Modifications of Modified Jacobi Sequences

Tingyao Xiong, and Jonathan I. Hall, *Member, IEEE,*

***Abstract*—The known families of binary sequences having asymptotic merit factor 6.0 are modifications to the families of Legendre sequences and Jacobi sequences. In this paper, we show that at $N = pq$, there are many suitable modifications other than the Jacobi or Modified Jacobi sequences. Furthermore, we will give three new modifications to the character sequences of length $N = pq$. Based on these new modifications, for any pair of large p and q, we can construct a binary sequence of length $2pq$ so that such families of sequences have asymptotic merit factor 6.0 without cyclic shifting of the base sequences.**

***Index Terms*—aperiodic correlation, character sequences, merit factor, primitive characters.**

I. Introduction

Let $x = (x_0, x_1, \ldots, x_{N-1})$ and $y = (y_0, y_1, \ldots, y_{N-1})$ be sequences of *length* N. The *aperiodic crosscorrelation* function between x and y at shift i is defined to be

$$A_{x,y}(i) = \sum_{j=0}^{N-i-1} x_j y_{j+i}\,, \quad i = 1, ..., N-1\,. \tag{1}$$

When $x = y$, denote

$$A_x(i) = A_{x,x}(i) = \sum_{j=0}^{N-i-1} x_j x_{j+i}\,, \quad i = 1, ..., N-1\,, \tag{2}$$

the *aperiodic autocorrelation* function of x at shift i.

The *periodic crosscorrelation* function between x and y at shift i is defined to be

$$P_{x,y}(i) = \sum_{j=0}^{N-1} x_j\, y_{j+i}, \quad i = 0, ..., N-1\,, \tag{3}$$

where all the subscripts are taken modulo N. Similarly, when $x = y$, put

$$P_x(i) = \sum_{j=0}^{N-1} x_j\, x_{j+i}, \quad i = 0, ..., N-1\,, \tag{4}$$

the *periodic autocorrelation* function of x at shift i where all the subscripts are taken modulo N.

If the sequence x is binary, which means that all the x_j's are $+1$ or -1, the *merit factor* of the sequence x, introduced by Golay [1], is defined as

$$F_x = \frac{N^2}{2\sum_{i=1}^{N-1} A_x^2(i)}\,. \tag{5}$$

J. I. Hall and T. Xiong are with the Department of Mathematics, Michigan State University, East Lansing, MI 48823.

J. I. Hall and T. Xiong are partially supported by the National Science Foundation.

Email: jhall@math.msu.edu, xiongtin@msu.edu

Moreover, for a family of sequences

$$S = \{x^1, x^2, \ldots, x^n, \ldots\}\,,$$

where for each $i \geq 1$, x^i is a binary sequence of increasing length N_i, if the limit of F_{x^i} exists as i approaches the infinity, we call

$$F = \lim_{i\to\infty} F_{x^i}\,,$$

the asymptotic merit factor of the sequence family S.

Since Golay proposed the merit factor concept, finding binary sequences with high merit factor has become a very active research area. Specifically, there are many important results on the asymptotic behavior of Legendre sequences and Jacobi sequences.

For p an odd prime, a Legendre sequence of length p is defined by the Legendre symbols

$$\alpha_j = \left(\frac{j}{p}\right), j = 0, \ldots, p-1,$$

$$\text{where } \left(\frac{j}{p}\right) = \begin{cases} 1, & \text{if } j \text{ is a square modulo } p\,; \\ -1, & \text{otherwise.} \end{cases} \tag{6}$$

In 1988, Høholdt and Jensen [2] proved the following theorem:

Theorem 1.1: The asymptotic merit factor F of Legendre sequences of length p offset by the factor f is

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \leq 1/2\,. \tag{7}$$

□

By Theorem 1.1, offset Legendre sequences have an asymptotic merit factor 6.0 at the fraction $|f| = \frac{1}{4}$. In [3], J.M. Jensen, and H.E. Jensen and Høholdt proved that the formula (7) is also correct for *Jacobi sequences* and *Modified Jacobi sequences* of length pq provided p and q satisfy

$$\frac{(p+q)^5 \log^4 N}{N^3} \to 0, \quad for\ N \to \infty\,. \tag{8}$$

We use (i, N) to represent the greatest common divisor of integers i and N. Given an odd prime p, the real primitive character modulo p takes the form

$$\chi_p(j) = \begin{cases} \left(\frac{j}{p}\right) & , \text{ if } (j,p) = 1\,; \\ 0 & , \text{ otherwise.} \end{cases} \tag{9}$$

where $\left(\frac{j}{p}\right)$ is the Legendre symbol as defined in expression (6). More generally, for an odd number N, where $N = p_1 p_2 \ldots p_r$ with $p_1 < p_2 < \cdots < p_r$ distinct odd primes, the real primitive character modulo N takes the form

$$\chi_N(j) = \chi_{P_1}(j) \cdot \chi_{P_2}(j) \ldots \chi_{P_{r-1}}(j) \cdot \chi_{P_r}(j)\,. \tag{10}$$

Results such as Theorem 1.1 are proved using Gauss Sums, (see, for instance, [12] page 233).

Theorem 1.2: (Gauss Sum) For any $j \in \mathbf{Z}$, let $\xi_j = e^{\frac{2\pi j}{N} i}$. The **Gauss sum** $\chi_N[\xi_j]$ associated to the primitive character χ mod N of (10) is defined to be the complex number

$$\chi_N[\xi_j] = \sum_{m=0}^{N-1} \chi_N(m)\xi_j^m \ .$$

Then

$$|\chi_N[\xi_j]| = \begin{cases} \sqrt{N}, & \text{if } (j,N) = 1 \ ; \\ 0, & otherwise \ . \end{cases} \tag{11}$$

□

TABLE I
PRIMITIVE CHARACTERS AND SEQUENCES OF LEGENDRE FAMILIES

x_k	$(k,N)=1$	$p \mid k$	$q \mid k$
Legendre sequence	$\chi_N(k)$	$+1$	$-$
Jacobi sequence	$\chi_N(k)$	$\chi_q(k/p)$	$\chi_p(k/q)$
Modified Jacobi sequence	$\chi_N(k)$	$+1$	-1

The Legendre sequences, Jacobi and Modified Jacobi sequences just redefine the value at the i-th position where $(i,N) > 1$. In this sense, all of the Legendre sequences, Jacobi and Modified Jacobi sequences are modifications of character sequences. TABLE I shows the close connection between the two categories.

So far, all the known families of sequences with high asymptotic merit factor are highly related to the primitive character sequences as defined in (10). For instance, performing calculations on the character forms (which are actually triple-valued), Borwein and Choi [4] proved that (7) is correct for all the sequences defined as in (10) under an improved restriction on p_i's

$$\frac{N^\epsilon}{p_1} \to \infty \text{ for any } \epsilon \text{ small enough} \ . \tag{12}$$

Particularly, when $N = pq$ for $p < q$ distinct odd primes, according to condition (8), we can give an upper bound of ϵ in (12) as

$$\frac{N^\epsilon}{p} \to \infty \text{ for any } 0 < \epsilon < \frac{2}{5} \ .$$

This statement will be used frequently in later sections.

Recently, inspired by Parker's work, an extension technique has been used to construct sequences with high asymptotic merit factor 6.0 of families of length $2p$([13]), $4p$ ([14]), $2pq$([13]), though there was some restriction to the values of $p, q \pmod 4$) and as both p and q approach ∞. Specifically, for the families of length $2p$ and $4p$, the merit factor values for all the rotations of the above two constructions are computed in [15].

From the discussion above, we see that research on binary sequences with high asymptotic merit factor has been focused on the modification of Legendre sequences and Jacobi sequences. However, Legendre sequences, Jacobi or modified Jacobi sequences are just modifications of character sequences by putting new definitions at positions i, with $(i,N) > 1$. When $N = pq$, since the number of those positions is greater than $\sqrt{N}$, people have been hesitant to change the values at those positions ([15], Proposition 1, page 138). However, surprisingly, we show in the following theorem that we are free to put any new values at those position i's with $(i,N) > 1$. The following theorem is the first result of this paper.

Theorem 1.3: Let $N = pq$, where $p < q$ are distinct odd primes. Then for each N, let the binary sequences $u^N = (u_0, u_1, \ldots, u_{N-1})$ satisfy

$$u_i = \begin{cases} \chi_N(i), & \text{if } (i,N) = 1 \ ; \\ \pm 1, & otherwise \ . \end{cases} \tag{13}$$

where the sequence χ_N is as defined in expression (10). Now construct any infinite sequence of such sequences

$$u = \{u^{N_1}, u^{N_2}, \ldots, u^{N_i}, \ldots\},$$

where $N_i = p_i q_i$ for $p_i < q_i$ distinct odd primes. Then u has the same asymptotic merit factor value F form as character sequence χ, given by

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

whenever

$$\frac{N^\epsilon}{p_i} \to 0 \quad \text{when } N_i \to \infty, \tag{14}$$

where f is the fraction of shifting and ϵ is any positive number satisfying $0 < \epsilon < \frac{2}{5}$.

We first give a proof of Theorem 1.3 in Section 2. In Section 3, we will give three constructions of binary sequences of length $N = pq$. Meanwhile, some results from [13] will be reviewed. In Section 4, we will give an upper bound for periodic autocorrelations of all the sequences constructed in Section 3. In Section 5, we will prove that all the sequences constructed in Section 3 can be doubled to obtain new sequences of length $2N$ with the high asymptotic merit factor 6.0 provided the condition (14) is satisfied.

II. PROOF TO THEOREM 1.3

Given a sequence $x = (x_0, x_1, \ldots, x_{N-1})$ of length N, we have the *Discrete Fourier Transform* (DFT) of the sequence, that is,

$$x[\xi_j] = \sum_{k=0}^{N-1} x_k \xi_j^k, \quad j = 0, 1, \ldots, N-1, \tag{15}$$

where $\xi_j = e^{\frac{2\pi j}{N} i}$.

Furthermore, for $0 \le t < N$, let $x^t = (x_t, x_{t+1}, \ldots, x_{N-1}, x_0, x_1, \ldots, x_{t-1})$ be the offset x sequence arising from t cyclic left shifts of sequence x. The *Discrete Fourier Transform* (DFT) of x^t is then

$$x^t[\xi_j] = \sum_{k=0}^{N-1} x_{k+t} \xi_j^k, \quad j = 0, 1, \ldots, N-1, \tag{16}$$

where all the subscripts are taken modulo N.

Property 2.1: Let $x = (x_0, x_1, \ldots, x_{N-1})$ be a real-valued sequence of length N, $\xi_j = e^{\frac{2\pi j}{N} i}$. For $x[\xi_j]$ the DFT of x as defined above,

$$\sum_{j=0}^{N-1} |x[\xi_j]|^2 = N\|x\|^2 \ ,$$

where $\|x\|^2 = \sum_{k=0}^{N-1} x_k^2$.

Proof. This is a well-known application of Parseval's Theorem in the form of the Discrete Fourier Transform (DFT). Readers can find the proof in many references, for instance, [6], page 33 and page 53. □

Property 2.2: Suppose we have sequences $a = (a_0, a_1, \ldots, a_{m-1})$, and $b = (b_0, b_1, \ldots, b_{n-1})$ with $(m, n) = 1$. Let $N = mn$ and consider $\sum_{j=0}^{N-1} a_j b_j$, where the subscripts are taken modulo m and n respectively. Then

$$\sum_{j=0}^{N-1} a_j b_j = \left(\sum_{k=0}^{m-1} a_k\right) \cdot \left(\sum_{s=0}^{n-1} b_s\right).$$

Proof.

$$\begin{aligned}\sum_{j=0}^{N-1} a_j b_j &= \sum_{k=0}^{m-1}\sum_{s=0}^{n-1} a_{kn+s} b_s \\ &= \sum_{s=0}^{n-1} b_s \sum_{k=0}^{m-1} a_{kn+s} = \left(\sum_{k=0}^{m-1} a_k\right) \cdot \left(\sum_{s=0}^{n-1} b_s\right),\end{aligned}$$

where the last equality follows from $(m, n) = 1$. □

Proof of Theorem 1.3

For each N, write $u^N = \chi_N + v^N$, where the sequence χ_N is the character sequence of (10) and u^N is as defined in (13). In the following proof, in order to simplify the notation, we write u, χ and v instead of u^N, χ_N and v^N. Then for each N, $0 \le t < N$, put $u^t = \chi^t + v^t$, where $u^t = (\ u_t, u_{t+1}, \ldots, u_{N-1}, u_0, u_1, \ldots, u_{t-1}\ )$ and similarly for χ^t and v^t.

For $\xi_j = e^{\frac{2\pi j}{N} i}$, where $0 \le j \le N-1$, for a fixed t, from the Discrete Fourier Transform as shown in (16),

$$u^t[\xi_j] = \chi^t[\xi_j] + v^t[\xi_j] = \chi^t[\xi_j] + a_j \ , \tag{17}$$

$$u^t[-\xi_j] = \chi^t[-\xi_j] + v^t[-\xi_j] = \chi^t[-\xi_j] + b_j \ , \tag{18}$$

where $a_j = v^t[\xi_j]$ and $b_j = v^t[-\xi_j]$.

Let $\widetilde{F}_t^N$ be the merit factor of χ^t. Then by Theorem 1.2 of [4] (page 35), when condition (14) is satisfied,

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{\widetilde{F}_t^N} &= \lim_{N\to\infty} \frac{1}{2N^3} \sum_{j=0}^{N-1} \left(\ |\chi^t[\xi_j]|^4 + |\chi^t[-\xi_j]|^4\ \right) - 1 \\ &= \frac{2}{3} - 4|f| + 8f^2 \ ,\end{aligned}$$

where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction.

Let F_t^N be the merit factor of u^t. Then from ([3], (5.4) page 624),

$$\frac{1}{F_t^N} = \frac{1}{2N^3} \sum_{j=0}^{N-1} \left(\ |u^t[\xi_j]|^4 + |u^t[-\xi_j]|^4\ \right) - 1 \ .$$

Put $1/F_t^N - 1/\widetilde{F}_t^N = G/2N^3$. Our goal is to prove that the limit of F_t^N takes exactly the same form as $\widetilde{F}_t^N$. In other words,

$$\lim_{N\to\infty} \frac{1}{F_t^N} = \frac{2}{3} - 4|f| + 8f^2 \ ,$$

provided condition (14) is satisfied, where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction. So it suffices to prove that

$$G/2N^3 \to 0 \quad \text{as } N \to \infty.$$

Again, using the form ([3], (5.10), page 624),

$$|G| \le \sum_{j=0}^{N-1} S_j + \sum_{j=0}^{N-1} T_j \tag{19}$$

where

$$S_j = |a_j|^4 + 6|\chi^t[\xi_j]|^2 \cdot |a_j|^2 + 4(\ |\chi^t[\xi_j]|^2 + |a_j|^2\ ) \cdot |a_j| \cdot |\chi^t[\xi_j]|$$

and

$$\begin{aligned}T_j = {} & |b_j|^4 + 6|\chi^t[-\xi_j]|^2 \cdot |b_j|^2 \\ & + 4(\ |\chi^t[-\xi_j]|^2 + |b_j|^2\ ) \cdot |b_j| \cdot |\chi^t[-\xi_j]|\end{aligned}$$

Now we look at the values of a_j and b_j, where $0 \le j \le N-1$.

$$a_j = v^t[\xi_j] = \xi_j^{-t} \left[\sum_{m=0}^{p-1} v_{mq} e^{\frac{2\pi m j}{p} i} + \sum_{k=1}^{q-1} v_{kp} e^{\frac{2\pi k j}{q} i} \right],$$

$$b_j = v^t[-\xi_j] = \xi_j^{-t} \left[\sum_{m=0}^{p-1} v'_{mq} e^{\frac{2\pi m j}{p} i} + \sum_{k=1}^{q-1} v'_{kp} e^{\frac{2\pi k j}{q} i} \right], \tag{20}$$

where $v_{mq}, v_{kp}, v'_{mq}, v'_{kp} \in \{+1, -1\}$, for $1 \le m < q$, $1 \le k < p$. Denote

$$\left| \xi_j^{-t} \sum_{m=0}^{p-1} v_{mq} e^{\frac{2\pi m j}{p} i} \right| = |v_p^j|, \qquad \left| \xi_j^{-t} \sum_{k=1}^{q-1} v_{kp} e^{\frac{2\pi k j}{q} i} \right| = |v_q^j|;$$

$$\left| \xi_j^{-t} \sum_{m=0}^{p-1} v'_{mq} e^{\frac{2\pi m j}{p} i} \right| = |\widetilde{v}_p^j|, \qquad \left| \xi_j^{-t} \sum_{k=1}^{q-1} v'_{kp} e^{\frac{2\pi k j}{q} i} \right| = |\widetilde{v}_q^j|.$$

For any j,

$$e^{\frac{2\pi m(j+p)}{p} i} = e^{\frac{2\pi m j}{p} i} \quad \text{and} \quad e^{\frac{2\pi k(j+q)}{q} i} = e^{\frac{2\pi k j}{q} i},$$

so we have for any j,

$$\begin{aligned}|v_p^j| = |v_p^{j+p}|, \ |\widetilde{v}_p^j| = |\widetilde{v}_p^{j+p}|; \\ |v_q^j| = |v_q^{j+q}|, \ |\widetilde{v}_q^j| = |\widetilde{v}_q^{j+q}|.\end{aligned} \tag{21}$$

From Property 2.1, we have

$$\sum_{j=0}^{p-1} |v_p^j|^2 = \sum_{j=0}^{p-1} |\widetilde{v}_p^j|^2 = p^2, \tag{22}$$

and

$$\sum_{j=0}^{q-1}|v_q^j|^2=\sum_{j=0}^{q-1}|\widetilde{v}_q^j|^2=q(q-1). \tag{23}$$

Now we estimate the upper bound of $\sum_{j=0}^{N-1}S_j$ in expression (19).

Note that $|a_j|\le|v_p^j|+|v_q^j|$, $|b_j|\le|\widetilde{v}_p^j|+|\widetilde{v}_q^j|$. Then for $1\le s\le 4$,

$$\begin{aligned}\sum_{j=0}^{N-1}|a_j|^s&\le\sum_{j=0}^{N-1}(|v_p^j|+|v_q^j|)^s\\&=\sum_{m=0}^{s}\sum_{j=0}^{N-1}\binom{s}{m}|v_p^j|^m\cdot|v_q^j|^{s-m},\\\sum_{j=0}^{N-1}|b_j|^s&\le\sum_{j=0}^{N-1}(|\widetilde{v}_p^j|+|\widetilde{v}_q^j|)^s\\&=\sum_{m=0}^{s}\sum_{j=0}^{N-1}\binom{s}{m}|\widetilde{v}_p^j|^m\cdot|\widetilde{v}_q^j|^{s-m}.\end{aligned}$$

The following calculations are the upper estimates to the values of $\sum_{m=0}^{s}\sum_{j=0}^{N-1}|v_p^j|^m\cdot|v_q^j|^{s-m}$, for $1\le s\le 4$. Suppose r is either p or q. Applying the result from (21), (22) and (23), we have

$$\begin{aligned}&\sum_{j=0}^{N-1}|v_r^j|^2=\frac{N}{r}\cdot\sum_{k=0}^{r-1}|v_r^k|^2\le Nr\ ;\\&\sum_{j=0}^{N-1}|v_r^j|^4=\frac{N}{r}\cdot\sum_{k=0}^{r-1}|v_r^k|^4\le\frac{N}{r}\cdot(\sum_{k=0}^{r-1}|v_r^k|^2)^2\le Nr^3\ ;\\&\sum_{j=0}^{N-1}|v_r^j|=\frac{N}{r}\cdot\sum_{k=0}^{r-1}|v_r^k|\le\frac{N}{r}\cdot\sqrt{\sum_{k=0}^{r-1}|v_r^k|^2\cdot r}\le N\sqrt{r}\ .\end{aligned}$$

Note that $(r,N/r)=1$. By Property 2.2 we have

$$\begin{aligned}&\sum_{j=0}^{N-1}|v_r^j|\cdot|v_{N/r}^j|\\&=\left[\sum_{k=0}^{r-1}|v_r^k|\right]\cdot\left[\sum_{m=0}^{N/r-1}|v_{N/r}^m|\right]\\&\le\sqrt{\sum_{k=0}^{r-1}|v_r^k|^2\cdot r}\times\sqrt{\sum_{m=0}^{N/r-1}|v_{N/r}^m|^2\cdot\frac{N}{r}}\le N^{\frac{3}{2}}\ .\end{aligned}\tag{25}$$

Furthermore, since $(r,N/r)=1$, from (21), Property 2.2 and the estimate shown in (24) and (25), we obtain

$$\begin{aligned}\sum_{j=0}^{N-1}|v_r^j|^3=&\frac{N}{r}\cdot\sum_{k=0}^{r-1}|v_r^k|^3\\\le&\frac{N}{r}\cdot\left(\sum_{k=0}^{r-1}|v_r^k|^2\right)\cdot\left(\sum_{k=0}^{r-1}|v_r^k|\right)\le Nr^{\frac{5}{2}}\ ;\\\sum_{j=0}^{N-1}|v_r^j|^3\cdot|v_{N/r}^j|&\\=&\left(\sum_{k=0}^{r-1}|v_r^k|^3\right)\cdot\left(\sum_{m=0}^{N/r-1}|v_{N/r}^m|\right)\le N^{\frac{3}{2}}r^2\ ;\\\sum_{j=0}^{N-1}|v_r^j|^2\cdot|v_{N/r}^j|^2&\\=&\left(\sum_{k=0}^{r-1}|v_r^k|^2\right)\cdot\left(\sum_{m=0}^{N/r-1}|v_{N/r}^m|^2\right)\le N^2\ ;\\\sum_{j=0}^{N-1}|v_r^j|^2\cdot|v_{N/r}^j|&\\=&\left(\sum_{k=0}^{r-1}|v_r^k|^2\right)\cdot\left(\sum_{m=0}^{N/r-1}|v_{N/r}^m|\right)\le N^{\frac{3}{2}}r^{\frac{1}{2}}\ .\end{aligned}\tag{26}$$

Combine all the results above, noting that we assume $p<q$. Then when p and q are large enough, we have

$$\begin{aligned}\sum_{j=0}^{N-1}|a_j|^4&\le\sum_{j=0}^{N-1}\left(\,|v_p^j|+|v_q^j|\,\right)^4\\&=\sum_{j=0}^{N-1}\left(\,|v_p^j|^4+|v_q^j|^4+4|v_p^j|^3\cdot|v_q^j|\,\right)\\&\quad+\sum_{j=0}^{N-1}\left(\,4|v_p^j|\cdot|v_q^j|^3+6|v_p^j|^2\cdot|v_q^j|^2\,\right)\\&\le Np^3+Nq^3+4N^{\frac{3}{2}}(p^2+q^2)+6N^2<10Nq^3.\end{aligned}\tag{27}$$

Similarly, under the same conditions for p and q, we get

$$\begin{aligned}&\sum_{j=0}^{N-1}|a_j|^3\le\sum_{j=0}^{N-1}(\,|v_p^j|+|v_q^j|\,)^3<3Nq^{\frac{5}{2}}\ ;\\&\sum_{j=0}^{N-1}|a_j|^2\le\sum_{j=0}^{N-1}(\,|v_p^j|+|v_q^j|\,)^2<4Nq\ ;\\&\sum_{j=0}^{N-1}|a_j|\le\sum_{j=0}^{N-1}(\,|v_p^j|+|v_q^j|\,)<2Nq^{\frac{1}{2}}\ .\end{aligned}\tag{28}$$

In the calculation above, if we replace v_p^j with $\widetilde{v}_p^j$, and v_q^j with $\widetilde{v}_q^j$, then for $0\le m\le s\le 4$, the upper bounds for $\sum_{j=0}^{N-1}|v_p^j|^m\cdot|v_q^j|^{s-m}$ as in (24) and (26) are also the upper bounds for $\sum_{j=0}^{N-1}|\widetilde{v}_p^j|^m\cdot|\widetilde{v}_q^j|^{s-m}$. As a result, the upper bounds for $\sum_{j=0}^{N-1}|a_j|^s$ are also upper bounds for $\sum_{j=0}^{N-1}|b_j|^s$, for each $1\le s\le 4$. By Theorem 1.2,

$$|\chi^t[\xi_j]|=|\xi_j^{-t}\chi_N[\xi_j]|=|\chi_N[\xi_j]|\le\sqrt{N}\ . \tag{29}$$

Using the interpolation formula ([2], (2.5), page 162)

$$\chi^t[-\xi_j]=\frac{2}{N}\sum_{k=0}^{N-1}\frac{\xi_k}{\xi_k+\xi_j}\chi^t[\xi_k]\ ,$$

and the inequality (for instance, [3], page 625),

$$\sum_{k=0}^{N-1}\left|\frac{\xi_k}{\xi_k+\xi_j}\right| \le N\log N\ ,$$

combined with the result in (29), we have

$$|\chi^t[-\xi_j]| \le 2\sqrt{N}\log N, \quad \text{for} \quad 0\le j\le N-1\ . \tag{30}$$

Combining the results from (29) and (30), we can write

$$|\chi^t[\pm\xi_j]| \le 2\sqrt{N}\log N, \quad \text{for} \quad 0\le j\le N-1\ . \tag{31}$$

Now we give an upper bound to $\sum_{j=0}^{N-1} S_j$ and $\sum_{j=0}^{N-1} T_j$ of form (19) simultaneously. We use symbol c_j to represent either a_j or b_j. Using (27), (28) and (31), we have that there exists a positive constant C independent of N, such that

$$\begin{aligned}
&\sum_{j=0}^{N-1}|c_j|^4 < CNq^3\ ;\\
&\sum_{j=0}^{N-1} 6|\chi^t(\pm\xi_j)|^2\cdot|c_j|^2 \le 24N\log^2 N\cdot\left(\sum_{j=0}^{N-1}|c_j|^2\right)\\
&\qquad\qquad < CN^2q\log^2 N\ ;\\
&\sum_{j=0}^{N-1} 4|\chi^t(\pm\xi_j)|^3\cdot|c_j| \le 32N^{\frac{3}{2}}\log^3 N\cdot\left(\sum_{j=0}^{N-1}|c_j|\right)\\
&\qquad\qquad < CN^{\frac{5}{2}}q^{\frac{1}{2}}\log^3 N\ ;\\
&\sum_{j=0}^{N-1} 4|\chi^t(\pm\xi_j)|\cdot|c_j|^3 \le 8\sqrt{N}\log N\cdot\left(\sum_{j=0}^{N-1}|c_j|^3\right)\\
&\qquad\qquad < CN^{\frac{3}{2}}q^{\frac{5}{2}}\log N\ .
\end{aligned}\tag{32}$$

Thus equation (19) becomes

$$|G| \le \sum_{j=0}^{N-1} S_j + \sum_{j=0}^{N-1} T_j = o(N^3)\ ,$$

provided the condition (14) is satisfied. This finishes the proof of Theorem 1.3. □

The proof for Theorem 1.3 uses similar notation and technique to the proof of Theorem 5.1 of [3], but Theorem 1.3 is a more general result since in the sequence u, u_j's are randomly defined when $(j,N)>1$.

III. Construction

In this section, starting from Theorem 1.3, we will give three new and specific modifications at the positions j, with $(j,N)>1$, based on the character sequence χ_N as defined in equation (10). These will be used in the construction of sequences of sequences with asymptotic merit factor 6.0.

Definition 3.1: Suppose r is an integer. For any $1\le i\le r$, if $(i,r)=1$, then there exists a unique $\overline{i_r}$, with $1\le\overline{i_r}\le r$, such that $i\cdot\overline{i_r}\equiv 1 \pmod r$. Put $\widetilde{i_r}=\overline{k_r}$, where $k=min\{i,r-i\}$.

For instance, when $r=5$, $i=3$, then $\overline{i_r}=\overline{3_5}=2$, because $3\times 2\equiv 1 \pmod 5$. While $\widetilde{i_r}=\widetilde{3_5}=\overline{2_5}=3$, because $2=\min\{3,5-3\}$.

As $(r-i)(r-\overline{i_r})\equiv 1 \pmod r$, we have

Lemma 3.2: Suppose r is a positive integer. For any integer i, if $(i,r)=1$, then $\overline{(r-i)_r}=r-\overline{i_r}$. □

For example, if $r=5$, $i=3$, then $\overline{(r-i)_r}=\overline{(5-3)_5}=\overline{2_5}=5-\overline{3_5}=3$.

Definition 3.3: A sequence $\alpha=(\alpha_0,\alpha_1,\ldots,\alpha_{N-1})$ of odd length N is *symmetric* if $\alpha_i=\alpha_{N-i}$, for $1\le i\le N-1$, and *antisymmetric* if $\alpha_i=-\alpha_{N-i}$, for $1\le i\le N-1$.

Lemma 3.4: Suppose N is an odd integer. We define a sequence $s=(s_0,s_1,\ldots,s_{N-1})$ of length N by

$$s_j=\begin{cases}(-1)^{\overline{j_N}} & ,\ \text{if } (j,N)=1;\\ 0 & ,\ \text{otherwise}\ .\end{cases}\tag{33}$$

Then the sequence s is antisymmetric.

Proof. For $1\le j\le N-1$, via Lemma 3.2 and 3.4, $s_{N-j}=(-1)^{\overline{N-j}}=(-1)^{N-\overline{j}}=-(-1)^{\overline{j}}=-s_j$ since N is odd. Therefore, s is antisymmetric. □

Let the character sequence χ_N be as defined in expression (10). Then we have the following lemma:

Lemma 3.5: χ_N is symmetric if $N\equiv 1 \pmod 4$, and antisymmetric if $N\equiv 3 \pmod 4$. In particular, $\chi_N(-1)=(-1)^{\frac{N-1}{2}}$ is 1 if $N\equiv 1 \pmod 4$ and -1 if $N\equiv 3 \pmod 4$.

Proof. First of all, we assume $N=p$, so $r=1$. But in Z_p^*, -1 is a square if and only if $p\equiv 1 \pmod 4$, as desired.

Now suppose $N=p_1p_2\ldots p_r$ with $r\ge 2$. Without loss of generality, suppose $p_1\equiv p_2\equiv\cdots\equiv p_k\equiv 3 \pmod 4$, and $p_{k+1}\equiv p_{k+2}\equiv\cdots\equiv p_r\equiv 1 \pmod 4$. Then by the $r=1$ case,

$$\begin{aligned}
\chi_N(-i) &= \chi_{p_1}(-i)\cdots\chi_{p_k}(-i)\cdot\chi_{p_{k+1}}(-i)\cdots\chi_{p_r}(-i)\\
&= (-1)^k\chi_{p_1}(i)\cdot\cdots\chi_{p_k}(i)\cdot\chi_{p_{k+1}}(i)\cdots\chi_{p_r}(i)\\
&= (-1)^k\chi_N(i)\ .
\end{aligned}$$

Therefore, if k is even, then $N\equiv 1 \pmod 4$, $\chi_N(-i)=\chi_N(i)$, and χ_N is symmetric; while if k is odd, then $N\equiv 3 \pmod 4$, $\chi_N(-i)=-\chi_N(i)$, and χ_N is antisymmetric. □

Property 3.6: Suppose N is odd. For the sequence $\alpha=(\alpha_0,\alpha_1,\ldots,\alpha_{N-1})$ of length N, let the sequence $\beta=(\beta_0,\beta_1,\ldots,\beta_{N-1})$ with $\beta_j=(-1)^j\alpha_j$. If α is symmetric, then β is antisymmetric, while if α is antisymmetric, then β is symmetric.

Proof. If α is symmetric, then $\alpha_j=\alpha_{N-j}$, for $1\le j\le N-1$. Therefore, $\beta_j=(-1)^j\alpha_j=(-1)^j\alpha_{N-j}=-(-1)^{N-j}\alpha_{N-j}=-\beta_{N-j}$ since N is odd. So β is antisymmetric. Interchanging the roles of α and β gives the other case. □

We define the triple-valued sequence V of length N to be

$$V_j=\begin{cases}\chi_N(j) & ,\ j=1,\ldots,N-1\ ;\\ 1 & ,\ j=0\ .\end{cases}\tag{34}$$

From Lemma 3.5, the sequence V is symmetric when $N \equiv 1 \pmod 4$ and antisymmetric when $N \equiv 3 \pmod 4$. Our goal is to construct specific families of binary sequences based on the triple-valued sequence V. These new sequences have the same symmetric type as the sequence V, depending upon the values of N modulo 4.

Definition 3.7: Suppose $N = pq$, where p and q are distinct odd primes. Let the sequence V of length N be as defined in (34). Then we define the binary sequences x, y and z of length N with

$$x_j = y_j = z_j = V_j, \qquad for\ j = 0 \ \ and \ \ (j, N) = 1.$$

Otherwise, for $\{r, d\} = \{p, q\}$ and $1 \le k \le r-1$, put

$$x_{kd} = \begin{cases} (-1)^{\overline{k_r}} & , if\ N \equiv 3 \pmod 4 ; \\ (-1)^{\widetilde{k_r}} & , if\ N \equiv 1 \pmod 4. \end{cases}$$

$$y_{kd} = \begin{cases} \chi_r(k) & , if\ k \le \frac{r-1}{2} ; \\ \chi_d(-1) \cdot \chi_r(k) & , if\ k > \frac{r-1}{2}. \end{cases}$$

$$z_{kd} = (\chi_d(-1))^k \cdot \chi_r(k).$$

To better understand the definitions of sequences x, y, and z, we will study a concrete example.

Example 1: Suppose $N = 3 \times 5 = 15$, the sequence V of length 15 is as defined in expression (34), and the Jacobi sequence J of length 15 is as shown in TABLE I. Then we put values of V_j's and J_j's in TABLE II:

TABLE II
V, AND J OF LENGTH $N = 15$.

position j	0	1	2	3	4	5	6	7
V_j	+1	+1	+1	0	+1	0	0	−1
J_j	+1	+1	+1	+1	+1	+1	−1	−1
				↑			↑	
				$\chi_5(1)$			$\chi_5(2)$	

position j	8	9	10	11	12	13	14
V_j	+1	0	0	−1	0	−1	−1
J_j	+1	−1	−1	−1	+1	−1	−1
		↑			↑		
		$\chi_5(3)$			$\chi_5(4)$		

Here V is antisymmetric because $15 \equiv 3 \pmod 4$. But the Jacobi sequence J is neither symmetric nor antisymmetric; indeed, the positions 0, 3, 6, 9, and 12 give a subsequence $(1, \chi_5(1), \chi_5(2), \chi_5(3), \chi_5(4))$ which is symmetric since $5 \equiv 1 \pmod 4$. The new sequences x, y, and z as defined in Definition 3.7 give new values on positions j, with $(j, 15) > 1$ as shown in TABLE III.

Therefore, we have the sequences x, y and z as shown in TABLE IV.

Note that in Example 1, x, y and z only differ at positions j, where $(j, N) > 1$, and all are antisymmetric, as is V. This is a concrete example of the following general result.

Lemma 3.8: Suppose $N = pq$, where p and q are distinct odd primes. Let the three binary sequences x, y and z of length N be as defined in Definition 3.7. Then x, y and z are symmetric if $N \equiv 1 (\bmod 4)$, and antisymmetric if $N \equiv 3 (\bmod 4)$.

TABLE III
COMPARISON AMONG J_j, x_j, y_j, AND z_j FOR $(J, N) > 1$.

position j	3	5	6
J_j	$\chi_5(1) = 1$	$\chi_3(1) = 1$	$\chi_5(2) = -1$
x_j	$(-1)^{\overline{1_5}} = -1$	$(-1)^{\overline{1_3}} = -1$	$(-1)^{\overline{2_5}} = -1$
y_j	$\chi_5(1) = 1$	$\chi_3(1) = 1$	$\chi_5(2) = -1$
z_j	$(-1)^1\chi_5(1) = -1$	$\chi_3(1) = 1$	$(-1)^2\chi_5(2) = -1$

position j	9	10	12
J_j	$\chi_5(3) = -1$	$\chi_3(2) = -1$	$\chi_5(4) = 1$
x_j	$(-1)^{\overline{3_5}} = 1$	$(-1)^{\overline{2_3}} = 1$	$(-1)^{\overline{4_5}} = 1$
y_j	$-\chi_5(3) = 1$	$\chi_3(2) = -1$	$-\chi_5(4) = -1$
z_j	$(-1)^3\chi_5(3) = 1$	$\chi_3(2) = -1$	$(-1)^4\chi_5(4) = 1$

TABLE IV
x, y, AND z FOR LENGTH $N = 15$.

position j	0	1	2	3	4	5	6	7	8
V_j	+1	+1	+1	***0***	+1	***0***	***0***	−1	+1
J_j	+1	+1	+1	***+1***	+1	***+1***	***-1***	−1	+1
x_j	+1	+1	+1	***-1***	+1	***-1***	***-1***	−1	+1
y_j	+1	+1	+1	***+1***	+1	***+1***	***-1***	−1	+1
z_j	+1	+1	+1	***-1***	+1	***+1***	***-1***	−1	+1

position j	9	10	11	12	13	14
V_j	***0***	***0***	−1	***0***	−1	−1
J_j	***-1***	***-1***	−1	***+1***	−1	−1
x_j	***+1***	***+1***	−1	***+1***	−1	−1
y_j	***+1***	***-1***	−1	***-1***	−1	−1
z_j	***+1***	***-1***	−1	***+1***	−1	−1

Proof. To shorten the proof, we use the notation u_j to represent one of x_j, y_j, or z_j.

If $(j, N) = 1$, $u_j = V_j$, thus by Lemma 3.5, we have

$$u_j = u_{N-j}, \text{ if } N \equiv 1 \pmod 4 ;$$
$$u_j = -u_{N-j}, \text{ if } N \equiv 3 \pmod 4 .$$

We wish to prove this for all j's with $1 \le j \le N-1$.

By Lemma 3.5, for $m \in \{p, q, N\}$, we have $\chi_m(-1) = (-1)^{\frac{m-1}{2}}$. In particular, the two equalities above are equivalent to the single equality

$$u_j \cdot u_{N-j} = \chi_N(-1).$$

Let $\{r, d\} = \{p, q\}$, so that $N = rd$ and $N - kd = (r-k) \cdot d$. Therefore to complete the proof of the lemma, it is enough to verify

$$u_{kd} \cdot u_{(r-k)d} = \chi_N(-1).$$

for all $1 \le k \le \frac{r-1}{2}$. We do this in cases.

First,

$$\begin{aligned} y_{kd} \cdot y_{(r-k)d} &= \chi_r(k) \cdot \chi_d(-1) \cdot \chi_r(r-k) \\ &= \chi_d(-1) \cdot \chi_r(k) \cdot \chi_r(-k) \\ &= \chi_d(-1) \cdot \chi_r(-1) \cdot (\chi_r(k))^2 = \chi_N(-1). \end{aligned}$$

Next,

$$\begin{aligned} z_{kd} \cdot z_{(r-k)d} &= (\chi_d(-1))^k \cdot \chi_r(k) \cdot (\chi_d(-1))^{r-k} \cdot \chi_r(r-k) \\ &= (\chi_d(-1))^r \cdot \chi_r(k) \cdot \chi_r(-k) \\ &= \chi_d(-1) \cdot \chi_r(-1) \cdot (\chi_r(k))^2 = \chi_N(-1), \end{aligned}$$

since when r is odd, $(\chi_d(-1))^r = \chi_d(-1)$.

Finally, if $N \equiv 1 \pmod 4$,

$$\begin{aligned} x_{kd} \cdot x_{(r-k)d} &= (-1)^{\widetilde{k_r}} \cdot (-1)^{\widetilde{(r-k)_r}} \\ &= (-1)^{\overline{k_r}} \cdot (-1)^{\overline{k_r}} = 1 = \chi_N(-1) \ , \end{aligned}$$

while if $N \equiv 3 \pmod 4$, then by Lemma 3.2

$$\begin{aligned} x_{kd} \cdot x_{(r-k)d} &= (-1)^{\overline{k_r}} \cdot (-1)^{\overline{(r-k)_r}} \\ &= (-1)^{\overline{k_r}} \cdot (-1)^{r-\overline{k_r}} \\ &= (-1)^r = -1 = \chi_N(-1). \end{aligned}$$

Combing all the results above, we have that x, y and z are symmetric when $N \equiv 1 \pmod 4$, and antisymmetric when $N \equiv 3 \pmod 4$. In other words, x, y and z have the same symmetric type as the sequence V. □

Definition 3.9: Given two sequences $u = (u_0, u_1, \ldots, u_{N-1})$ and $e = (e_0, e_1, \ldots, e_{N-1})$, we define the product sequence $b = u*e$ by $b_i = u_i e_i$, for $i = 0, 1, ..., N-1$.

Definition 3.10: For $\delta = 0, 1$, let the four sequences $\pm e^{(\delta)}$ be given by

$$e_j^{(\delta)} = (-1)^{\binom{j+\delta}{2}} \ . \tag{35}$$

In [13], certain sequences $b = (u, u) * (\pm e^{(\delta)})$ give rise to sequences with asymptotic merit factor $4 \times F$ once the following are demonstrated:

(a) u is symmetric or antisymmetric ;
(b) the sequences u have asymptotic merit factor F ;
(c) the periodic autocorrelations have $\sum_{i=1}^{N-1} P_u^2(i) = o(N^2)$.

Here Lemma 3.8 provides (a), and Theorem 1.3 gives (b) with $F = 1.5$. Therefore we will be able to prove the following theorem, the second main result of this paper, once we have studied autocorrelations in the next section.

Theorem 3.11: For each $N = p_N q_N$, where $p_N < q_N$ are distinct odd primes, let u^N be any one of the binary sequences x, y and z as in Definition 3.7. Let the sequence e^N of length $2N$ be one of the four sequences $\pm e^{(\delta)}$ from the Definition 3.10. Let $b_N = \{u^N, u^N\} * e^N$, be a sequence of length $2N$. Then the sequence of sequences $\{b_N\}$ has asymptotic merit factor 6.0 provided

$$\frac{N^\epsilon}{p_N} \to 0 \quad \text{when } N \to \infty \ , \tag{36}$$

where ϵ satisfies $0 < \epsilon < \frac{2}{5}$.

Note that condition (36) in Theorem 3.11 is the same as condition (14) in Theorem 1.3.

IV. Periodic Autocorrelation of Sequences X, Y and Z

The following well known number theoretic result can be found in many references, for instance, Lemma 2 in [7].

Lemma 4.1: Suppose χ_p is as defined in form (9), then the periodic autocorrelations of χ_p are

$$P_{\chi_p}(k) = \sum_{n=0}^{p-1} \chi_p(n)\chi_p(n-k) = \begin{cases} p-1 & , \ if \ p|k; \\ -1 & , \ otherwise. \end{cases}$$

□

Let $N = pq$, where $p < q$ are odd primes. For $1 \le j \le N-1$, by Property 2.2 and Lemma 4.1, the periodic autocorrelations of χ_N are

$$P_{\chi_N}(j) = P_{\chi_p}(j) \times P_{\chi_q}(j) = \begin{cases} 1-p & , \ if \ p \mid j \ ; \\ 1-q & , \ if \ q \mid j \ ; \\ +1 & , \ otherwise \ . \end{cases}$$

Therefore, the periodic autocorrelations of the sequence V of (34) satisfy

$$|P_V(j)| \le \begin{cases} 1+p & , \ if \ p \mid j \ ; \\ 1+q & , \ if \ q \mid j \ ; \\ +3 & , \ otherwise \ . \end{cases} \tag{37}$$

Property 4.2: For p an odd prime, let χ_p be the primitive character modulo p as defined in form (9). Then for any k, we have

$$\left| \sum_{n=0}^{p-1} (-1)^n \chi_p(n)\chi_p(n+k) \right| \le \begin{cases} 36p^{\frac{1}{2}} \log p \ + 1, & if \ p \nmid k; \\ 0, & if \ p \mid k. \end{cases}$$

Proof. The result is obviously correct when $p|k$. So now suppose $p \nmid k$.

From Lemma 4.1,

$$\begin{aligned} & |\sum_{n=0}^{p-1} (-1)^n \chi_p(n)\chi_p(n+k)| \\ &= |\sum_{j=1}^{\frac{p-1}{2}} \chi_p(2j)\chi_p(2j+k) - \sum_{j=1}^{\frac{p-1}{2}} \chi_p(2j-1)\chi_p(2j-1+k)| \\ &\le |\sum_{j=1}^{\frac{p-1}{2}} \chi_p(2j)\chi_p(2j+k)| \\ &+ |\sum_{j=1}^{\frac{p-1}{2}} \chi_p(2j-1)\chi_p(2j-1+k)| \\ &\le 2|\sum_{j=1}^{\frac{p-1}{2}} \chi_p(2j)\chi_p(2j+k)| + 1 \\ &= 2|\sum_{j=1}^{\frac{p-1}{2}} \chi_p(j(j+2^{-1}k))| + 1 \ . \end{aligned}$$

Weil [9] proved that the Riemann Hypothesis is true for the zeta-function of an algebraic function field over a finite field.

A specifically useful consequence is that, for any integers u and v with $v > 0$,

$$|\sum_{u<j<u+v} \chi_p(f(j))| \le 9mp^{\frac{1}{2}} \log p \,, \tag{38}$$

where $f(x) \in F_p[x]$ is a polynomial of degree m not of the form $b(g(x))^2$ with $b \in F_p$, $g(x) \in F_p[x]$. (The readers can find a detailed proof for equation (38) in [8] Corollary 1.) When $p \nmid k$, the polynomial $x(x + 2^{-1}k)$ is not the square of any polynomial over $F_p[x]$, so

$$|\sum_{j=1}^{\frac{p-1}{2}} \chi_p(j(j + 2^{-1}k))| \le 18p^{\frac{1}{2}} \log p \,,$$

hence

$$|\sum_{n=0}^{p-1} (-1)^n \chi_p(n)\chi_p(n+k)| \le 36p^{\frac{1}{2}} \log p + 1 \,.$$

□

For the triple-valued sequence V defined in (34), write $u_j = V_j + v_j^u$, where u could be any one of the binary sequences x, y or z of length N as defined in Definition 3.7. For instance, for $\{r, d\} = \{p, q\}$ and $1 \le k \le r-1$, when $u = x$,

$$v_j^x = \begin{cases} (-1)^{\overline{k_r}} & , \, if \;\; j = kd, \;\text{and}\;\; N \equiv 3 \pmod 4 \,; \\ (-1)^{\widetilde{k_r}} & , \, if \;\; j = kd, \;\text{and}\;\; N \equiv 1 \pmod 4 \,; \\ 0 & , \, otherwise; \end{cases}$$

and if $u = z$,

$$v_j^z = \begin{cases} \left(\chi_d(-1)\right)^k \cdot \chi_r(k) & , \, if \;\; j = kd \,; \\ 0 & , \, otherwise. \end{cases} \tag{39}$$

In all three cases, we have

$$\sum_{j=0}^{N-1} |v_j^u| \le pq - (p-1)(q-1) = p + q - 1 < 2q \,. \tag{40}$$

as $p < q$. As remarked in the previous section, we wish to prove that $\sum_{i=1}^{N-1} P_u^2(i) = o(N^2)$. The most important part of that is the following technical lemma.

Lemma 4.3: Suppose $N = pq$, where p, q are distinct odd primes with $p < q$. Let the sequence V be as defined in form (34), and write $u_j = V_j + v_j^u$, where u could be any one of the binary sequences x, y or z of length N as defined in Definition 3.7. Then when p and q are large enough, for $\{r, d\} = \{p, q\}$, we have

$$|P_{v^u}(i)| \le \begin{cases} 2, & \text{if } (i, N) = 1, \\ 4r^{\frac{1}{2}} \log^3(r), & \text{if } (i, N) = d. \end{cases}$$

Proof. For any $1 \le i \le N-1$, $P_{v^u}(i) = \sum_{j=0}^{N-1} v_j^u v_{j+i}^u$, while from the definition

$$v_j^u v_{j+i}^u \ne 0 \Leftrightarrow (j, N) = m_1 > 1, \;\text{ and }\; (j+i, N) = m_2 > 1 \,.$$

We break the proof into cases:

Case 1 $m_1 \ne m_2$, and $(i, N) = 1$.

Case 2 $m_1 = m_2 = (i, N) = d$, with $\{r, d\} = \{p, q\}$.

We first note that this handles all situations in which nonzero coefficients occur. Clearly if $m_1 = m_2$, then $(i, N) = m_1 = m_2$. If $m_1 \ne m_2$, there must be $0 < k < q$ and $0 < s < p$ with

$$kp \pm i \equiv sq \pmod N \,.$$

As $p \nmid s$ we have $p \nmid i$, and similarly $q \nmid i$ as $q \nmid k$. Therefore $m_1 \ne m_2$ implies $(i, N) = 1$.

Case 1 $m_1 \ne m_2$ and $(i, N) = 1$.

First suppose $p = m_1$, $q = m_2$. Then as above there exist $0 < k < q$ and $0 < s < p$, such that

$$kp + i = j + i \equiv sq \pmod N \,, \tag{41}$$

Such a pair k and s is unique. Indeed if there exists another pair $0 < k' < q$ and $0 < s' < p$, such that

$$k'p + i \equiv s'q \pmod N \,,$$

then $(k-k')p \equiv (s-s')q \pmod N$. As $p|N$ and $p|(k-k')p$, we find $p|(s-s')$ with $0 < s, s' < p$. Therefore, $s = s'$, and similarly, $k = k'$.

In addition, if expression (41) is satisfied, then $kp + i \equiv sq \pmod N$ implies $(p-s)q + i \equiv (q-k)p \pmod N$, and this must give the unique solution pair when $q = m_1$ and $p = m_2$. Therefore, when $(i, N) = 1$,

$$|P_v^u(i)| \le |v_{kp}^u v_{sq}^u + v_{-kp}^u v_{-sq}^u| \le 2 \,.$$

Case 2 $m_1 = m_2 = (i, N) = d$ with $\{r, d\} = \{p, q\}$.

There is an s with $0 < s < r$, and

$$P_{v^u}(i) = \sum_{j=1}^{r-1} v_{jd}^u v_{(s+j)d}^u \,. \tag{42}$$

Case 2.1 $(i, N) = d$ and $u = x$.

In 1998, W. Zhang [16] proved that for any integer t,

$$\sum_{\substack{n=1 \\ r \nmid n+t}}^{r-1} (-1)^{\overline{n_r} + \overline{(n+t)_r}} \le \sqrt{r} \, \log^2 r \,. \tag{43}$$

where $\overline{n_r}$ is as in Definition 3.1.

More generally, for any integers t, t_1 and t_2 with $t > 0$, H. Liu proved [17]

$$|\sum_{\substack{t1<n<t2 \\ r \nmid n, n+t}} (-1)^{\overline{n_r} + \overline{(n+t)_r}}| \le \sqrt{r} \, \log^3 r \,. \tag{44}$$

In the following proof, to simplify the notations, we use notation $\overline{j}$ instead of $\overline{j_r}$.

When $N \equiv 3 \pmod 4$, from (43),

$$P_{v^x}(i) = \sum_{j=1}^{r-1} v_{jd}^x v_{(s+j)d}^x = \sum_{\substack{j=1 \\ r \nmid j+s}}^{r-1} (-1)^{\overline{j} + \overline{s+j}} \le \sqrt{r} \, \log^2 r \,,$$

When $N \equiv 1 \pmod 4$, suppose $s \le (r-1)/2$. Then from Lemma 3.2 and expression (44),

$$|P_{v^x}(i)| = |\sum_{j=1}^{r-1} v^x_{jd} v^x_{(s+j)d}|$$

$$= |(\sum_{j=1}^{\frac{r-1}{2}-s} + \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} + \sum_{j=\frac{r-1}{2}+1}^{r-1-s} + \sum_{j=r-s}^{r-1}) v^x_{jd} v^x_{(s+j)d}|$$

$$= |\sum_{j=1}^{\frac{r-1}{2}-s} (-1)^{\overline{j+s+j}} - \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} (-1)^{\overline{j+s+j}}$$

$$+ \sum_{j=\frac{r-1}{2}+1}^{r-1-s} (-1)^{\overline{j+s+j}} - \sum_{j=r-s}^{r-1} (-1)^{\overline{j+s+j}}|$$

$$\le |\sum_{j=1}^{\frac{r-1}{2}-s} (-1)^{\overline{j+s+j}}| + |\sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} (-1)^{\overline{j+s+j}}|$$

$$+ |\sum_{j=\frac{r-1}{2}+1}^{r-1-s} (-1)^{\overline{j+s+j}}| + |\sum_{j=r-s}^{r-1} (-1)^{\overline{j+s+j}}|$$

$$\le 4\sqrt{r}\ \log^3 r\ .$$

Case 2.2 $(i, N) = d$ and $u = y$.

If $d \equiv 1 \pmod 4$, then from Lemma 4.1, expression (42) is

$$P_{v^y}(i) = \sum_{j=1}^{r-1} v^y_{jd} v^y_{(s+j)d} = \sum_{j=1}^{r-1} \chi_r(j)\chi_r(j+s) = -1\ .$$

If $d \equiv 3 \pmod 4$, then expression (42) becomes

$$|P_{v^y}(i)| = |\sum_{j=1}^{r-1} v^y_{jd} v^y_{(s+j)d}|$$

$$= |(\sum_{j=1}^{\frac{r-1}{2}-s} + \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} + \sum_{j=\frac{r-1}{2}+1}^{r-1-s} + \sum_{j=r-s}^{r-1}) v^y_{jd} v^y_{(s+j)d}|$$

$$\le |\sum_{j=1}^{\frac{r-1}{2}-s} \chi_r(j)\chi_r(s+j)| + |\sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} \chi_r(j)\chi_r(s+j)|$$

$$+ |\sum_{j=\frac{r-1}{2}+1}^{r-1-s} \chi_r(j)\chi_r(s+j)| + |\sum_{j=r-s}^{r-1} \chi_r(j)\chi_r(s+j)|$$

$$\le 72\sqrt{r}\ \log r\ ,$$

The last inequality follows from equation (38) by taking the degree $m = 2$.

Case 2.3 $(i, N) = d$ and $u = z$.

Equation (42) becomes

$$|P_{v^z}(i)| = |\sum_{j=1}^{r-1} v^z_{jd} v^z_{(s+j)d}|$$

$$= |\sum_{j=1}^{r-1} (\chi_d(-1))^j \cdot \chi_r(j) \cdot (\chi_d(-1))^{(s+j)_r} \cdot \chi_r(s+j)|,$$

where $0 \le (s+j)_r \le r-1$, and $(s+j)_r \equiv s+j \pmod r$.

Now we study the values of $\zeta_j = (\chi_d(-1))^{j+(s+j)_r}$. From Definition 3.7, we have

1) $\zeta_j = 1$, if $d \equiv 1 \pmod 4$.
2) $\zeta_j = (-1)^{j+(s+j)_r}$, if $d \equiv 3 \pmod 4$.

If $d \equiv 1 \pmod 4$,

$$|\sum_{j=1}^{r-1} \chi_r(j) \cdot \chi_r(s+j)| = 1\ , \quad \text{since } d \nmid s.$$

If $d \equiv 3 \pmod 4$, let j_1 be the number such that $s + j_1 < r$, but $s + j_1 + 1 \ge r$. Then

$$|P_{v^z}(i)| = |\sum_{j=1}^{j_1} \chi_r(j)\chi_r(s+j) - \sum_{j=j_1+1}^{r-1} \chi_r(j)\chi_r(s+j)|$$

$$\le |\sum_{j=1}^{j_1} \chi_r(j)\chi_r(s+j)| + |\sum_{j=j_1+1}^{r-1} \chi_r(j)\chi_r(s+j)|$$

$$\le 36\sqrt{r}\ \log r\ .$$

Again, the last inequality comes from equation (38) by putting the degree $m = 2$. □

Now we are ready to prove that $\sum_{i=1}^{N-1} P_u^2(i) = o(N^2)$:

Lemma 4.4: Suppose $N = pq$, where $p < q$ are distinct odd primes. Then when $q \le p^2$, and both p and q are large enough, we have

$$\sum_{i=1}^{N-1} P_u^2(i) \le cNq\ ,$$

where u may be any one of binary sequences x, y and z of length N as defined in Definition 3.7 and c is a constant independent of N.

Proof. Again, using the notation of Lemma 4.3, we write $u = V + v$, where v may be any one of sequences v^x, v^y, or v^z. Then we can separate the summation $\sum_{i=1}^{N-1} P_u^2(i)$ as

following:

$$\begin{aligned}
&\sum_{i=1}^{N-1} P_u^2(i) = \sum_{i=1}^{N-1}(\sum_{j=0}^{N-1} u_j u_{j+i})^2 \\
&= \sum_{i=1}^{N-1}[\sum_{j=0}^{N-1}(V_j+v_j)(V_{j+i}+v_{j+i})\,]^2 \\
&= \sum_{i=1}^{N-1}[\,P_V(i)+P_{V,v}(i)+P_{v,V}(i)+P_v(i)\,]^2 \\
&= \sum_{i=1}^{N-1} P_V^2(i) + \sum_{i=1}^{N-1} P_v^2(i) + 2\sum_{i=1}^{N-1} P_V(i)P_v(i) \\
&+ \sum_{i=1}^{N-1}[\,2P_V(i)P_{V,v}(i)+2P_V(i)P_{v,V}(i)\,] \\
&+ \sum_{i=1}^{N-1}[\,2P_v(i)P_{V,v}(i)+2P_v(i)P_{v,V}(i)\,] \\
&+ \sum_{i=1}^{N-1}[\,2P_{V,v}(i)P_{v,V}(i)+P_{V,v}^2(i)+P_{v,V}^2(i)\,] \\
&= A+B+C+D+E+F \qquad (45)
\end{aligned}$$

In expression (45), we have separated the summands into six groups. For instance $A = \sum_{i=1}^{N-1} P_V^2(i)$, and $F = \sum_{i=1}^{N-1}[\,2P_{V,v}(i)P_{v,V}(i)+P_{V,v}^2(i)+P_{v,V}^2(i)\,]$. In the following, each of the sums $X \in \{A,B,C,D,E,F\}$ will be bounded above by $c_X \cdot N \cdot q$ for appropriate constants c_X. To simplify the notation, it should be understood that all of the following statements are valid when p and q are **large enough**.

For group A, from equation (37),

$$\begin{aligned}
&\sum_{i=1}^{N-1} P_V^2(i) \\
&= \sum_{(i,N)=1}^{N-1} P_V^2(i) + \sum_{(i,N)=p}^{N-1} P_V^2(i) + \sum_{(i,N)=q}^{N-1} P_V^2(i) \\
&\le\ 9\phi(N) + q\times(1+p)^2 + p\times(1+q)^2 < 3Nq\,. \qquad (46)
\end{aligned}$$

For group B, using Lemma 4.3, we have

$$\begin{aligned}
\sum_{i=1}^{N-1} P_v^2(i) &= \sum_{(i,N)=1} P_v^2(i) + \sum_{(i,N)=p} P_v^2(i) + \sum_{(i,N)=q} P_v^2(i) \\
&\le 4\phi(N) + 16q^2\log^6 q + 16p^2\log^6 p < Nq\,.
\end{aligned}$$

Also from Lemma 4.3,

$$\begin{aligned}
|C| &\le 2\sum_{i=1}^{N-1}|P_V(i)P_v(i)| \\
&= 2\sum_{(i,N)=1}|P_V(i)P_v(i)| + 2\sum_{(i,N)=p}|P_V(i)P_v(i)| \\
&\quad + 2\sum_{(i,N)=q}|P_V(i)P_v(i)| \\
&\le 12\phi(N) + 9Np^{\frac{1}{2}}\log^3 p + 9Nq^{\frac{1}{2}}\log^3 q \\
&< 19Nq^{\frac{1}{2}}\log^3 q < Nq\,.
\end{aligned}$$

For group D, by equations (37) and (40), the absolute value of the first item is

$$\begin{aligned}
&|\sum_{i=1}^{N-1} P_V(i)P_{V,v}(i)| = \left|\sum_{i=1}^{N-1} P_V(i)\left(\sum_{m=0}^{N-1} v_m V_{m-i}\right)\right| \\
&\le \sum_{i=1}^{N-1}|P_V(i)|\sum_{m=0}^{N-1}|v_m| < 2q\times\sum_{i=1}^{N-1}|P_V(i)|\,;
\end{aligned}$$

Similarly, we can show that any other item in group D is bounded above by $2q\times\sum_{i=1}^{N-1}|P_V(i)|$. Again from (37), we have

$$\begin{aligned}
|D| &\le 8q\times\sum_{i=1}^{N-1}|P_V(i)| \\
&\le 8q\times[\sum_{\substack{i=1\\(i,N)=1}}^{N-1}|P_V(i)| + \sum_{\substack{i=1\\(i,N)>1}}^{N-1}|P_V(i)|\ \ ] \\
&\le 8q\times[3\phi(N)+3N] < 48Nq\,.
\end{aligned}$$

Now for group E. Again, consider the absolute value of item

$$\begin{aligned}
|\sum_{i=1}^{N-1} P_{v,V}(i)P_v(i)| &= |\sum_{i=1}^{N-1} P_v(i)(\sum_{j=0}^{N-1} v_j V_{j+i})| \\
&\le \sum_{i=1}^{N-1}|P_v(i)|\left(\sum_{j=0}^{N-1}|v_j|\right) \\
&< 2q\sum_{i=1}^{N-1}|P_v(i)|\,.
\end{aligned}$$

Similarly any other item in group E has absolute value bounded above by $2q\sum_{i=1}^{N-1}|P_v(i)|$. Thus using Lemma 4.3 and expression (40),

$$\begin{aligned}
|E| &\le 8q\sum_{i=1}^{N-1}|P_v(i)| \\
&\le 8q\times[\sum_{(i,N)=1}|P_v(i)| + \sum_{(i,N)=p}|P_v(i)| + \sum_{(i,N)=q}|P_v(i)|\,] \\
&\le 8q\times[2\phi(N)+4p^{\frac{3}{2}}\log^3 p + 4q^{\frac{3}{2}}\log^3 q] \\
&\le 17Nq\,,
\end{aligned}$$

where the last inequality follows from the assumption that $q \le p^2$.

Finally, we consider the first item in group F.

$$
\begin{aligned}
&|\sum_{i=1}^{N-1} P_{V,v}(i)P_{v,V}(i)| = |\sum_{i=1}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} V_j v_{j+i} v_m V_{m+i}| \\
&= |\sum_{i=1}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m V_{j-i} V_{m+i}| \\
&= |\chi_N(-1)\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m (\sum_{i=1}^{N-1} V_{i-j} V_{m+i})| \\
&= |\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m P_V(m+j)| \\
&= |\sum_{s=0}^{N-1}\sum_{j=0}^{N-1} v_{-j} v_{s-j} P_V(s)| \qquad \text{where } s = m+j \\
&= |\sum_{s=0}^{N-1} P_v(s) P_V(s)| \, .
\end{aligned}
$$

Similarly, we can prove that any other item in group F has the same absolute value $|\sum_{s=0}^{N-1} P_v(s)P_V(s)|$. So

$$
\begin{aligned}
|F| &\le 4|\sum_{s=0}^{N-1} P_v(s)P_V(s)| \\
&\le 4 \times \left(|P_v(0)P_V(0)| + |\sum_{s=1}^{N-1} P_v(s)P_V(s)| \right) \, .
\end{aligned}
$$

From equation (40),

$$
P_v(0)P_V(0) < 2Nq \, ; \tag{47}
$$

From the estimate for group C, we know that

$$
|\sum_{s=1}^{N-1} P_v(s)P_V(s)| < 19Nq^{\frac{1}{2}} \log^3 q < Nq \, ; \tag{48}
$$

Now (47) and (48) imply that

$$
|F| < 12Nq \, .
$$

Combining all of the inequalities above, we obtain the desired result. □

Lemma 4.4 shows that when condition (36) is satisfied, $\sum_{i=1}^{N-1} P_u^2(i) = O(Nq) = o(N^2)$, where u may be any one of the binary sequences x, y and z as defined in Definition 3.7. Therefore, as remarked at the end of the previous section, we are now ready to prove Theorem 3.11.

V. Proof of Theorem 3.11

The following is Lemma 2.7 of [13], page 933.

Lemma 5.1: Suppose $\alpha = (\ \alpha_0, \alpha_1, ...\alpha_{N-1}\ )$ is a symmetric or antisymmetric binary sequence of odd length N. Let the sequence e of length $2N$ be one of the four sequences $\pm e^{(\delta)}$ from the Definition 3.10. Put $b = (\ \alpha, \alpha\ ) * e$, then

$$
\begin{aligned}
\sum_{k=1}^{2N-1} A_b^2(k) =& N + \sum_{k=1}^{N-1} A_\alpha^2(k) \\
&+ 2\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha^2(k) \, .
\end{aligned}
$$

□

Proof of Theorem 3.11.

For each odd $N = p_N q_N$ with $p_N < q_N$, Lemma 3.8 shows that each of the three sequences x, y and z is symmetric or antisymmetric. Let

$$
b_N = (\ u^N, u^N\ ) * e \, ,
$$

where $u^N = x, y$ or z as defined in Definition 3.7. In the following, without confusion, we use b and u instead of b_N and u^N. Then Lemma 5.1 gives

$$
\begin{aligned}
\sum_{k=1}^{2N-1} A_b^2(k) =& N + \sum_{k=1}^{N-1} A_u^2(k) \\
&+ 2\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u(k)A_u(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u^2(k) \, .
\end{aligned}
$$

When condition (36) holds, Theorem 1.3 shows that

$$
2\sum_{k=1}^{N-1} A_u^2(k) \sim \frac{2}{3}N^2 \, , \tag{49}
$$

If the condition (36) holds, Lemma 4.4 shows that

$$
\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u^2(k) \le \sum_{k=1}^{N-1} P_u^2(k) = O(Nq) \, .
$$

Then given condition (36), by the Cauchy-Schwarz inequality

$$
\begin{aligned}
\left| \sum_{k=1}^{N-1} P_u(k)A_u(k) \right| \le& \sqrt{\left[\sum_{k=1}^{N-1} A_u^2(k) \right] \times \mathrm{O}(Nq)} \\
\sim& N^{\frac{3}{2}} q^{\frac{1}{2}} = o(N^2) \, .
\end{aligned}
$$

Therefore, for p and q subject to (36), the asymptotic merit factor of the sequence $\{b_N\}$ is

$$
\begin{aligned}
\lim_{N\to\infty}(F_{b_N}) &= \lim_{N\to\infty} \frac{(2N)^2}{2(\sum_{k=1}^{2N-1} A_{b_N}^2(k))} \\
&= \lim_{N\to\infty} \frac{4N^2}{2\sum_{k=1}^{N-1} A_u^2(k)} \\
&= 4 \times \frac{3}{2} = 6 \, .
\end{aligned}
$$

This finishes the proof of Theorem 3.11. □

VI. Conclusion

For a character sequence of length $N = pq$, the number of positions j with $(j, N) > 1$ is larger than $\sqrt{N}$, so those "modified" positions are large enough to make a difference in the merit factor. However, Theorem 1.3 shows that subject to condition (14), any modification on these positions will give the same asymptotic merit factor values as the character sequences. The authors were informed recently that Jedwab and Schmidt have obtained the same result independently under an improved condition ([19]). In [13], the doubling technique shown in Lemma 5.1 was only applied to some of the Jacobi

or modified Jacobi sequences with additional restriction to the values of $p, q \pmod 4$. Here we have constructed new sequences considerably different from the canonical Jacobi or modified Jacobi sequences and with no restrictions on the values of $p, q \pmod 4$, yet achieving the same asymptotic merit factor, as seen in Theorem 3.11.

ACKNOWLEDGMENT

The authors want to take this opportunity to express deepest appreciation to the valuable suggestions from the referees. They also thank Professor Jedwab for his encouragement and for providing them with [19].

REFERENCES

[1] M. J. E. Golay, "Sieves for Low Autocorreation Binary Sequences", IEEE Trans. Inform. Theory, vol. 23 no. 1, Jan. 1977, Page 43–51.
[2] T. Høholdt, H. E. Jensen, "Determination of the Merit Factor of Legendre Sequences", IEEE Transactions on Inform. Theory, vol. 34 no. 1, Jan. 1988, Page 161–164.
[3] J. M. Jensen, H. E. Jensen, T. Høholdt, "The Merit Factor of Binary Sequences Related to Difference Sets", IEEE Transactions on Inform. Theory, vol. 37 no. 3, May 1991, Page 617–625.
[4] P. Borwein, K-K. S. Choi, "Merit Factors of Polynomials Formed by Jacobi Symbols", Canad. J. Math. vol. 53 (1), 2001, Page 33-50.
[5] P. Borwein, K-K. S. Choi, J. Jedwab, "Binary Sequences with Merit Factor Greater Than 6.34", IEEE Transactions on Inform. Theory, vol. 50 no. 12, Dec. 2004, Page 3234–3249.
[6] C. Gasquet, P. Witomski, "Fourier Analysis and Applications", Springer, 1999.
[7] B. Conrey, A. Granville, B. Poonen, K. Soundararajan, "Zeros of Fekete Polynomials", Annales de l'institut Fourier, 50 no. 3, 2000, Page 865-889.
[8] C. Mauduit, A. Sárközy, "On Finite Pseudorandom Binary Sequences I: Measure of Pseudorandomness, the Legendre Symbol", Acta Arithmetica, LXXXII.4 ,1997, Page 365-377.
[9] A. Weil, "Sur les Courbes Algebriques et les Varietes Qui s'en Deduisent", Actualites Math. Sci. No.1041, Paris, 1945, Deuxieme Partie, §IV.
[10] A. A. Karatsuba, "Sums of Characters With Prime Numbers and Their Applications", Tatra Mt. Math. Publ. 20, 2000, Page 155-162.
[11] W. M. Schmidt, "Equations over Finite Fields: an Elementary Approach", Springer, 1976.
[12] G. Everest, T. Ward, "An Introduction to Number Theory", Springer, 2005.
[13] T. Xiong, J. I. Hall, "Construction of Even Length Binary Sequences With Asymptotic Merit Factor 6", IEEE Transactions on Information Theory 54(2): 2008, Page 931-935.
[14] N. Y. Yu, G. Gong, "The Perfect Binary Sequence of Period 4 for Low Periodic and Aperiodic Autocorrelations", Sequences, Subsequences, and Consequences, Springer-Verlag, Berlin, 2007, Page 37-49.
[15] K. Schmidt, J. Jedwab, M. G. Parker, "Two Binary Sequence Families With Large Merit Factor", Advances in Mathmatics of Communications, vol. 3, no.2, 2009, Page 135-156.
[16] W. Zhang, "On a problem of P. Gallagher", Acta Math. Hungar. 78, 1998, Page 345-357, .
[17] H. N. Liu, "New Pseudorandom Sequences Constructed Using Multiplicative Inverses", Acta Arith. 125, 2006, Page 11-19.
[18] R. Kristiansen, M. G. Parker, "Binary Sequences with Merit Factor > 6.3", IEEE Trans. Inform. Theory, vol 50, Dec. 2004, Page 3385-3389.
[19] J. Jedwab, K. Schmidt, "The Merit Factor of Binary Sequences Derived from the Jacobi Symbol", Preprint, 2010.

Tingyao Xiong Tingyao Xiong received the Ph.D. degree in Mathematics from Michigan State University, East Lansing, MI, under supervision of Professor Jonathan I. Hall in 2010. Her research interest includes Sequences, Coding Theory, and Number Theory. She is currently a Visiting Assistant Professor at Radford University, Radford, VA.

Jonathan I. Hall (M'81) received the B.S. degree in Mathematics from the California Institute of Technology (USA) in 1971 and M.Sc. and D.Phil. degrees in Mathematics from the University of Oxford (UK) in 1973 and 1974. He spent 1974 to 1976 as a Foreign Research Fellow at the Technological University Endihoven (NL) and 1976-7 as a Visiting Assistant Professor at the University of Oregon (USA). Since 1977 he has been with the Department of Mathematics at Michigan State University (USA), holding the rank of Professor since 1985.