Aperiodic Correlations and the Merit Factor of a Class of Binary Sequences

TOM HØHOLDT, HELGE ELBRØND JENSEN, AND JØRN JUSTESEN

***Abstract*—A class of binary sequences of length $N = 2^m$ is considered, and it is shown that their aperiodic autocorrelations can be calculated recursively in a simple way. Based on this, the merit factor of the sequences is calculated and it is shown that the asymptotic value is 3. Finally, it is proved that the magnitude of the maximal aperiodic autocorrelation is bounded by $N^{0.9}$.**

I. Introduction

The problem of finding $+1, -1$ sequences (x_i), $i = 0,1,\cdots,N-1$ for which the magnitudes of the aperiodic autocorrelations

$$c_k = \sum_{i=0}^{N-k-1} x_i x_{i+k}, \qquad 1 \le k \le N-1 \tag{1.1}$$

are small seems extremely difficult [1], and apart from the results on Barker sequences [2], [3] not much is known. In fact, no one has exhibited an infinite class of sequences for which one could actually calculate the correlations. In [4] Golay defined the merit factor of binary sequences by

$$F = N^2 \Big/ \left(2\sum_{k=1}^{N-1} c_k^2\right) \tag{1.2}$$

and conjectured that $F \le 12.32$, for all binary sequences, with the exception of the Barker sequence of length 13, for which $F = 14.08$. In a recent paper Golay [5] argued that the merit factor of Legendre sequences, shifted by one quarter of their lengths, has the highly probable asymptotic value 6, but he did not prove this.

For maximal-length shift register sequences, one can see from [6] that if one considers the ensemble consisting of all cyclic shifts of a maximal-length sequence, then the average value of $(2\Sigma_{k=1}^{N-1}c_k^2)/N^2$ is approximately $1/3$. Thus, there exist maximal-length sequences with merit factor of approximately 3. Skaug [7] has calculated the actual values of the aperiodic autocorrelations for a number of maximal-length shift register sequences, and from his calculations it seems possible that the magnitude of the largest correlation is of order $\sqrt{N}$. Based on results of Niederreiter [8], McEliece in [9] has proven a number of bounds, from which one can see that the magnitude of the largest aperiodic autocorrelation for maximal length shift register sequences of length N is bounded by $\sqrt{N}\log N$.

In this correspondence we consider sequences of length $N = 2^m$ defined recursively by

$$\begin{aligned} x_0 &= 1, \\ x_{2^i+j} &= (-1)^{j+f(i)} x_{2^i-j-1}, \qquad 0 \le j \le 2^i - 1, \\ & \qquad\qquad i = 0,1,\cdots,m-1, \end{aligned} \tag{1.3}$$

where f is any function mapping the set of natural numbers into $\{0,1\}$. For these sequences we prove a simple recursion, which gives all the aperiodic autocorrelations, and based on this we calculate the merit factor and prove that the asymptotic value is 3. Finally, we prove that the magnitude of maximal aperiodic autocorrelation is $O(N^{0.9})$.

We note that if one chooses the function f as $f(0) = f(2k-1) = 0$ and $f(2k) = 1$, $k > 0$, then we get the first 2^m elements of the Rudin–Shapiro sequence [10], which have been proposed for use in phasing multitone signals to minimize peak factors [11].

Manuscript received January 23, 1984; revised January 3, 1985.

T. Høholdt and H. E. Jensen are with the Mathematical Institute, Technical University of Denmark, Building 303, DK-2800 Lyngby, Denmark.

J. Justesen is with the Institute of Circuit Theory and Telecommunication, Technical University of Denmark, Building 343, DK-2800 Lyngby, Denmark.

II. Calculation of the Aperiodic Correlations and the Merit Factor

Theorem 2.1: The sequences defined by (1.3) have zero aperiodic autocorrelation for even shifts.

Proof: Let $C(m,k)$ denote the kth autocorrelation for a sequence of length $N = 2^m$.

If $k \ge N/2$ we get

$$\begin{aligned} C(m,k) &= \sum_{i=0}^{N-k-1} x_i x_{i+k} = \sum_{i=0}^{N-k-1} x_i x_{N/2+(k-N/2)+i} \\ &= \sum_{i=0}^{N-k-1} x_i x_{N/2-(k-N/2+i)-1}(-1)^{k-N/2+i+f(m-1)} \\ &= \sum_{i=0}^{N-k-1} x_i x_{N-k-i-1}(-1)^{k+i+f(m-1)}. \end{aligned}$$

If k is even we get

$$\begin{aligned} C(m,k) &= \sum_{i=0}^{(N-k)/2-1} x_i x_{N-k-i-1}(-1)^{i+f(m-1)} \\ &\quad + \sum_{i=(N-k)/2}^{N-k-1} x_i x_{N-k-i-1}(-1)^{i+f(m-1)} \\ &= \sum_{i=0}^{(N-k)/2-1} x_i x_{N-k-i-1}(-1)^{i+f(m-1)} \\ &\quad + \sum_{j=0}^{(N-k)/2-1} x_{N-k-j-1} x_j (-1)^{N-j-1+f(m-1)}, \\ &\qquad\qquad j := N-k-i-1 \\ &= 0. \end{aligned}$$

If $0 < k < N/2$ we get

$$\begin{aligned} C(m,k) &= \sum_{i=0}^{N-k-1} x_i x_{i+k} \\ &= \sum_{i=0}^{N/2-k-1} x_i x_{i+k} + \sum_{i=N/2-k}^{N/2-1} x_i x_{i+k} + \sum_{i=N/2}^{N-k-1} x_i x_{i+k} \\ &= C(m-1,k) + \sum_{i=0}^{k-1} x_{N/2-k+i} x_{N/2+i} \\ &\quad + \sum_{i=0}^{N/2-k-1} x_{i+N/2} x_{i+k+N/2} \\ &= \sum_{i=0}^{k-1} x_{N/2-k+i} x_{N/2+i} + C(m-1,k) \\ &\quad + \sum_{i=0}^{N/2-k-1} x_{N/2-i-1} x_{N/2-k-i-1}(-1)^k \\ &= \sum_{i=0}^{k-1} x_{N/2-k+i} x_{N/2+i} + C(m-1,k) \\ &\quad + \sum_{j=0}^{N/2-k-1} x_{j+k} x_j (-1)^k, \qquad j := N/2-k-i-1 \\ &= \sum_{i=0}^{k-1} x_{N/2-k+i} x_{N/2+i} + \left(1+(-1)^k\right) C(m-1,k). \end{aligned} \tag{2.1}$$

0018-9448/85/0700-0549$01.00 ©1985 IEEE

If k is even we have

$$\begin{aligned}
&\sum_{i=0}^{k-1} x_{N/2-k+i}x_{N/2+i} \\
&\quad = \sum_{i=0}^{k/2-1} x_{N/2-k+i}x_{N/2+i} + \sum_{i=k/2}^{k-1} x_{N/2-k+i}x_{N/2+i} \\
&\quad = \sum_{i=0}^{k/2-1} x_{N/2-k+i}x_{N/2-i-1}(-1)^{i+f(m-1)} \\
&\qquad + \sum_{j=0}^{k/2-1} x_{N/2-j-1}x_{N/2+k-j-1}, \qquad j := k-1-i \\
&\quad = \sum_{i=0}^{k/2-1} x_{N/2-k+i}x_{N/2-i-1}(-1)^{i+f(m-1)} \\
&\qquad + \sum_{j=0}^{k/2-1} x_{N/2-j-1}x_{N/2-k+j}(-1)^{k-j-1+f(m-1)} \\
&\quad = 0.
\end{aligned}$$

So, for k even, (2.1) becomes

$$C(m,k) = 2C(m-1,k), \qquad m \geq 3,$$

and since $C(2,2) = 1 \cdot (-1)^{f(0)+f(1)}(1-1) = 0$, we get by induction that $C(m,k) = 0$ for k even, and hence the theorem is proved.

Since $x_{N/2}, \cdots, x_{N-1}$ is obtained from $x_0, x_1, \cdots, x_{N/2-1}$ by reversing the order of the symbols and changing the sign of alternate symbols, it follows from, for example, [12, eqs. (5.16) and (5.20)] and Theorem 2.1 that

$$x_0, x_1, \cdots, x_{N/2-1} \quad \text{and} \quad x_{N/2}, \cdots, x_{N-1}$$

are a pair of complementary sequences.

We will now consider the correlations for odd k and prove the following theorem.

Theorem 2.2: For $m \geq 3$, $0 < 2k+1 < 2^{m-2}$, the autocorrelations for the sequences defined by (1.3) satisfy

$$C(m,2k+1) = -C(m-1,2^{m-1}-2k-1)(-1)^{f(m-1)+f(m-2)} \quad (2.2a)$$

$$\begin{aligned}
C(m,2^{m-1}-2k-1) &= [-C(m-1,2k+1) - 2C(m-2,2k+1)] \\
&\quad \cdot (-1)^{f(m-1)+f(m-2)} \qquad (2.2b)
\end{aligned}$$

$$\begin{aligned}
C(m,2^{m-1}+2k+1) &= [C(m-1,2k+1) - 2C(m-2,2k+1)] \\
&\quad \cdot (-1)^{f(m-1)+f(m-2)} \qquad (2.2c)
\end{aligned}$$

$$C(m,2^m-2k-1) = C(m-1,2^{m-1}-2k-1)(-1)^{f(m-1)+f(m-2)}. \quad (2.2d)$$

Proof: If $l < N/2$ is odd we get from (2.1) that

$$\begin{aligned}
C(m,l) &= \sum_{i=0}^{l-1} x_{N/2-l-i}x_{N/2+i} \\
&= \sum_{i=0}^{N/2-(N/2-l)-1} x_{N/2-i-1}x_{N/2+i}
\end{aligned}$$

But, for $i < N/4$ we have

$$\begin{aligned}
x_{N/2+i} &= x_{N/2-i-1}(-1)^{i+f(m-1)} \\
&= (-1)^{i+f(m-1)}x_{N/4+(N/4-i-1)} \\
&= (-1)^{i+f(m-1)}x_{N/4-(N/4-i-1)-1} \\
&\quad \cdot (-1)^{N/4-i-1+f(m-2)} \\
&= -x_i(-1)^{f(m-1)+f(m-2)}. \qquad (2.3)
\end{aligned}$$

Therefore, for $l < N/4$ we get

$$C(m,l) = -C(m-1,N/2-l)(-1)^{f(m-1)+f(m-2)}$$

and therefore (2.2a) is proved. A similar calculation gives (2.2d). Next we consider $C(m,2^{m-1}-l)$, $0 < l < N/4$, l odd. From (2.1) we see that

$$\begin{aligned}
C(m,2^{m-1}-l) &= \sum_{i=0}^{N/2-l-1} x_{l+i}x_{N/2+i} \\
&= \sum_{i=0}^{N/4-l-1} x_{l+i}x_{N/2+i} + \sum_{i=N/4-l}^{N/4-1} x_{l+i}x_{N/2+i} \\
&\quad + \sum_{i=N/4}^{N/2-l-1} x_{l+i}x_{N/2+i}.
\end{aligned}$$

But for $i < N/4$ we have from (2.3) that $x_{N/2+i} = -x_i(-1)^{f(m-1)+f(m-2)}$, and so

$$\begin{aligned}
C(m,2^{m-1}-l) &= (-1)^{f(m-1)+f(m-2)} \\
&\quad \cdot \left[-C(m-2,l) - \sum_{i=0}^{l-1} x_{N/4+i}x_{N/4+i+l}\right] \\
&\quad + \sum_{i=N/4}^{N/2-l-1} x_{l+i}x_{N/2+i}.
\end{aligned}$$

Therefore, by (2.3)

$$\begin{aligned}
&C(m,2^{m-1}-l) \\
&\quad = (-1)^{f(m-1)+f(m-2)} \\
&\qquad \cdot [-C(m-2,l) - C(m-1,l)] + \sum_{i=N/4}^{N/2-l-1} x_{l+i}x_{N/2+i}.
\end{aligned}$$

Now

$$\begin{aligned}
&\sum_{i=N/4}^{N/2-l-1} x_{l+i}x_{N/2+i} \\
&\quad = \sum_{i=N/4}^{N/2-l-1} x_{i+l}x_{N/2-i-1}(-1)^{i+f(m-1)} \\
&\quad = \sum_{j=0}^{N/4-l-1} x_{N/2-j-1}x_{j+l}(-1)^{-j+f(m-1)}, \\
&\qquad\qquad j := N/2-l-1-i \\
&\quad = \sum_{j=0}^{N/4-l-1} x_{N/4+(N/4-j-1)}x_{j+l}(-1)^{-j+f(m-1)} \\
&\quad = \sum_{j=0}^{N/4-l-1} x_{N/4-(N/4-j-1)-1}(-1)^{-j-1+f(m-2)}
\end{aligned}$$

$$= -(-1)^{f(m-1)+f(m-2)} \sum_{j=0}^{N/4-l-1} x_j x_{j+l}$$

$$= -(-1)^{f(m-1)+f(m-2)} C(m-2,l).$$

So we get

$$C(m,2^{m-1}-l) = [-C(m-1,l) - 2C(m-2,l)] \cdot (-1)^{f(m-1)+f(m-2)},$$

and hence (2.2b) is proved. A similar calculation gives (2.2c) and the proof of the theorem is finished.

Let $S(m) = \sum_{k=1}^{2^{m-1}} C^2(m,k)$. For the sequences defined by (1.3) the merit factor is

$$F(m) = (2^m)/2S(m).$$

Theorem 2.3:

$$S(m) = 2S(m-1) + 8S(m-2), \qquad m \geq 3$$

$$F(m) = 3/\left(1 - \left(-\tfrac{1}{2}\right)^m\right).$$

Proof:

$$S(m) = \sum_{k=1}^{N-1} C^2(m,k) = \sum_{k=1}^{N/4-1} C^2(m,k) + C^2(m,N-k) + C^2(m,N/2-k) + C^2(m,N/2+k),$$

so, using Theorems 2.1 and 2.2 we get

$$\begin{aligned} S(m) &= \sum_{k=1}^{N/4-1} C^2(m-1,N/2-k) + C^2(m-1,N/2-k) \\ &\quad + [C(m-1,k) + 2C(m-2,k)]^2 \\ &\quad + [C(m-1,k) - 2C(m-2,k)]^2 \\ &= \sum_{k=1}^{N/4-1} 2C^2(m-1,N/2-k) \\ &\quad + 2C^2(m-1,k) + 8C^2(m-2,k) \\ &= 2S(m-1) + 8S(m-2). \end{aligned}$$

From this we get

$$S(m) = 4^m(2S(2) + S(3))/96 + (-2)^m(4S(2) - S(3))/24.$$

Now $S(2) = 2$ and $S(3) = 12$, so

$$S(m) = \tfrac{1}{6} \cdot 4^m - \tfrac{1}{6}(-2)^m,$$

which in turn gives $F(m) = 3/(1 - (-\frac{1}{2})^m)$ and the theorem is proved.

Obviously, the asymptotic value of the merit factor is 3.

One could hope that by starting with a sequence (e.g., a Barker sequence) with a high merit factor, and then applying the process of reversing an sign changing, it would be possible to generate long sequences with a high merit factor. Unfortunately, this is not the case. By calculations similar to those above, we can prove that no matter what the starting sequence is, the asymptotic value of the merit factor is at most 3.

III. Bounds on the Magnitude of the Largest Aperiodic Autocorrelation

Based on the recursions in Theorem 2.2, one can derive further recursions.

1) If $0 < 2k+1 < 2^{m-2}$ we have

$$C(m,2k+1) = C(m-2,2k+1)(-1)^{f(m-1)+f(m-2)} + 2C(m-2,2k+1+2^{m-2})(-1)^{f(m-1)+f(m-2)}$$

and therefore

$$\max_{l<2^{m-2}} |C(m,l)| \leq \max_l |C(m-1,l)|. \tag{3.1}$$

From this we derive the following.

2) If $2^{m-2} < 2k+1 < 5 \cdot 2^{m-4}$ we get

$$\begin{aligned} C(m,2k+1) &= C(m-2,2k+1-2^{m-2})(-1)^{f(m-1)+f(m-3)} \\ &\quad + 2C(m-3,2K+1-2^{m-2})(-1)^{f(m-2)+f(m-3)} \\ &\quad - 2C(m-3,3\cdot 2^{m-3}-2k-1) \\ &\quad \cdot (-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)} \end{aligned}$$

and therefore

$$\max_{2^{m-2}<l<5\cdot 2^{m-4}} |C(m,l)| \leq \max_l |C(m-2,l)| + 4\max_l |C(m-3,l)|. \tag{3.2}$$

3) If $5 \cdot 2^{m-4} < 2k+1 < 3 \cdot 2^{m-3}$ we get

$$\begin{aligned} C(m,2k+1) &= C(m-3,3\cdot 2^{m-3}-2k-1)\left[-(-1)^{f(m-1)+f(m-4)}\right. \\ &\quad \left. -2(-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)}\right] \\ &\quad + 2C(m-3,2k+1-2^{m-2})(-1)^{f(m-1)+f(m-3)} \\ &\quad + C(m-4,3\cdot 2^{m-3}-2k-1)\left[-2(-1)^{f(m-1)+f(m-4)}\right. \\ &\quad \left. +4(-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)}\right]. \end{aligned}$$

The absolute value of the quantity in the first bracket is either 3 or 1. Correspondingly, the absolute value of the quantity in the second bracket is 2 or 6. We conclude that either

$$\max_{5\cdot 2^{m-4}<l<3\cdot 2^{m-3}} |C(m,l)| \leq 5\max_l |C(m-3,l)| + 2\max_l |C(m-4,l)| \tag{3.3}$$

or

$$\max_{5\cdot 2^{m-4}<l<3\cdot 2^{m-3}} |C(m,l)| \leq 3\max_l |C(m-3,l)| + 6\max_l |C(m-4,l)|. \tag{3.4}$$

4) If $3 \cdot 2^{m-3} < 2k+1 < 7 \cdot 2^{m-4}$ we get

$$\begin{aligned} C(m,2k+1) &= C(m-3,2k+1-3\cdot 2^{m-3})\left[(-1)^{f(m-1)+f(m-4)}\right. \\ &\quad \left. +2(-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)}\right] \\ &\quad + C(m-4),2k+1-3\cdot 2^{m-3})\left[-2(-1)^{f(m-1)+f(m-4)}\right. \\ &\quad \left. +4(-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)}\right], \end{aligned}$$

so that

$$\max_{3\cdot 2^{m-3}<l<7\cdot 2^{m-4}} |C(m,l)| \leq 3\max_l |C(m-3,l)| + 6\max_l |C(m-4,l)|. \tag{3.5}$$

5) If $7 \cdot 2^{m-4} < 2k+1 < 2^{m-1}$ we have

$$C(m,2k+1) = C(m-2,2k+1-2^{m-2})(-1)^{f(m-1)+f(m-3)} + 2C(m-3,2k+1-3\cdot 2^{m-3})$$

$$(-1)^{f(m-1)+f(m-2)+f(m-3)+f(m-4)}.$$

so that

$$\max_{7\cdot 2^{m-4}<l<2^{m-1}} |C(m,l)|$$
$$\leq \max_l |C(m-2,l)| + 2\max_l |C(m-3,l)|. \quad (3.6)$$

Exactly the same expressions can be derived for $2k+1 > 2^{m-1}$.

In case 3), by considering the sequence given by $a_n = \max\{5a_{n-3} + 2a_{n-4},\ 3a_{n-3} + 6a_{n-4}\}$, one can see that $\max|C(m,l)|$ is bounded by (a constant times) the maximum of the solutions to (3.3) and (3.4) with equality.

Of the difference equations connected with the inequalities (3.1)–(3.6), it is the characteristic equation for (3.4) whose roots have maximal magnitude, and this is bounded by 1.85, so we conclude that

$$\max_k |C(m,k)| \leq A(1.85)^m = A\cdot(2^m)^{\log_2 1.85},$$

so

$$\max_k |C(m,k)| \leq A\cdot N^{0.9}. \quad (3.7)$$

The bound in (3.7) may seem rather crude, and indeed it is possible to obtain better bounds by further iterations of the equations in Theorem 2.2. Nevertheless, it is not possible to obtain a significant general improvement, as we shall now see.

We consider the sequences defined by (1.3), where we choose the function f, such that $f(2p) = 0$ and $f(2p+1) = 1$. Let

$$C_m = \begin{cases} C(m, \frac{1}{3}(2^m - 1)), & \text{if } m \text{ is even} \\ C(m, \frac{1}{3}(2^m + 1)), & \text{if } m \text{ is odd} \end{cases}.$$

From the recursions in Theorem 2.2 one easily obtains

$$C_m = -C_{m-1} - 2C_{m-2} - 4C_{m-3}.$$

The greatest magnitude of the roots of the corresponding characteristic equation is 1.65, so C_m is of order $(1.65)^m$, which in turn gives $N^{0.73}$, so this is comparable to the bound given by (3.7).

Of course, it is possible that by choosing a less regular function f, one would be able to obtain better results, but there is no evidence of that. All the sequences defined by (1.3) have the same merit factor, which leads us to believe that significant improvements in (3.7) are unlikely.

Acknowledgment

The authors wish to thank the referees for their valuable suggestions and comments.

References

[1] R. Turyn, "Sequences with small correlation," in *Error Correcting Codes*, H. B. Mann, Ed. New York: Wiley, 1968, pp. 195–228.
[2] R. H. Barker, "Group synchronizing of binary digital systems," in *Communication Theory*, W. Jackson, Ed. London: Butterworth, 1953, pp. 273–287.
[3] J. Storer and R. Turyn, "On binary sequences," in *Proc. Amer. Math. Soc.*, vol. 12, 1961, pp. 394–399.
[4] M. J. E. Golay, "Sieves for low autocorrelation binary sequences," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 43–51, Jan. 1977.
[5] M. J. E. Golay, "The merit factor of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 934–936, Nov. 1983.
[6] James H. Lindholm, "An analysis of the pseudo-randomness properties of subsequences of long m-sequences," *IEEE Trans. Inform. Theory*, vol. IT-14, no. 4, pp. 569–576, July 1968.
[7] R. Skaug, "Numerical evaluation of the nonperiodic autocorrelation parameter for optimal phases of maximal length sequences," in *Proc. IEEE*, vol. 127, pt. 7, no. 3, June 1980, pp. 230–237.
[8] H. Niederreiter, "Some new exponential sums with applications to pseudo-random numbers," in *Topics in Number Theory*. Debrecen, Hungary, 1974; also *Colloq. Math. Soc. Janoes Bolyai*, vol. 13. Amsterdam: North-Holland, 1976, pp. 209–223.
[9] R. J. McEliece, "Correlation properties of sets of sequences derived from irreducible cyclic codes," *Inform. Contr.*, vol. 45, pp. 18–25, 1980.
[10] W. Rudin, "Some theorems on Fourier coefficients," in *Proc. Amer. Math. Soc.*, vol. 10, Dec. 1959, pp. 855–859.
[11] L. J. Greenstein and P. J. Fitzgerald, "Phasing multitone signals to minimize peak factors," *IEEE Trans. Commun.*, vol. COM-29, no. 7, pp. 1072–1074, July 1981.
[12] D. V. Sarwate and M. B. Pursley, "Cross correlation properties of pseudo-random and related sequences," in *Proc. IEEE*, vol. 68, May 1980, pp. 593–619.