HAMMING CORRELATION OF HIGHER ORDER

MING SU∗
Department of Computer Science
Nankai University, Tianjin, China

ARNE WINTERHOF
Johann Radon Institute for Computational and Applied Mathematics
Altenberger Straße 69, A-4040 Linz, Austria

(Communicated by Ferruh Özbudak)

Abstract. We introduce a new measure of pseudorandomness, the (periodic) Hamming correlation of order \( \ell \) which generalizes the Hamming autocorrelation \((\ell = 2)\). We analyze the relation between the Hamming correlation of order \( \ell \) and the periodic analog of the correlation measure of order \( \ell \) introduced by Mauduit and Sarközy. Roughly speaking, the correlation measure of order \( \ell \) is a finer measure than the Hamming correlation of order \( \ell \). However, the latter can be much faster calculated and still detects some undesirable linear structures.

We analyze examples of sequences with optimal Hamming correlation and show that they have large Hamming correlation of order \( \ell \) for some very small \( \ell > 2 \). Thus they have some undesirable linear structures, in particular in view of cryptographic applications such as secure communications.

1. Introduction

Sequences with ideal pseudorandomness properties have been widely used in wireless communications and cryptography. Frequency hopping sequences (FHSs) are an essential part of spread spectrum communication systems such as frequency hopping code division multiple access (FH-CDMA) systems and multiuser radar systems, see for example [4, Chapter 15]. The Hamming autocorrelation is an important measure for FHSs [20].

The conventional definition of correlation as the sum of products of corresponding sequence components is mostly suitable for phase-modulation techniques. For other modulation techniques where large sets of mutual orthogonal signals are employed, the appropriate measure for correlation is the Hamming correlation. More precisely, for a \( T \)-periodic sequence \( X = (x_n) \) over a given alphabet \( \mathcal{A} \) of size \( m \), the Hamming autocorrelation function \( H_X(d) \) of \( X \) was proposed by Lempel and Greenberger [20]:

\[
H_X(d) = \sum_{n=0}^{T-1} \delta(x_n, x_{n+d}), \quad 0 \leq d < T,
\]

where

\[
\delta(x, y) = \begin{cases} 
0 & \text{if } x \neq y, \\
1 & \text{if } x = y,
\end{cases}
\]

2010 Mathematics Subject Classification: 94A55, 11K45, 11T71, 94A05, 94A60.
Key words and phrases: Pseudorandomness, Hamming autocorrelation, frequency hopping sequence, correlation measure of order \( \ell \), cryptography.

* Corresponding author: Ming Su.
is the Kronecker delta. The maximum nontrivial Hamming autocorrelation of \( X \) is denoted by

\[
H(X) = \max_{0 < d < T} H_X(d).
\]

Lempel and Greenberger proved the first lower bound on \( H(X) \) for a given period \( T \) and alphabet size \( m \) [20]. Later many FHSs meeting the Lempel-Greenberger bound were constructed, see for example [8, 9, 17]. We call such sequences attaining the Lempel-Greenberger bound optimal.

Mauduit and Sarkozy [22, 23, 30] introduced a pseudorandomness measure for finite sequences. We consider its analog for periodic sequences, see [29].

Let \( E_m = \{\varepsilon_1, \ldots, \varepsilon_m\} \) be the set of the complex \( m \)-th roots of unity and \( F \) be the set of the \( m! \) bijections between \( A \) and \( E_m \). For a \( T \)-periodic sequence \( X = (x_0, x_1, \ldots) \) over \( A \) the periodic correlation measure of order \( \ell \) is defined as

\[
\Gamma_\ell(X) = \max_{\Phi,D} \left| \sum_{n=0}^{T-1} \varphi_1(x_{n+d_1})\varphi_2(x_{n+d_2})\cdots\varphi_\ell(x_{n+d_\ell}) \right|,
\]

where the maximum is taken over all \( \Phi = (\varphi_1, \varphi_2, \ldots, \varphi_\ell) \in F^\ell \) and \( D = (d_1, d_2, \ldots, d_\ell) \) with \( 0 \leq d_1 < \cdots < d_\ell < T \). In particular, the correlation measure of order \( \ell \) detects undesirable linear structures. For other figures of merit for finding linear structures and their relations see [3, 6, 10, 11, 15, 25] as well as the surveys [24, 26, 31, 32].

In this paper we introduce the Hamming correlation of order \( \ell \), which generalizes the Hamming autocorrelation (\( \ell = 2 \)) and compare this new measure with the correlation measure of order \( \ell \), see Theorem 1 below. Roughly speaking, the correlation measure of order \( \ell \) is a finer measure but the Hamming correlation of order \( \ell \) is easier to calculate since it does not depend on the \( (m!)^\ell \) choices of \( \Phi \). Though many frequency hopping sequences with optimal Hamming autocorrelation have been proposed, they may still have some intrinsic linear structures. Such undesirable structures can be detected by studying the Hamming correlation of order \( \ell > 2 \). It is possible to determine the subsequent carrier frequencies from the previous ones during frequency hopping data transmission and predict further data from given partial data, resulting in security risks.

The paper is organized as follows. In Section 2, we define the Hamming correlation of order \( \ell \) of a periodic sequence and analyze the relationship between this measure and the correlation measure of order \( \ell \). In Sections 3.1-3.3 we show that some sequences with optimal Hamming autocorrelation have very large Hamming correlation of order \( \ell \) for some small \( \ell > 2 \). In Section 3.4 we also study some character sequences and show that they have small Hamming correlation of order \( \ell \) up to a very large \( \ell \).

2. Hamming Correlation Measure of Order \( \ell \)

In this section we generalize the Hamming autocorrelation to the Hamming correlation of order \( \ell \) for studying the intrinsic linear structure of sequences. We restrict ourselves to sequences over \( A = \mathbb{Z}_m \). However, this definition can be easily extended to an arbitrary alphabet \( A \) of size \( m \) using any fixed bijection between \( A \) and \( \mathbb{Z}_m \).

Let \( X = \{x_n\} \) be a \( T \)-periodic sequence over \( \mathbb{Z}_m \) and \( \ell \) be a positive integer. Now we define using Kronecker’s delta
\[(1)\quad H_{\ell,a}(X) = \max_{D,S} \frac{T-1}{m} \sum_{n=0}^{T-1} \delta \left( \sum_{j \in S} x_{n+d_j}, \sum_{j \in \{1,2,\ldots,\ell\} \setminus S} x_{n+d_j} + a \right), \]

where the maximum is taken over all \(D = (d_1,d_2,\ldots,d_\ell) \in \{0,1,\ldots,T-1\}^\ell\) with 0 \(\leq d_1 < d_2 < \cdots < d_\ell < T\) and \(\emptyset \neq S \subset \{1,2,\ldots,\ell\}\). (Note that the sums inside the large brackets in (1) are considered modulo \(m\).)

For \(a = 0\), we denote the Hamming correlation of order \(\ell\) of \(X\) by \(H_\ell(X) = H_{\ell,0}(X)\). Note that the Hamming autocorrelation is \(H(X) = H_2(X)\).

Next we state and prove a relation between \(H_{\ell,a}(X)\) and the correlation measure of order \(\ell\).

**Theorem 1.**

\[
\left| H_{\ell,a}(X) - \frac{T}{m} \right| \leq \begin{cases} 
\frac{m-1}{m} \frac{1}{\sqrt{2}} \Gamma_\ell(X) & \text{if } m \text{ is a prime,} \\
\frac{3}{m^2} \Gamma_\ell(X) & \text{if } m = 4, \\
\frac{3}{m^2} \max_{1 \leq \ell \leq T} \Gamma_\ell(X) & \text{if } m > 4 \text{ is composite.}
\end{cases}
\]

**Proof.** Put \(\omega = e^{2\pi \sqrt{-1}/m}\). Since

\[
\sum_{i=0}^{m-1} \omega^{ix} = \begin{cases} 
m, & x = 0, \\
0, & x \in \mathbb{Z}_m \setminus \{0\},
\end{cases}
\]

we can write

\[
(2) \quad \delta(x,y) = \frac{1}{m} \sum_{i=0}^{m-1} \omega^{i(x-y)}, \quad x, y \in \mathbb{Z}_m.
\]

By (1) and (2) we obtain

\[
H_{\ell,a}(X) = \max_{D,S} \frac{1}{m} \frac{1}{m} \sum_{i=0}^{m-1} \sum_{n=0}^{T-1} \left( \prod_{j \in S} \omega^{x_{n+d_j}} \prod_{j \in \{1,2,\ldots,\ell\} \setminus S} \omega^{-x_{n+d_j}} \omega^{-a} \right)^i.
\]

Separating the summand for \(i = 0\) we obtain

\[
(3) \quad \left| H_{\ell,a}(X) - \frac{T}{m} \right| \leq \frac{m-1}{m} \max_{1 \leq \ell \leq T} \left| \sum_{n=0}^{T-1} \prod_{j \in S} \omega^{ix_{n+d_j}} \prod_{j \in \{1,2,\ldots,\ell\} \setminus S} \omega^{-ix_{n+d_j}} \right|.
\]

If \(m\) is a prime, \(x \mapsto \omega^{ix}\) is a bijection between \(\mathbb{Z}_m\) and the set of complex \(m\)-th roots of unity \(\mathcal{E}_m\) for any \(i = 1, \ldots, m-1\) and the maximum on the right hand side of (3) is bounded by \(\Gamma_\ell(X)\). For composite \(m\) the result follows from [6, Propositions 1 and 2].

**Remark 1.** The correlation measure of order \(\ell\) of a random sequence is small up to a sufficiently large \(\ell\), see [1, 2]. Hence, the Hamming correlation of order \(\ell\) of a pseudorandom sequence should be close to \(\frac{T}{m}\) for all small \(\ell\).

We present a simple corollary of the Lempel-Greenberger bound [20, Lemma 4] stated in [14, Corollary 1.2]:

\[
(4) \quad H(X) = H_2(X) \geq \begin{cases} 
\left\lceil \frac{T}{m} \right\rceil & \text{if } T \neq m, \\
0 & \text{if } T = m.
\end{cases}
\]

The following result reveals that the Hamming correlation of some order \(\ell\) attains high peak values if there is some approximate linear structure in a given sequence.
Corollary 1. Let $X$ be a $T$-periodic sequence over $\mathbb{Z}_m$ satisfying a linear recurrence relation of length $L$ on a subset $U \subseteq \{0, \ldots, T - 1\}$

$$x_{n+L} = \sum_{t=0}^{L-1} x_{n+t}c_t \quad \text{for all } n \in U$$

with all coefficients $c_t = \pm 1$ or 0 but at least one $c_t = 1$. Then we have

$$H_\ell(X) \geq |U| \text{ for } \ell = L + 1 - |\{t : c_t = 0\}|.$$  

Proof. We choose $M = \{t : c_t = -1\} \cup \{L\}$ and get

$$\sum_{t \in M} x_{n+t} = \sum_{t \in \{0, \ldots, L\} \setminus M, c_t \neq 0} x_{n+t}, \quad n \in U.$$  

Then the result follows by the definition of $H_\ell(X)$, see (1).

Conversely, if $H_\ell(X)$ is large, then there is a linear recurrence of $\ell - 1$ summands with coefficients $\pm 1$ satisfied by many sequence elements.

3. Examples

In this section, we study $H_{\ell,a}(X)$ for some sequences with optimal Hamming autocorrelation. We show that their Hamming correlation of order $\ell$ can be large for some small $\ell > 2$ if the parameters are not carefully chosen.

We identify $\mathbb{Z}_m$ with the set of integers $\{0, 1, \ldots, m - 1\}$.

3.1. A construction of Lempel and Greenberger. We study a sequence construction $Y$ of [20] over $\mathbb{Z}_{p^k}$ of period $p^n - 1$ with $H(Y) = p^{n-k} - 1$ meeting the bound (4) by [20, Theorem 1]. We show that in some cases there is a small $\ell > 2$ and some $a$ with large $H_{\ell,a}(Y)$.

It is constructed as follows.

Let $p$ be a prime. We start with a maximum length sequence $X$ over $\mathbb{Z}_p$ of period $p^n - 1$, that is, $X = (x_j)$ satisfies a linear recurrence over $\mathbb{Z}_p$ of length $n$,

$$x_{j+n} \equiv \sum_{i=0}^{n-1} x_{j+i}c_t \quad (\text{mod } p), \quad j \geq 0.$$  

(5)

For $1 \leq k < n$ we derive from each $k$ consecutive elements of $X$ an element of $\mathbb{Z}_{p^k}$

$$y_j = \sum_{i=0}^{k-1} x_{j+i}p^i, \quad j \geq 0,$$  

(6)

and derive a sequence $Y = (y_j)$ over $\mathbb{Z}_{p^k}$ of period $p^n - 1$ which meets the Lempel-Greenberger bound, see also [20, Lemma 3].

For $0 \leq j < p^n - 1$ we have

$$y_{j+n} - \sum_{t=0}^{n-1} y_{j+t}c_t = \sum_{i=0}^{k-1} (x_{j+n+i} - \sum_{t=0}^{n-1} x_{j+t+i}c_t)p^i$$

$$\equiv \sum_{i=0}^{k-2} (x_{j+n+i} - \sum_{t=0}^{n-1} x_{j+t+i}c_t)p^i \quad (\text{mod } p^k),$$  

(7)
by (6) and (5). Note that for $k \geq 2$

$$
\sum_{i=0}^{k-2}(x_{j+n+i} - \sum_{t=0}^{n-1} x_{j+t+i}c_t)p^i \equiv x_{j+n} - \sum_{t=0}^{n-1} x_{j+t}c_t \pmod{p^2}
$$

by (5) again. Hence, by the pigeonhole principle there exists $b \in \mathbb{Z}_{p^{k-2}}$ such that

$$
y_{j+n} - \sum_{t=0}^{n-1} y_{j+t}c_t \in [bp^2, (b+1)p^2)
$$

for at least $\left\lceil \frac{p^n - 1}{p - 1} \right\rceil \geq p^{n-k+2}$ different $0 \leq j < p^n - 1$ if $k \geq 3$.

Now we assume that $c_t \in \{-1, 0, 1\}$. Then $x_{j+n} - \sum_{t=0}^{n-1} x_{j+t}c_t$ lies in $[-(p - 1)[0 \leq t < n : c_t = 1], (p - 1)(1 + |\{0 \leq t < n : c_t = -1\}|) \cap \mathbb{Z}$ of size at most $(n + 1)(p - 1) + 1 \leq (n + 1)p$ and is divisible by $p$ because of (5). Therefore, there exists some $a \in [bp^2, (b+1)p^2)$ (divisible by $p$) such that

$$
y_{j+n} - \sum_{t=0}^{n-1} y_{j+t}c_t = a
$$

for at least $\frac{p^{n-k+2}}{n+1}$ different $0 \leq j < p^n - 1$. If $c_t = 1$ for at least one $0 \leq t < n$, we have for $\ell = n + 1 - |\{t : c_t = 0\}|$,

$$
H_{\ell,a}(Y) \geq \frac{p^{n-k+2}}{n+1}, \quad k \geq 3,
$$

which is larger than the desired value close to $p^{n-k}$, see Theorem 1, if $n$ is small with respect to $p$.

Now we study the concrete example given above [20, Theorem 1] in more detail: We start with a linear recurrence of order 3,

$$
x_{j+3} = x_{j+2} - x_j \pmod{3}, \quad j \geq 0,
$$

and derive via (6) a sequence over $\mathbb{Z}_9$ of period 26 satisfying

$$
y_{j+3} - y_{j+2} + y_j \equiv x_{j+3} - x_{j+2} + x_j \pmod{3^2}, \quad j \geq 0.
$$

Note that $x_{j+3} - x_{j+2} + x_j \in \{0, 3\}$ by (7) and thus $y_{j+3} - y_{j+2} + y_j \equiv 0, 3$ (mod $3^2$). Since the period of $X$ is 26 we have $\{(x_j, x_{j+1}, x_{j+2}) : j = 0, 1, \ldots, 26\} = \mathbb{Z}_9^3 \setminus \{(0, 0, 0)\}$. If $x_{j+2} < x_j$, we must have $x_{j+3} - x_{j+2} + x_j = 3$ and otherwise $x_{j+3} - x_{j+2} + x_j = 0$. The first case occurs 9 times and the latter 17 times, consequently, $H_3(Y) \geq 17$ which is much larger than the desired value $\frac{26}{9}$.

3.2. FHSs based on discrete logarithms of $\mathbb{Z}_{p^n}$. In [21], some classes of FHSs meeting the Lempel-Greenberger bound were constructed based on discrete logarithms in $\mathbb{Z}_{p^n}$ (or generalized cyclotomy). Let $p = ef + 1$ be an odd prime such that $f$ is odd, $n$ a positive integer, and $g$ a primitive root modulo $p^n$. For our purposes it is enough to define $X = (x_j)$ only for $x_j$ with $j \in \mathbb{Z}_{p^n}^*$ by

$$
x_j = \log_g(j) \pmod{ep^{n-1}}
$$

or equivalently

$$
x_j = i \quad \text{if and only if} \quad j = g^{i+tep^{n-1}} \pmod{ep^{n-1}}, \quad 0 \leq i < ep^{n-1}.
$$
Hence (8) is satisfied for at least \( \phi(X) \) we have
\[
\frac{\log p}{\log 2} \geq \frac{H(Y(X))}{H(Y)}.
\]
For any integers \( k \) and we also define \( H(Y(X)) = \frac{\log p}{\log 2} \) for some integers \( p \), and thus
\[
H(Y(X)) \geq p^n - p^{n-1} \quad \text{for } n \geq 4 \text{ or } n = 2, 3 \text{ and } p > 3.
\]

In [21, Method A] a method is described how to destroy the linear structure of \( X \).

Let \( \pi : \{ 0, 1, \ldots, e(p^n-1) \} \rightarrow Z(p^n-1)/f \) be any injective mapping. We study any \( p^n \)-periodic sequence \( Y = (y_j) \) over \( Z(p^n-1)/f \) satisfying
\[
y_j = \pi(x_j), \quad \gcd(j, p) = 1.
\]
By (8) and since \( |x_{j1} - x_{j2}| < e(p^n-1) \), we have
\[
x_j + x_{j+3p^{n/2}} - (x_{j+p^{n/2}} + x_{j+2p^{n/2}}) \in \{ 0, \pm e(p^n-1) \}.
\]
If \( \pi \) is of the form
\[
\pi(x) = bx + c \pmod{(p^n-1)/f}
\]
for some integers \( b, c \) with \( \gcd(b, (p^n-1)/f) = 1 \), there exists some \( a \in \{ 0, \pm e(p^n-1) \} \), such that
\[
x_j + x_{j+3p^{n/2}} - (x_{j+p^{n/2}} + x_{j+2p^{n/2}}) \equiv a \pmod{(p^n-1)/f}
\]
for at least \( p^n - p^{n-1} \) different \( j \), which implies
\[
y_j + y_{j+3p^{n/2}} - (y_{j+p^{n/2}} + y_{j+2p^{n/2}}) \equiv a' \pmod{(p^n-1)/f}
\]
for some \( a' \) and at least \( p^n - p^{n-1} \) different \( j \), and thus
\[
H_{4,a'}(Y) \geq (p^n - p^{n-1})/3
\]
which is much larger than the expected value close to \( f \).

3.3. SEQUENCES DERIVED FROM FERMAT QUOTIENTS. Next we give another very interesting sequence of optimal Hamming autocorrelation but with Hamming correlation measure of order 4 equal to its period.

For a prime \( p \) and an integer \( u \) with \( \gcd(u, p) = 1 \) the Fermat quotient \( q_p(u) \) modulo \( p \) is defined as
\[
q_p(u) = \frac{u^{p-1} - 1}{p} \pmod{p},
\]
and we also define \( q_p(kp) = 0 \) for \( k \in Z \).

Some well-known properties of Fermat quotients are discussed for example in [13]. For any integers \( k \) and \( u \) we have
\[
q_p(u + kp) \equiv q_p(u) - k[p^{p-2}] \pmod{p}.
\]
Some pseudorandomness measures of the binary sequences derived from Fermat quotients are discussed in [5, 7, 12, 16, 18, 27]. A collection of optimal families of perfect polyphase sequences using the Fermat quotient sequences is proposed in [28]. Note that \( q_p(u) \) is a \( p^2 \)-periodic sequence over \( Z_p \), and we have the following result.

**Proposition 1.** The sequence \( Q = (q_p(u)) \) is a \( (p^2, p, p) \) optimal FHS sequence, but \( H_4(Q) = p^2 \), where \( p > 3 \).
**Proof.** First we proof \( H_Q(\tau) = p \) for any \( 0 < \tau < p^2 \). The following equations are all over \( \mathbb{F}_p \). In order to investigate the number of solutions for the equation

\[
q_p(u + vp) = q_p(u + \tau + vp)
\]

over \( \mathbb{F}_p \) for some \( \tau \), we need to discuss two cases.

(i) \( p \nmid \tau \)

From (9) and (10) we derive

\[
q_p(u) - vu^{p-2} = q_p(u + \tau) - v(u + \tau)^{p-2},
\]

so for \( 0 \leq u \leq p - 1 \), we have a unique solution

\[
v = \frac{q_p(u) - q_p(u + \tau)}{u^{p-2} - (u + \tau)^{p-2}}.
\]

Therefore, by the definition of Hamming correlation we obtain \( H_Q(\tau) = p \).

(ii) \( p |\tau \)

Let \( \tau = pv \) for some integer \( v \neq 0 \). For \( 0 \leq v \leq p - 1 \), from (9) and (10) we derive

\[
q_p(u) - vu^{p-2} = q_p(u) - (v + v_\tau)u^{p-2},
\]

which implies \( u = 0 \) and we get \( H_Q(\tau) = p \).

Therefore, \( Q = (q_p(u)) \) is a \((p^2, p, p)\) optimal FHS sequence.

We verify that \( H_4(Q) = p^2 \) by taking lags \( D = (0, p, 2p, (p - 1)p) \) since

\[
q_p(u + vp) + q_p(u + vp + p) = 2q_p(u) - (2v + 1)u^{p-2} = 2q_p(u) - (2v + 2 + (p - 1))u^{p-2} = q_p(u + vp + 2p) + q_p(u + vp + (p - 1)p),
\]

which completes the proof.

3.4. Multiplicative character sequences. We consider the \( e \)-ary character sequence modulo \( p \), see also [8, 23]. Let \( p \) be a prime with \( p \equiv 1 \) (mod \( e \)) and \( \chi \) a multiplicative character of \( \mathbb{F}_p \) of order \( e \). For \( n = 1, \ldots \) we define the sequence \( X = (x_n) \) as

\[
x_n = \begin{cases} 0, & p | n, \\ j, & \chi(n) = \varepsilon_j, 0 \leq j < e, p \nmid n, \end{cases}
\]

where \( \varepsilon_e \) is a \( e \)-th root of unity. It was shown [29] that this sequence has small discrete Fourier transform and small ambiguity measures. Using the convention \( \chi(0) = 1 \) and [19, Lemma 7.3.7], for \( 1 \leq d < p \) we have

\[
\sum_{n=0}^{p-1} \chi(n)\bar{\chi}(n + d) = -1 + \bar{\chi}(d) + \chi(-d).
\]

For the Hamming autocorrelation \((\ell = 2)\) of this sequence, we have

\[
H_X(d) = \sum_{n=0}^{p-1} \delta(x_n, x_{n+d}) = \sum_{n=0}^{p-1} \left( \frac{1}{e} \sum_{j=0}^{e-1} (\chi(n)\bar{\chi}(n + d))^{j} \right).
\]
By (11) and (12) we obtain

\[ H_X(d) = \frac{p}{e} + \frac{1}{e} \sum_{j=1}^{e-1} (-1 + \bar{\chi}(d) + \chi(d)) , \]

and thus

\[ \left| H(X) - \frac{p}{e} \right| \leq \frac{3(e - 1)}{e} , \]

which is very close to the Lempel-Greenberger bound [20, Lemma 4]. Note that if \( e \) is even and \( f \) is odd, then \( H(X) = (p - 1)/e \) is optimal, see [8, Corollary 2]. We explain this more carefully for the convenience of the reader by giving a short alternative proof. The condition that \( f \) is odd implies \( \chi(-1) = (-1)^f = -1 \). If \( \chi(d) = \pm 1 \), we have

\[ H_X(d) = \frac{p}{e} + \frac{1}{e} \sum_{j=1}^{e-1} (-1)^j \]

and thus \( H_X(d) = \frac{p-1}{e} \) if \( e \) is even. If \( \chi(d) \neq \pm 1 \), we get

\[ H_X(d) = \frac{p - e + 1}{e} + \frac{1}{e} \left( \frac{\chi(d) - \bar{\chi}(d)}{\bar{\chi}(d) - 1} + \frac{\chi(d) + \chi(d)}{-\chi(d) - 1} \right) = \frac{p - 1}{e} - 1. \]

We show that also \( H_\ell(X) \) is close to \( p/e \) up to some rather high orders \( \ell \). Analogously to [23] we can show that the (periodic) correlation measure of order \( \ell \) of \( X \) is of order of magnitude \( O(\ell p^{1/2}) \). Hence, Theorem 1 implies

\[ \left| H_{\ell,a}(X) - \frac{p}{e} \right| = O(\ell p^{1/2}) \]

if \( e \) is prime and analogous but weaker results if \( e \) is composite.

Acknowledgment

The First author thanks for the hospitality during his visit to RICAM, Austrian Academy of Science, and for the support by ÖAD Ernst-Mach follow-up scholarship and SFB. The second author is partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: Typical values, Lond. Math. Soc. (3), 95 (2007), 778–812.
[2] G. Bérczi, On finite pseudorandom sequences of \( k \) symbols, Period. Math. Hungar., 47 (2003), 29–44.
[3] N. Brandstätter and A. Winterhof, Linear complexity profile of binary sequences with small correlation measure, Period. Math. Hungar., 52 (2006), 1–8.
[4] L. Chen and G. Gong, Communication Systems Security, Chapman & Hall/CRC Cryptography and Network Security, CRC Press, Boca Raton, FL, 2012.
[5] Z. Chen, A. Ostafe and A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, Lecture Notes in Comput. Sci., 6087 (2010), 73–85.
[6] Z. Chen and A. Winterhof, Linear complexity profile of \( m \)-ary pseudorandom sequences with small correlation measure, Indag. Mathem., 20 (2009), 631–640.
[7] Z. Chen and A. Winterhof, Interpolation of Fermat quotients, SIAM J. Discrete Math., 28 (2014), 1–7.
[8] W. Chu and C. J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, IEEE Trans. Inform. Theory, 51 (2005), 1139–1141.
[9] J. H. Chung and K. Yang, Optimal frequency-hopping sequences with new parameters, IEEE Trans. Inform. Theory, 56 (2010), 1685–1693.
G. Dorfer and A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, *Appl. Algebra Engrg. Comm. Comput.*, 13 (2003), 499–508.

G. Dorfer and A. Winterhof, A lattice structure of nonlinear pseudorandom number generators in parts of the period, in *Monte Carlo and Quasi-Monte Carlo Methods 2002*, Springer, Berlin, (2004), 199–211.

X. Du, C. Wu and W. Wei, An extension of binary threshold sequences from Fermat quotients, *Adv. Math. Commun.*, 10 (2016), 743–752.

R. Ernvall and T. Metsänkylä, On the \(p\)-divisibility of Fermat quotients, *Math. Comp.*, 66 (1997), 1353–1365.

R. Fuji-Hara, Y. Miao and M. Mishima, Optimal frequency hopping sequences: A combinatorial approach, *IEEE Trans. Inform. Theory*, 50 (2004), 2408–2420.

D. Gómez-Pérez and J. Gutierrez, On the linear complexity and lattice test of nonlinear pseudorandom number generators, in *Applied Algebra and Number Theory*, Cambridge Univ. Press, Cambridge, (2014), 91–101.

D. Gómez and A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hungar.*, 64 (2012), 161–168.

Y. K. Han and K. Yang, On the Sidelnikov sequences as frequency-hopping sequences, *IEEE Trans. Inform. Theory*, 55 (2009), 4279–4285.

G. Harman and I. E. Shparlinski, Products of small integers in residue classes and additive properties of Fermat quotients, *Int. Math. Res. Not.*, (2016), 1424–1446.

D. Jungnickel, *Finite Fields, Structure and Arithmetics*, B. I.-Wissenschaftsverlag, Mannheim, 1993.

A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Inform. Theory*, 20 (1974), 90–94.

F. Liu, D. Peng, Z. Zhou and X. Tang, New constructions of optimal frequency hopping sequences with new parameters, *Adv. Math. Commun.*, 7 (2013), 91–101.

C. Mauduit and A. Sarközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, 82 (1997), 365–377.

C. Mauduit and A. Sarközy, On finite pseudorandom sequences of \(k\) symbols, *Indag. Math. (N.S.)*, 13 (2002), 89–101.

W. Meidl and A. Winterhof, Linear complexity of sequences and multisequences, in *Handbook of finite fields*, CRC Press, Boca Raton, FL, (2013), 324–336.

L. Mérai, H. Niederreiter and A. Winterhof, Expansion complexity and linear complexity of sequences over finite fields, *Cryptogr. Commun.*, 9 (2017), 501–509.

H. Niederreiter, Linear complexity and related complexity measures for sequences, in *Progress in Cryptology-INDOCRYPT 2003*, Lecture Notes in Comput. Sci., 2904, Springer, Berlin, (2003), 1–17.

A. Ostafe and I. E. Shparlinski, Pseudorandomness and dynamics of Fermat quotients, *SIAM J. Discrete Math.*, 25 (2011), 50–71.

K. Park, H. Song, D. S. Kim and S. W. Golomb, Optimal families of perfect polyphase sequences from the array structure of Fermat-Quotient sequences, *IEEE Trans. Inform. Theory*, 62 (2016), 1076–1086.

G. I. Pirsic and A. Winterhof, On discrete Fourier transform, ambiguity, and Hamming-autocorrelation of pseudorandom sequences, *Des. Codes Cryptography*, 73 (2014), 319–328.

A. Sarközy, On finite pseudorandom binary sequences and their applications in cryptography, *Tatra Mt. Math. Publ.*, 37 (2007), 123–136.

A. Topuzoğlu and A. Winterhof, Pseudorandom sequences, in *Topics in Geometry, Coding Theory and Cryptography*, Algebr. Appl., 6, Springer, Dordrecht, (2007), 135–166.

A. Winterhof, Linear complexity and related complexity measures, in *Selected Topics in Information and Coding Theory*, Ser. Coding Theory Cryptol., 7, World Sci. Publ., Hackensack, NJ, (2010), 3–40.

Received June 2017; revised March 2018.

E-mail address: nksuker@gmail.com
E-mail address: arne.winterhof@oeaw.ac.at