The Merit Factor of Binary Sequences Related to Difference Sets

Jørn M. Jensen, Helge Elbrønd Jensen, and Tom Høholdt

Abstract—**Long binary sequences related to cyclic difference sets are investigated. Among all known constructions of cyclic difference sets we show that only sequences constructed from Hadamard difference sets can have an asymptotic nonzero merit factor. Maximal length shift register sequences, Legendre, and twin-prime sequences are all constructed from Hadamard difference sets. We prove that the asymptotic merit factor of any maximal length shift register sequence is three. For twin-prime sequences it is shown that the best asymptotic merit factor is six. This value is obtained by shifting the twin-prime sequence one quarter of its length. It turns out that Legendre sequences and twin-prime sequences have similar behavior. Based on the Jacobi symbol we investigate Jacobi sequences. The best asymptotic merit factor is shown to be six. Through the introduction of product sequences, it is argued that the maximal merit factor among all sequences of length N is at least six when N is large. We also demonstrate that it is fairly easy to construct sequences of moderate composite length with merit factor close to six.**

Index Terms—**Sequences, correlation, cyclic difference sets.**

I. Introduction

LET x_j, $0 \le j \le N-1$, be a sequence of N elements of value $+1$ or -1. The *aperiodic correlations* are defined by

$$c_k = \sum_{j=0}^{N-k-1} x_j x_{j+k}, \qquad k = 1, \cdots, N-1 \tag{1.1}$$

and the *merit factor* of the sequence, introduced by Golay [1], is defined by

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

Binary sequences with small correlations play an important role in many communication systems, ranging from radar to modulation techniques and testing of systems [2]. The significance of the merit factor in these situations comes from the relation between the merit factor and the spectral properties of the signal corresponding to the sequence. More precisely, let

$$Q(e^{i\omega}) = \sum_{j=0}^{N-1} x_j e^{ij\omega} \tag{1.3}$$

be the *Fourier transform* of the sequence x_j. An easy calculation gives

$$2 \sum_{k=1}^{N-1} c_k^2 = \frac{1}{2\pi} \int_0^{2\pi} \left[|Q(e^{i\omega})|^2 - N \right]^2 d\omega. \tag{1.4}$$

Hence the denominator in (1.2) measures—in terms of power—how much the amplitude spectrum of the signal deviates from the constant value N, and a sequence with maximal merit factor F gives a signal with maximally flat spectrum (for fixed N). The problem is then to find sequences with large merit factors. One way to do this is by computer search. For lengths N up to 40 [3], it is possible to carry out a complete search. Except for $N = 11$ and $N = 13$, the maximal merit factor is in the interval from 3.3 to 9.85. For $N = 11$ one gets 12.1 and for $N = 13$ the maximum is 14.08 [3]. In both cases these sequences are Barker sequences (binary sequences for which all aperiodic correlations are either 0 or ± 1).

For larger values of N, a complete search is not possible. There are many results of partial searches ([1], [4], [5], [6]). For lengths up to 117, the highest known merit factor is between 8 and 9.56 and for lengths from 118 to 200, the best factor known is close to 6. For N greater than 200 various statistical search methods have been used, [4], [7], [8], giving sequences with a merit factor of no more than 5.

Apart from different search methods, which have not led to a deeper theoretical understanding of the behavior of the merit factor, another approach is to look for general principles for construction of sequences of arbitrary length with a reasonably high merit factor [9]. Yet another approach is to carry out a theoretical study of special classes of sequences, and this is the approach adapted here.

The first problem in such an investigation is the lack of a simple analytical technique. Calculation of the merit factor is apparently a complicated process, which appears to be difficult to attack with analytical methods. In [10] we proposed a general method for treating merit factors, and this method will be the basic tool in the present paper. The method, which only works for sequences with odd length N, is based on the knowledge of the *Discrete*

Manuscript received June 21, 1989; revised July 9, 1990. This work was presented in part at the IEEE International Symposium on Information Theory, San Diego, CA, January 14–19, 1990.

The authors with the Mathematical Institute, Technical University of Denmark, Building 303, DK-2800, Lyngby, Denmark.

IEEE Log Number 9041979.

Fourier Transform (DFT) of the sequence, that is, the numbers

$$Q(\epsilon_j)=\sum_{k=0}^{N-1} x_k\epsilon_j^k, \qquad j=0,\cdots,N-1, \tag{1.5}$$

where $\epsilon_j=\exp(i2\pi/Nj)$. The method is technically rather complicated, involving many calculations. However, using this method it was possible to determine the asymptotic merit factor of Legendre sequences and offsets of such sequences.

A Legendre sequence has length equal to an odd prime N, and is defined by the Legendre symbols

$$x_j=\left(\frac{j}{N}\right), \qquad j=0,\cdots,N-1. \tag{1.6}$$

which gives

$$x_0=1, \qquad x_j=\begin{cases} 1, & \text{if } j \text{ is a square } (\text{mod } N) \\ -1, & \text{if } j \text{ is a nonsquare } (\text{mod } N). \end{cases} \tag{1.7}$$

An "offset" sequence is one in which a fraction f of its elements is chopped off at one end of the sequence and appended at the other, in other words, a cyclic shift of fN places.

In [10] it was proved that, if F is the merit factor for $N\to\infty$ for an offset Legendre sequence corresponding to the fraction f, then

$$1/F=2/3-4|f|+8f^2, \qquad |f|\le 1/2. \tag{1.8}$$

This gives the highest merit factor $F=6$ for $|f|=1/4$. The formula (1.8) was obtained earlier by Golay [11] using probability theory and an "external" assumption. This was that, for the asymptotic case, one can consider the correlations c_k in (1.1) to be independent random variables, which they certainly are not for fixed N. Nevertheless, Golay was able to obtain the correct asymptotic formula in this case.

The method used in [10] is as follows. Let F be the merit factor of a sequence of odd length N. Then

$$\begin{aligned} 1/F&=\left[2\sum_{k=1}^{N-1}c_k^2\right]\Big/N^2 \\ &=\left[\sum_{k=1}^{N-1}(c_k+c_{N-k})^2+\sum_{k=1}^{N-1}(c_k-c_{N-k})^2\right]\Big/2N^2 \\ &=\left[\sum_{j=0}^{N-1}|Q(\epsilon_j)|^4+\sum_{j=0}^{N-1}|Q(-\epsilon_j)|^4\right]\Big/2N^3-1 \\ &=(S+S_1)/2N^3+1, \end{aligned} \tag{1.9}$$

where

$$S=\sum_{j=0}^{N-1}|Q(\epsilon_j)|^4 \quad \text{and} \quad S_1=\sum_{j=0}^{N-1}|Q(-\epsilon_j)|^4.$$

Since, by interpolation,

$$Q(-\epsilon_j)=\frac{2}{N}\sum_{k=0}^{N-1}\frac{\epsilon_k}{\epsilon_j+\epsilon_k}Q(\epsilon_k),$$

this gives $S_1=16(A+B+C+D)/N^4$, where

$$A=\frac{1}{16}\left(\frac{1}{3}N^4+\frac{2}{3}N^2\right)\sum_{a=0}^{N-1}|Q(\epsilon_a)|^4$$

$$B=\frac{N^2}{8}\sum_{\substack{a,b=0\\a\neq b}}^{N-1}2|Q(\epsilon_a)|^2\left(\overline{Q}(\epsilon_a)Q(\epsilon_b)\epsilon_b+Q(\epsilon_a)\overline{Q}(\epsilon_b)\epsilon_a\right)\left(\frac{\epsilon_a+\epsilon_b}{(\epsilon_b-\epsilon_a)^2}\right)$$

$$C=-\frac{N^2}{4}\sum_{\substack{a,b,c=0\\b\neq a\neq c}}^{N-1}2|Q(\epsilon_a)|^2\left(\frac{Q(\epsilon_b)\overline{Q}(\epsilon_c)\epsilon_a\epsilon_b+\overline{Q}(\epsilon_b)Q(\epsilon_c)\epsilon_a\epsilon_c}{(\epsilon_b-\epsilon_a)(\epsilon_c-\epsilon_a)}\right)$$

$$-\frac{N^2}{4}\sum_{\substack{a,b,c=0\\b\neq a\neq c}}^{N-1}\frac{Q^2(\epsilon_a)\overline{Q}(\epsilon_b)\overline{Q}(\epsilon_c)\epsilon_a^2+\overline{Q}^2(\epsilon_a)Q(\epsilon_b)Q(\epsilon_c)\epsilon_b\epsilon_c}{(\epsilon_b-\epsilon_a)(\epsilon_c-\epsilon_a)}$$

$$D=-\frac{N^2}{2}\cdot\frac{1}{2}\sum_{\substack{a,b=0\\a\neq b}}^{N-1}\frac{4|Q(\epsilon_a)|^2|Q(\epsilon_b)|^2\epsilon_a\epsilon_b+Q^2(\epsilon_b)\overline{Q}^2(\epsilon_a)\epsilon_b^2+Q^2(\epsilon_a)\overline{Q}^2(\epsilon_b)\epsilon_a^2}{(\epsilon_a-\epsilon_b)^2}. \tag{1.10}$$

For Legendre sequences, it is known that

$$Q(1)=1,$$

$$Q(\epsilon_j)=\begin{cases} 1+x_j\sqrt{N}, & \text{if } N\equiv 1\ (\text{mod}4) \\ 1+ix_j\sqrt{N}, & \text{if } N\equiv 3\ (\text{mod}4) \end{cases}, \quad j\neq 0. \tag{1.11}$$

For $N\equiv 3\ (\text{mod}4)$ it follows from (1.11), that

$$|Q(\epsilon_j)| \text{ is independent of } j=1,\cdots,N-1. \tag{1.12}$$

This property highly facilitates the calculations in (1.9), and it turns out that the case $N\equiv 1\ (\text{mod}4)$ asymptotically can be treated as if (1.12) were satisfied.

In this paper we use (1.9) to determine the asymptotic merit factor of several classes of binary sequences. In Section II we note that sequences for which (1.12) holds arise from cyclic difference sets, a very well-studied subject with a long tradition. Among all known constructions of cyclic difference sets we show that only the Hadamard difference sets have the possibility of producing se-

quences with an asymptotic nonzero merit factor. Three classes of sequences constructed from Hadamard difference sets are: *maximal length shift register sequences, Legendre sequences, and twin-prime sequences.* In Section III we prove that the asymptotic merit factor of any cyclic shifted maximal length shift register sequence is 3. In Section V we show that the asymptotic merit factor of a twin-prime sequence is given by the formula (1.8).

In Section IV we introduce *Jacobi sequences* defined by use of the Jacobi symbol, known from number theory. Jacobi sequences are closely related to Legendre sequences. This relation is formulated through the notion of the *product* of two sequences. The product is defined for any two sequences of length N_1 and N_2 with $\gcd(N_1, N_2) = 1$, and the product sequence has length $N = N_1 \cdot N_2$. One interesting fact about this construction is a very simple formula for the DFT of the product sequence in terms of the DFT of the two "factors." Also in Section IV we introduce modified Jacobi sequences, which contain twin-prime sequences as a special case. The merit factor of a modified Jacobi sequence is better than the merit factor of the corresponding Jacobi sequence. In Section V we use (1.9) to determine the asymptotic merit factor of the product of two Legendre sequences, which in fact is the same as a Jacobi sequence, and cyclic shifts of such sequences. We also treat modified Jacobi sequences, and the result for both types of sequences is again the formula (1.8).

II. Sequences from Cyclic Difference Sets

We recall the definition of a cyclic difference set [13]: A set $D = \{i_1, i_2, \cdots, i_k\}$ of k residues mod v is called a *(v, k, λ)-difference set*, if the equation $x - y \equiv j \pmod v$ has exactly λ solutions $(x, y) \in D \times D$ for each $j \in \{1, 2, \cdots, v-1\}$. If D is a difference set, we construct a binary sequence x_n, $n = 0, 1, \cdots, v-1$, by

$$x_n = \begin{cases} -1, & \text{if } n \in D \\ 1, & \text{if } n \notin D. \end{cases} \tag{2.1}$$

The periodic correlations, $\theta_j = \sum_{l=0}^{v-1} x_l x_{l+j}$, where the indexes are calculated modulo v, are given by [13]

$$\theta_j = \begin{cases} v, & \text{if } j = 0 \\ v - 4(k-\lambda), & \text{if } j \in \{1, \cdots, v-1\}. \end{cases} \tag{2.2a}$$

Thus the periodic correlations take on only two values. This in fact characterize the sequences coming from cyclic difference set. [13]. Moreover, since

$$|Q(\epsilon_j)|^2 = \sum_{l=0}^{v-1} \theta_l \epsilon_j^l, \tag{2.2b}$$

condition (2.2a) is equivalent to the statement that $|Q(\epsilon_j)|$ is independent of $j = 1, 2, \cdots, N-1$.

In the following we use the notation $\boldsymbol{x}_N$ for a sequence $x_0, x_1, \cdots, x_{N-1}$.

In order to decide which difference sets one shall investigate with respect to the merit factor, we need the following theorem.

Theorem 2.1: Consider an infinite number of binary sequences $\boldsymbol{x}_N$ of increasing length N. For each N, let F_N denote the merit factor of the sequence, and let D_N denote the number of -1's in the sequence $\boldsymbol{x}_N$. Suppose that $D_N/N \to a$ for $N \to \infty$. If $a \neq 1/2$, then $F_N \to 0$ for $N \to \infty$.

Proof: If $\boldsymbol{x}_N = x_0, x_1, \cdots, x_{N-1}$, we have

$$(N - 2D_N)^2 = (x_0 + x_1 + \cdots + x_{N-1})^2 = N + 2\sum_{j=1}^{N-1} c_j. \qquad \square \tag{2.3}$$

From the Cauchy–Schwartz inequality, it follows that

$$\left| \sum_{j=1}^{N-1} c_j \right| \le \sqrt{N-1} \left(\sum_{j=1}^{N-1} c_j^2 \right)^{1/2}$$

and hence from (2.3)

$$\frac{1}{F_N} \ge \frac{\left[(N-2D_N)^2 - N\right]^2}{2N^2(N-1)} = \frac{\left[N(1-2D_N/N)^2 - 1\right]^2}{2(N-1)},$$

which gives the desired conclusion.

Many classes of difference sets are known [13]. By examining these sets, it follows from Theorem 2.1 that only the Hadamard difference sets that have parameters $(v, k, \lambda) = (4t-1, 2t-1, t-1)$ can give sequences with an asymptotic merit factor different from zero. The Hadamard difference sets can be classified according to the value of $v = 4t - 1$ from [13].

Case a) $v = 2^n - 1$: Then there exist the Singer difference sets and the Gordon–Mills–Welch difference sets.

Case b) v is a prime: Then the quadratic residues modulo v give a difference set and, if $v = 4x^2 + 27$, there exists another class called Hall-sets.

Case c) $v = p(p+2)$ where both p and $p+2$ are primes: Then there exist the twin-prime difference sets.

We consider three classes of sequences coming from these difference sets, one class from each case. The sequences arising from Singer difference sets are the maximal length shift register sequences (ML-sequences) and the sequences from the quadratic residues are the Legendre sequences. The sequences from c) are defined by

$$x_j = \begin{cases} 1, & j = 0, p+2, 2(p+2), \cdots, (p-1)(p+2), \\ -1, & j = p, 2p, \cdots, (p+1)p, \\ \left(\frac{j}{p}\right)\left(\frac{j}{p+2}\right), & \gcd(j, p(p+2)) = 1, \end{cases} \tag{2.4}$$

where $(-)$ denotes the Legendre symbol.

The following theorems summarize the results.

Theorem 2.2: The asymptotic merit factor of any maximal length shift register sequence is 3.

Proof: See Theorem 3.7 in Section III. $\square$

Sarwate showed in [12] that among all the 2^n-1 cyclic shifted versions of a ML-sequence there exists at least one sequence with a merit factor of 3 or more. In order to actually find such a sequence, one has to make a computer search, [12]. However, since a cyclic shifted ML-sequence again is a ML-sequence, it follows from Theorem 2.2 that the merit factor of all these sequences is 3.

The merit factor of Legendre sequences was determined in [10]. For completeness we state the result in the next theorem.

Theorem 2.3: The asymptotic merit factor F of a Legendre sequence shifted t places is given by the formula

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \le 1/2,$$

where $f = t/N$.

Theorem 2.4: The asymptotic merit factor F of a twin-prime sequence shifted t places is given by the formula

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \le 1/2,$$

where $f = t/N$.

Proof: Follows from Theorem 5.1 in Section V by setting q equal to $p+2$.

For both Legendre- and twin-prime sequences the best possible merit factor is 6, and this value is obtained by shifting the sequence one quarter of its length. In Sections IV and V we explain why Legendre sequences and twin-prime sequences have the same asymptotic merit factor.

The asymptotic merit factor for Hall sequences and Gordon–Mills–Welch sequences are currently unknown. The GMW-sequences have the ML-sequences as a special case, and these are treated next. □

III. The Asymptotic Merit Factor of Maximal Length Shift Register Sequences

Let α be a primitive element of the finite field GF(2^n) and β a fixed element of GF(2^n). A maximal length shift register sequence—a ML-sequence—can be defined as

$$x_j = (-1)^{\mathrm{tr}(\beta\alpha^j)}, \qquad j = 0,1,\cdots,N = 2^n-1, \quad (3.1)$$

where $\mathrm{tr}(x)$ denotes the trace-function from GF(2^n) to GF(2). For the basic facts of these sequences see [14].

It is known [13], [14], that these sequences arise from a difference set with parameters $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$ and hence it follows from (2.2a) and (2.2b) that

$$Q(1) = 1,$$
$$|Q(\epsilon_j)|^2 = 2^n = N+1, \qquad j = 1,2,\cdots,N-1. \quad (3.2)$$

The property (3.2) is not sufficient to determine the merit factor using (1.9). However, by invoking the shift- and add-property of these sequences, it is possible to carry through the calculations.

The shift- and add-property states [14, Theorem 10.6] that there exists a permutation π of $\{1,2,\cdots,N-1\}$ such that

$$x_m x_{m+s} = x_{m+\pi(s)},$$
$$\text{for all } m \in \{0,1,\cdots,N-1\} \text{ and } s \neq 0. \quad (3.3)$$

Moreover, using (3.1), it is seen that this permutation satisfies

$$\alpha^{\pi(s)} = \alpha^s + 1, \qquad \text{for } s \in \{1,\cdots,N-1\}. \quad (3.4)$$

We will now calculate the asymptotic merit factor of a ML-sequence using (1.9).

It is easily seen from (3.2) that

$$S = \sum_{j=0}^{N-1} |Q(\epsilon_j)|^4 = N^3 + O(N^2). \quad (3.5)$$

The sums A, B, C, and D from (1.10) are now treated in a series of lemmas.

The lemmas below follow from (3.5).

Lemma 3.1: For any ML-sequence $A = 1/48N^7 + O(N^6)$.

Lemma 3.2: for any ML-sequence $B = O(N^{11/2})$.

Proof:

$$B = -\frac{N^2}{4} \sum_{\substack{a,b=0 \\ a\neq b}}^{N-1} |Q(\epsilon_a)|^2 \cdot \left(\frac{\overline{Q}(\epsilon_a)Q(\epsilon_b)}{|1-\epsilon_{b-a}|^2}(1+\epsilon_{b-a}) + \frac{Q(\epsilon_a)\overline{Q}(\epsilon_b)}{|1-\epsilon_{a-b}|^2}(1+\epsilon_{a-b}) \right)$$
$$= -\frac{N^2}{2} \mathrm{Re}\left(\sum_{a=0}^{N-1} |Q(\epsilon_a)|^2 \sum_{k=1}^{N-1} \frac{1+\epsilon_k}{|1-\epsilon_k|^2} Q(\epsilon_a)Q(\epsilon_{k-a}) \right)$$
$$= -\frac{N^2}{2} \mathrm{Re}\left(|Q(1)|^2 \sum_{k=1}^{N-1} \frac{1+\epsilon_k}{|1-\epsilon_k|^2} Q(\epsilon_k) + \sum_{a=1}^{N-1} |Q(\epsilon_a)|^2 \sum_{k=1}^{N-1} \frac{1+\epsilon_k}{|1-\epsilon_k|^2} Q(\epsilon_a)Q(\epsilon_{k-a}) \right). \quad \square$$

Using

$$\sum_{k=1}^{N-1} \frac{1}{|1-\epsilon_k|^2} = \frac{1}{12}N^2 - \frac{1}{12}$$

from [10] and

$$|Q(\epsilon_a)|^2 = N+1,$$

it is seen that the first sum is $O(N^{5/2})$. The second sum is $O(N^{7/2})$ by the same observations and using

$$\sum_{a=1}^{N-1} Q(\epsilon_a)Q(\epsilon_{k-a}) = -Q(1)Q(\epsilon_k).$$

We split the C-sum in the two parts, C_1 and C_2, in which it is written in (1.10). Arguing as in the proof of lemma 3.2, it is easy to see.

Lemma 3.3: For any NL-sequence, $C_1 = O(N^{11/2})$.

The second part, C_2, is treated below. First, however, to simplify the calculations we need a rewriting of the

D-sum. We split this sum in two parts:

$$D_1 = -N^2 \sum_{\substack{a,b=0 \\ a\neq b}}^{N-1} \frac{|Q(\epsilon_a)|^2|Q(\epsilon_b)|^2\epsilon_a\epsilon_b}{(\epsilon_a-\epsilon_b)^2} \quad (3.6a)$$

and

$$D_2 = \frac{-N^2}{2}\sum_{a=0}^{N-1}\sum_{k=1}^{N-1}\frac{Q^2(\epsilon_a)\overline{Q}^2(\epsilon_{a+k})}{(\epsilon_k-1)^2}. \quad (3.6b)$$

We want to express D_1 in terms of the cyclic correlations of the sequence. Substituting

$$|Q(\epsilon_l)|^2 = \sum_{j=0}^{N-1}\theta_j\epsilon_l^j, \qquad l=a,b,$$

into (3.6a) and using a rewriting similar to that used in the proof of Lemma 3.2, we get

$$D_1 = N^2\sum_{a=0}^{N-1}\sum_{k=1}^{N-1}\frac{1}{|1-\epsilon_k|^2}$$
$$\cdot\left(N^2+N\sum_{j=1}^{N-1}\theta_j(\epsilon_a^j+\epsilon_{k-a}^j)+\sum_{j=1}^{N-1}\sum_{l=1}^{N-1}\theta_j\theta_l\epsilon_a^j\epsilon_{k-a}^l\right)$$
$$= N^5\sum_{k=1}^{N-1}\frac{1}{|1-\epsilon_k|^2}+N^3\sum_{k=1}^{N-1}\sum_{j=1}^{N-1}\theta_j^2\frac{\epsilon_k^j}{|1-\epsilon_k|^2},$$

by summing over a. Using that

$$\sum_{k=1}^{N-1}\frac{\epsilon_k^j}{|1-\epsilon_k|^2} = \left(\frac{1}{12}N^2-\frac{1}{12}\right)-\frac{1}{2}j(N-j),$$

which can be seen from [10], we get

$$D_1 = \left(\frac{1}{12}N^2-\frac{1}{12}\right)N^5+\left(\frac{1}{12}N^2-\frac{1}{12}\right)N^3$$
$$\cdot\sum_{j=1}^{N-1}\theta_j^2-\frac{1}{2}N^3\sum_{j=1}^{N-1}j(N-j)\theta_j^2. \quad (3.7)$$

From (2.2), we have that $\theta_j=-1$ and therefore the following lemma holds.

Lemma 3.4: For any ML-sequence $D_1 = 1/12N^7 + O(N^6)$.

The remaining terms, that is C_2 and D_2, can be treated together since

$$C_2+D_2 = -\frac{N^2}{2}\sum_{a=0}^{N-1}\sum_{k-1}^{N-1}\sum_{l-1}^{N-1}\frac{Q^2(\epsilon_a)\overline{Q}(\epsilon_{a+k})\overline{Q}(\epsilon_{a+l})}{(\epsilon_k-1)(\epsilon_l-1)}, \quad (3.8)$$

by the same kind of rewriting as in Lemma 3.2.

Here the summation over $k\neq l$ yields C_2 and $k=l$ yields D_2. We first calculate $Q(\epsilon_a)\overline{Q}(\epsilon_{a+k})$, and get

$$Q(\epsilon_a)\overline{Q}(\epsilon_{a+k}) = \sum_{m,p=0}^{N-1}x_mx_p\epsilon_a^{m-p}\epsilon_k^{-p}$$
$$= \sum_{s,p=0}^{N-1}x_px_{p+s}\epsilon_a^s\epsilon_k^{-p},$$

where the indexes of the sequence are calculated mod N.

Using the shift- and add-property (3.3), we get

$$Q(\epsilon_a)\overline{Q}(\epsilon_{a+k}) = \sum_{\substack{p=0\\ s=1}}^{N-1}x_{p+\pi(s)}\epsilon_a^s\cdot\epsilon_k^{-p}+\sum_{p=0}^{N-1}\epsilon_k^{-p}$$
$$= \overline{Q}(\epsilon_k)\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)}\cdot\epsilon_a^s.$$

Substitution of this into (3.8) and summing over a gives

$$C_2+D_2 = -\frac{N^3}{2}\sum_{k=1}^{N-1}\sum_{l=1}^{N-1}\frac{\overline{Q}(\epsilon_k)}{(\epsilon_k-1)}\frac{\overline{Q}(\epsilon_l)}{(\epsilon_l-1)}$$
$$\cdot\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)}\cdot\epsilon_l^{\pi(N-s)}.$$

Since from (3.2)

$$|Q(\epsilon_k)| = \sqrt{N+1} \quad \text{and} \quad \sum_{k=1}^{N-1}\frac{1}{|\epsilon_k-1|}\leq N\log N$$

from [10], it follows that

$$|C_2+D_2| \leq N^6(\log N)^2$$
$$\cdot\max_{k,l=1,\cdots,N-1}\left\{\left|\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)}\cdot\epsilon_l^{\pi(N-s)}\right|\right\}. \quad (3.9)$$

To finish the estimations we prove the following lemma.

Lemma 3.5:

$$\left|\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)+\pi(N-s)}\right|\leq\sqrt{N+1}$$

and

$$\left|\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)}\cdot\epsilon_l^{\pi(N-s)}\right|\leq\sqrt{N+1} \qquad l,k\geq 1\ l\neq k.$$

The proof of this lemma relies on the fact that the sums are related to character sums, since the multiplicative character ψ_k is defined as $\psi_k(\alpha^p)=\epsilon_k^p$ [15 p. 187].

If we consider the polynomial $g(x)=x^{N-1}(x+1)^2$, we have

$$\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)+\pi(N-s)} = \sum_{s=1}^{N-1}\psi_k(g(\alpha^s)) \quad (3.10)$$

since

$$g(\alpha^s) = \alpha^{sN-s}(\alpha^s+1)^2$$
$$= \alpha^{-s}(\alpha^s+1)^2 = (\alpha^s+1)(\alpha^{-s}+1) = \alpha^{\pi(s)}\cdot\alpha^{\pi(N-s)},$$

where we have used (3.4).

We now invoke [15, Theorem 5.41], using the fact that ψ_k has order $m=N/\gcd(N,k)$ so m is odd and $g(x)$ is not an mth power of a polynomial. Moreover, since $g(x)$ has only two roots, we get from the theorem that

$$\left|\sum_{s=1}^{N-1}\epsilon_k^{\pi(s)+\pi(N-s)}\right|\leq\sqrt{N+1}.$$

For the second statement in the lemma we let, for fixed

$l, k \in \{1,2,\cdots,N-1\}$, $l \neq k$, $h(x)$ be the polynomial $h(x) =$
$x+1)^{k+l}x^{(N-1)l}$.

We then have

$$\sum_{s=1}^{N-1} \epsilon_k^{\pi(s)} \cdot \epsilon_l^{\pi(N-s)} = \sum_{s=1}^{N-1} \psi_1(h(\alpha^s)) \qquad (3.11)$$

since

$$h(\alpha^s) = (\alpha^s+1)^{k+l}\alpha^{s(N-1)l} = (\alpha^s+1)^k(\alpha^{-s}+1)^l$$
$$= (\alpha^{\pi(s)})^k(\alpha^{\pi(N-s)})^l$$

again using (3.4).

Now ψ_1 has order N, and $h(x)$ is not an Nth power of a polynomial. Since $h(x)$ has only two roots, Theorem 5.41 of [15] again gives the result.

Lemma 3.6 below follows from (3.9) and Lemma 3.5.

Lemma 3.6: For any ML-sequence,

$$C_2 + D_2 = O\left(N^{13/2}(\log N)^2\right).$$

We can now prove the main result of this section.

Theorem 3.7: The asymptotic merit factor of any ML-sequence is 3.

The theorem follows from (1.9), (3.5), and Lemmas 3.1–3.4, and 3.6. We note that the result is independent of cyclic shifts, since a cyclic shift of a ML-sequence is a ML-sequence.

IV. The Product Construction and Jacobi Sequences

We first recall the product construction [16].

Definition 4.1: Let $\boldsymbol{x} = x_0, x_1, \cdots, x_{N_1-1}$ and $\boldsymbol{y} = y_0, y_1, \cdots, y_{N_2-1}$ be two sequences with $\gcd(N_1, N_2) = 1$. The product sequence $\boldsymbol{z} = z_0, z_1, \cdots, z_{N-1}$ of length $N = N_1 \cdot N_2$ is defined by

$$z_l = x_{l_1} \cdot y_{l_2}, \qquad l = 0,1,\cdots,N-1, \qquad (4.1)$$

where $l_1 = l \pmod{N_1}$ and $l_2 = l \pmod{N_2}$.

The product sequence is denoted by $\boldsymbol{z} = \boldsymbol{x} \otimes \boldsymbol{y}$. The construction is illustrated in the following.

Example 4.1: Let $\boldsymbol{x} = x_0, x_1, x_2 = 1\ 1\ -1$ and $\boldsymbol{y} = y_0, y_1, \cdots, y_6 = 1\ 1\ 1\ -1\ 1\ -1\ -1$. To construct the product sequence we consider the 3×7 matrix

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 \end{pmatrix},$$

where the first row is $x_0\boldsymbol{y}$, the second row is $x_1\boldsymbol{y}$ and the third row is $x_2\boldsymbol{y}$. The product sequence $\boldsymbol{z} = \boldsymbol{x} \otimes \boldsymbol{y}$ is

$$1\ 1\ -1\ -1\ 1\ 1\ -1\ 1\ -1\ 1$$
$$-1\ -1\ -1\ -1\ -1\ 1\ 1\ 1\ 1\ -1\ 1,$$

which one obtains from the above matrix by reading off along the extended diagonal starting at the upper left corner.

The basic properties of the product construction are formulated in the next theorem, where capital letters denote the discrete Fourier transforms.

Theorem 4.2: Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be sequences of length N_1 and N_2, for which the product $\boldsymbol{z} = \boldsymbol{x} \otimes \boldsymbol{y}$ of length $N = N_1 \cdot N_2$ is defined. For $j = 0,1,\cdots,N-1$ let $j_1 = j \bmod N_1$ and $j_2 = j \bmod N_2$.

1) The periodic correlations are

$$\theta_j(z) = \theta_{j_1}(\boldsymbol{x})\theta_{j_2}(\boldsymbol{y}), \qquad j = 0,1,\cdots,N-1. \quad (4.2)$$

2) Let s and t be integers such that $sN_1 + tN_2 = 1$. Then

$$Z(\epsilon_j) = X(\epsilon_{tN_2 \cdot j_1})Y(\epsilon_{sN_1 \cdot j_2}), \qquad j = 0,1,\cdots,N-1. \quad (4.3)$$

Proof: 1) See [16]. 2) Since $(N_1, N_2) = 1$, the numbers s and t exist. By the Chinese remainder theorem, we have $j \equiv j_1 \cdot tN_2 + j_2 \cdot sN_1 \pmod{N}$. Using this we get

$$Z(\epsilon_j) = \sum_{l=0}^{N-1} z_l \epsilon_j^l = \sum_{l=0}^{N-1} z_l (\epsilon_{tN_2 \cdot j_1})^l (\epsilon_{sN_1 \cdot j_2})^l$$
$$= \sum_{l_1=0}^{N_1-1} \sum_{l_2=0}^{N_2-1} x_{l_1} y_{l_2} (\epsilon_{tN_2 \cdot j_1})^{l_1} (\epsilon_{sN_1 \cdot j_2})^{l_2}$$
$$= \left[\sum_{l_1=0}^{N_1-1} x_{l_1} (\epsilon_{tN_2 \cdot j_1})^{l_1}\right]\left[\sum_{l_2=0}^{N_2-1} y_{l_2} (\epsilon_{sN_1 \cdot j_2})^{l_2}\right]$$
$$= X(\epsilon_{tN_2 \cdot j_1})Y(\epsilon_{sN_1 \cdot j_2}).$$

Note that ϵ_{tN_2}, resp. ϵ_{sN_1}, is a power of a complex root of unity of order N_1, resp. N_2, so by (4.3) the DFT of the product can be computed from the DFT of the factors.

Jacobi symbols are known from number theory. These symbols are usually denoted in the same way as Legendre symbols. If $N = pq$, where p and q are different primes, the Jacobi symbol (j/N) is defined by

$$\left(\frac{j}{N}\right) = \left(\frac{j}{p}\right)\left(\frac{j}{q}\right), \qquad (4.4)$$

where the terms on the right-hand side are the Legendre symbols defined in (1.6) and (1.7). We recall that if p is a prime and $\gcd(j,p) > 1$, then $(j/p) = 1$. With this notation, a *Jacobi sequence* $\boldsymbol{z} = z_0, z_1, \cdots, z_{N-1}$ of length $N = pq$ is defined by

$$z_l = \left(\frac{l}{N}\right), \qquad l = 0,1,\cdots,N-1. \qquad (4.5)$$

It is easily seen, from (4.1) and (4.4), that a Jacobi sequence is the product of two Legendre sequences, that is, $\boldsymbol{z} = \boldsymbol{x} \otimes \boldsymbol{y}$. Hence the DFT of a Jacobi sequence can be calculated from (1.11) and Theorem 4.2. This result can

be formulated as follows:

$$Z(\epsilon_j)=\begin{cases}1, & j=0\\ 1+\xi_2 y_{j_2}\sqrt{q}\,, & j=p,2p,\cdots,(q-1)p\\ 1+\xi_1 x_{j_1}\sqrt{p}\,, & j=q,2q,\cdots,(p-1)q\\ \left(1+\xi_1 x_{j_1}\sqrt{p}\right)\left(1+\xi_2 y_{j_2}\sqrt{q}\right), & \gcd(j,N)=1\end{cases} \tag{4.6}$$

where $j_1=j \pmod p$, $j_2=j \pmod q$, $j=1,\cdots,N-1$, and where $\xi_1,\xi_2\in\{\pm 1,\pm i\}$. To see this, consider for example the case where $p\equiv 1 \pmod 4$ and $q\equiv 3 \pmod 4$. From (1.11) and (4.3) we have, for $(j,N)=1$,

$$\begin{aligned}Z(\epsilon_j)&=\left(1+x_{tqj_1}\sqrt{p}\right)\left(1+iy_{spj_2}\sqrt{q}\right)\\&=\left(1+x_{tq}x_{j_1}\sqrt{p}\right)\left(1+iy_{sp}y_{j_2}\sqrt{q}\right),\end{aligned}$$

which gives (4.6) for $\xi_1=x_{tq}$ and $\xi_2=iy_{sp}$.

In Fig. 1 the merit factors of some Jacobi sequences of length $p(p+4)=N$ are plotted as a function of $\log_2 N$. The merit factor was calculated for each cyclic shift of a Jacobi sequence and only the largest merit factor is plotted in the figure. For example, the best merit factor is 3.30 for a length 77 sequence shifted 61 places. For a length $13\times 17=221$ Jacobi sequence shifted 66 places, the merit factor is 1.66. Also, as indicated in the figure, the merit factor seems to increase (although slowly) with increasing length. This behavior of shifted Jacobi sequences is quite different from the behavior of shifted Legendre sequences of comparable length where the highest merit factor is close to 6. In order to get better sequences, one can note that in the case $q=p+2$ the Jacobi sequence (4.5) is not identical with the twin-prime sequence (2.4), and therefore does not satisfy the condition (1.12). We have therefore considered modifications of Jacobi sequences.

A *modified Jacobi sequence* $z=z_0,z_1,\cdots,z_{N-1}$ of length $N=pq$, where p and q are different primes, is defined as

$$z_j=\begin{cases}+1, & j=0,q,2q,\cdots,(p-1)q,\\ -1, & j=p,2p,\cdots,(q-1)p,\\ \left(\dfrac{j}{N}\right), & \gcd(j,N)=1.\end{cases} \tag{4.7}$$

This construction is similar to the method used in [17] for construction of arrays. For $q=p+2$, the definition (4.7) is the same as (2.4).

In Fig. 1 the merit factors of some modified Jacobi sequences of length $N=p(p+4)$ are plotted in the same way as for Jacobi sequences. For example the merit factor is 5.09 for a length 77 sequence shifted 17 places. For a length $13\times 17=221$ modified Jacobi sequence shifted 58 places, the merit factor is 5.72. (The corresponding numbers for Jacobi sequences are 3.30 and 1.66, respectively). The figure also indicates that the merit factor of modified Jacobi sequences of length $p(p+4)$ increases smoothly and rapidly to the value six. (This can also be observed for other values of q as well). However, when $q-p\equiv 0 \pmod 4$ it appears that the merit factor of modified Jacobi sequences increases more rapidly than for sequences where $q-p\equiv 2 \pmod 4$, e.g., compare the curve for twin-prime sequences in Fig. 1 with the curve for modified Jacobi sequences. We have not yet been able to give a reasonable explanation of this phenomenon.

In the next section we determine the asymptotic behavior of the merit factor for Jacobi sequences and modified Jacobi sequences. Two such sequences are only different on a small fraction of the positions, but nevertheless, this fraction is too large to conclude that the two classes have the same asymptotic behavior (and for moderate lengths we have seen a significant difference). It is therefore necessary to determine the DFT of a modified Jacobi sequence.

If $z=x\otimes y$ is a Jacobi sequence of length $N=pq$, and u is the modified Jacobi sequence (4.7), we have $u=z+v$, where

$$v_l=\begin{cases}1-\left(\dfrac{l}{p}\right), & l=q,2q,\cdots,(p-1)q,\\ -1-\left(\dfrac{l}{q}\right), & l=p,2p,\cdots,(q-1)p,\\ 0, & \text{otherwise.}\end{cases} \tag{4.8}$$

For $j=0,1,\cdots,N-1$ let $j_1=j \bmod p$, $j_2=j \bmod q$. For the DFT of the sequence v, we then have

$$\begin{aligned}V(\epsilon_j)&=\sum_{s=1}^{p-1}\left(1-\left(\frac{sq}{p}\right)\right)\epsilon_j^{sq}+\sum_{s=1}^{q-1}\left(-1-\left(\frac{sp}{q}\right)\right)\epsilon_j^{sp}\\&=\sum_{s=1}^{p-1}\epsilon_j^{sq}-\sum_{s=1}^{q-1}\epsilon_j^{sp}-\sum_{s=1}^{p-1}\left(\frac{q}{p}\right)\left(\frac{s}{p}\right)\epsilon_{j_1}^{sq}\\&\quad-\sum_{s=1}^{q-1}\left(\frac{p}{q}\right)\left(\frac{s}{q}\right)\epsilon_{j_2}^{sp}.\end{aligned}$$

Using (1.11), there exist elements $\eta_1,\eta_2\in\{\pm 1,\pm i\}$ such that

$$V(\epsilon_j)=\begin{cases}p-q, & j=0,\\ -q+\eta_1 x_{j_1}\sqrt{p}\,, & j=q,2q,\cdots,(p-1)q,\\ p+\eta_2 y_{j_2}\sqrt{q}\,, & j=p,2p,\cdots,(q-1)p,\\ \eta_1 x_{j_1}\sqrt{p}+\eta_2 y_{j_2}\sqrt{q}\,, & \gcd(j,N)=1.\end{cases} \tag{4.9}$$

The DFT of the modified Jacobi sequence u is then

$$U(\epsilon_j)=Z(\epsilon_j)+V(\epsilon_j), \tag{4.10}$$

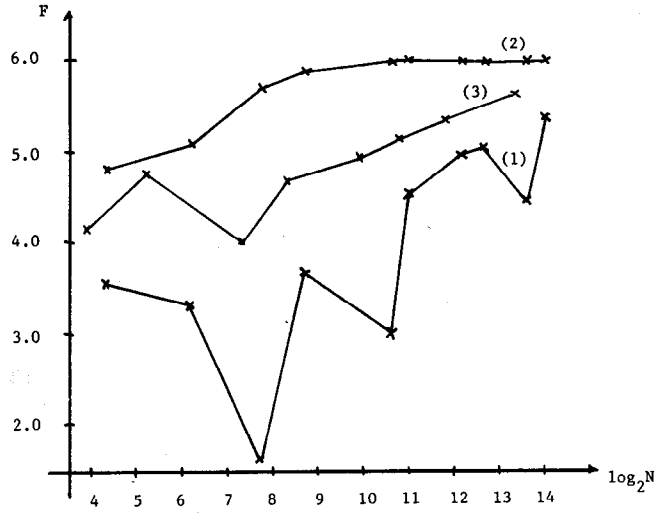

Fig. 1. Merit factor of: 1) Jacobi sequences, 2) modified Jacobi sequences, 3) twin-prime sequences.

where the terms on the right-hand side are given by (4.6) and (4.9).

In the next section we shall further need a bound on the cyclic correlations θ_j of Jacobi and modified Jacobi sequences. For Jacobi sequences it immediately follows from Theorem 4.2, that

$$|\theta_j| \le p+q, \qquad j=1,\cdots,N-1. \tag{4.11}$$

For a modified Jacobi sequence, which is different from the Jacobi sequence in at most $p+q$ positions, it follows from (4.11) that

$$|\theta_j| \le 3(p+q), \qquad j=1,\cdots,N-1. \tag{4.12}$$

V. The Asymptotic Merit Factor of Jacobi and Modified Jacobi Sequences

Based on the formulas (4.6), (4.9), and (4.10), we shall in this section (under some conditions on p and q) determine the asymptotic merit factor of the sequences constructed in Section IV. One way to do this is to treat the sums A, B, C, D from (1.10) for each type of sequence as we did in Section III. However, we will use a slightly different procedure that explains the result better.

If the sequence in question is $z=z_0,z_1,\cdots,z_{N-1}$, it follows from (4.6), (4.9), and (4.10) that there is an $\xi \in \{\pm 1, \pm i\}$ such that

$$Q(\epsilon_j) = 1+\xi z_j\sqrt{N}+a_j, \qquad j\ge 1, \tag{5.1}$$

where the correction terms a_j satisfy the inequalities

$$|a_j| \le 2\left(\sqrt{p}+\sqrt{q}\right), \quad \text{if } \gcd(j,N)=1, \tag{5.2}$$

$$|a_j| \le \sqrt{N}+\max\left\{2\sqrt{p}+q, 2\sqrt{q}+p\right\}, \quad \text{if } \gcd(j,N)>1. \tag{5.3}$$

The bounds on the correction terms are chosen such that they are satisfied for both Jacobi sequences and modified Jacobi sequences. Hence we treat both types of sequences simultaneously.

We will also treat shifted versions of the sequences, and by (1.9) the merit factor of the sequence z shifted t positions is

$$1/F = \frac{1}{2N^3}\left(\sum_{j=0}^{N-1}\left|Q_t(\epsilon_j)\right|^4+\left|Q_t(-\epsilon_j)\right|^4\right)-1, \tag{5.4}$$

where $Q_t(\epsilon_j)=\epsilon_j^{-t}Q(\epsilon_j)$ is the DFT of the shifted sequence.The numbers $Q_t(-\epsilon_j)$ can be calculated from $Q_t(\epsilon_j)$, $j=0,1,\cdots,N-1$, as in (1.10).

Now, let us assume that the correction terms a_j are so small that they can be disregarded in the calculation of (5.4). This means that instead of $Q(\epsilon_j)$ we can consider

$$\tilde{Q}(\epsilon_j) = 1+\xi z_j\sqrt{N}. \tag{5.5}$$

This, however, is exactly the same expression as the DFT of a Legendre sequence. The calculations in [10] are only based on the formula (5.5), the interpolation formula

$$\tilde{Q}(-\epsilon_j) = \frac{2}{N}\sum_{k=0}^{N-1}\frac{\epsilon_k}{\epsilon_j+\epsilon_k}\tilde{Q}(\epsilon_k), \tag{5.6}$$

and the fact that the cyclic correlations of the sequence are small compared to N. For the sequences z considered here, we have the estimations (4.11) and (4.12). Therefore, if we assume that $(p+q)/N \to 0$ for $N\to\infty$, then it follows from the calculations in [10] that the expression

$$1/\tilde{F} = \frac{1}{2N^3}\sum_{j=0}^{N-1}\left(\left|\tilde{Q}_t(\epsilon_j)\right|^4+\left|\tilde{Q}_t(-\epsilon_j)\right|^4\right)-1 \tag{5.7}$$

gives the asymptotic formula (1.8). Here $\tilde{Q}_t(\epsilon_j)=\epsilon_j^{-t}\tilde{Q}(\epsilon_j)$ and similarly for $\tilde{Q}_t(-\epsilon_j)$. We now find simple conditions on p and q under which (5.4) and (5.7) are asymptotically equal. To this end, it is sufficient to consider the unshifted sequence.

From (5.1) and (5.5), we have

$$Q(\epsilon_j) = \tilde{Q}(\epsilon_j)+a_j \tag{5.8}$$

and, if we define b_j such that

$$Q(-\epsilon_j) = \tilde{Q}(-\epsilon_j)+b_j, \tag{5.9}$$

then direct calculations give

$$1/F-1/\tilde{F} = G/2N^3,$$

where

$$\begin{aligned}|G| \le \sum_{j=0}^{N-1}&\Big(|a_j|^4+6\left|\tilde{Q}(\epsilon_j)\right|^2|a_j|^2\\ &+4\left(\left|\tilde{Q}(\epsilon_j)\right|^2+|a_j|^2\right)|a_j|\left|\tilde{Q}(\epsilon_j)\right|\Big)\\ &+\sum_{j=0}^{N-1}\Big(|b_j|^4+6\left|\tilde{Q}(-\epsilon_j)\right|^2|b_j|^2\\ &+4\left(\left|\tilde{Q}(-\epsilon_j)\right|^2+|b_j|^2\right)|b_j|\left|\tilde{Q}(-\epsilon_j)\right|\Big).\end{aligned} \tag{5.10}$$

Clearly $|\tilde{Q}(\epsilon_j)| \le 2\sqrt{N}$. Using (5.2) and (5.3), it follows that the first sum in (5.10) is upper bounded by

$$\begin{aligned} G_1 = (N-(p+q-1))\big[&16(p^2+q^2+6N+4\sqrt{N}(p+q)) \\ &+6\cdot 4N\cdot 4(p+q+2\sqrt{N}) \\ &+4\big(4N+(p+q+2\sqrt{N})\big)2\big(\sqrt{p}+\sqrt{q}\big)\sqrt{N}\cdot 2\big] \\ &+(p+q-1)\Big[(\sqrt{N}+m)^2+24N(\sqrt{N}+m)^2 \\ &+4\big(4N+(\sqrt{N}+m)^2\big)(\sqrt{N}+m)2\sqrt{N}\Big], \end{aligned}$$

where $m = \max\{2\sqrt{p}+q,\ 2\sqrt{q}+p\}$. Examining these terms and recalling that $N = pq$, it follows that, if $(p+q)^5/N^3 \to 0$ as $N \to \infty$, then $G_1/N^3 \to 0$ as $N \to \infty$.

Let us next consider the second sum in (5.10). To estimate the terms b_j in (5. 9), we use the interpolation formula

$$Q(-\epsilon_j) = \frac{2}{N}\sum_{k=0}^{N-1}\frac{\epsilon_k}{\epsilon_k+\epsilon_j}Q(\epsilon_k).$$

From this and (5.6), we then have

$$|b_j| \le 2(\log N)\cdot \max_l\{|a_l|\}$$

and

$$|\tilde{Q}(-\epsilon_j)| \le 4\sqrt{N}\log N,$$

where we have used that

$$\sum_{j=0}^{N-1}\frac{1}{|1+\epsilon_j|} \le N\log N,$$

which can be proved in the same way as (3.6) of [10]. We can then proceed as with G_1. The conclusion is that, if

$$\frac{(p+q)^5\log^4 N}{N^3} \to 0, \qquad \text{for } N\to\infty, \qquad (5.11)$$

then the second sum in (5.10) divided by N^3 goes to zero for N going to infinity. Thus we have proved the following theorem.

Theorem 5.1: Let the numbers p and q satisfy the condition (5.11), where $N = pq$. The asymptotic merit factor F of a Jacobi or modified Jacobi sequence shifted t places is given by the formula

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \le 1/2, \qquad (5.12)$$

where $f = t/N$.

One consequence of the condition (5.11) is that both p and q shall increase; moreover, if q is the smallest, then $p \in [q, q^{3/2-\delta}]$ for a fixed $\delta > 0$. The estimations used to derive (5.11) are crude, and clearly the condition can be weakened somewhat. It should also be remarked that if instead of the procedure used here one directly examines the sums in (1.10), one gets, still by crude estimations, a weaker condition than (5.11). For instance instead of $p \in [q, q^{3/2-\delta}]$, it suffices with $p \in [q, q^{2-\delta}]$. However, such improvements are not of importance.

The way Theorem 5.1 was proved also shows that, if one considers the product of finitely many Legendre sequences, then (under certain conditions) the formula (5.12) is again obtained. The reason is that the DFT of this sequence is obtained from Theorem 4.2, and therefore one gets an expression of the form (5.1) where the correction terms a_j can be disregarded under conditions similar to (5.11). This means that, for any sufficiently large N, we can construct a sequence of length N with merit factor close to 6.

VI. Conclusion and Remarks

In this paper we have investigated the merit factor of long binary sequences constructed from cyclic Hadamard difference sets. We have shown that the asmptotic merit factor of any maximal length shift register sequence is 3 and that the asymptotic merit factor of a twin-prime sequence is 6 for the optimal shift. Legendre sequences are known [10] to also have merit factor 6 for the optimal shift. It is currently an open problem to find the asymptotic merit factor for sequences constructed from GMW and Hall difference sets. The asymptotic merit factor of a Jacobi sequence, modified or not, was shown to be 6 for the optimal shift. Thus we have demonstrated large classes of long binary sequences with merit factor 6, which is the highest value presently known. Using the product construction and Legendre sequences, we have argued that the largest possible merit factor is at least 6 for N sufficiently large. Finally, by introducing modified Jacobi sequences, we have demonstrated that it is fairly easy to construct sequences with merit factor close to 6 for moderate composite lengths.

Acknowledgment

The authors wish to thank the referees for their comments that improved the readability of this paper.

References

[1] M. J. E. Golay, "Sieves for low autocorrelation binary sequences," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 43–51, Jan. 1977.
[2] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.
[3] J. Lindner, "Binary sequences up to length 40 with best possible autocorrelation function," *Electron. Lett.*, vol. 11, p. 507, Oct. 1975.
[4] J. Bernasconi, "Low autocorrelation binary sequences: statistical mechanics and configuration space analysis," *J. Phys.*, vol. 48, pp. 559–567, Apr. 1987.
[5] G. F. M. Beenker, T. A. C. M. Claasen, and P. W. C. Heimes, "Binary sequences with a maximally flat amplitude spectrum," *Phillips J. Res.*, vol. 40, no. 5, pp. 289–304, 1985.
[6] M. J. E. Golay and D. Harris, "A new search for skewsymmetric binary sequences with optimal merit factors," *IEEE Trans. Inform. Theory*, vol. 36, no. 5, pp. 1163–1166, Sept. 1990.
[7] J. Bernasconi, "Optimization problems and statistical mechanics," *Proc. Workshop on Chaos and Complexity*, Torino, Italy, Oct. 5–10, 1987. Singapore: World Scientific, 1988.
[8] D. J. Newmann and J. S. Byrnes, "The L^4 norm of a polynomial with coefficients ± 1," *Amer. Math. Monthly*, vol. 97, no. 1, pp. 42–45, Jan. 1990.
[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. IT-31, no. 4, pp. 549–552, July 1985.

[10] T. Høholdt and H. E. Jensen, "Determination of the merit factor of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. 34, no. 1, pp. 161–164, Jan. 1988.
[11] M. J. E. Golay, "The merit factor of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 934–936, Nov. 1983.
[12] D. V. Sarwate, "Mean-square correlation of shift-register sequences," *IEE-Proc.*, vol. 131, pt. F, no. 2, pp. 101–106, Apr. 1984.
[13] L. D. Baumert, *Cyclic Difference Sets*. Berlin: Springer Lecture Notes in Mathematics, vol. 189, 1971.
[14] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston: Kluwer Academic, 1987.
[15] R. Liedl and H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and Its Applications, vol. 20*. Reading, MA: Addison Wesley, 1982.
[16] H. D. Lüke, "Sequences and arrays with perfect periodic correlation," *IEEE Trans. Aerospace Electron. Syst.*, vol. 24, no. 3, pp. 287–294, May 1988.
[17] D. Calabro and J. K. Wolf, "On the synthesis of two-dimensional arrays with desirable correlation properties," *Inform. Contr.*, vol. 11, pp. 537–560, 1968.