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, RM(1, m), cosets of 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 $\sigma_n$ 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 $\approx 6.34$ [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, Høytteknologisenteret 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, $s$, is defined as

$$a_k = \sum_{i=0}^{N-1} s_i s^*_{i+k}, \quad -N < k < N$$

(1)

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

The sum-of-squares value, $\sigma$, is then given by

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

(2)

The one-dimensional aperiodic Merit Factor is defined as

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

(3)

where $2\sigma$ is the sum-of-squares of the one-dimensional aperiodic autocorrelation coefficients, excluding the zero'th coefficient. (The factor of 2 is required because $\sigma$ 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, $\chi$, where

$$\chi = N^2 + 2\sigma.$$  

(4)

For a completely flat spectrum, $\chi = N^2$. The sum of the difference between $\chi$ 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

$$\frac{\chi - N^2}{N^2} = \frac{2\sigma}{N^2} = \frac{1}{\text{MF}}.$$  

(5)

We can also think of the sequence, $s$, 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 $s$ can also be computed as the polynomial multiplication,

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

(6)

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

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

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

(7)

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

$$\frac{1}{\text{MF}(s)} = \frac{\|s\|_4^4 - \|s\|_2^4}{\|s\|_2^4}$$

(8)

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

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 $i$, $k$ and $v$ be length $n$ vectors such that,

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

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

$s$ is multi-dimensionally aperiodic iff $s_i = 0$, \quad $\forall i \in Z, j \in \{0, 1\}$, for one or more $j$ values

We now define the vector operation ‘+’ as follows

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

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

$$a_k = \sum_{i=(11,1)}^{i=(00,0)} s_i \overline{s_{i+k}}, \quad k_j \in \{-1, 0, 1\}, \forall j$$

(10)

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

$$a_k = a_{k'}^*,$$ \quad if $k'_j = -k_j, \forall j$

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

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

(11)

The multi-dimensional Merit Factor is given by

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

(12)

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

$$s(z) = s(z_0, z_1, \ldots, z_{n-1}) = s_0 + s_1 z_1 + s_2 z_1^2 + s_3 z_1^3 + \ldots + s_{n-1} z_{n-1}.$$  

(13)

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

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

(14)

$2\sigma$ 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 $\alpha$th power of the simultaneous evaluations of $s(x)$ on $n$ unit circles, and then taking the $\alpha$th root of the result. We thus define the $L_{n,4}$-norm of a sequence, $\mathbf{s}$, by

$$\|s\|_{n,\alpha} = \left(\int_{0}^{2\pi} \int_{0}^{2\pi} \cdots \int_{0}^{2\pi} \left|s(e^{i\theta_0}, e^{i\theta_1}, \ldots, e^{i\theta_{n-1}})\right|^\alpha d\theta_0 d\theta_1 \ldots d\theta_{n-1}\right)^{1/\alpha}.$$  

Then

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

(16)

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

C. Multi-dimensional Symmetries

The MMF metric induces invariance classes under certain symmetry operations. Let the $i$th element of $\mathbf{s}$ be $s_i$, where $i$ 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

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

(17)

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

C.2 Affine Offset

We define the affine offset as taking \( s \) to \( s' \), where
\[
s'_i = (-1)^{e + \sum_{j=1}^{n} d_j i_j} s_i
\]
where \( e, d_j \in \{0, 1\}, \forall j \). Then \( \text{MMF}(s') = \text{MMF}(s) \).

C.3 Multi-dimensional Cyclic Shift

Let \( f = (f_0, f_1, \ldots, f_{n-1}) \) be a length \( n \) vector where \( f_j \in \{0, 1\}, \forall j \). Then, if \( s' \) is such that
\[
s'_i = s_{i \oplus f}
\]
where \( i \oplus f \) implies \( i_j \oplus f_j, \forall j \), where \( \oplus \) means addition, mod 2, then \( \text{MMF}(s') = \text{MMF}(s) \).

D. Tensor Product of Sequences

Let \( s_0 \) and \( s_1 \) be two sequences of lengths \( N_0 \) and \( N_1 \), respectively, with values \( \sigma_0 \) and \( \sigma_1 \) for their sum-of-squares, respectively, whether one- or multi-dimensional. Let \( s \) be the length \( N_0 N_1 \) sequence, \( s = s_0 \otimes s_1 \), where \( \otimes \) means tensor product. Then the one or multi-dimensional sum-of-squares value, \( \sigma \), of \( s \) satisfies
\[
\sigma = 2\sigma_0 \sigma_1 + N^2_0 \sigma_1 + N^2_1 \sigma_0.
\]
For the special case where \( \sigma_0 = \sigma_1 \) and \( N_0 = N_1 \), (20) reduces to,
\[
\sigma = 2\sigma_0 (\sigma_0 + N^2).
\]
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 \( s_0 \) and \( s_1 \) always vanishes as \( N \to \infty \).

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

Consider the multivariate boolean function
\[ p(x) = p(x_0, x_1, \ldots, x_{n-1}) : Z^n_2 \to Z_2 \]
where \( x_i \in Z_2 \). Then \( s = s(x) : Z^n_2 \to \{1, -1\} \), can be defined by
\[
s = s(x) = (-1)^{p(x)}.
\]
We use the ANF to describe \( p(x) \), and hence \( s \), where
\[
p(x) = p_0 + p_1 x_0 + p_2 x_1 + p_3 x_0 x_1 + \ldots + p_{2^n-1} x_0 x_1 \ldots x_{n-1}, \quad p_j \in Z_2.
\]

F. Aperiodic Multi-dimensional Autocorrelation of Algebraic Normal Forms

Let \( s = s(x) = (-1)^{p(x)} \). We can write \( a_k \) in terms of \( p(x) \), as follows. Let \( Q_k \) and \( R_k \) be integer sets where, for a given \( k \) with \( k_j \in \{-1, 0, 1\} \)
\[
Q_k = \{t | k_t = 1\}, \quad R_k = \{t | k_t = -1\}.
\]

Define \( q(x)_k \) to be \( p(x) \) restricted to the subspace obtained when all variables \( x_t \), with indicies, \( t \), in \( Q \cup R \), are fixed.
\[
q(x)_k = p(x) |_{x_t = 0, \forall t \in Q_k} + p(x) |_{x_t = 1, \forall t \in R_k}
\]
\[
(23)
\]
\( q(x)_k \) is defined over a subspace of \( n - |Q_k| - |R_k| \) binary variables, and \( a_k \) is related to the weight of \( q(x)_k \) as follows
\[
a_k = 2wt(q(x)_k) - 2^{n - |Q_k| - |R_k|}
\]
\[
(24)
\]
where \( \text{wt}(q) \) means the binary weight of the output of \( q \) when evaluated over the remaining variables in \( x \) that are not contained in \( Q \cup R \). In this paper we only construct \( p(x) \) with quadratic form. When \( p(x) \) is quadratic then \( q(x)_k \) only has degree 0 or 1, in which case (24) simplifies to
\[
a_k = 0 \quad \text{iff} \quad \deg(p(x)) = 2 \quad \text{and} \quad k_j = 0 \Rightarrow k'_j = 0.
\]
\[
(25)
\]
Moreover, when \( p(x) \) is quadratic it is straightforward to show the following, using (23) and (25)
\[
a_k = a_k \quad \text{iff} \quad \deg(p(x)) = 2 \quad \text{and} \quad k_j = 0 \Rightarrow k'_j = 0.
\]
\[
(26)
\]
Therefore, in this paper we only consider \( a_k \), 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 \( p(x) \to p(x) + (\sum_{j=0}^{n-1} d_j x_j) + e, e, d_j \in \{0, 1\}, \forall j \). Finally, (19) is equivalent to invariance with respect to substituting \( x_j + 1 \) for \( x_j \) in \( p(x) \), for any \( j \).
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 \( p(x) \) is constant or linear. The maximum possible \( \sigma \) satisfies \( \sigma_n = 6\sigma_{n-1} + 2^{2n-2} - \frac{6^n - 4^n}{2} \), giving a minimum MMF of \( \frac{2^n}{\sigma_n} \). 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 \( p(x) = x_0x_1 \), 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.

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 graph satisfies the sum-of-squares recursion, \( \sigma_n = 4 \times (3\sigma_{n-1} - 11\sigma_{n-2} + 12\sigma_{n-3}) \) so that \( \sigma_n = 2^n - \frac{12}{5} + \frac{6^n}{5} \), 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

\section*{Proven Results for the Multidimensional Merit Factor of Various Constructions}

\begin{table}[h]
\centering
\begin{tabular}{|l|l|l|}
\hline
Graph & \( p(x) \) & \( \sigma_n; \text{Closed-Form} \) & \( \sigma_n; \text{Recursion} \) & MMF Asymp. \\
\hline
\hline
Line & \( \sum_{i=0}^{n-2} x_i x_{i+1} \) & \( \frac{4^n}{6} - \frac{(-2)^n}{6} \) & \( 2\sigma_{n-1} + 8\sigma_{n-2} \) & \( 3 \) \\
\hline
Circle & \( x_{n-1} x_1 + \sum_{i=0}^{n-1} x_i x_{i+1} \) & \( \frac{(-2)^n}{2} + \frac{1}{2} \sum \) & \( 2\sigma_{n-1} + 8\sigma_{n-2} \) & \( 1 \) \\
\hline
Clique & \( \sum_{i=0}^{n-1} x_i x_j \) & \( \frac{2^n}{2} + \frac{1}{2} \sum \) & \( 2 \times (5\sigma_{n-1} - 10\sigma_{n-2} - 20\sigma_{n-3} + 48\sigma_{n-4}) \) & \( 0 \) \\
\hline
Star & \( x_0 \sum_{i=0}^{n-1} x_i \) & \( \frac{2^n}{2} - \frac{(-2)^n}{2} + \frac{1}{2} \sum \) & \( 4 \times (3\sigma_{n-1} - 11\sigma_{n-2} + 12\sigma_{n-3}) \) & \( 0 \) \\
\hline
Triangles & \( x_0 x_1 + \sum_{i=0}^{n-2} x_i x_{i+1} x_{i+2} + x_{i+1} x_{i+2} \) & \( \frac{2^n}{2} + \frac{1}{2} \sum \) & \( 2\sigma_{n-1} + 16\sigma_{n-2} + 256\sigma_{n-3} \) & \( \frac{1}{3} \) \\
\hline
Squares & \( x_0 x_1 + \sum_{i=0}^{n-2} \sum_{j=0}^{n-2} x_i x_{i+1} x_{i+2} + x_{i+1} x_{i+2} \) & \( \frac{2^n}{2} + \frac{1}{2} \sum \) & \( 12\sigma_{n-1} + 32\sigma_{n-2} + 1024\sigma_{n-3} - 8192\sigma_{n-4} + \) & \( \frac{1}{3} \) \\
\hline
\hline
\end{tabular}
\caption{TABLE I \ Proven Results for the Multidimensional Merit Factor of Various Constructions}
\end{table}

\section*{Computational Results for the Merit Factor of Various Constructions}

\begin{table}[h]
\centering
\begin{tabular}{|l|l|l|}
\hline
Graph & \( p(x) \) & \( \sigma_n; \text{Recursion} \) & MF Asymp. \\
\hline
\hline
Line & \( \sum_{i=0}^{n-2} x_i x_{i+1} \) & \( \frac{4^n}{6} - \frac{(-2)^n}{6} \) & \( 2\sigma_{n-1} + 8\sigma_{n-2} \) & \( 3 \) \\
\hline
Circle & \( x_{n-1} x_1 + \sum_{i=0}^{n-1} x_i x_{i+1} \) & \( \frac{(-2)^n}{2} + \frac{1}{2} \sum \) & \( 4\sigma_{n-1} + 12\sigma_{n-2} - 64\sigma_{n-3} + 256\sigma_{n-5} \) & \( 1 \) \\
\hline
Clique & \( \sum_{i=0}^{n-1} x_i x_j \) & \( \frac{2^n}{2} + \frac{1}{2} \sum \) & \( 10\sigma_{n-1} - 36\sigma_{n-2} + 88\sigma_{n-3} - 96\sigma_{n-4} - 512\sigma_{n-5} + 1024\sigma_{n-6} \) & \( 0 \) \\
\hline
Star & \( x_0 \sum_{i=0}^{n-1} x_i \) & \( \frac{2^n}{2} + \frac{1}{2} \sum \) & \( 16\sigma_{n-1} - 68\sigma_{n-2} - 48\sigma_{n-3} + 768\sigma_{n-4} - 1024\sigma_{n-5} \) & \( 0 \) \\
\hline
\hline
\end{tabular}
\caption{TABLE II \ Computational Results for the Merit Factor of Various Constructions}
\end{table}