The Multi-Dimensional Aperiodic Merit Factor of Binary Sequences

T. Aaron Gulliver, and Matthew G. Parker

Abstract

A new metric, the Multi-Dimensional aperiodic Merit Factor, is presented, and various recursive quadratic sequence constructions are given for which both the one and multi-dimensional aperiodic Merit Factors can be computed exactly. In some cases these constructions lead to Merit Factors with non-vanishing asymptotes.

I. Introduction

We introduce the *Multi-dimensional aperiodic Merit Factor* (MMF) metric and provide infinite binary constructions for which the MMF can be computed exactly. Unlike the MMF, the *one-dimensional* aperiodic *Merit Factor* (MF) has a long history [6], as sequences with high MF have applications in telecommunications, information theory, physics, and chemistry. However they are also very difficult to find and/or construct, in particular as sequence length increases. Merit Factor is interesting because $\frac{1}{\text{MF}}$ evaluates the squared-difference between the *continuous* power Fourier spectrum of the sequence and the flat power spectrum. If the MF of a sequence is large, then the continuous Fourier power spectrum of the sequence is nearly flat, which is a very desirable property in many contexts. Similarly, $\frac{1}{\text{MMF}}$ evaluates the squared-difference between the continuous multi-dimensional Fourier power spectrum and the flat multi-dimensional Fourier power spectrum.

Rudin-Shapiro sequences [18], [17], [1] are the foremost example of Golay Complementary Sequences [5], and their interpretation as certain Reed-Muller, $\text{RM}(1,m)$, cosets of $\text{RM}(2,m)$ has recently been exploited by Davis and Jedwab [3], and generalised by Parker and Tellambura [16]. The fundamental Rudin-Shapiro set possesses an aperiodic Merit Factor that can be computed *exactly* for any length $N = 2^n$ by means of a recursion on sum-of-squares values [9]

$$\sigma_n = 2\sigma_{n-1} + 8\sigma_{n-2}$$

where σ_n is the sum-of-squares value for a sequence of length 2^n. The Merit Factor (MF) of a sequence is given by

$$\text{MF} = \frac{N^2}{2\sigma_n}$$

so the asymptotic MF of the fundamental Rudin-Shapiro set is 3. The recursion on sum-of-squares is a surprising and satisfying number-theoretic result, and motivates the question as to whether other sequence constructions can be found which obey similar recursive formulas for their one-dimensional sum-of-squares values. In this paper we identify, computationally, a number of constructions for which similar recursions appear to exist. Although we examine the one-dimensional Merit Factor for certain sequence constructions, our primary aim here is to introduce the *aperiodic Multi-dimensional Merit Factor* (MMF) as an interesting metric for sequences of length $N = 2^n$. In particular, we identify certain infinite sequence constructions where the MMF can be computed exactly because the multi-dimensional sum-of-squares values obey recursions. To the best of our knowledge the aperiodic MMF is a new metric. However, the *periodic* sum-of-squares metric is already known, and is considered a useful measure of cryptographic strength for boolean functions used in the design of certain stream ciphers [19]. Moreover, the multi-dimensional *periodic* autocorrelation is the underlying structure exploited by Differential Cryptanalysis, as applied to Block Ciphers. The novelty in this paper is that we propose to examine *aperiodic* measures as opposed to *periodic* measures. One implicit aim of this work is to determine the large-scale properties of undirected graphs constructed from simple local rules, as we envisage that graphs of this type will have application to the design of iterative decoders for Low-Density Parity Check Codes [10], and also to the future design of practical quantum computers [14], [15], [4], [8]. For the constructions proposed in this paper, the MMF is found to have a constant asymptote in a number of cases. For those cases where there is no asymptote, the MMF vanishes as the sequence length, N, goes to infinity. This is similar to the one-dimensional case, where the MF either has an asymptote or vanishes. We therefore conjecture that no one-dimensional or multi-dimensional binary sequence construction exists such that the MF or MMF, respectively, of the sequence goes to infinity as N goes to infinity. The highest asymptotic MF known is $\simeq 6.34$ [12], [2], but we have not yet found a binary sequence construction for which the MMF has a higher asymptote than 3.0. This may be because we have, thus far, only considered sequences constructed from quadratic boolean functions.

T.A. Gulliver is with the Dept. of Elec. & Computer Eng., University of Victoria, P.O.Box 3055, STN CSC, Victoria, B.C., Canada V8W 3P6 E-mail: `agullive@ece.uvic.ca`

M.G. Parker is with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: `matthew@ii.uib.no`. Web: `http://www.ii.uib.no/~matthew/`

II. Definitions and Theory

A. The One-Dimensional Case

The one-dimensional aperiodic autocorrelation of a length N sequence, $\mathbf{s}$, is defined as

$$a_k = \sum_{i=0}^{N-1} s_i s_{i+k}^*, \qquad -N < k < N \tag{1}$$

where $s_i \in \mathcal{C}$, $s_i = 0$ for $i < 0$ and $i \geq N$, and $*$ means complex conjugate.

The sum-of-squares value, σ, is then given by

$$2\sigma = \sum_{k=1-N, k\neq 0}^{N-1} |a_k|^2. \tag{2}$$

The one-dimensional aperiodic Merit Factor is defined as

$$\mathrm{MF} = \frac{N^2}{2\sigma} \tag{3}$$

where 2σ is the sum-of-squares of the one-dimensional aperiodic autocorrelation coefficients, excluding the zero'th coefficient. (The factor of 2 is required because σ only takes into account half of the coefficients and by symmetry, the other half will be identical). The Aperiodic Merit Factor has a particularly nice interpretation in the spectral domain as the integral of the squared difference between its power spectrum and the flat power spectrum. By Parseval's theorem, the sum-of-squares of the autocorrelation coefficients, including N^2 for the zero'th coefficient, is equal to the sum of the square of the power spectrum coefficients, χ, where

$$\chi = N^2 + 2\sigma. \tag{4}$$

For a completely flat spectrum, $\chi = N^2$. The sum of the difference between χ and the flat power spectrum is given by $\chi - N^2$. We normalise this value by dividing by N^2. Therefore the normalised difference is given by

$$\frac{\chi - N^2}{N^2} = \frac{2\sigma}{N^2} = \frac{1}{\mathrm{MF}}. \tag{5}$$

We can also think of the sequence, $\mathbf{s}$, as a polynomial, $s(z) = s_0 + s_1 z + s_2 z^2 + \ldots + s_{N-1} z^{N-1}$. Then the aperiodic autocorrelation of $\mathbf{s}$ can also be computed as the polynomial multiplication,

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

where the coefficients of $a(z)$ are the aperiodic autocorrelation coefficients.

Finding the Merit Factor of a sequence, $\mathbf{s}$, is equivalent to finding its L_4-norm. The L_α-norm, $\|\mathbf{s}\|_\alpha$, is computed by integrating the αth power of the evaluations of $s(x)$ on the unit circle, and then taking the αth root of the result [13].

$$\|\mathbf{s}\|_\alpha = \left(\frac{1}{2\pi}\int_0^{2\pi} |s(e^{i\theta})|^\alpha d\theta\right)^{1/\alpha} \tag{7}$$

where $i^2 = -1$. Then,

$$\frac{1}{\mathrm{MF}(\mathbf{s})} = \frac{\|\mathbf{s}\|_4^4 - \|\mathbf{s}\|_2^4}{\|\mathbf{s}\|_2^4} \tag{8}$$

where, from (5), $\|\mathbf{s}\|_4^4 = \chi$ and $\|\mathbf{s}\|_2^4 = N^2$.

B. The Multi-Dimensional Case

For the multi-dimensional case we proceed in a similar fashion to the one-dimensional case above (in this paper we only consider the case where each dimension is of length 2). Let $\mathbf{i}$, $\mathbf{k}$ and $\mathbf{v}$ be length n vectors such that,

$$\mathbf{i} = (i_0, i_1, \ldots, i_{n-1}), \qquad \mathbf{k} = (k_0, k_1, \ldots, k_{n-1}), \qquad \mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \tag{9}$$

where $i_j \in \{0, 1\}$, $k_j \in \{-1, 0, 1\}$, and $v_j \in \{-1, 0, 1, 2\}$, $\forall j$.

We define the length $N = 2^n$ sequence, $\mathbf{s}$, to have elements $s_{\mathbf{i}} \in \mathcal{C}$. We can also think of $\mathbf{s}$ as having elements s_i, where i is the radix-2 evaluation of vector $\mathbf{i}$ such that $i = \sum_{j=0}^{n-1} i_j 2^j$. Aperiodicity of $\mathbf{s}$ is ensured as follows

$$\mathbf{s} \text{ is multi-dimensionally aperiodic iff } s_{\mathbf{i}} = 0, \qquad \{\forall \mathbf{i} | i_j \notin \{0,1\}, \text{ for one or more } j \text{ values}\}$$

We now define the vector operation '+' as follows

$$\mathbf{v} = \mathbf{i} + \mathbf{k} \qquad \text{implies } v_j = i_j + k_j,$$

Therefore the multi-dimensional aperiodic autocorrelation of $\mathbf{s}$ is defined by

$$a_{\mathbf{k}} = \sum_{\mathbf{i}=(00\ldots0)}^{\mathbf{i}=(11\ldots1)} s_{\mathbf{i}} s^*_{\mathbf{i}+\mathbf{k}}, \qquad k_j \in \{-1,0,1\}, \forall j \tag{10}$$

There are 3^n multi-dimensional aperiodic autocorrelation coefficients, a_k, because $k_j \in \{-1,0,1\}$. However

$$a_{\mathbf{k}} = a^*_{\mathbf{k}'}, \qquad \text{if } k'_j = -k_j, \forall j$$

Therefore, if we exclude $\mathbf{k} = 0$, there are only $\frac{3^n-1}{2}$ different sum-of-square values, $|a_{\mathbf{k}}|^2$, to consider. The sum-of-squares of the aperiodic autocorrelation coefficients is

$$2\sigma = \sum_{\mathbf{k}|k_j \in \{-1,0,1\}, \forall j, \mathbf{k} \neq 0} |a_{\mathbf{k}}|^2. \tag{11}$$

The multi-dimensional Merit Factor is given by

$$\text{MMF} = \frac{N^2}{2\sigma}. \tag{12}$$

We can also think of the sequence, $\mathbf{s}$ as a polynomial

$$s(\mathbf{z}) = s(z_0, z_1, \ldots, z_{n-1}) = s_0 + s_1 z_0 + s_2 z_1 + s_3 z_0 z_1 + s_4 z_2 + \ldots + s_{2^n-1} z_0 z_1 z_2 \ldots z_{n-1} \tag{13}$$

The multi-dimensional aperiodic autocorrelation of $\mathbf{s}$ is then given by the coefficients of

$$a(z_0, z_1, \ldots, z_{n-1}) = s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})^* \tag{14}$$

2σ is therefore equal to the sum-of-squares of the out-of-phase coefficients of $a(z_0, z_1, \ldots, z_{n-1})$.

The Multi-dimensional Merit Factor of an n-dimensional sequence, $\mathbf{s}$, is equivalent to finding its $L_{n,4}$-norm, where we define the $L_{n,\alpha}$-norms as the multi-integral of the αth power of the simultaneous evaluations of $s(\mathbf{x})$ on n unit circles, and then taking the αth root of the result. We thus define the $L_{n,\alpha}$-norm of a sequence, $\mathbf{s}$, by

$$\|\mathbf{s}\|_{n,\alpha} = \left(\frac{1}{(2\pi)^n} \int_0^{2\pi} \int_0^{2\pi} \ldots \int_0^{2\pi} |s(e^{i\theta_0}, e^{i\theta_1}, \ldots, e^{i\theta_{n-1}})|^\alpha d\theta_0 d\theta_1 \ldots d\theta_{n-1} \right)^{1/\alpha}. \tag{15}$$

Then

$$\frac{1}{\text{MMF}(\mathbf{s})} = \frac{\|\mathbf{s}\|^4_{n,4} - \|\mathbf{s}\|^4_{n,2}}{\|\mathbf{s}\|^4_{n,2}} \tag{16}$$

where $\|\mathbf{s}\|^4_{n,4} = \chi$ and $\|\mathbf{s}\|^4_{n,2} = N^2$.

C. Multi-dimensional Symmetries

The MMF metric induces invariance classes under certain symmetry operations. Let the $\mathbf{i}$th element of $\mathbf{s}$ be $s_{\mathbf{i}}$, where $\mathbf{i}$ is, itself, a vector with elements $i_j \in \{0,1\}$.

C.1 Symmetric Permutation

Unlike the one-dimensional Merit Factor, the multi-dimensional Merit Factor is always invariant with respect to a certain large subset of permutations of the sequence indices. Let $\pi : Z_n \rightarrow Z_n$ be any permutation of Z_n, and

$$\mathbf{i}' = (i_{\pi(0)}, i_{\pi(1)}, \ldots, i_{\pi(n-1)}) \tag{17}$$

where $\mathbf{i}$ was previously defined in (9). If $s'_{\mathbf{i}'} = s_{\mathbf{i}}$, $\forall \mathbf{i}$, then $\text{MMF}(\mathbf{s}') = \text{MMF}(\mathbf{s})$.

C.2 Affine Offset

We define the affine offset as taking $\mathbf{s}$ to $\mathbf{s}'$, where

$$s'_{\mathbf{i}} = (-1)^{e+\sum_{j=0}^{n-1} d_j i_j} s_{\mathbf{i}} \tag{18}$$

where $e, d_j \in \{0,1\}, \forall j$. Then $\text{MMF}(\mathbf{s}') = \text{MMF}(\mathbf{s})$.

C.3 Multi-dimensional Cyclic Shift

Let $\mathbf{f} = (f_0, f_1, \ldots, f_{n-1})$ be a length n vector where $f_j \in \{0,1\}$, $\forall j$. Then, if $\mathbf{s}'$ is such that

$$s'_{\mathbf{i}} = s_{\mathbf{i}\oplus\mathbf{f}} \tag{19}$$

where $\mathbf{i} \oplus \mathbf{f}$ implies $i_j \oplus f_j$, $\forall j$, where '$\oplus$' means addition, mod 2, then $\text{MMF}(\mathbf{s}') = \text{MMF}(\mathbf{s})$.

D. Tensor Product of Sequences

Let $\mathbf{s_0}$ and $\mathbf{s_1}$ be two sequences of lengths N_0 and N_1, respectively, with values σ_0 and σ_1 for their sum-of-squares, respectively, whether one- or multi- dimensional. Let $\mathbf{s}$ be the length $N_0 N_1$ sequence, $\mathbf{s} = \mathbf{s_0} \otimes \mathbf{s_1}$, where '$\otimes$' means tensor product. Then the one or multi-dimensional sum-of-squares value, σ, of $\mathbf{s}$ satisfies

$$\sigma = 2\sigma_0\sigma_1 + N_0^2\sigma_1 + N_1^2\sigma_0. \tag{20}$$

For the special case where $\sigma_0 = \sigma_1$ and $N_0 = N_1$, (20) reduces to,

$$\sigma = 2\sigma_0(\sigma_0 + N^2). \tag{21}$$

Equations (20) and (21) allow us to concentrate on constructions which cannot be written as tensor products. From (12) and (20), the MF or MMF of the tensor product of $\mathbf{s_0}$ and $\mathbf{s_1}$ always vanishes as $N \to \infty$.

E. Using Algebraic Normal Form (ANF) to Represent Sequences

Consider the multivariate boolean function

$$p(\mathbf{x}) = p(x_0, x_1, \ldots, x_{n-1}) \qquad : \qquad Z_2^n \to Z_2$$

where $x_i \in Z_2$. Then $\mathbf{s} = s(\mathbf{x}) : Z_2^n \to \{1, -1\}$, can be defined by

$$\mathbf{s} = s(\mathbf{x}) = (-1)^{p(\mathbf{x})}. \tag{22}$$

We use the ANF to describe $p(\mathbf{x})$, and hence $\mathbf{s}$, where

$$p(\mathbf{x}) = p_0 + p_1x_0 + p_2x_1 + p_3x_0x_1 + \ldots + p_{2^n-1}x_0x_1\ldots x_{n-1}, \qquad p_j \in Z_2.$$

F. Aperiodic Multi-dimensional Autocorrelation of Algebraic Normal Forms

Let $\mathbf{s} = s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$. We can write $a_{\mathbf{k}}$ in terms of $p(\mathbf{x})$, as follows. Let $\mathbf{Q}_k$ and $\mathbf{R}_k$ be integer sets where, for a given $\mathbf{k}$ with $k_j \in \{-1, 0, 1\}$

$$\mathbf{Q_k} = \{t | k_t = 1\}, \qquad \mathbf{R_k} = \{t | k_t = -1\}.$$

Define $q(\mathbf{x})_{\mathbf{k}}$ to be $p(\mathbf{x})$ restricted to the subspace obtained when all variables x_t, with indicies, t, in $\mathbf{Q} \bigcup \mathbf{R}$, are fixed.

$$q(\mathbf{x})_{\mathbf{k}} = p(\mathbf{x})_{\substack{x_t = 0, \forall t \in \mathbf{Q_k} \\ x_t = 1, \forall t \in \mathbf{R_k}}} + p(\mathbf{x})_{\substack{x_t = 1, \forall t \in \mathbf{Q_k} \\ x_t = 0, \forall t \in \mathbf{R_k}}} \tag{23}$$

$q(\mathbf{x})_{\mathbf{k}}$ is defined over a subspace of $n - |\mathbf{Q_k}| - |\mathbf{R_k}|$ binary variables, and $a_{\mathbf{k}}$ is related to the weight of $q(\mathbf{x})_{\mathbf{k}}$ as follows

$$a_{\mathbf{k}} = 2\text{wt}(q(\mathbf{x})_{\mathbf{k}}) - 2^{n-|\mathbf{Q_k}|-|\mathbf{R_k}|} \tag{24}$$

where 'wt(q)' means the binary weight of the output of q when evaluated over the remaining variables in $\mathbf{x}$ that are not contained in $\mathbf{Q} \bigcup \mathbf{R}$. In this paper we only construct $p(\mathbf{x})$ with quadratic form. When $p(\mathbf{x})$ is quadratic then $q(\mathbf{x})_{\mathbf{k}}$ only has degree 0 or 1, in which case (24) simplifies to

$$\begin{array}{ll} a_{\mathbf{k}} = 0 & \deg(q(\mathbf{x})_{\mathbf{k}}) = 1 \\ a_{\mathbf{k}} = 2^{n-|\mathbf{Q_k}|-|\mathbf{R_k}|} & \deg(q(\mathbf{x})_{\mathbf{k}}) = 0. \end{array} \tag{25}$$

Moreover, when $p(\mathbf{x})$ is quadratic it is straightforward to show the following, using (23) and (25)

$$a_{\mathbf{k}} = a_{\mathbf{k}'} \qquad \text{iff } \deg(p(\mathbf{x})) = 2 \text{ and } k_j = 0 \Rightarrow k'_j = 0. \tag{26}$$

Therefore, in this paper we only consider $a_{\mathbf{k}}$, where $k_j \in \{0,1\}$ as the case $k_j = -1$ is the same as for $k_j = 1$. The MMF invariance symmetries of subsection II-C are simply described using the ANF. Equation (17) is equivalent to invariance with respect to the permutation $x_j \to x_{\pi(j)}$. (18) is equivalent to invariance with respect to the operation $p(\mathbf{x}) \to p(\mathbf{x}) + (\sum_{j=0}^{n-1} d_j x_j) + e$, $e, d_j \in \{0,1\}$, $\forall j$. Finally, (19) is equivalent to invariance with respect to substituting $x_j + 1$ for x_j in $p(\mathbf{x})$, for any j.

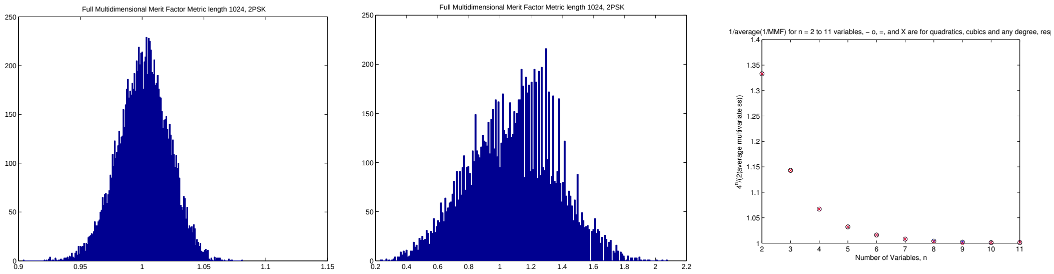

Fig. 1. Random MMFs for $n = 10$: (left) - general, (middle) - quadratic, (right) - $\frac{1}{\text{average}(\frac{1}{\mathcal{MMF}})}$ for sampled quadratics, 'o', cubics, 'x', and boolean functions of any degree, 'X', for $n = 2$ to 11

III. An Overview of Multi-Dimensional Merit Factor (MMF) for Binary Sequences

A. *The MMF of Worst-Case and Best-Case Binary Sequences*

The worst-case (lowest possible) MMF occurs when $p(\mathbf{x})$ is constant or linear. The maximum possible σ satisfies $\sigma_n = 6\sigma_{n-1} + 2^{2n-2} = \frac{6^n - 4^n}{2}$, giving a minimum MMF of $\frac{2^n}{3^n - 2^n}$. This worst-case MMF vanishes as $n \to \infty$. It is an open-problem as to the best-case (highest possible) MMF. The highest MMF found so far is for the trivial length $N = 4$ binary sequence where $p(\mathbf{x}) = x_0 x_1$, which attains an MMF of 4.0.

B. *The MMF of a Random Binary Sequence and of a Random Quadratic Binary Sequence*

Fig 1 (left) shows computations for the expected MMF for a random binary sequence when $n = 10$ (12000 samples). The average MMF for n from 4 to 15 is plotted in Fig 1 (right) with an 'o'. The average MMF of a random binary sequence appears to be around 1.0, similar to the one-dimensional case [11]. We are particularly interested in cases where the MMF asymptote is greater than 1.0. However constructions that only achieve an asymptote of 1.0 are still interesting as they provide a non-vanishing asymptote via a simple recursive (non-random) construction. Next we computed the expected MMF for $\mathbf{s} = s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$ where $p(\mathbf{x})$ is a homogeneous quadratic function. Fig 1 (middle) shows the results for $n = 10$ (12000 samples). One can also compute the average multivariate sum-of-squares for a given number of variables, n, and Fig 1 (right) shows the results for $n = 2$ to $n = 11$ variables, expressed as $\frac{1}{\text{average}(1/\mathcal{MMF})}$ for samplings of quadratics, cubics, and boolean functions of any degree. The results suggest that the asymptotic average multivariate sum-of-squares is $2^{n-1}(2^n - 1)$, leading to an average value for $\frac{1}{\mathcal{FM}}$ of 1.0.

IV. Some Constructions

We examine a number of constructions for quadratic boolean functions, determine the recursions obeyed by the sum-of-squares and, from these recursions, identify whether or not the MMF and/or MF asymptote is a non-vanishing constant. We refer to the constructions by self-evident, graphical names. Table IV gives the MMF results. For instance, the Star construction satisfies the sum-of-squares recursion, $\sigma_n = 4 \times (3\sigma_{n-1} - 11\sigma_{n-2} + 12\sigma_{n-3})$ so that $\sigma_n = 2^n - \frac{4^n}{2} + \frac{6^n}{6}$, giving an asymptotic MMF of 0 as $n \to \infty$. All proofs are omitted because of page limitations.

Table IV gives the computational MF results for those graphs for which we were able to ascertain a recursive relationship. It remains an open problem to prove these results (apart from the Line [9]).

V. Conclusion

Recursions have been identified for the Multidimensional and One-dimensional Merit Factors of some binary quadratic sequence constructions. Open problems as to the highest possible Merit Factors remain, asymptotic or otherwise.

References

[1] P. Borwein and M. Mossinghoff, "Rudin-Shapiro Like Polynomials in L_4", http://www.cecm.sfu.ca/~pborwein/ 1997.
[2] P. Borwein, S. Choi, J. Jedwab, "Binary Sequences with Merit Factor Greater than 6.34", http://www.cecm.sfu.ca/~pborwein/, 2003.
[3] J.A. Davis and J. Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp 2397–2417, Nov. 1999.
[4] D.G. Glynn, "On Self-Dual Quantum Codes and Graphs", submitted to *Electronic J. Combin.*, http://homepage.mac.com/dglynn/quantum_files/Personal3.html, Apr. 2000.
[5] M.J.E. Golay, "Complementary Series", *IRE Trans. Inform. Theory*, vol. 7, pp. 82–87, Apr. 1961.
[6] M.J.E. Golay, "Sieves for Low Autocorrelation Binary Sequences", *IEEE Trans. Inform. Theory*, vol. 23, no. 1, pp 43–51, Jan. 1977.
[7] M. Grassl, A. Klappenecker and M. Rotteler, "Graphs, Quadratic Forms, and Quantum Codes," Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, June–July, 2002.
[8] M. Hein, J. Eisert and H.J. Briegel, "Multi-Party Entanglement in Graph States", *quant-ph/0307130 v2*, July 2003.
[9] T. Høholdt, H.E. Jensen and J. Justesen, "Aperiodic Correlations and the Merit Factor of a Class of Binary Sequences," *IEEE Trans. Inform. Theory*, vol. 31, no. 4, pp 549–552, July 1985.
[10] "Special Issue on Codes on Graphs and Iterative Algorithms", *IEEE Trans. Inform. Theory*, vol. 47, no. 2, Feb. 2001.

Graph	$p(\mathbf{x})$	σ_n: Recursion	MMF Asymp.
	σ_n: Closed-Form		
Line	$\sum_{i=0}^{n-2} x_i x_{i+1}$	$2\sigma_{n-1} + 8\sigma_{n-2}$	3
	$\frac{4^n}{6} - \frac{(-2)^n}{6}$		
Circle	$x_{n-1}x_1 + \sum_{i=0}^{n-2} x_i x_{i+1}$	$2\sigma_{n-1} + 8\sigma_{n-2}$	1
	$\frac{(-2)^n}{2} + \frac{4^n}{2}$		
Clique	$\sum_{i=0,j<i}^{i=n-1} x_i x_j$	$2 \times (5\sigma_{n-1} - 10\sigma_{n-2} - 20\sigma_{n-3} + 48\sigma_{n-4})$	0
	$\frac{2^n}{2} + \frac{6^n}{4} - \frac{4^n}{2} - \frac{(-2)^n}{4}$		
Star	$x_0 \sum_{i=1}^{n-1} x_i$	$4 \times (3\sigma_{n-1} - 11\sigma_{n-2} + 12\sigma_{n-3})$	0
	$2^n - \frac{4^n}{2} + \frac{6^n}{6}$		
Triangles	$x_0x_1 + \sum_{i=0}^{n-3} x_i x_{i+2} + x_{i+1}x_{i+2}$	$2\sigma_{n-1} + 16\sigma_{n-3} + 256\sigma_{n-5}$	$\frac{5}{3}$
	$(\frac{5}{84}i\sqrt{7} - \frac{1}{12})(1+\sqrt{7}i)^n - (\frac{5}{84}i\sqrt{7} + \frac{1}{12})(1-\sqrt{7}i)^n - (\frac{1}{15} + \frac{2}{15}i)(-2+2i)^n - (\frac{1}{15} - \frac{2}{15}i)(-2-2i)^n + \frac{3}{10}4^n$		
Squares	$x_0x_1 + \sum_{i=0}^{n/2-1} x_{2i}x_{2i+2} + x_{2i+1}x_{2i+3} + x_{2i+2}x_{2i+3}$	$12\sigma_{n-2} + 32\sigma_{n-4} + 1024\sigma_{n-6} - 8192\sigma_{n-8}$	$\frac{5}{3}$
n even	$3\frac{16^n}{10} + \left(\sum_r \frac{(384r^2-40r-3)(\frac{1}{r})^n}{(15360r^2-640r-40)r}\right), r \in$ roots of $512z^3 - 32z^2 - 4z - 1$		
Wheel	$(x_0 \sum_{i=1}^{n-1} x_i) + x_{n-1}x_1 + \sum_{i=0}^{n-2} x_i x_{i+1}$	$4\sigma_{n-2} + 32\sigma_{n-3} + 64\sigma_{n-4}$	1
	$\frac{4^n}{2} - \frac{(-2)^n}{2} - (\frac{1}{4} + \frac{1}{4}i\sqrt{7})(-1+\sqrt{7}i)^n + (-\frac{1}{4} + \frac{1}{4}i\sqrt{7})(-1-\sqrt{7}i)^n$		

TABLE I
PROVEN RESULTS FOR THE MULTIDIMENSIONAL MERIT FACTOR OF VARIOUS CONSTRUCTIONS

Graph	$p(\mathbf{x})$	σ_n: Recursion	MF Asymp.
	σ_n: Closed-Form		
Line[9]	$\sum_{i=0}^{n-2} x_i x_{i+1}$	$2\sigma_{n-1} + 8\sigma_{n-2}$	3
	$\frac{4^n}{6} - \frac{(-2)^n}{6}$		
Circle	$x_{n-1}x_1 + \sum_{i=0}^{n-2} x_i x_{i+1}$	$4\sigma_{n-1} + 12\sigma_{n-2} - 64\sigma_{n-3} + 256\sigma_{n-5}$	1
	$\frac{(-2)^n}{2} + \frac{4^n}{2} + \left(\sum_r \frac{-(1-2r)(\frac{1}{r})^n}{(192r^2-32r-4)r}\right), r \in$ roots of $32z^3 - 8z^2 - 2z + 1$		
Clique	$\sum_{i=0,j<i}^{i=n-1} x_i x_j$	$10\sigma_{n-1} - 36\sigma_{n-2} + 88\sigma_{n-3} - 96\sigma_{n-4} - 512\sigma_{n-5} + 1024\sigma_{n-6}$	0
	$\frac{2^n}{2} - \frac{4^n}{2} - \frac{(-2)^n}{4} + \left(\sum_r \frac{-(1+16r^2)(\frac{1}{r})^n}{(768r^2-128r+24)r}\right), r \in$ roots of $64z^3 - 16z^2 + 6z - 1$		
Star	$x_0 \sum_{i=1}^{n-1} x_i$	$16\sigma_{n-1} - 68\sigma_{n-2} - 48\sigma_{n-3} + 768\sigma_{n-4} - 1024\sigma_{n-5}$	0
	$\frac{8^n}{24} - \frac{4^n}{2} + \frac{13\cdot 2^n}{12} + (\frac{3\sqrt{17}}{272} + \frac{1}{16})(1+\sqrt{17})^n + (\frac{1}{16} - \frac{3\sqrt{17}}{272})(1-\sqrt{17})^n$		

TABLE II
COMPUTATIONAL RESULTS FOR THE MERIT FACTOR OF VARIOUS CONSTRUCTIONS

[11] T. Høholdt, "The Merit Factor of Binary Sequences", *Difference Sets, Sequences and their Correlation Properties*, A. Pott et al. (eds.), Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers, vol. 542, pp 227–237, 1999.

[12] R. Kristiansen and M.G. Parker, "Binary Sequences with Asymptotic Aperiodic Merit Factor > 6.3," submitted to *IEEE Trans. Inform. Theory*, June 2003.

[13] J.E. Littlewood, *Some Problems in Real and Complex Analysis,* Heath Mathematical Monographs, Lexington, MA, 1968.

[14] M.G. Parker, "Quantum Factor Graphs," *Annals of Telecom.'*, pp. 472–483, July–Aug. 2001, (preprint: quant-ph/0010043 2000).

[15] M.G. Parker and V. Rijmen, "The Quantum Entanglement of Binary and Bipolar Sequences," short version in *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science Series, SpringerVerlag, 2001, long version at *http://xxx.soton.ac.uk/ps/quant-ph/0107106* or *http://www.ii.uib.no/∼matthew/* June 2001.

[16] M.G. Parker and C. Tellambura, "A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio", *Technical Report No 242*, Dept. of Informatics, University of Bergen, Norway, Feb 2003.

[17] W. Rudin, "Some Theorems on Fourier Coefficients", *Proc. Amer. Math. Soc.*, vol. 10, pp. 855–859, 1959.

[18] H.S. Shapiro, *Extremal Problems for Polynomials,* M.S. Thesis, M.I.T., 1951.

[19] X.-M. Zhang and Y. Zheng, "GAC - the Criterion for Global Avalanche Characteristics of Cryptographic Functions", *J. Universal Computer Science*, vol. 1, no. 5, pp. 320–337, 1995.