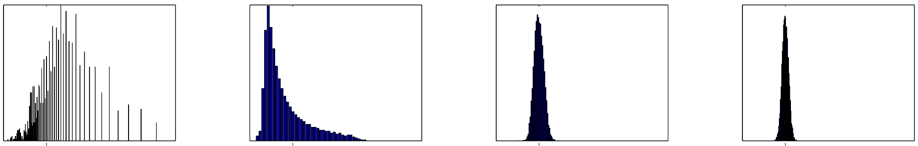
So, from (8), we can use (11) instead of (6) to compute γ. (10) follows directly from (11) and (12) because we can factorise (11) into two residue computations mod $(z^N - \eta)$ and mod $(z^N + \eta)$, where η is a complex root of one of order $2t$ such that $\eta^2 = \epsilon$. Then $s(z)s(z^{-1})^*$ mod $(z^N - \eta)$ and $s(z)s(z^{-1})^*$ mod $(z^N + \eta)$ can be computed by evaluating $s(z)s(z^{-1})^*$ at the N residues $z \in \{e^{\frac{\pi i(2tk+c)}{L}} | 0 \le k < N\}$, and at the N residues $z \in \{e^{\frac{\pi i(2tk+c')}{L}} | 0 \le k < N\}$, respectively. In particular $u'(e^{\frac{\pi i(2tk+d)}{L}}) = |S_k(L,d)|^2$, $d \in \{c, c'\}$. One then obtains (10) by Parseval (or the Chinese Remainder Theorem). The main point here is that we obtain (10) and exactly the same value of γ for any choice of complex root, ϵ, of order $2t$. By considering all such ϵ, $|S_k(L,d)|$ ranges over the continuous fourier magnitude spectrum and, therefore, as γ is independent of ϵ, γ evaluates a property of the continuous fourier spectra, namely the mean-square deviation from the flat continuous fourier power spectrum. Specifically,

$$\gamma = \frac{1}{4\pi} \int_0^{2\pi} (|s(e^{i\omega})|^2 - N)^2 d\omega.$$

In this paper we choose to compute γ by selecting $\epsilon = 1$, leading to $L = N$ and $(c, c') = (0, 1)$, and allowing us to abbreviate $S_k(L,d)$ to S_k and S'_k for $d = c$ and $d = c'$, respectively, as done in Section 1.2.

2.2 Expected Values and Constructions

The maximum merit factor known is for the length $N = 13$ sequence, 0101001100000, for which $\mathcal{MF} = 14.083$, although there is no proof that this is the true maximum over all N. $\mathcal{F}$ exists for many infinite sequence constructions. Experimental results suggest that, for a random binary sequence, $\mathcal{F} = 1.0$, as indicated by the following graphs of random samplings for (from left to right) $N = 16$, 64, 512, and 1024, with merit factor and # sequences on x and y-axes, respectively, with x-axes ranging linearly from 0 to 4, and where the highest peak is centred around $\mathcal{MF} = 1.0$ ever more tightly as N increases (we leave the graph axes unmarked as we simply wish to indicate the general trend as N increases):



Although binary sequences with merit factors around 8.0 or 9.0 have been found up to lengths $N = 250$, the maximum known asymptotic merit factor was, until recently, $\mathcal{F} = 6.0$. This asymptote is satisfied by the *Legendre* construction [6, 10, 41], the *Jacobi* and *modified Jacobi* construction [8, 42], and is conjectured to be satisfied by a negaperiodic construction of Parker [43]. In his recent master's thesis [11], Kristiansen describes a construction based on an extended Legendre sequence which satisfies, experimentally, $\mathcal{F} > 6.3$. Independently, Borwein, Choi and Jedwab [13] proposed a construction which satisfies, experimentally, $\mathcal{F} = 6.3421\ldots$. These two constructions generate essentially the same sequence, although only [13] discovered the periodic form of the extension and provided theoretical arguments as to the precise values of the asymptote and construction parameters. Detailed descriptions of the constructions can be found in [12] and [13], and elsewhere in this publication [14]. Both Kristiansen and Parker, and Borwein, Choi and Jedwab were influenced by prior work of two master's students of Jim Davis, Kirilusha and Narayanaswamy [44], who first developed the essential form of the construction by realising that extending a $\frac{1}{4}$-rotated Legendre sequence by up to $O(\sqrt{N})$ elements does not change $\mathcal{F}$ from 6.0. Moreover they noticed that if the extension was periodic they could even increase $\mathcal{F}$ above 6.0, although they did not uncover an asymptote. A summary of some of the constructions with large $\mathcal{F}$ is now given.

Legendre Construction [10]

- Select a prime integer, m.
- Construct the $\{1, -1\}$ sequence, $l = (l_0, l_1, \ldots, l_{m-1})^T$, of length m, such that $l_j = 1$ if $\exists k$ such that $k^2 = j \bmod m$, (in which case j is called a *quadratic residue*, mod m). Otherwise $l_j = -1$. By convention, $l_0 = 1$.

– Construct s as the periodic rotation of l by $\frac{1}{4}$ of its length:

$$s_j = l_{j+\lfloor \frac{m}{4} \rfloor \bmod m}.$$

l is the *Legendre sequence* and satisfies $\mathcal{F}(l) = 1.5$.

Theorem 1 *For s a $\frac{1}{4}$-rotated Legendre sequence:*

$$\mathcal{F}(s) = 6.0.$$

Construction - Borwein, Choi and Jedwab [13]

– Construct a Legendre sequence, l, using a prime, m.
– Construct l^r to be a periodic rotation of l by $0.2211m$ (or by $0.7211m$):

$$l^r_j = l_{j+\lfloor rm \rfloor \bmod m}, \qquad r \in \{0.2211, 0.7211\}.$$

– Construct the length $1.0578m$ "BCJ-sequence", s, as the periodic extension of l^r by $0.0578m$:

$$s_j = l^r_j, \qquad 0 \le j < m, \qquad\qquad s_{j+m} = l^r_j, \qquad 0 \le j \le \lfloor 0.0578m \rfloor.$$

Conjecture 1 *For s a "BCJ-sequence":*

$$\mathcal{F}(s) = 6.3421\ldots.$$

Construction - Kristiansen [11, 12]

– Construct a Legendre sequence, l, using a prime, m.
– Assign $k = 0$ and $l^k = l$.
– Step A: Construct l^+ and l^- as the periodic and negaperiodic rotations of l^k by one element:

$$l^+_j = l^k_{j+1 \bmod m}, \qquad\qquad l^-_j = (-1)^{\lfloor \frac{j+1}{m} \rfloor} l^k_{j+1 \bmod m}, \qquad\qquad 0 \le j < m.$$

– If $\mathcal{MF}(l^+) \ge \mathcal{MF}(l^-)$ then assign $l^{k+1} = l^+$ else assign $l^{k+1} = l^-$.
– Assign $k = k + 1$.
– If $k < 0.31m$ then loop back to step A.
– Construct the sequence, $\mathcal{T}$, such that,

$$\mathcal{T} = l|l^1_{m-1}|l^2_{m-1}| \ldots |l^k_{m-1},$$

where '$a|b$' means concatenate b onto the end of a.

– Construct the "K-sequence", s^r, of length $\lfloor 1.059m \rfloor$, such that,

$$s^r_j = \mathcal{T}_{j+rm}, \qquad 0 \le j < \lfloor 1.059m \rfloor,$$

where $r < 0.242m$.

Conjecture 2 *For s_r a "K-sequence", $\exists r$ such that*

$$\mathcal{F}(s^r) > 6.3\ldots.$$

The intuition behind the construction of Kristiansen and Parker is that a sequence with high merit factor should contain subsequences with moderately high merit factor. After becoming aware of the preprint [13], Kristiansen and Parker realised that, in all but four small-length cases, $\mathcal{MF}(l^+)$ appears to be always greater than $\mathcal{MF}(l^-)$ for each k-iteration. It follows that, to within some inaccuracies in periodic extension and rotation length, the optimal "K-sequence" is the "BCJ-sequence".

Construction - Parker

Empirical evidence indicates that the asymptote of $\mathcal{F}(s) = 6.3421\ldots$ also holds true for a periodic rotation and extension of the (modified)-Jacobi construction. We here summarise yet another construction that appears to satisfy the same asymptote, namely the negaperiodic rotation and extension of the negaperiodic construction of [43].

– Construct a Legendre sequence, l, using a prime, m.
– Construct $\mathcal{N}$ such that

$$\mathcal{N} = (l|l) \odot (1, 1, -1, -1, 1, 1, -1, -1, \ldots)^T,$$

where '$a|b$' is the concatenation of vectors, and $(w) = (u) \odot (v)$ implies $w_i = u_i v_i$.
– Construct $\mathcal{N}^r$ as the negaperiodic rotation of l by $0.4705(2m)$ (or by $0.9705(2m)$):

$$\mathcal{N}^r_j = (-1)^{\frac{h}{2m}} \mathcal{N}_{h \bmod 2m},$$

where $h = j + \lfloor r(2m) \rfloor$, $0 \le j < 2m$, and $r \in \{0.4705, 0.9705\}$.
– Construct the length $1.0578(2m)$ "P-sequence", s, as the negaperiodic extension of $\mathcal{N}^r$ by $0.0578(2m)$:

$$s_j = \mathcal{N}^r_j, \qquad 0 \le j < 2m, \qquad\qquad s_{j+2m} = -\mathcal{N}^r_j, \qquad 0 \le j \le \lfloor 0.0578(2m) \rfloor.$$

Conjecture 3

$$\mathcal{F}(\mathcal{N}) = 6.0.$$

Conjecture 4 *For s a "P-sequence":*

$$\mathcal{F}(s) = 6.34\ldots.$$

An alternative periodic version of the same construction is as follows.

– Construct a Legendre sequence, l, using a prime, m.
– Construct $\mathcal{L}$ such that
$$\mathcal{L} = (l|l)$$
– Construct $\mathcal{L}^r$ as the periodic rotation of l by $0.4705(2m)$ (or by $0.9705(2m)$):
$$\mathcal{L}^r_j = \mathcal{L}_{j+\lfloor r(2m)\rfloor \bmod 2m},$$
where $0 \leq j < 2m$ and $r \in \{0.4705, 0.9705\}$.
– Construct the length $1.0578(2m)$ sequence, s', as the periodic extension of $\mathcal{L}^r$ by $0.0578(2m)$:
$$s'_j = \mathcal{L}^r_j, \qquad 0 \leq j < 2m, \qquad\qquad s'_{j+2m} = \mathcal{L}^r_j, \qquad 0 \leq j \leq \lfloor 0.0578(2m)\rfloor.$$
– Construct the length $1.0578(2m)$ "P-sequence", s, such that
$$s = s' \odot (1, 1, -1, -1, 1, 1, -1, -1, \ldots)^T.$$

The Golay-Rudin-Shapiro Construction

Both the *m-sequence* and *Golay-Rudin-Shapiro sequence* [18–20] satisfy $\mathcal{F} = 3.0$. The latter construction can be described using Boolean functions as shown by Davis and Jedwab [45]. Define $p(\mathbf{x}) : \mathcal{Z}_2^n \rightarrow \mathcal{Z}_2$ as

$$p(\mathbf{x}) = (\sum_{i=0}^{n-2} x_{\pi(i)}x_{\pi(i+1)}) + (\sum_{i=0}^{n-1} c_i x_i) + d, \tag{13}$$

where $\pi : \mathcal{Z}_n \rightarrow \mathcal{Z}_n$ is a permutation of the integers, mod n, $c_i, d \in \mathcal{Z}_2$.

– Construct the length 2^n sequence, s^π, such that,
$$s^\pi_j = (-1)^{p(x_i = j_i)}, \tag{14}$$
where $j = \sum_{i=0}^{n-1} 2^{j_i}$ and $j_i \in \{0, 1\}$, $\forall i$.

Theorem 2 *[1, 5] When π is the identity permutation, then $s = s^\pi$ is the Golay-Rudin-Shapiro sequence and*

$$\mathcal{F}(s) = 3.0.$$

Proof. Let γ_n be the sum-of-squares for s constructed from p over n binary variables. It can be shown that [5],

$$\gamma_n = 2\gamma_{n-1} + 8\gamma_{n-2}.$$

In closed form, $\gamma_n = \frac{4^n}{6} - \frac{(-2)^n}{6}$. The asymptote follows from (9) as $n \to \infty$. $\square$

Remark: It is currently unclear whether $\mathcal{F}(s^\pi) = 3.0$ over the complete set of permutations, π, or whether asymptotes above and below 3.0 can be obtained by suitable choice of permutation [11]. For instance, for $n = 8$, $2.27 \le \mathcal{MF}(s^\pi) \le 4.49$.

Other Graphical Constructions

Quadratic Boolean functions, $p(\mathbf{x})$, have a natural interpretation as graphs where, for $p(\mathbf{x}) = \sum_{i<j} a_{ij}x_ix_j$, the adjacency matrix, Γ, of the associated graph satisfies $\Gamma_{ij} = \Gamma_{ji} = a_{ij}$ for $i < j$ and $\Gamma_{ii} = 0$. Thus one can view the Golay-Rudin-Shapiro sequence as the *path graph* with a particular ordering of the vertices. Table 1 summarises conjectures, first presented in [17], as to the value of $\mathcal{MF}$ for a few other simple recursive graph constructions.

graph	$p(\mathbf{x})$	$\mathcal{F}(s)$	γ_n - recursion
circle	$(\sum_{i=0}^{n-2} x_ix_{i+1}) + x_{n-1}x_0$	1	$4\gamma_{n-1} + 12\gamma_{n-2} - 64\gamma_{n-3} + 256\gamma_{n-5}$
complete	$\sum_{i<j,1\le j<n} x_ix_j$	0	$\gamma_n = 10\gamma_{n-1} - 36\gamma_{n-2} + 88\gamma_{n-3}$
			$-96\gamma_{n-4} - 512\gamma_{n-5} + 1024\gamma_{n-6}$
star	$x_0(x_1 + x_2 + \ldots + x_{n-1})$	0	$\gamma_n = 16\gamma_{n-1} - 68\gamma_{n-2} - 48\gamma_{n-3}$
			$+768\gamma_{n-4} - 1024\gamma_{n-5}$

Table 1. Conjectures on $\mathcal{F}$ for certain graphical constructions

3 Multivariate merit factor

The multivariate merit factor $\mathcal{MMF}$ was first investigated by Gulliver and Parker in [17], as a modification of the metric first introduced by Kristiansen in [11]. Define the multivariate sequence, s, with each dimension of s of length 2, such that,

$$\begin{array}{ll} s = (s_{0\ldots00}, s_{0\ldots01}, s_{0\ldots10}, \ldots, s_{1\ldots11})^T & \\ s_{\mathbf{j}} \in \{1,-1\}, & \mathbf{j} \in \{0,1\}^n \\ s_{\mathbf{j}} = 0, & \text{otherwise.} \end{array}$$

The multivariate sequence, s, is always, in this paper, constructed via its associated Boolean function, p, such that,

$$s = (-1)^{p(\mathbf{x})},$$

where $s_{\mathbf{j}} = (-1)^{p(\mathbf{x}=\mathbf{j})}$, and $\mathbf{x}, \mathbf{j} \in \mathcal{Z}_2^n$.

The *multivariate aperiodic autocorrelation* of s is given by,

$$u_{\mathbf{k}} = \sum_{\mathbf{j} \in \{0,1\}^n} s_{\mathbf{j}} s^*_{\mathbf{j}+\mathbf{k}}, \qquad \mathbf{k} \in \{-1,0,1\}^n. \tag{15}$$

Alternatively, by representing s as a multivariate polynomial,

$$s(z_0, z_1, \ldots, z_{n-1}) = s_{0\ldots00} + s_{0\ldots01} z_0 + s_{0\ldots10} z_1 + \ldots + s_{1\ldots11} z_{n-1} \ldots z_1 z_0,$$

we can compute u where,

$$u(z_0, z_1, \ldots, z_{n-1}) = s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})^*. \tag{16}$$

Define the *multivariate continuous fourier transform* of s by,

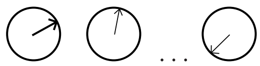
$$S_{\mathbf{k}}(\mathbf{L}, \mathbf{c}) = 2^{-\frac{n}{2}} s(z_j = e^{\frac{\pi i (2t_j k_j + c_j)}{L_j}} \quad | \quad 0 \le j < n), \qquad \mathbf{k} \in \{0,1\}^n, \tag{17}$$

where $\mathbf{L} = 2\mathbf{t}$, $t_j \in \{1, 2, \ldots, \infty\}$, with $c_j \in \{\{1, 2, \ldots, 2t_j - 1\} | \gcd(c_j, 2t_j) = 1\} + \{0, t_j\} \bmod 2t_j$ if t_j odd, and $c_j \in \{\{1, 2, \ldots, 2t_j - 1\} | \gcd(c_j, 2t_j) = 1\}$ if t_j even. Each $(\mathbf{L}, \mathbf{c})$ pair defines a different $2^n \times 2^n$ unitary transform, $T(\mathbf{L}, \mathbf{c})$, such that $S(\mathbf{L}, \mathbf{c}) = T(\mathbf{L}, \mathbf{c}) s$, where

$$T(\mathbf{L}, \mathbf{c}) = 2^{-\frac{n}{2}} \bigotimes_{j=0}^{n-1} \begin{pmatrix} 1 & e^{\frac{\pi i c_j}{L_j}} \\ 1 & -e^{\frac{\pi i c_j}{L_j}} \end{pmatrix},$$

and the infinite set of spectral points, $\{S_{\mathbf{k}}(\mathbf{L}, \mathbf{c})\}$, for valid vector triples $(\mathbf{k}, \mathbf{L}, \mathbf{c})$ approximates the continuous multivariate Fourier transform spectra infinitely closely. From section 1.1 it is apparent that

$$\{T(\mathbf{L}, \mathbf{c})\} = \{V\}.$$

(17) evaluates $s(z_0, z_1, \ldots, z_{n-1})$ at all points on the multi-unit circle. We symbolically represent this evaluation as  .

Definition 4 *The* multivariate sum-of-squares, *σ, of the sequence, s, is given by,*

$$\sigma = \frac{1}{2}\left(\left(\sum_{\mathbf{k} \in \{-1,0,1\}^n} |u_{\mathbf{k}}|^2\right) - 4^n\right) = \frac{1}{2} \sum_{\mathbf{k} \in \{-1,0,1\}^n, \mathbf{k} \neq \mathbf{0}} |u_{\mathbf{k}}|^2. \tag{18}$$

Definition 5 *The* multivariate merit factor, *$\mathcal{MMF}$, of the sequence, s, is given by,*

$$\mathcal{MMF} = \frac{4^n}{2\sigma}. \tag{19}$$

Definition 6 *Let $s_{\mathcal{A}}$ be a length 2^n multivariate sequence generated by construction $\mathcal{A}$. Then the* asymptotic multivariate merit factor *of $s_{\mathcal{A}}$ is given by,*

$$\mathcal{F}^{\mathcal{M}} = \lim_{n \to \infty} \mathcal{MMF}(s_{\mathcal{A}}).$$

$\mathcal{MMF}$ Symmetries

Lemma 1 *Let $s = (-1)^{p(\mathbf{x})}$, where p is a Boolean function of n variables. Let $s' = (-1)^{p'(\mathbf{x})}$, where*

$$p'(\mathbf{x}) = p(\tilde{x}_{\pi(0)}, \tilde{x}_{\pi(1)}, \ldots, \tilde{x}_{\pi(n-1)}) + (\sum_{i=0}^{n-1} c_i x_i) + d,$$

where $\tilde{x} \in \{x, x+1\}$, $\pi : \mathcal{Z}_n \rightarrow \mathcal{Z}_n$ is a permutation of the integers, mod n, and $c_i, d \in \mathcal{Z}_2$. Then,

$$\mathcal{MMF}(s') = \mathcal{MMF}(s).$$

3.1 Transform $\Leftrightarrow$ Autocorrelation Duality

Let $\mathbf{r} \in \{0,1\}^n$ and define $\mathbf{d}(\mathbf{r}) = (d(r)_0, d(r)_1, \ldots, d(r)_{n-1})$ such that

$$d(r)_j = c_j + r_j t_j, \ \bmod 2t_j,$$

where $c_j \in \{\{1,2,\ldots,2t_j-1\} | \gcd(c_j, 2t_j) = 1\}$ if t_j odd, and $c_j \in \{\{1,2,\ldots,t_j-1\} | \gcd(c_j, 2t_j) = 1\}$ if t_j even, $0 \le j < n$. A multivariate version of the *Wiener-Kinchine theorem* states that (15) and (17) are related by

$$\sum_{\mathbf{k} \in \{-1,0,1\}^n} |u_{\mathbf{k}}|^2 = \sum_{\mathbf{k},\mathbf{r} \in \{0,1\}^n} |S_{\mathbf{k}}(\mathbf{L}, \mathbf{d}(\mathbf{r}))|^4. \tag{20}$$

We realise the aperiodic autocorrelation by embedding the non-modular polynomial multiplication (16) in a polynomial modulus: Let

$$u'(z_0, z_1, \ldots, z_{n-1}) = s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})^* \bmod \prod_{j=0}^{n-1} (z_j^4 - \epsilon_j) \tag{21}$$

where ϵ_j is a complex root of one of order t_j, $t_j \in \{1, 2, \ldots, \infty\}$, $0 \le j < n$. Then, with $\mathbf{k} \in \{-1,0,1\}^n$ and $\mathbf{k}' \in \{0,1,3\}^n$,

$$u'_{\mathbf{k}'} = (\prod_{j=0}^{n-1} \epsilon_j^{-\lfloor \frac{k'_j}{2} \rfloor}) u_{\mathbf{k}}, \qquad k'_j = k_j \bmod 4.$$

In particular,

$$\sum_{\mathbf{k}' \in \{0,1,3\}^n} |u'_{\mathbf{k}'}|^v = \sum_{\mathbf{k} \in \{-1,0,1\}^n} |u_{\mathbf{k}}|^v, \qquad \forall v. \tag{22}$$

So, from (18), we can use u' instead of u to compute σ. (20) follows directly from (21) and (22) because we can factorise (21) into two residue computations per dimension, mod $(z_j^2 - \eta_j)$ and mod $(z_j^2 + \eta_j)$, where η_j is a complex root of one of order $2t_j$ such that $\eta_j^2 = \epsilon_j$. The two residue computations per dimension are realised by left-multiplication by matrices, F_{α_j} and F'_{α_j} (see (4)), where $\eta_j = \alpha_j^2$. Then, for each $\mathbf{r} \in \{0,1\}^n$, we compute $s(z_0, z_1, \ldots, z_{n-1})s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})^*$ mod $\prod_{j=0}^{n-1}(z_j^2 - (-1)^{r_j}\eta_j)$ by evaluating $s(z)s(z^{-1})^*$ at the 2^n residues, $z_j \in \{e^{\frac{\pi i(2t_j k_j + d(r)_j)}{L_j}} | \mathbf{k} \in \{0,1\}^n\}$. In particular $u'(z_j = e^{\frac{\pi i(2t_j k_j + d(r)_j)}{L_j}} \mid 0 \le j < n) = |S_{\mathbf{k}}(\mathbf{L}, \mathbf{d}(\mathbf{r}))|^2$. One then obtains (20) by Parseval (or the Chinese Remainder Theorem). We obtain (20) and exactly the same value of σ for any choice of vector of complex roots, $\bar{\epsilon} = (\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1})$, where ϵ_j has order t_j. The infinite set of transforms $\{V\}^n$ is obtained by considering all such $\bar{\epsilon}$, so that $|S_{\mathbf{k}}(\mathbf{L}, \mathbf{d}(\mathbf{r}))|$ ranges over the continuous multivariate fourier spectrum. Therefore, σ evaluates the mean-square deviation from the flat continuous multivariate fourier power spectrum. Specifically,

$$\sigma = \frac{1}{4\pi}\int_0^{2\pi}\int_0^{2\pi}\cdots\int_0^{2\pi}(|s(e^{i\omega_0}, e^{i\omega_1}, \ldots, e^{i\omega_{n-1}})|^2 - 2^n)^2 d\bar{\omega},$$

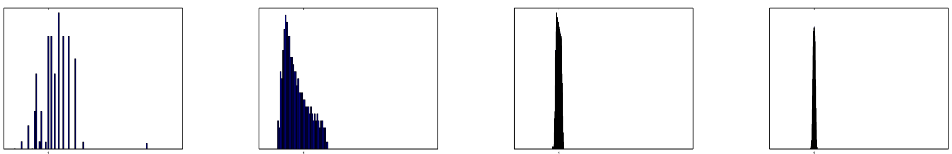
where $\bar{\omega} = (\omega_0, \omega_1, \ldots, \omega_{n-1})$.

In this paper we choose to compute σ by selecting $\bar{\eta} = (1, 1, \ldots, 1)$, leading to $L_j = 2$ and $(c_j, c'_j) = (0, 1)$, $\forall j$. Therefore $T(\mathbf{L}, \mathbf{c}) = \{H, N\}^n$ for H and N as defined in Section 1.1, and $S_{\mathbf{k}}(\mathbf{L}, \mathbf{d}(\mathbf{r}))$ can be abbreviated to $S_{\mathbf{k}}^{\mathbf{r}}$, as done in Section 1.2. $\{S_{\mathbf{k}}^{\mathbf{r}}\}$ is a set of 4^n spectral points.

3.2 Expected Values and Constructions

Maximising the $\mathcal{MMF}$ of a Boolean function indicates a minimum mean-square deviation from the flat continuous multivariate fourier power spectrum. Unlike the univariate case, the Boolean multivariate problem does not appear to have been investigated before [17]. Initial investigations suggest that the maximum $\mathcal{MMF}$ may be for the $n = 2$ variable sequence 0001, for which $\mathcal{MMF} = 4$. Table 3.2 shows the equivalence classes for Boolean functions of $n = 2$ to 5 variables, where the set of inequivalent functions is obtained from [46].

Experimental results suggest that, for a random Boolean function of n variables, $\mathcal{F}^{\mathcal{M}} = 1.0$, as indicated here by the random samplings for (from left to right) $n = 4, 6, 9$ and 10, where $\mathcal{MMF}$ and #sequences are x and y-axes, respectively, with x-axes ranging linearly from $\mathcal{MMF} = 0$ to 4, and where the highest peak approaches $\mathcal{F}^{\mathcal{M}} = 1.0$ as n increases.

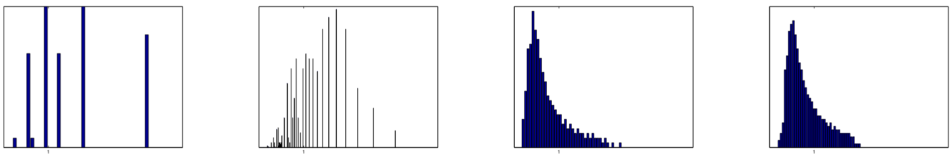


In comparison, a sampling of just quadratic Boolean functions for $n = 4, 6, 9$ and 10 indicates a wider range of $\mathcal{MMF}$s for a given n than for the full space of Boolean functions although, once again, the highest peak appears to approach

n	# inequivalent functions	# equivalence classes with list of $\mathcal{MMF}$s
2	2	2 classes **4.000**, 0.8
3	5	3 classes **2.667**, 1.143, 0.421
4	39	18 classes **3.200**, 1.778, 1.600, 1.455, 1.333, 1.231, 1.143, 1.067, 1.000, 0.941, 0.842, 0.800, 0.727, 0.696, 0.640, 0.552, 0.400, 0.246
5	22442	80 classes **2.909** − 0.152

Table 2. Complete set of multivariate merit factors for $n = 2$ to $n = 5$

$\mathcal{F}^{\mathcal{M}} = 1.0$ as n gets large. Once again, the x-axis ranges linearly from $\mathcal{MMF} = 0$ to 4 and the y-axis indicates #sequences.



Conjecture 5 *A random Boolean function satisfies,*

$$\mathcal{F}^{\mathcal{M}} = 1.0.$$

Definition 7 *Define $\mathcal{Q}$ to be the complete set of homogeneous quadratic Boolean functions over n variables, i.e. $q \in \mathcal{Q}$ iff $q = \sum_{j<k} c_{jk} x_j x_k$, $c_{jk} \in \mathcal{Z}_2$.*

Definition 8 *Let $\mathcal{S}$ be an arbitrary subset of n-variable Boolean functions. Define $\mathcal{S}_{\mathcal{Q}} = \{s + q \quad | \quad \forall s \in \mathcal{S}, q \in \mathcal{Q}\}$.*

Theorem 3 *The average value of $\frac{1}{\mathcal{MMF}}$ with respect to any set $\mathcal{S}_{\mathcal{Q}}$ is,*

$$\textit{average}_{\ \mathcal{S}_{\mathcal{Q}}}\left(\frac{1}{\mathcal{MMF}}\right) = \frac{2^n - 1}{2^n}.$$

Proof. Using arguments similar to [9], observe, from (16) and (18), that,

$$2\sigma + 4^n = \sum_{\mathbf{j}+\mathbf{k}=\mathbf{l}+\mathbf{m}} s_{\mathbf{j}} s_{\mathbf{k}} s_{\mathbf{l}} s_{\mathbf{m}}, \tag{23}$$

where $\mathbf{j}, \mathbf{k}, \mathbf{l}, \mathbf{m} \in \{0,1\}^n$ and the '+' for the subscript of the summation is not mod 2. Now $p(\mathbf{x}) = 0$ if $p(\mathbf{x})$ is a homogeneous quadratic and $\text{wt}(\mathbf{x}) \leq 1$, where $\text{wt}(\mathbf{y})$ means the number of non-zero components of $\mathbf{y}$. We partition the summation (23) as follows:

– $\mathrm{wt}(\mathbf{j}), \mathrm{wt}(\mathbf{k}), \mathrm{wt}(\mathbf{l}), \mathrm{wt}(\mathbf{m}) \leq 1$:
  - $\mathbf{j} = \mathbf{k} = \mathbf{l} = \mathbf{m} \rightarrow$ this case contributes 2^n to the summation.
  - $\mathbf{j} = \mathbf{l}$, $\mathbf{k} = \mathbf{m}$, or $\mathbf{j} = \mathbf{m}$, $\mathbf{k} = \mathbf{l}$. $\rightarrow$ there are $\frac{2^n(2^n-1)}{2}$ pairs in 4 configurations each, contributing a total of $4\frac{2^n(2^n-1)}{2}$ to the summation.

– Otherwise there are one or more of $\mathbf{j}, \mathbf{k}, \mathbf{l}$ and $\mathbf{m}$ with weight > 1. W.l.o.g. assume that $\mathbf{j}$ has weight 2 or greater. In particular, assume that $\mathbf{j}$ is 1 in positions j_a and j_b. We are summing over $|\mathcal{S}|$ copies of each of the homogeneous quadratics. Exactly half of these quadratics will contain the monomial $x_a x_b$. Therefore the contribution to the summation in this case is zero.

Therefore (23) evaluates to $2^n + 4\frac{2^n(2^n-1)}{2}$ and Theorem 3 follows. □

Corollary 1 *The set of n-variable Boolean functions of degree d or less satisfies, average $(\frac{1}{\mathcal{MMF}}) = \frac{2^n-1}{2^n}$ for any d, $2 \leq d \leq n$, and, consequently, average $(\frac{1}{\mathcal{MMF}}) \rightarrow 1.0$ as $n \rightarrow \infty$.*

Remark: Theorem 3 is similar to a theorem by Newman and Byrnes [9] for the univariate case which states that, for a random binary sequence of length N, average $(\frac{1}{\mathcal{MF}}) = \frac{N-1}{N}$.

Table 3 is taken from [17] and summarises constructions, described by Boolean functions, $p(\mathbf{x})$, where $s = (-1)^{p(\mathbf{x})}$. The constructions represent a larger class of $\mathcal{MMF}$-invariant sequences, as generated by Lemma 1, and the recursions have all been proven. σ_n is the value of σ for the construction over n variables.

graph	$p(\mathbf{x})$	$\mathcal{F}^{\mathcal{M}}(s)$	σ_n - recursion	σ_n - closed form
path	$\sum_{i=0}^{n-2} x_i x_{i+1}$	3	$2\sigma_{n-1} + 8\sigma_{n-2}$	$\frac{4^n}{6} - \frac{(-2)^n}{6}$
circle	$(\sum_{i=0}^{n-2} x_i x_{i+1}) + x_{n-1}x_0$	1	$2\sigma_{n-1} + 8\sigma_{n-2}$	$\frac{4^n}{2} - \frac{(-2)^n}{2}$
complete	$\sum_{i<j, 1 \leq j < n} x_i x_j$	0	$10\sigma_{n-1} - 20\sigma_{n-2}$ $-40\sigma_{n-3} + 96\sigma_{n-4}$	$\frac{6^n}{4} - \frac{4^n}{2} + \frac{2^n}{2} - \frac{(-2)^n}{4}$
star	$x_0(x_1 + x_2 + \ldots + x_{n-1})$	0	$12\sigma_{n-1} - 44\sigma_{n-2}$ $+48\sigma_{n-3}$	$2^n - \frac{4^n}{2} + \frac{6^n}{6}$

Table 3. $\mathcal{F}^{\mathcal{M}}$ for certain graphical constructions [17]

Remark: From Theorems 2 and Table 3 the values for univariate and multivariate sum-of-squares for the path are the same if π is the identity permutation.

Conjecture 6 *The maximum $\mathcal{MMF}$ is always obtained by the path graph.*

It is expected that a much larger class of Boolean functions which generalises the path graph, as described in [40], will generate a large set of multivariate sequences with maximal or near-maximal $\mathcal{MMF}$. This set can also be seen as arising from the union of certain *Golay complementary sets* of length 2^n [18, 47] and satisfies a tight upper-bound on the *peak-to-average power ratio* of the spectra with respect to $\{V\}^n$ - for this reason the sequences should have high $\mathcal{MMF}$.

4 Towards a Quantum merit factor

Section 3 has established that $\mathcal{MMF}$ quantifies a spectral property with respect to the infinite set of $2^n \times 2^n$ local unitary transforms, $\{V\}^n$. In contrast, one quantifies the spectral properties of a *pure quantum state* of n qubits with respect to the infinite set of all possible $2^n \times 2^n$ local unitary transforms, $\mathcal{D}^n\{U\}^n$, (see (1) and (2)), where $\{V\} \subset \{U\}$ [21,25,32,48]. This leads to the idea of a *quantum merit factor* ($\mathcal{QMF}$), derived from a *quantum sum-of-squares* metric.

Lemma 2 *Let T and T' be two $2^n \times 2^n$ matrices such that $T' \simeq T$ (see (3)). Let $S = Ts$ and $S' = T's$. Then,*

$$\sum_{\mathbf{k}} |S'_{\mathbf{k}}|^v = \sum_{\mathbf{k}} |S_{\mathbf{k}}|^v, \qquad v \geq 0.$$

We wish to compute $\mathcal{QMF}$ by summing the fourth powers of spectral magnitudes with respect to $\mathcal{D}^n\{U\}^n$ but it follows from Lemma 2 that we need only sum over the spectra with respect to $\{U\}^n$ to compute $\mathcal{QMF}$. Symbolically, for $n = 1$, we view this as summarising the fourth powers over the complete sphere (otherwise known as the *Bloch Sphere* [48]):

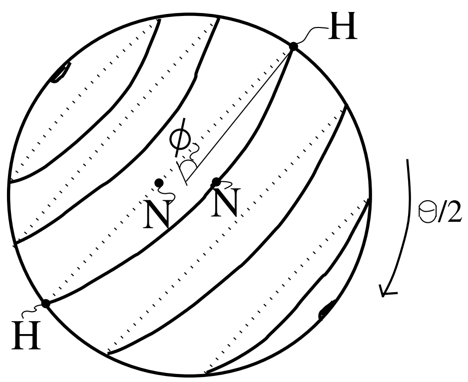
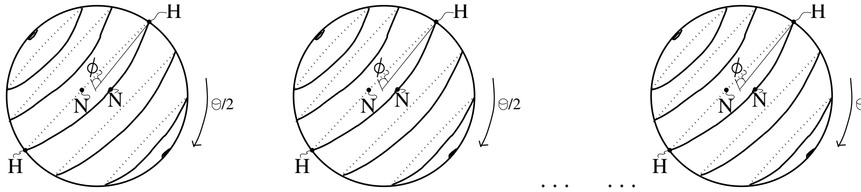


Fig. 2. The Bloch Sphere with points on the sphere described by $U(\theta, \phi)$ (see (1))

where H and N are indicated on the 'equator' of each sphere. For $n > 1$ this becomes a summation over the joint n-sphere:



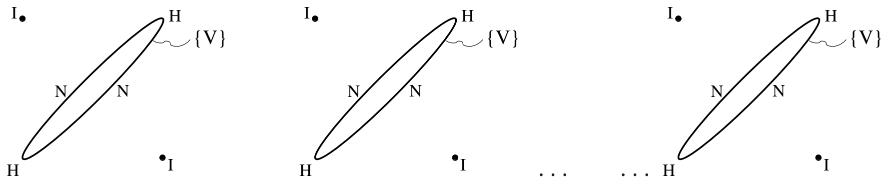
$\mathcal{MMF}$ only quantifies merit factor with respect to the equators of the n-sphere. In section 5 we characterise and investigate the *Clifford merit factor* ($\mathcal{CMF}$), which we show quantifies merit factor with respect to three pole/equator pairs. We then generalise to show that $\mathcal{CMF}$ quantifies merit factor with respect to the complete n-sphere, and is therefore equal to $\mathcal{QMF}$.

5 Clifford Merit Factor

Definition 9 *For F_α, F'_α as defined in (4), let $\{V^I\}$ be an infinite multi-set of transforms, where $\frac{1}{3}$ of all elements in $\{V^I\}$ are the 2×2 identity, I, and where,*

$$\{V^I\} = \{\{I, F_\alpha, F'_\alpha\} \quad | \quad \forall \alpha \in \mathcal{C}, |\alpha| = 1\}.$$

Note that $|\{V^I\}| = \frac{3}{2}|\{V\}|$. Just as it is sufficient to compute merit factor with respect to $\{V\}^n$ by summing fourth powers of spectral magnitudes with respect to $\{H, N\}^n$ so, for the merit factor with respect to $\{V^I\}^n$, it is sufficient to sum up fourth powers of spectral magnitudes with respect to $\{I, H, N\}^n$. We represent this transform set visually as,



which evaluates a merit factor with respect to any tensor combination of discrete 'poles', I, and continuous 'equators', $\{H, N\}$.

For the multivariate sequence, s, as defined in Section 3, we evaluate the set of 3^n spectra, $\{S\}$, with respect to $\{I, H, N\}^n$, where

$$S = \{S^{\mathbf{r}}\} = \{S^{00\ldots0}, S^{00\ldots1}, S^{00\ldots2} \ldots, S^{22\ldots2}\} = \{I, H, N\}^n s,$$

and

$$S^{\mathbf{r}} = \{S^{\mathbf{r}}_{\mathbf{k}}\} = (S^{\mathbf{r}}_{00\ldots0}, S^{\mathbf{r}}_{00\ldots1} \ldots S^{\mathbf{r}}_{11\ldots1})^T,$$

where $\mathbf{r} \in \{0, 1, 2\}^n$, $\mathbf{k} \in \{0, 1\}^n$, and $r_i = 0, 1$ or 2 implies I, H or N, respectively, in tensor position i. $\{S^{\mathbf{r}}_{\mathbf{k}}\}$ is a set of 6^n spectral points.

Definition 10 *The* Clifford sum-of-squares*, $\mathcal{E}$, of the sequence, s, is given by,*

$$\mathcal{E} = \frac{1}{2}((\sum_{\substack{\mathbf{k} \in \{0,1\}^n \\ \mathbf{r} \in \{0,1,2\}^n}} |S^{\mathbf{r}}_{\mathbf{k}}|^4) - 6^n). \tag{24}$$

Definition 11 *The* Clifford merit factor*, $\mathcal{CMF}$, of the sequence, s, is given by,*

$$\mathcal{CMF} = \frac{6^n}{2\mathcal{E}}. \tag{25}$$

Definition 12 *Let $s_{\mathcal{A}}$ be a length 2^n multivariate sequence generated by construction $\mathcal{A}$. Then the* asymptotic Clifford merit factor *of $s_{\mathcal{A}}$ is given by,*

$$\mathcal{F}^{\mathcal{C}} = \lim_{n\to\infty} \mathcal{CMF}(s_{\mathcal{A}}).$$

Let $\mathbf{b}, \mathbf{e} \in \mathcal{Z}_2^n$. Let $\mathrm{wt}(\mathbf{b})$ be the binary weight of vector $\mathbf{b}$. Let $p(\mathbf{x_{b,e}}) : \mathcal{Z}_2^{n-\mathrm{wt}(\mathbf{e})} \to Z_2$, be the restriction of p to $n - \mathrm{wt}(\mathbf{e})$ variables, where $x_i = b_i$ if $e_i = 1$, where $\mathbf{b} \preceq \mathbf{e}$, and '$\preceq$' means that $b_i \le e_i$, $\forall i$.

Define $s_{\mathbf{e},\mathbf{b}} = (-1)^{p(\mathbf{x_{b,e}})}$, where $s_{\mathbf{j},\mathbf{e},\mathbf{b}} = (-1)^{p(\mathbf{x_{b,e}}=\mathbf{j})}$, $\mathbf{j} \in \mathcal{Z}_2^{n-\mathrm{wt}(\mathbf{e})}$, $s_{\mathbf{j},\mathbf{e},\mathbf{b}} = 0$ otherwise. The *fixed-aperiodic autocorrelation* [36] of s is given by,

$$u_{\mathbf{k},\mathbf{b},\mathbf{e}} = \sum_{\mathbf{j}\in\{0,1\}^{n-\mathrm{wt}(\mathbf{e})}} s_{\mathbf{j},\mathbf{b},\mathbf{e}} s^*_{\mathbf{j}+\mathbf{k},\mathbf{b},\mathbf{e}}, \qquad \mathbf{k} \in \{-1,0,1\}^{n-\mathrm{wt}(\mathbf{e})}. \tag{26}$$

An alternative to Definition 10 for $\mathcal{E}$ is given by Definition 13.

Definition 13 *The* Clifford sum-of-squares*, $\mathcal{E}$, of the sequence, s, is given by,*

$$\begin{aligned}\mathcal{E} &= \tfrac{1}{2}\Big(\Big(\sum_{\mathbf{e}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n, \mathbf{b}\preceq\mathbf{e}} \sum_{\mathbf{k}\in\{-1,0,1\}^{n-wt(\mathbf{e})}} |u_{\mathbf{k},\mathbf{b},\mathbf{e}}|^2\Big) - 6^n\Big) \\ &= \tfrac{1}{2} \sum_{\mathbf{e}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n, \mathbf{b}\preceq\mathbf{e}} \sum_{\substack{\mathbf{k}\,\in\,\{-1,0,1\}^{n-wt(\mathbf{e})} \\ \mathbf{k}\,\ne\,\{0\}^{n-wt(\mathbf{e})}}} |u_{\mathbf{k},\mathbf{b},\mathbf{e}}|^2.\end{aligned} \tag{27}$$

We refer to these metrics as "Clifford" because the unitary matrix set, $\{I, H, N\}$, generates the *Local Clifford Group* [24,34,49]. This means that $\{I, H, N\}$ *stabilize* the *Pauli matrices*, I, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $i\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

$\mathcal{CMF}$ Symmetries

If $|S^{\mathbf{r}}_{\mathbf{k}}| = |S^{\mathbf{r}}_{\mathbf{j}}|$, $\forall \mathbf{j}, \mathbf{k} \in \mathcal{Z}_2^n$, then we call $S^{\mathbf{r}}$ a *flat* spectra. In such a case we express $S^{\mathbf{r}}$ as

$$S^{\mathbf{r}} = \omega^{4p^{\mathbf{r}}(\mathbf{x}) + a(\mathbf{x})},$$

where ω is a complex root of one of order 8 and $p^{\mathbf{r}}(\mathbf{x}) : \mathcal{Z}_2^n \to \mathcal{Z}_2$ is a Boolean function. Let $s^{\mathbf{r}} = (-1)^{p^{\mathbf{r}}(\mathbf{x})}$.

Definition 14 *Define the* IHN-orbit*, s_{orb}, of s, by*

$$s_{orb} = \{s^{\mathbf{r}} \quad | \quad \forall \mathbf{r} \textit{ such that } S^{\mathbf{r}} \textit{ is flat and } \deg(a(\mathbf{x})) \le 1\}.$$

Let s' and $p'(\mathbf{x})$ be as defined in Lemma 1. Then,

Lemma 3 *For $s^{\mathbf{r}} \in s_{orb}$,*

$$\mathcal{CMF}(s'^{\mathbf{r}}) = \mathcal{CMF}(s).$$

The IHN-orbit is largest in size for $p(\mathbf{x})$ quadratic where the symmetry reduces to a graphical symmetry called *local complementation* [37, 50, 51], also referred to as *vertex-neighbour-complementation* [30].

5.1 Transform ⇔ Autocorrelation Duality

From (24) and (27),

$$\sum_{\mathbf{e}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n, \mathbf{b}\preceq\mathbf{e}} \sum_{\mathbf{k}\in\{-1,0,1\}^{n-\text{ wt }(\mathbf{e})}} |u_{\mathbf{k},\mathbf{b},\mathbf{e}}|^2 = \sum_{\substack{\mathbf{k}\,\in\,\{0,1\}^n \\ \mathbf{r}\,\in\,\{0,1,2\}^n}} |S_{\mathbf{k}}^{\mathbf{r}}|^4. \tag{28}$$

Proof. The autocorrelation of (26) is the union of a set of multivariate aperiodic autocorrelations where, for fixed $\mathbf{e}$ and $\mathbf{b}$, each such autocorrelation is of the form of (15) and is computed over $n - \text{wt}(\mathbf{e})$ variables, after having fixed $\text{wt}(\mathbf{e})$ variables, x_i, to b_i, if $e_i = 1$. This fixing is mirrored in the spectral domain by assigning $r_i = 0$ iff $e_i = 1$. In other words, matrix I occurs in the ith tensor position of the transform $T \in \{I, H, N\}^n$ iff $e_i = 1$, where the first and second rows of I reflect $x_i = b_i = 0$ and $x_i = b_i = 1$, respectively. (28) follows by summing instances of (20) for each choice of $\mathbf{e}$ and $\mathbf{b}$. □

5.2 Clifford Merit Factor is Quantum Merit Factor

Definition 15 *The* normalised quantum sum-of-squares *with respect to the transform set, $\{A\}^n$, is given by,*

$$\mathcal{E}_{\{A\}^n} = \frac{3^n}{2}\left(\frac{||S||^4_{\{A\}^n}}{|\{A\}|^n} - 2^n\right), \tag{29}$$

where $||S||^4_{\{A\}^n}$ is the sum of the fourth powers of the spectral magnitudes with respect to the transform set $\{A\}^n$.

We recover definition 10 from (29) by assigning $\{A\} = \{I, H, N\}$. For $\{A\} = \{V^I\}$ we obtain $\mathcal{E}_{\{V^I\}^n} = 2^{n-1}\left(\frac{||S||^4_{\{V^I\}^n}}{|\{V\}|^n} - 1\right)$, by substituting $|\{V^I\}| = \frac{3|\{V\}|}{2}$.

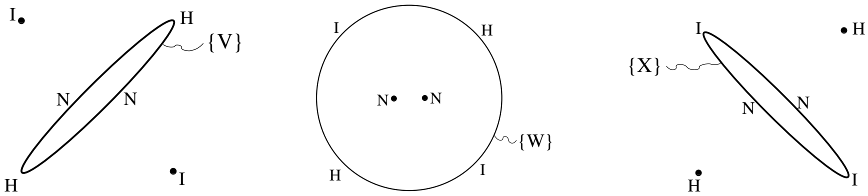
Lemma 4

$$\mathcal{E}_{\{I,H,N\}^n Z} = \mathcal{E}_{\{V^I\}^n Z}, \qquad \forall Z \in \mathcal{D}^n\{U\}^n.$$

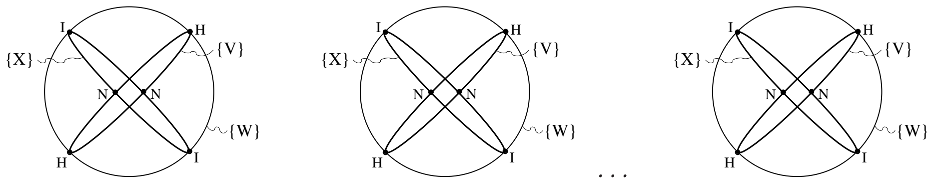
Recalling section 1.1, (3), (4), and definition 9,

Definition 16 *Define $\{W^N\} \simeq \{V^I\}N$, and $\{X^H\} \simeq \{W^N\}N$.*

$\{V^I\}, \{W^N\}$, and $\{X^H\}$ describe the following pole/equator pairs, respectively:



Proposition 1 $\mathcal{E}_{\{A\}^n} = \mathcal{E}$ *for* $\{A\} = \{\{V^I\},\{W^N\},\{X^H\}\}$, *and* $\{A\} = \{\{V\},\{W\},\{X\}\}$, *which we visualise as:*



Proof. We know that $\mathcal{E}_{\{V^I\}} = \mathcal{E}$. As $\{W^N\} \simeq \{V^I\}N$ it follows, from Lemma 4, that $\mathcal{E}_{\{W^N\}} = \mathcal{E}_{\{I,H,N\}N} = \mathcal{E}_{\{N,I,H\}} = \mathcal{E}$. Likewise, as $\{X^H\} \simeq \{V^I\}N^2$ it follows, from Lemma 4, that $\mathcal{E}_{\{X^H\}} = \mathcal{E}_{\{I,H,N\}N^2} = \mathcal{E}_{\{H,N,I\}} = \mathcal{E}$. The simplification to $\{\{V\},\{W\},\{X\}\}$ occurs because we can remove surplus element triples, $\{I,H,N\}$, from $\{\{V^I\},\{W^N\},\{X^H\}\}$ without changing the normalised spectral sum. The argument extends to any tensor combination of the three pole/equator pairs when $n > 1$. □

Let $F_{\tilde{\alpha}} = F_{\alpha_0} \otimes F_{\alpha_1} \otimes \ldots \otimes F_{\alpha_{n-1}}$, where F_α was defined in (4). We now generalise $\{A\}$ in proposition 1 by assigning $\{A\} = \{V^I\}^n\{I^n, F_{\tilde{\alpha}}, F_{\tilde{\alpha}}F_{\tilde{\beta}}\}$:

Theorem 4

$$\mathcal{E}_{\{V^I\}^n\{I^n,F_{\tilde{\alpha}},F_{\tilde{\alpha}}F_{\tilde{\beta}}\}} = \mathcal{E}, \qquad \forall F_{\tilde{\alpha}}, F_{\tilde{\beta}} \in \{V\}^n.$$

Proof. We see that $\{I,H,N\}F_\alpha \simeq \{F_\alpha, I, F'_\alpha\}$, and we already know that $\mathcal{E}_{\{F_\alpha,I,F'_\alpha\}} = \mathcal{E}$. Therefore, from Lemma 4, $\mathcal{E}_{\{V^I\}F_\alpha} = \mathcal{E}$. Using Lemma 4 repeatedly, $\mathcal{E}_{\{V^I\}F_\alpha F_\beta} = \mathcal{E}_{\{I,H,N\}F_\alpha F_\beta} = \mathcal{E}_{\{F_\alpha,I,F'_\alpha\}F_\beta} = \mathcal{E}_{\{V^I\}F_\beta} = \mathcal{E}$. The argument extends to any tensor combination when $n > 1$. □

Lemma 5

$$\{U\} \simeq \{V\}\{V\}.$$

Proof. $F_\alpha F_\beta = \frac{(1+\alpha)}{2}\begin{pmatrix} 1 & \frac{(1-\alpha)}{(1+\alpha)}\beta \\ \frac{(1-\alpha)}{(1+\alpha)} & \beta \end{pmatrix} = \mu \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \frac{(1+\alpha)}{2\mu} \begin{pmatrix} 1 & \frac{(1-\alpha)}{(1+\alpha)}\beta \\ i\frac{(1-\alpha)}{(1+\alpha)} & i\beta \end{pmatrix}$, $\forall F_\alpha, F_\beta \in \{V\}$, where $\mu = \sqrt{\alpha}$. The lemma follows by assigning $\beta = e^{i\phi}$, $\cos\theta = \frac{(1+\alpha)}{2\mu}$, and $\sin\theta = i\frac{(1-\alpha)}{2\mu}$. □

Theorem 5

$$\mathcal{CMF}(Ts) = \mathcal{CMF}(s), \qquad \forall T \in \mathcal{D}^n\{U\}^n.$$

Proof. Follows directly from Definition 11, and lemmas 2, 4 and 5. □

Theorem 5 implies that $\mathcal{CMF}$ is an entanglement metric as it is invariant with respect to local unitary transform of the state, s [25].

Theorem 6 *$\mathcal{CMF}$ is $\mathcal{QMF}$.*

Proof. From figure 2, and lemma 5, we see that α and β specify θ and ϕ, respectively. Over all $\alpha, \beta \in \mathcal{C}$, and $d \in \mathcal{D}$, we have, from theorem 5 that, for $n = 1$, $\mathcal{E}_{\mathcal{D}\{U\}} = \mathcal{E}_{I,H,N} = \mathcal{E}$ is invariant, where each spectral point is counted the same number of times. The argument extends to tensor products when $n > 1$. □

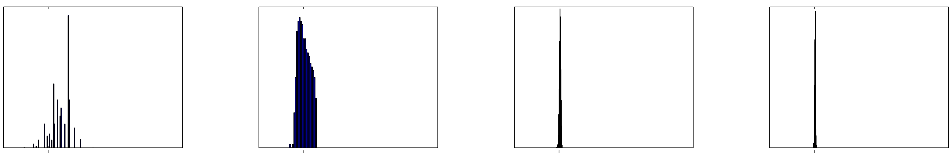
5.3 Expected Values and Constructions

Maximising Clifford merit factor ($\mathcal{CMF}$) of a Boolean function indicates a minimum mean-square deviation from the joint flat continuous multivariate fourier power spectrum of the sequences associated to the Boolean function and all its subspace fixings. Table 5.3 shows equivalence classes for Boolean functions of $n = 2$ to 5 variables, where sets of inequivalent functions are obtained from [46].

n	# inequivalent functions	# equivalence classes with list of $\mathcal{CMF}$s
2	2	2 classes **3.0**, 1.286
3	4	4 classes **2.077**, 1.421, 1.286, 0.730
4	34	18 classes **1.723**, 1.588, 1.473, 1.446, 1.373, 1.286, 1.266, 1.209, 1.141, 1.125, 1.080, 1.025, 0.976, 0.920, 0.786, 0.730, 0.675, 0.463
5	22050	193 classes **1.723** − 0.311

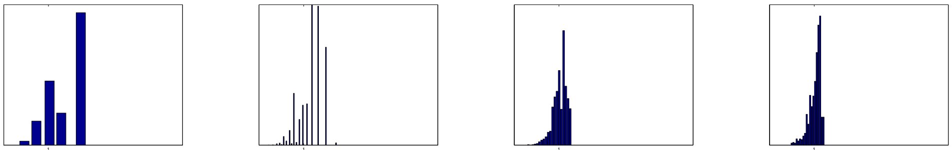
Table 4. complete set of Clifford merit factors for $n = 2$ to $n = 5$

Experimental results suggest that, for a random Boolean function of n variables, $\mathcal{F}^{\mathcal{C}} = 1.0$, as indicated here by the random samplings for (from left to right) $n = 4, 6, 9$ and 10, where $\mathcal{CMF}$ and #sequences are x and y-axes, respectively, with x-axes ranging from $\mathcal{CMF} = 0$ to 4, and where the highest peak approaches $\mathcal{F}^{\mathcal{C}} = 1.0$ as n increases.



In comparison, a sampling of just the quadratic Boolean functions for $n = 4, 6, 9$ and 10 indicates a wider range of $\mathcal{CMF}$s for a given n than for the full space of Boolean functions although, once again, the highest peak appears to approach $\mathcal{F}^{\mathcal{C}} = 1.0$ as n gets large. Once again, the x-axes range linearly from $\mathcal{CMF} = 0$

to 4, and the y-axes indicate #sequences.



Conjecture 7 *A random Boolean function satisfies,*

$$\mathcal{F}^{\mathcal{C}} = 1.0.$$

Theorem 7 *The average value of* $\frac{1}{\mathcal{CMF}}$ *with respect to any set* $\mathcal{S}_{\mathcal{Q}}$ *(see definition 8) is,*

$$average_{\ \mathcal{S}_{\mathcal{Q}}}(\frac{1}{\mathcal{CMF}}) = \frac{3^n - 2^n}{3^n}.$$

Proof. It follows directly from Theorem 3, by summing up the multivariate sum-of-squares over every fixed-subspace of $\mathcal{S}_{\mathcal{Q}}$. Each member of each coset of $\mathcal{Q}$ is represented the same number of times over each subspace. $\square$

Corollary 2 *The set of* n*-variable Boolean functions of degree* d *or less satisfies,*

$$average\ (\frac{1}{\mathcal{CMF}}) = \frac{3^n - 2^n}{3^n}$$

for any d*,* $2 \leq d \leq n$*, and, consequently, average* $(\frac{1}{\mathcal{CMF}}) \to 1.0$ *as* $n \to \infty$*.*

Table 5 summarises constructions described by Boolean functions, $p(\mathbf{x})$, where $s = (-1)^{p(\mathbf{x})}$. The associated recursions originate from [52]. The constructions represent a larger class of $\mathcal{CMF}$-invariant sequences, as generated by Lemma 3, and the recursions have all been proven using the results of [39]. The star and complete graph are in the same IHN-orbit. None of the constructions in Table 5 satisfy a non-vanishing value for $\mathcal{F}^{\mathcal{C}}$. We appear to obtain maximum values of $\mathcal{CMF}$ for s constructed from quadratic Boolean functions which describe optimal QECCs [30,33,36,37,39,46,53]. Table 6 shows maximal values of $\mathcal{CMF}$ for $n = 2$ to 5, and highest found values of $\mathcal{CMF}$ for $n = 6$ to 9, and all represent QECCs with optimal distance. The associated QECC is obtained from an additive $[n, 2^n, \text{distance}]$ code over GF(4) where the associated generator matrix, G, satisfies $G = \omega\mathcal{I} + \Gamma$, where Γ is the adjacency matrix of the graph associated with the quadratic Boolean function, $p(\mathbf{x})$, $\mathcal{I}$ is the $n \times n$ identity matrix, and $\omega^2 + \omega + 1 = 0$ over GF(4). The results are only exhaustive for $n = 2$ to 5. In the table, expressions of the form $ab, cd, \ldots$ are short for $x_a x_b + x_c x_d + \ldots$.

A few cubics and quartics have recently been found which equal the $\mathcal{CMF}$ values in Table 6 [54], but none have been found yet with greater $\mathcal{CMF}$.

graph	$\mathcal{F}^{\mathcal{C}}(s)$	$\mathcal{E}_n$ - recursion	$\mathcal{E}_n$ - closed form
path	0	$10\mathcal{E}_{n-1} - 8\mathcal{E}_{n-2} - 96\mathcal{E}_{n-3}$	$\frac{6^n}{2} + (\frac{5-3\sqrt{5}}{20})(2-2\sqrt{5})^n$ $+(\frac{5+3\sqrt{5}}{20})(2+2\sqrt{5})^n$
circle	0	$14\mathcal{E}_{n-1} - 48\mathcal{E}_{n-2} - 64\mathcal{E}_{n-3} + 38\mathcal{E}_{n-4}$	$\frac{4^n}{2} + \frac{(2-2\sqrt{5})^n}{2} + \frac{(2+2\sqrt{5})^n}{2} - \frac{6^n}{2}$
complete $\equiv$ star	0	$18\mathcal{E}_{n-1} - 104\mathcal{E}_{n-2} - 192\mathcal{E}_{n-3}$	$\frac{8^n}{4} - \frac{6^n}{2} + \frac{4^n}{2}$

Table 5. $\mathcal{F}^{\mathcal{C}}$ for certain graphical constructions

n	$p(\mathbf{x})$	$\mathcal{CMF}(s)$	QECC distance
2	01	**3.0**	2
3	$01, 02$	**2.08**	2
4	$01, 12, 23$	**1.72**	2
5	$01, 02, 13, 24, 34$	**1.72**	3
6	$01, 02, 03, 04, 05, 12, 23, 34, 45, 51$	1.72	4
7	$03, 06, 14, 16, 25, 26, 34, 35, 45$	1.43	3
8	$02, 03, 04, 12, 13, 15, 26, 37, 46, 47, 56, 57, 67$	1.40	4
	$05, 06, 07, 13, 15, 17, 24, 25, 27, 36, 37, 46, 47, 67$	1.40	4
9	$02, 04, 08, 13, 15, 18, 26, 28, 37, 38, 47, 48, 56, 58, 67, 68, 78$	1.30	4
	$04, 07, 08, 13, 14, 18, 24, 25, 28, 36, 37, 56, 57, 58, 67, 68$	1.30	4
	$06, 07, 08, 14, 16, 18, 25, 26, 28, 34, 35, 37, 38, 47, 48, 57, 58, 68$	1.30	4
	$04, 07, 08, 14, 16, 18, 25, 26, 28, 34, 35, 37, 57, 58, 67, 68$	1.30	4
	$01, 07, 08, 14, 18, 23, 25, 28, 36, 37, 45, 46, 57, 58, 67, 68$	1.30	4

Table 6. Boolean functions with maximal $\mathcal{CMF}$ for $n = 2$ to 5 and large (possibly maximal) $\mathcal{CMF}$ for $n = 6$ to 9 with their associated QECC distances

Many high-distance QECCs are of (bordered) quadratic-residue [30]. Let l be a Legendre sequence of prime length m, where $m = 4k + 1$, as described in Section 2. Construct $p(\mathbf{x})$ over $n = m$ variables such that,

$$p(\mathbf{x}) = \sum_{j=0}^{n-1} l_j \sum_{i=0}^{n-j-1} x_i x_{i+j}.$$

For the bordered version, construct $p(\mathbf{x})$ over $n = m + 1$ variables such that,

$$p(\mathbf{x}) = \sum_{j=1}^{n-1} x_0 x_i + \sum_{j=1}^{n-1} l_j \sum_{i=1}^{n-j-1} x_i x_{i+j}.$$

Then, for both non-bordered and bordered versions, $s = (-1)^{p(\mathbf{x})}$ has a relatively high and sometimes optimal $\mathcal{CMF}$. The examples in Table 6 for $n = 5$ and 6 are equivalent, by Lemma 3, to (bordered)-quadratic residue constructions.

There is a connection with recent results in graph theory. Aigner and van der Holst have defined an *interlace polynomial*, $Q(z)$, which summarises various spectral properties of a graph [55], this being a generalisation of an interlace polynomial, $q(z)$, defined by Arratia, Bollobas, and Sorkin [56], where both polynomials are variants of *Tutte* and *Tutte-Martin* polynomials as defined by Bouchet [57]. Moreover a further interlace polynomial, $Q_{HN}(z)$ has recently been defined in [58], and it is shown there that, for sequences constructed from quadratic Boolean functions, $\sigma_n = 2^{n-1}(Q_{HN,n}(4) - 2^n)$ and $\mathcal{E}_n = 2^{n-1}(Q_n(4) - 3^n)$.

In contrast to $\mathcal{CMF}$, most entanglement measures are computationally infeasible beyond about 4 qubits. So $\mathcal{CMF}$ is a useful measure in a quantum context as it is (currently) computationally viable up to about $n = 12$ qubits. Moreover, for graph states and, in particular, recursively constructed graph states, $\mathcal{CMF}$ gives us an entanglement measure of a pure multipartite system for large n.

6 Conclusion

The univariate, multivariate, and Clifford merit factors ($\mathcal{MF}$, $\mathcal{MMF}$, and $\mathcal{CMF}$, resp.) have been reviewed. Constructions which achieve the best-known asymptotic merit factor, $\mathcal{F}$, have been described. $\mathcal{MMF}$ has been characterised for the extreme case where each dimension is of length 2. The associated multivariate sequences therefore have a natural description via Boolean functions. The average value for $\frac{1}{\mathcal{MMF}}$ was established. We presented 'graphical' constructions for which recursions in multivariate sum-of-squares exist leading, in some cases, to non-vanishing asymptotic multivariate merit factor $\mathcal{F}^{\mathcal{M}}$. We conjectured that maximal $\mathcal{F}^{\mathcal{M}}$ is satisfied by the path graph. We characterised $\mathcal{CMF}$ as a generalisation of $\mathcal{MMF}$ and proved it is invariant to local unitary transform and is, moreover, a quantum merit factor, $\mathcal{QMF}$. The average value for $\frac{1}{\mathcal{CMF}}$ was established. We presented 'graphical' constructions for which recursions in Clifford sum-of-squares exist, although all associated asymptotic Clifford merit factors, $\mathcal{F}^{\mathcal{C}}$, are zero. We demonstrated that sequences constructed from quantum error correcting codes appear to maximise $\mathcal{CMF}$.

We finish with a list of open problems suggested by this paper:

- Establish whether $\mathcal{MF} = 14.083$ is maximal over all binary sequences.
- Prove $\mathcal{F} = 6.3421\ldots$ for the relevant constructions of Section 2.
- Establish the range of $\mathcal{F}$ for the univariate sequence constructed via the path graph under all possible index permutations.
- Prove the recursions in univariate sum-of-squares for the recursive graphical constructions of Section 2.
- Prove that $\mathcal{F} = \mathcal{F}^{\mathcal{M}} = \mathcal{F}^{\mathcal{C}} = 1.0$ for a random univariate or multivariate sequence of length N, 2^n, or 2^n, respectively.
- Establish whether the maximum $\mathcal{MMF}$ and $\mathcal{CMF}$ over all multivariate binary sequences are 4.00 and 3.00, respectively for the sequence constructed from $p(\mathbf{x}) = x_0x_1$.
- Prove that the maximal $\mathcal{MMF}$ over n variables and, therefore, the maximal $\mathcal{F}^{\mathcal{M}}$ is always obtained by the path graph.
- Find an infinite multivariate sequence construction such that $\mathcal{F}^{\mathcal{C}} > 0$.
- Prove whether, for n variables, $\mathcal{CMF}$ is always optimised by quadratic Boolean functions, or give a counter-example.

References

1. Littlewood, J.E.: Some Problems in Real and Complex Analysis. Heath Mathematical Monographs (1968)
2. Golay, M.J.E.: A class of finite binary sequences with alternate autocorrelation values equal to zero. IEEE Trans. Inform. Theory **IT-18** (1972) pp. 449–450
3. Golay, M.J.E.: The merit factor of long low autocorrelation binary sequences. IEEE Trans. Inform. Theory **28** (1982) pp. 543–549
4. Golay, M.J.E.: A new search for skewsymmetric binary sequences with optimal merit factors. IEEE Trans. Inform. Theory **36** (1990) pp. 1163–1166
5. Høholdt, T., Jensen, H.E., Justesen, J.: Aperiodic correlations and the merit factor of a class of binary sequences. IEEE Trans. Inform. Theory **31** (1985) pp. 549–552
6. Høholdt, T., Jensen, H.E.: Determination of the merit factor of Legendre sequences. IEEE Trans. Inform. Theory **IT-34** (1988) pp. 161–164
7. Høholdt, T.: The merit factor of binary sequences. In Pott, A., Kumar, P.V., Helleseth, T., Jungnickel, D., eds.: Difference Sets, Sequences and their Correlation Properties, Bad Winsheim, 2–14 August 1998. Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers (1999) pp. 227–237 Long version: `http://arxiv.org/quant-ph/0107106`.
8. Jensen, J.M., Jensen, H.E., Høholdt, T.: The merit factor of binary sequences related to difference sets. IEEE Trans. Inform. Theory **37** (1991) pp. 617–626
9. Newman, D.J., Byrnes, J.S.: The l^4 norm of a polynomial with coefficients ± 1. Amer. Math. Monthly **97** (1990) pp. 42–45
10. Golay, M.J.E.: The merit factor of legendre sequences. IEEE Trans. Inform. Theory **29** (1983) pp. 934–936
11. Kristiansen, R.A.: On the aperiodic autocorrelation of binary sequences. Master's thesis, Selmer Centre, Inst. for Informatics, University of Bergen, Norway (2003) `http://www.ii.uib.no/~matthew/Masters/notes.ps`.
12. Kristiansen, R.A., Parker, M.G.: Binary sequences with merit factor > 6.3. IEEE Trans. Inform. Theory **50** (2004) pp. 3385–3389
13. Borwein, P., Choi, K.K.S., Jedwab, J.: Binary sequences with merit factor greater than 6.34. IEEE Trans. Inform. Theory **50** (2004) pp. 3234–3249
14. Jedwab, J.: A survey of the merit factor problem for binary sequences. In: Proc. of SETA04. Lecture Notes in Computer Science. Springer-Verlag (2005) this issue.
15. Ramakrishna, G.S., Mow, W.H.: A new search for optimal binary arrays with minimum peak sidelobe levels. In: Proc. of SETA04. Lecture Notes in Computer Science, Springer-Verlag (2005) This issue.
16. Zhang, X.M., Zheng, Y.: Gac - the criterion for global avalanche characteristics of cryptographic functions. J. Universal Computer Science **1** (1995) pp. 320–337
17. Gulliver, T.A., Parker, M.G.: The multi-dimensional aperiodic merit factor of binary sequences. preprint, `http://www.ii.uib.no/~matthew/ISITRecursions.pdf` (2003)
18. Golay, M.J.E.: Multislit spectroscopy. J. Opt. Soc. Amer. **39** (1949) pp. 437–444
19. Shapiro, H.S.: Extremal problems for polynomials. Master's thesis, M.I.T. (1951)
20. Rudin, W.: Some theorems on fourier coefficients. Proc. Amer. Math. Soc. **10** (1959)
21. 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 (2001) Long version: `http://arxiv.org/quant-ph/0107106`.

22. Riera, C., Parker, M.G.: Generalised bent criteria for boolean functions (i). preprint, http://www.ii.uib.no/~matthew/LCPartIf.pdf (2004)
23. Briegel, H.J., Raussendorf, R.: Persistent entanglement in arrays of interacting particles. Physical Review Letters **86** (2001) pp. 910–913
24. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. Phys. Rev. A **69** (2004) http://arxiv.org/quant-ph/0307130.
25. Verstraete, F.: A Study of Entanglement in Quantum Information Theory. PhD thesis, Dept. Elektrotechniek, Katholieke Universiteit, Leuven, Belgium (2002)
26. Parker, M.G.: Quantum factor graphs. Annals of Telecom. (2001) pp. 472–483 http://arxiv.org/quant-ph/0010043.
27. Schlingemann, D., Werner, R.F.: Quantum error-correcting codes associated with graphs. Phys. Rev. A **65** (2002) http://arxiv.org/quant-ph/0012111.
28. Glynn, D.G.: On self-dual quantum codes and graphs. Submitted to Elect. J. Combinatorics. http://homepage.mac.com/dglynn/.cv/dglynn/Public/SD-G3.pdf-link.pdf (2002)
29. Grassl, M., Klappenecker, A., Rotteler, M.: Graphs, quadratic forms, and quantum codes. In: Proc. IEEE Int. Symp. Inform. Theory. (2002) p. 45
30. Glynn, D.G., Gulliver, T.A., Maks, J.G., Gupta, M.K.: The Geometry of Additive Quantum Codes. Springer-Verlag (2004)
31. Raussendorf, R., Briegel, H.J.: A one-way quantum computer. Phys. Rev. Lett. **86** (2001) pp. 5188–5191
32. Zyczkowski, K., Bengtsson, I.: Relativity of pure states entanglement. Ann. Phys. **295** (2002)
33. 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.
34. Klappenecker, A., Rotteler, M.: Clifford codes. In Brylinski, R., Chen, G., eds.: Mathematics of Quantum Computation. CRC Press (2002)
35. Gottesman, D.: Stabilizer Codes and Quantum Error Correction. PhD thesis, California Institute of Technology (1997) http://arxiv.org/quant-ph/9705052.
36. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic propagation criteria for Boolean functions. ECRYPT Internal Document, STVL-UiB-1-APC-1.0. http://www.ii.uib.no/~matthew/GenDiff4.pdf (2004)
37. Danielsen, L.E., Parker, M.G.: Spectral orbits and peak-to-average power ratio of boolean functions with respect to the $\{I,H,N\}^n$ transform. In: Proc. of SETA04. Lecture Notes in Computer Science, Springer-Verlag (2005) this issue, http://www.ii.uib.no/~matthew/seta04-parihn.pdf.
38. 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.
39. Riera, C., Petrides, G., Parker, M.G.: Generalised bent criteria for boolean functions (ii). preprint, http://www.ii.uib.no/~matthew/LCPartIIf.pdf (2004)
40. 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, update at:http://www.ii.uib.no/~matthew/Construct04.pdf.
41. Borwein, P., Choi, K.K.S.: Explicit merit factor formulae for fekete and turyn polynomials. Trans. Amer. Math. Soc. **354** (2002) pp. 219–234
42. Borwein, P., Choi, K.K.S.: Merit factors of polynomials formed by jacobi symbols. Canad. J. Math. **53** (2001) pp. 33–50

43. Parker, M.G.: Even length binary sequence families with low negaperiodic autocorrelation. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14 Proceedings. Number 2227 in Lecture Notes in Computer Science. Springer-Verlag (2001) p. 200–209
44. Kirilusha, A., Narayanaswamy, G.: Construction of new asymptotic classes of binary sequences based on existing asymptotic classes. Technical report, Dept. Math. and Comput. Science, Univ. of Richmond (1999) http://www.mathcs.richmond.edu/~jad/summer.html.
45. 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
46. Danielsen, L.E.: Database of self-dual quantum codes. Web page (2004) http://www.ii.uib.no/~larsed/vncorbits/.
47. Golay, M.J.E.: Complementary series. IRE Trans. Inform. Theory **IT-7** (1961) pp. 82–87
48. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
49. 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.
50. Bouchet, A.: Isotropic systems. European J. Combin. **8** (1987) pp. 231–244
51. Bouchet, A.: Recognizing locally equivalent graphs. Discrete Math. **114** (1993) pp. 75–86
52. Storøy, D.: Master's thesis - in preparation. Selmer Centre, Inst. for Informatics, University of Bergen, Bergen, Norway (2005)
53. 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
54. Danielsen, L.E.: Master's thesis - in preparation. Selmer Centre, Inst. for Informatics, University of Bergen, Bergen, Norway (2005)
55. Aigner, M., van der Holst, H.: Interlace polynomials. Linear Algebra and its Applications **377** (2004) pp. 11–30
56. Arratia, R., Bollobas, B., Sorkin, G.B.: The interlace polynomial of a graph. J. Combin. Theory Ser. B **92** (2004) pp. 199–233 http://arxiv.org/abs/math/0209045.
57. Bouchet, A.: Tutte-martin polynomials and orienting vectors of isotropic systems. Graphs Combin. **7** (1991) pp. 235–252
58. Riera, C., Parker, M.G.: Spectral interpretations of the interlace polynomial. preprint, http://www.ii.uib.no/~matthew/WCC4.pdf (2004)