Electronic Research Archive

https://www.aimspress.com/journal/era

ERA, 33(2): 849–866
DOI: 10.3934/era.2025038
Received: 03 December 2024
Revised: 24 January 2025
Accepted: 06 February 2025
Published: 14 February 2025

Research article

Arithmetic autocorrelation and pattern distribution of binary sequences

Xi Liu and Huaning Liu*

Research Center for Number Theory and its Applications, School of Mathematics, Northwest University, Xi'an 710127, China

* **Correspondence:** Email: hnliu@nwu.edu.cn.

Abstract: We clarify a relation between the arithmetic autocorrelation and pattern distribution of binary sequences, then we apply the relation to study the upper bound of arithmetic autocorrelation for two binary sequences constructed by Fermat quotient and the generalized cyclotomic class of order 2, respectively. Our results indicate that the sequences with large "long term" correlations may have small "short term" pattern distribution; and thus have rather small arithmetic autocorrelations.

Keywords: arithmetic autocorrelation; Fermat quotient; generalized cyclotomic; binary sequence; character sum

1. Introduction

Pseudorandom sequences are widely used in measurement, code-division multiple-access (CDMA) systems, wireless communication systems, digital communication systems, and cryptography. The correlation properties analysis of pseudorandom sequences is an important problem for pseudorandom sequences theory.

The arithmetic autocorrelation of a (purely) periodic binary sequence is investigated by Mandelbaum [1] on arithmetic codes. Let (a_n) be a binary sequence of (purely) period T. For $1 \le \tau < T$, let $(a_{n+\tau})$ be the shift of (a_n). Put

$$x_\tau = \sum_{n=0}^{T-1} a_{n+\tau} 2^n \quad \text{and} \quad \alpha_\tau = \sum_{n=0}^{\infty} a_{n+\tau} 2^n, \quad 0 \le \tau < T.$$

Write

$$\alpha_0 - \alpha_\tau = \sum_{n=0}^{\infty} s_{n,\tau} 2^n \tag{1.1}$$

with unique $s_{n,\tau} \in \{0, 1\}$. If $x_0 \ge x_\tau$, $(s_{n,\tau})$ is (purely) periodic with period T; otherwise, $(s_{n,\tau})$ is eventually periodic with period T from T on (see [2]). In terms of the case, the arithmetic autocorrelation

function $A(\tau)$ of (a_n) is defined as

$$A(\tau) = N_0 - N_1, \quad 1 \le \tau < T, \tag{1.2}$$

where $N_i = |\{T \le n \le 2T-1 : s_{n,\tau} = i\}|$, $i = 0, 1$.

Compared to the classical autocorrelation, arithmetic autocorrelation is the with-carry correlation function of pseudorandom sequences. Goresky and Klapper [3] extended the arithmetic autocorrelation to cross-correlation and gave large families of binary sequences which have ideal arithmetic cross-correlations. Later, they generalized the arithmetic autocorrelation to non-binary sequences in [4, 5]. For more background, the reader is referred to [6].

The arithmetic correlation of sequences is expected to be as small as possible. A nontrivial bound on the arithmetic autocorrelation of the Legendre sequence was proposed in [2]. Hofer, Mérai, and Winterhof [7] proved the arithmetic autocorrelation and the correlation measure of higher orders have the relation as follows:

Proposition 1.1. *[7] Put*

$$\Gamma_s = \max_{\substack{0 \le d_1 < \cdots < d_{\ell-1} < T \\ 1 \le \ell \le s}} \left| \sum_{n=0}^{T-1} (-1)^{e_n + e_{n+d_1} + \cdots + e_{n+d_{\ell-1}}} \right|.$$

Then the arithmetic autocorrelation function of a T-periodic binary sequence (e_n) satisfies

$$A(\tau) \ll \min\left\{ T^{1/2} \Gamma_{\lfloor \log T \rfloor}^{1/2}, 2^r \Gamma_{\lfloor \log T \rfloor} \log T \right\},$$

where $r = \min\{\tau, T - \tau\}$ for $1 \le \tau \le T - 1$.

We write $f(n) = O(g(n))$ or $f(n) \ll g(n)$ if $|f(n)| \le cg(n)$ for some absolute constant $c > 0$.

Pattern distribution is an important randomness feature of pseudorandom sequences, which reflects any pattern (for fixed length) appearing in a period of the sequence. More precisely, let (b_n) be a binary sequence with period T, and let the binary vector $\underline{f} = \{f_0, f_1, \cdots, f_{\ell-1}\} \in \{0, 1\}^\ell$ be any pattern (with fixed length ℓ). The number of pattern distribution is

$$N = |\{0 \le n < T : (b_n, b_{n+1}, \cdots, b_{n+\ell-1}) = (f_0, f_1, \cdots, f_{\ell-1})\}|.$$

Ding [8] proved the bounds of the pattern distribution of binary Legendre sequences. Golomb [9] presented the pattern distribution of binary m-sequences. Liu and Ren [10] showed the M-ary sequences derived from Sidel'nikov sequences have asymptotical uniform pattern distribution. Mauduit and Sárközy [11] introduced a relation of pattern distribution and correlation measure of high order. In view of the relation, Hofer, Mérai, and Winterhof [7] obtained another relation between correlation measures of high order and arithmetic autocorrelation, indicating that pseudorandom binary sequences with a small correlation measure of high order also have a small arithmetic autocorrelation; that is Proposition 1.1.

Noting that many binary sequences with large "long term" correlations may have small "short term" pattern distributions and thus they still have small arithmetic autocorrelations. In other words, there are binary sequences that have a great value correlation measure of order ℓ for large value lags $d_{\ell-1}$, but a small pattern distribution for short lengths of patterns, and then they may have small arithmetic autocorrelation. We shall establish the relation between the arithmetic autocorrelation and the pattern distribution by using the idea in [7] with certain modifications.

Theorem 1.2. *Let $E_T = \{e_0, e_1, \cdots, e_{T-1}\} \in \{0,1\}^T$ be a binary sequence of period T. Let $k \geq 1$, $1 \leq \tau \leq T-1$ be integers. For any binary vectors $\underline{a} = \{a_0, \cdots, a_k\} \in \{0,1\}^{k+1}$, $\underline{b} = \{b_0, \cdots, b_k\} \in \{0,1\}^{k+1}$ and $\underline{c} = \{c_0, \cdots, c_{k+\tau}\} \in \{0,1\}^{k+\tau+1}$, we write pattern distribution as*

$$N_{(\underline{a},\underline{b},k,\tau)}(E_T) = |\{n : \ T \leq n \leq 2T-1, (e_{n-k}, e_{n-k+1}, \cdots, e_n) = (a_0, a_1, \cdots, a_k) \text{ and } (e_{n-k+\tau}, e_{n-k+\tau+1}, \cdots, e_{n+\tau}) = (b_0, b_1, \cdots, b_k)\}|,$$

when $\tau > k$, otherwise

$$N_{(\underline{c},k,\tau)}(E_T) = |\{n : \ T \leq n \leq 2T-1, (e_{n-k}, e_{n-k+1}, \cdots, e_{n+\tau}) = (c_0, c_1, \cdots, c_{k+\tau})\}|.$$

Denote

$$\delta_{2k+2}(E_T) = \max_{\underline{a},\underline{b}} \left| N_{(\underline{a},\underline{b},k,\tau)}(E_T) - \frac{T}{2^{2k+2}} \right|, \tag{1.3}$$

and

$$\lambda_{k+\tau+1}(E_T) = \max_{\underline{c}} \left| N_{\underline{c},k,\tau}(E_T) - \frac{T}{2^{k+\tau+1}} \right|, \tag{1.4}$$

where the above maximums are taken over all binary vectors $\underline{a}, \underline{b}, \underline{c}$, respectively, and any integer τ with $1 \leq \tau < T$. Put

$$\Delta_s = \max_{1 \leq h_1, h_2 \leq s} \{\delta_{h_1}(E_T), \lambda_{h_2}(E_T)\}.$$

Then we have

$$A(\tau) \ll \min\left\{T^{1/2}\Delta_{\lfloor \log T \rfloor}^{1/2}, 2^r \Delta_{\lfloor \log T \rfloor} \log T\right\}, \tag{1.5}$$

where $r = \min\{\tau, T-\tau\}$ for $1 \leq \tau \leq T-1$.

This paper is organized as follows. We establish a relation between arithmetic autocorrelation and pattern distribution of binary sequences; and prove the relation in Section 2. In terms of the relation, we consider the arithmetic autocorrelation of two types of binary sequences constructed by Fermat quotient and generalized cyclotomic classes of order 2 in Section 3.

2. Arithmetic autocorrelation and pattern distribution

In this section, our main content is to prove Theorem 1.2 using the idea of Proposition 1.1, with the difference being that we focus on the direct relation between arithmetic autocorrelation and more specific pattern distributions with "short term".

Now we prove Theorem 1.2. As the arithmetic autocorrelation is symmetric with $A(\tau) = A(T-\tau)$([7], Proposition 2.1.), we consider $1 \leq \tau \leq \lfloor \frac{T}{2} \rfloor$ in the following. Let $1 \leq k < m$ be integers. Take $a \in \{0,1\}$, assume

$$\begin{aligned} &(e_{n-k}, e_{n-k+\tau}) = (a, 1-a), \\ &e_{n-k+j} = e_{n-k+\tau+j}, \quad j = 1, \cdots, k-1 \\ &(e_n, e_{n+\tau}) \in \{0,1\}^2, \end{aligned} \tag{2.1}$$

for $k = 1, \cdots, m-1$ and $n = T, \cdots, 2T-1$. First we let $m+1 \leq \tau \leq \lfloor \frac{T}{2} \rfloor$. For fixed a, from (1.3) we have the number of patterns

$$\begin{pmatrix} e_{n-k} & e_{n-k+1} & \cdots & e_n \\ e_{n-k+\tau} & e_{n-k+\tau+1} & \cdots & e_{n+\tau} \end{pmatrix} \tag{2.2}$$

that satisfy the assumptions (2.1) is at least $\frac{T}{2^{2k+2}} - \delta_{2k+2}$. We discuss the specific cases of assumption (2.1). If $a = 1$, from (1.1) we have

$$2^{n-k+1} > \sum_{n=0}^{n-k}(e_n 2^n - e_{n+\tau}2^n) = \sum_{n=0}^{n-k-1}(e_n 2^n - e_{n+\tau}2^n) + 2^{n-k} \geq 1.$$

This means there is no need to carry to make $s_{n-k,\tau} \geq 0$ for the subtraction of $e_{n-k+\tau} = 0$ from $e_{n-k} = 1$. Hence

$$s_{n,\tau} = \begin{cases} 1, & \text{if } e_n \neq e_{n+\tau}, \\ 0, & \text{if } e_n = e_{n+\tau}. \end{cases}$$

Obviously, there are 2^k possibilities of the pattern (2.2), then we have at least $\frac{T}{2^{k+2}} - 2^k\delta_{2k+2}$ different n with $T \leq n < 2T$ such that $s_{n,\tau} = 1$.

If $a = 0$, from (1.1) we have

$$\sum_{n=0}^{n-k}(e_n 2^n - e_{n+\tau}2^n) = \sum_{n=0}^{n-k-1}(e_n 2^n - e_{n+\tau}2^n) - 2^{n-k} < 0.$$

This means there is a need to give a carry for the subtraction of 1 from 0. Hence

$$s_{n,\tau} = \begin{cases} 1, & \text{if } e_n = e_{n+\tau}, \\ 0, & \text{if } e_n \neq e_{n+\tau}. \end{cases}$$

There are also 2^k possibilities of the pattern (2.2); thus we have at least $\frac{T}{2^{k+2}} - 2^k\delta_{2k+2}$ different n with $T \leq n < 2T$ such that $s_{n,\tau} = 1$.

In both cases, we count at least $\frac{T}{2^{k+1}} - 2^{k+1}\delta_{2k+2}$ different n with $T \leq n < 2T$ satisfying $e_{n-k} \neq e_{n-k+\tau}$, $(e_{n-k+j}, e_{n-k+\tau+j}) \in \{(0,0),(1,1)\}$ for $j = 1, \cdots, k-1$ and $s_{n,\tau} = 1$. Then we have

$$\begin{aligned} N_1 &\geq \frac{1}{2}\left(\sum_{k=1}^{m-1}\frac{1}{2^k}\right)T - \sum_{k=1}^{m-1}2^{k+1}\delta_{2k+2} \\ &\geq \frac{T}{2} - 2^{-m}T - 2^{m+1}\Delta_{2m}. \end{aligned}$$

Analogously, we have the number N_0 satisfies

$$N_0 \geq \frac{T}{2} - 2^{-m}T - 2^{m+1}\Delta_{2m}.$$

Hence, we obtain

$$|A(\tau)| = |N_0 - N_1| \leq 2^{-m+1}T + 2^{m+2}\Delta_{2m}.$$

Next, we let $1 \leq \tau \leq m$, that indicates some indices in pattern (2.2) coincide, so we have two types of pattern distributions. For fixed a, if $k \leq \tau - 1$, from (1.3) we have the number of patterns (2.2) that satisfy the assumptions (2.1) is at least

$$\frac{T}{2^{2k+2}} - \delta_{2k+2},$$

if $k \geq \tau$, we have the pattern as

$$\begin{pmatrix} e_{n-k} & e_{n-k+1} & \cdots & e_n & e_{n+1} & \cdots & e_{n+\tau} \end{pmatrix}. \tag{2.3}$$

From (1.4), we know the number of patterns (2.3) satisfies the assumption (2.1) is at least

$$\frac{T}{2^{k+\tau+1}} - \lambda_{k+\tau+1}.$$

Similar to before, if $a = 1$, we have

$$s_{n,\tau} = \begin{cases} 1, & if\ e_n \neq e_{n+\tau}, \\ 0, & if\ e_n = e_{n+\tau}. \end{cases}$$

If $a = 0$, we have

$$s_{n,\tau} = \begin{cases} 1, & if\ e_n = e_{n+\tau}, \\ 0, & if\ e_n \neq e_{n+\tau}. \end{cases}$$

In each case, we have 2^k possibilities of pattern (2.2) and $2^{\tau-1}$ possible choices of pattern (2.3). Thus, we have at least

$$\frac{T}{2^{k+1}} - 2^{k+1}\delta_{2k+2}, \quad k \leq \tau - 1,$$
$$\frac{T}{2^{k+1}} - 2^{\tau}\lambda_{k+\tau+1}, \quad k \geq \tau.$$

different n with $T \leq n < 2T$ satisfies $e_{n-k} \neq e_{n-k+\tau}$, $(e_{n-k+j}, e_{n-k+\tau+j}) \in \{(0,0),(1,1)\}$ for $j = 1, \cdots, k-1$ and $s_{n,\tau} = 1$.

Let $m' = 2m - \tau$, we obtain

$$\begin{aligned} N_1 &\geq \frac{T}{2}\sum_{k=1}^{m'-1} 2^{-k} - \sum_{k=1}^{\tau-1} 2^{k+1}\delta_{2k+2} - \sum_{k=\tau}^{m'-1} 2^{\tau}\lambda_{k+\tau+1} \\ &\geq \frac{T}{2} - 2^{-2m+\tau}T - 2^{\tau+1}(m-\tau+1)\Delta_{2m}, \end{aligned}$$

and

$$N_0 \geq \frac{T}{2} - 2^{-2m+\tau}T - 2^{\tau+1}(m-\tau+1)\Delta_{2m}.$$

Therefore

$$|A(\tau)| \leq 2^{-2m+\tau+1}T + 2^{\tau+2}(m-\tau+1)\Delta_{2m}.$$

Choosing

$$m = \left\lfloor \frac{1}{2}\log\frac{T}{\Delta_{\lfloor \log T \rfloor}} \right\rfloor,$$

We prove the result of Theorem 1.2.

3. Arithmetic autocorrelation of binary sequences

We shall study the arithmetic autocorrelation of two pseudorandom binary sequences by applying Theorem 1.2.

3.1. Binary sequence related to Fermat quotient

Let p be a prime and let n be an integer with $(n, p) = 1$. The Fermat quotient $q_p(n)$ is defined as

$$q_p(n) \equiv \frac{n^{p-1} - 1}{p} \pmod{p}, \quad 0 \le q_p(n) \le p - 1.$$

We also define $q_p(kp) = 0$ for $k \in \mathbb{Z}$. Fermat quotients have numerous applications in computational and algebraic number theory, and many authors studied their properties (see [12–19] for details). For example, Gómez and Winterhof [15] defined the binary sequence $E_{p^2} = \left(e_0, e_1, \cdots, e_{p^2-1}\right) \in \{0, 1\}^{p^2}$ as follows:

$$e_n = \begin{cases} 0, & \text{if } q_p(n) \text{ is a quadratic residue modulo } p \text{ or } q_p(n) = 0, \\ 1, & \text{otherwise,} \end{cases} \tag{3.1}$$

and showed that the upper bound of the f-correlation measure of order ℓ is $\ell p^{\frac{5}{3}}$. The high linear complexity of E_{p^2} was studied in [20]. Chen [21] described the trace representation of the above binary sequence E_{p^2} by determining the defining pairs of all binary characteristic sequences of cosets. There is the research on generalizations of the sequence E_{p^2} (see [22, 23]). The binary sequence E_{p^2} has the desired pseudorandomness; however, the arithmetic correlation of the sequence E_{p^2} remains open. We would study the arithmetic autocorrelation of the sequence E_{p^2} through Theorem 1.2.

In order to calculate the pattern distribution of the binary sequence E_{p^2}, an upper bound estimate for multiplicative character sums of Fermat quotients is needed.

Lemma 3.1. *[15] Let $\chi_1, \cdots, \chi_\ell$ be nontrivial multiplicative characters modulo p. Then we have*

$$\sum_{n=0}^{N-1} \chi_1(q_p(n + d_1)) \cdots \chi_\ell(q_p(n + d_\ell)) \ll \max\left\{\frac{\ell N}{p^{1/3}}, \ell p^{3/2} \log p\right\}$$

for any integers $0 \le d_1 < \cdots < d_\ell \le p^2 - 1$ and $1 \le N \le p^2$.

We use the lemma to analyze the pattern distribution of the binary sequence.

Lemma 3.2. *Let E_{p^2} be the binary sequence with period p^2 defined in* (3.1)*. Let $1 \le k < \tau < p^2$ be integers. For any pattern $\underline{a} = \{a_0, \cdots, a_k\} \in \{0, 1\}^{k+1}$ and $\underline{b} = \{b_0, \cdots, b_k\} \in \{0, 1\}^{k+1}$, we know*

$$N_{(\underline{a},\underline{b},k,\tau)}(E_{p^2}) = |\{n : \ p^2 \le n \le 2p^2 - 1, (e_{n-k}, e_{n-k+1}, \cdots, e_n) = (a_0, a_1, \cdots, a_k) \text{ and } (e_{n-k+\tau}, e_{n-k+\tau+1}, \cdots, e_{n+\tau}) = (b_0, b_1, \cdots, b_k)\}|,$$

then

$$\delta_{2k+2}(E_{p^2}) \ll (2k + 2)p^{\frac{5}{3}}, \tag{3.2}$$

for $1 \le k < \frac{1}{6 \log_2 p}$.

Proof. From the definition of pattern distribution, we have

$$\begin{aligned} N_{(\underline{a},\underline{b},k,\tau)}(E_{p^2}) - \frac{p^2}{2^{2k+2}} &= \frac{1}{2^{2k+2}} \sum_{n=p^2}^{2p^2-1} \prod_{j=0}^{k} \left(1 + (-1)^{e_{n-k+j}+a_j}\right)\left(1 + (-1)^{e_{n-k+\tau+j}+b_j}\right) - \frac{p^2}{2^{2k+2}} \\ &= \frac{1}{2^{2k+2}} \sum_{\substack{U,V \subseteq \{0,1,\cdots,k\} \\ U \cup V \neq \emptyset}} \sum_{n=p^2}^{2p^2-1} \prod_{j_1 \in U} (-1)^{e_{n-k+j_1}+a_{j_1}} \prod_{j_2 \in V} (-1)^{e_{n-k+\tau+j_2}+b_{j_2}}. \end{aligned}$$

In the following, we classify and discuss the first sum in the above equation. Let η be the Legendre symbol modulo p. When $U \neq \emptyset$ and $V = \emptyset$, by (3.1) and Lemma 3.1, we have

$$\begin{aligned}
&\frac{1}{2^{2k+2}} \sum_{U\subseteq\{0,1,\cdots,k\}\setminus\{\emptyset\}} \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} (-1)^{e_{n-k+j_1}+a_{j_1}} \\
&\leq \frac{2^{k+1}-1}{2^{2k+2}} \max_{U\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} (-1)^{e_{n-k+j_1}} \right| \\
&\leq \frac{2^{k+1}-1}{2^{2k+2}} \max_{U\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} \eta(q_p(n-k+j_1)) + |U|\cdot p \right| \\
&\ll \frac{1}{2^{k+1}}(k+1)p^{\frac{5}{3}}, \qquad (3.3)
\end{aligned}$$

where $|U|$ denotes the number of elements in set U. When $U = \emptyset$ and $V \neq \emptyset$, we also have

$$\frac{2^{k+1}-1}{2^{2k+2}} \max_{V\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j_2\in V} (-1)^{e_{n-k+\tau+j_2}} \right| \ll \frac{1}{2^{k+1}}(k+1)p^{\frac{5}{3}}. \qquad (3.4)$$

When $U \neq \emptyset$ and $V \neq \emptyset$, by (3.1) and Lemma 3.1 we obtain

$$\begin{aligned}
&\frac{1}{2^{2k+2}} \sum_{U,V\subseteq\{0,1,\cdots,k\}\setminus\{\emptyset\}} \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} (-1)^{e_{n-k+j_1}+a_{j_1}} \prod_{j_2\in V} (-1)^{e_{n-k+\tau+j_2}+b_{j_2}} \\
&\leq \frac{2^{2k+2}-2^{k+2}+1}{2^{2k+2}} \max_{U,V\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} (-1)^{e_{n-k+j_1}} \prod_{j_2\in V} (-1)^{e_{n-k+\tau+j_2}} \right| \\
&\leq \max_{U,V\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j_1\in U} \eta(q_p(n-k+j_1)) \prod_{j_2\in V} \eta(q_p(n-k+\tau+j_2)) + (|U|+|V|)\cdot p \right| \\
&\ll (2k+2)p^{\frac{5}{3}}. \qquad (3.5)
\end{aligned}$$

Combing (3.3)–(3.5), we immediately obtain

$$\left| N_{(\underline{a},\underline{b},k,\tau)}(E_{p^2}) - \frac{p^2}{2^{2k+2}} \right| \ll (2k+2)p^{\frac{5}{3}}.$$

This completes the proof of lemma. □

Lemma 3.3. *Let E_{p^2} be the binary sequence with period p^2 defined in* (3.1)*. Let $1 \leq \tau \leq k$ be integers. For any pattern $\underline{c} = \{c_0, c_1, \cdots, c_{k+\tau}\} \in \{0,1\}^{k+\tau+1}$, we have*

$$N_{(\underline{c},k,\tau)}(E_{p^2}) = |\{n :\ p^2 \leq n \leq 2p^2-1, (e_{n-k}, e_{n-k+1}, \cdots, e_{n+\tau}) = (c_0, c_1, \cdots, c_{k+\tau})\}|,$$

then

$$\lambda_{k+\tau+1}(E_{p^2}) \ll (k+\tau+1)p^{\frac{5}{3}}, \qquad (3.6)$$

for $1 \leq k < \frac{1}{6\log_2 p}$.

Proof. Similar to the proof of Lemma 3.2. Let η be the Legendre symbol modulo p, from (3.1) and Lemma 3.1 we have

$$\begin{aligned} N_{(\underline{c},k,\tau)}(E_{p^2}) - \frac{p^2}{2^{k+\tau+1}} &= \frac{1}{2^{k+\tau+1}} \sum_{n=p^2}^{2p^2-1} \prod_{j=0}^{k+\tau} (1+(-1)^{e_{n-k+j}+c_j}) - \frac{p^2}{2^{k+\tau+1}} \\ &= \frac{1}{2^{k+\tau+1}} \sum_{W\subseteq\{0,1,\cdots,k+\tau\}\setminus\{\emptyset\}} \sum_{n=p^2}^{2p^2-1} \prod_{j\in W} (-1)^{e_{n-k+j}+c_j} \\ &\le \frac{2^{k+\tau+1}-1}{2^{k+\tau+1}} \max_{W\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j\in W} (-1)^{e_{n-k+j}} \right| \\ &\le \max_{W\neq\emptyset} \left| \sum_{n=p^2}^{2p^2-1} \prod_{j\in W} \eta(q_p(n-k+j)) + |W|\cdot p \right| \\ &\ll (k+\tau+1)p^{\frac{5}{3}}. \end{aligned}$$

Hence, we obtain

$$\left| N_{(\underline{c},k,\tau)}(E_{p^2}) - \frac{p^2}{2^{k+\tau+1}} \right| \ll (k+\tau+1)p^{\frac{5}{3}}.$$

This completes the proof of lemma. □

As a direct result of Theorem 1.2, Lemmas 3.2 and 3.3, we obtain the arithmetic autocorrelation of binary sequence in (3.1).

Theorem 3.4. *Let E_{p^2} be the binary sequence with period p^2 defined by* (3.1)*. The arithmetic autocorrelation of sequence E_{p^2} satisfies*

$$A(\tau) \ll \min\left\{ \sqrt{2}p^{\frac{11}{6}}(\log p)^{\frac{1}{2}}, 2^{r+2}p^{\frac{5}{3}}(\log p)^2 \right\}, \tag{3.7}$$

where $r = \min\{\tau, p^2-\tau\}$ for $1 \le \tau \le p^2-1$.

We illustrate the upper bound derived from Theorem 3.4 with some actual maximum arithmetic autocorrelation values of the binary sequence E_{p^2} in Figure 1. Then Theorem 3.4 implies that the binary sequence E_{p^2} has a small arithmetic autocorrelation for a large enough period p^2. In addition, the ε-correlation measure of sequence E_{p^2} was mentioned in [15], we have the upper bound of arithmetic autocorrelation of order of magnitude $O(p^{\frac{11}{6}}(\log p)^{\frac{1}{2}})$ from Proposition 1.1 that equals the upper bound of arithmetic autocorrelation of order of magnitude in Theorem 3.4.

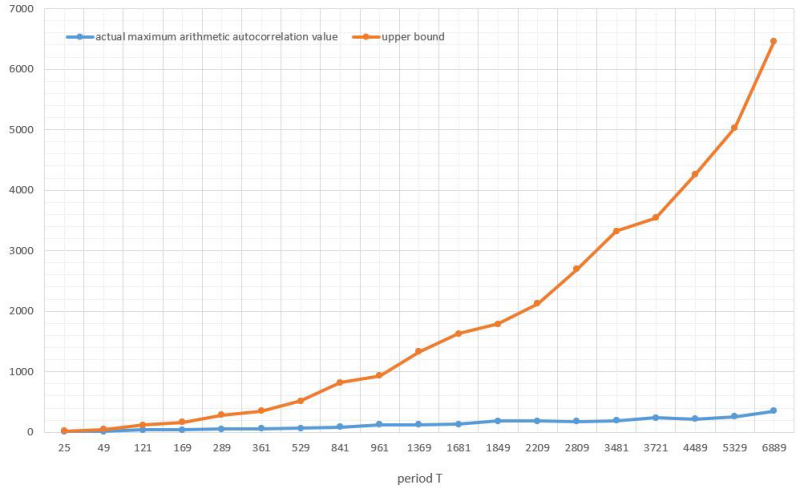

Figure 1. The actual maximum arithmetic autocorrelation values and the upper bounds of binary sequence E_{p^2}.

3.2. The generalized cyclotomic sequence of order 2

Let p and q be distinct primes, $T = pq$. Let $\gcd(p-1, q-1) = d$ and $e = \frac{(p-1)(q-1)}{d}$. By the Chinese Remainder Theorem: there exists a common primitive root g of both p and q, and an integer x such that

$$x \equiv g(\text{mod } p), \quad x \equiv 1(\text{mod } q),$$

and $ord_T(g) = e$. A generalized cyclotomic class of order d is defined by Whiteman [24] as

$$D_i = \{g^s x^i | s = 0, 1, \cdots, e-1\}, \ i = 0, 1, \cdots, d-1.$$

Let $\mathbb{Z}_{pq}$ be the residue class ring modulo pq. Whiteman [24] proved

$$\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{d-1} D_i, \ D_i \cap D_j = \emptyset, \quad \text{for} \quad i \neq j.$$

The generalized cyclotomic classes is an important approach to constructing pseudorandom sequences. Let $P = \{p, 2p, \cdots, (q-1)p\}$, $Q = \{q, 2q, \cdots, (p-1)q\}$, and $Q_0 = Q \cup \{0\}$. Take $d = 2$, Ding [25] defined the generalized cyclotomic sequence of order 2 $S_{pq} = \{s_0, s_1, \cdots, s_{pq-1}\}$ by

$$s_n = \begin{cases} 0, & \text{if } n \text{ mod } pq \in Q_0, \\ 1, & \text{if } n \text{ mod } pq \in P, \\ i, & \text{if } n \text{ mod } pq \in D_i, \end{cases} \tag{3.8}$$

obviously, the sequence is periodic with pq and can be expressed as [26]

$$s_n = \begin{cases} 0, & \text{if } n \text{ mod } pq \in Q_0, \\ 1, & \text{if } n \text{ mod } pq \in P, \\ \frac{1-(\frac{n}{p})(\frac{n}{q})}{2}, & \text{otherwise}, \end{cases}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol.

The high linear complexity and low autocorrelation values with certain properties of the primes of the generalized cyclotomic sequences S_{pq} have been determined by Ding [25, 27], respectively. Brandstätter and Winterhof [28] got the lower bound of linear complexity profile and the upper bound of aperiodic autocorrelation. Dai et al. [29] showed the trace representation of the generalized cyclotomic sequence S_{pq}. Hofer and Winterhof [30] demonstrated the 2-adic complexity of the above generalized cyclotomic sequence S_{pq} is close to the period. More generalization refers to [31–34]. As we know, the arithmetic autocorrelation of the generalized cyclotomic sequence of order 2 has yet to be concerned.

We would study the arithmetic autocorrelation of the generalized cyclotomic sequence S_{pq} based on the upper bound estimates of multiplicative character sums with composite moduli.

Lemma 3.5. *[35] Let p, q be distinct prime numbers and $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and X, Y are real numbers with $0 < Y \le pq$. Let χ be a primitive multiplicative character modulo pq and write $\chi = \chi_1\chi_2$, where χ_1 is a character modulo p of order $d_p > 1$ and χ_2 is a character modulo q of order $d_q > 1$. Assume that in $\mathbb{F}_p[x]$, $f(x)$ is not the constant multiple of the d_p-power of a polynomial and it has s_p distinct zeros in $\overline{\mathbb{F}}_p$, and in $\mathbb{F}_q[x]$, $f(x)$ is not the constant multiple of the d_q-power of a polynomial, and it has s_q distinct zeros in $\overline{\mathbb{F}}_q$, we have*

$$\left|\sum_{X<x\le X+Y}\chi(f(x))\right| \ll \ell^2 p^{1/2} q^{1/2}\log(pq).$$

We first represent the generalized cyclotomic sequence using a multiplicative character. Let χ be the multiplicative character modulo pq. By the orthogonality relations of multiplicative character, we have

$$\begin{aligned} n \in D_i &\Longleftrightarrow \text{there is s with } 0 \le s \le e-1 \text{ such that } n \equiv g^s x^i (\mathrm{mod}\ pq)\\ &\Longleftrightarrow \frac{1}{\phi(pq)}\sum_{s=0}^{e-1}\sum_{\chi \bmod pq}\chi(n)\overline{\chi}(g^s x^i) = 1\\ &\Longleftrightarrow \frac{1}{\phi(pq)}\sum_{\chi \bmod pq}\chi(n)\overline{\chi}(x^i)\sum_{s=0}^{e-1}\overline{\chi}(g^s) = 1\\ &\Longleftrightarrow \frac{1}{2}\sum_{\substack{\chi \bmod pq\\ \overline{\chi}(g)=1}}\chi(n)\overline{\chi}(x^i) = 1. \end{aligned}$$

That means

$$\frac{1}{2}\sum_{\substack{\chi \bmod pq\\ \overline{\chi}(g)=1}}\chi(n) = \begin{cases} 1, & \text{if } n \bmod pq \in D_0 \cup Q_0,\\ 0, & \text{if } n \bmod pq \in D_1 \cup P. \end{cases}$$

Let $\mathcal{H} = \{\chi \bmod pq \mid \chi(g) = 1 \text{ and } \chi \text{ is non-trivial}\}$. Since the order of χ modulo pq is 2, we have $|\mathcal{H}| = 1$ and $\chi \in \mathcal{H}$ is the primitive multiplicative character modulo pq, denoted by χ_{pq}. Hence

$$(-1)^{s_n} = \begin{cases} +1, & \text{if } n \bmod pq \in Q_0,\\ -1, & \text{if } n \bmod pq \in P,\\ \chi_{pq}(n), & \text{if } n \bmod pq \in \mathbb{Z}_{pq}^*. \end{cases} \tag{3.9}$$

According to Theorem 1.2, we will calculate the pattern distribution of the generalized cyclotomic sequence of order 2 in (3.8).

Lemma 3.6. *Let p and q be two distinct primes with* $\gcd(p-1, q-1) = 2$. *Let S_{pq} be the binary sequence with period pq defined in* (3.8). *Let $1 \le k < \tau < pq$ be integers. For any pattern $\underline{a} = \{a_0, \cdots, a_k\} \in \{0,1\}^{k+1}$ and $\underline{b} = \{b_0, \cdots, b_k\} \in \{0,1\}^{k+1}$, we know*

$$N_{(\underline{a},\underline{b},k,\tau)}(S_{pq}) = |\{n : \ pq \le n \le 2pq-1, (s_{n-k}, s_{n-k+1}, \cdots, s_n) = (a_0, a_1, \cdots, a_k) \quad \text{and} \\ (s_{n-k+\tau}, s_{n-k+\tau+1}, \cdots, s_{n+\tau}) = (b_0, b_1, \cdots, b_k)\}|,$$

then

$$\delta_{2k+2}(S_{pq}) \ll (2k+2)^2 p^{1/2} q^{1/2} \log(pq) + (2k+2)(p+q), \tag{3.10}$$

for $1 \le k < \frac{\log_2 p + \log_2 q}{4}$.

Proof. From (1.3) we have

$$\begin{aligned}
N_{(\underline{a},\underline{b},k,\tau)}(S_{pq}) - \frac{pq}{2^{2k+2}} &= \frac{1}{2^{2k+2}} \sum_{n=pq}^{2pq-1} \prod_{j=0}^{k} \left(1 + (-1)^{s_{n-k+j}+a_j}\right)\left(1 + (-1)^{s_{n-k+\tau+j}+b_j}\right) - \frac{pq}{2^{2k+2}} \\
&= \frac{1}{2^{2k+2}} \sum_{\substack{U,V \subseteq \{0,1,\cdots,k\} \\ U \cup V \neq \emptyset}} \sum_{n=pq}^{2pq-1} \prod_{j_1 \in U} (-1)^{s_{n-k+j_1}+a_{j_1}} \prod_{j_2 \in V} (-1)^{s_{n-k+\tau+j_2}+b_{j_2}} \\
&= \frac{1}{2^{2k+2}} \sum_{U,V \subseteq \{0,1,\cdots,k\} \setminus \{\emptyset\}} \sum_{n=pq}^{2pq-1} \prod_{j_1 \in U} (-1)^{s_{n-k+j_1}+a_{j_1}} \prod_{j_2 \in V} (-1)^{s_{n-k+\tau+j_2}+b_{j_2}} \\
&\quad + \frac{1}{2^{2k+2}} \sum_{\substack{U \subseteq \{0,1,\cdots,k\} \setminus \{\emptyset\} \\ V=\emptyset}} \sum_{n=pq}^{2pq-1} \prod_{j_1 \in U} (-1)^{s_{n-k+j_1}+a_{j_1}} \\
&\quad + \frac{1}{2^{2k+2}} \sum_{\substack{V \subseteq \{0,1,\cdots,k\} \setminus \{\emptyset\} \\ U=\emptyset}} \sum_{n=pq}^{2pq-1} \prod_{j_2 \in V} (-1)^{s_{n-k+\tau+j_2}+b_{j_2}} \\
&= \sum_1 + \sum_2 + \sum_3.
\end{aligned}$$

Next, we discuss the above three sum equations separately. By (3.9) and Lemma 3.5 we have

$$\begin{aligned}
\sum_1 &\le \frac{2^{2k+2} - 2^{k+2} + 1}{2^{2k+2}} \max_{U,V \neq \emptyset} \left| \sum_{n=pq}^{2pq-1} \prod_{j_1 \in U} (-1)^{s_{n-k+j_1}} \prod_{j_2 \in V} (-1)^{s_{n-k+\tau+j_2}} \right| \\
&\le \frac{2^{2k+2} - 2^{k+2} + 1}{2^{2k+2}} \max_{U,V \neq \emptyset} \left| \sum_{\substack{n=0 \\ n-k+j_1 \in \mathbb{Z}_{pq^*} \\ n-k+\tau+j_2 \in \mathbb{Z}^*_{pq}}}^{pq-1} \prod_{j_1 \in U} (-1)^{s_{pq+n-k+j_1}} \prod_{j_2 \in V} (-1)^{s_{pq+n-k+\tau+j_2}} \right|
\end{aligned}$$

$$
\begin{aligned}
&\quad + (2k+2)(p+q)\\
&\le \max_{U,V\neq\emptyset}\left|\sum_{n\in\mathbb{Z}_{pq}}\chi_{pq}\left(\prod_{j_1\in U}(pq+n-k+j_1)\right)\chi_{pq}\left(\prod_{j_2\in V}(pq+n-k+\tau+j_2)\right)\right|\\
&\quad + (2k+2)(p+q)\\
&\ll (2k+2)^2p^{1/2}q^{1/2}\log(pq)+(2k+2)(p+q),
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{2} &\le \frac{2^{k+1}-1}{2^{2k+2}}\max_{U\neq\emptyset}\left|\sum_{n=pq}^{2pq-1}\prod_{j_1\in U}(-1)^{s_{n-k+j_1}}\right|\\
&\le \frac{2^{k+1}-1}{2^{2k+2}}\max_{U\neq\emptyset}\left|\sum_{n\in\mathbb{Z}_{pq}}\chi_{pq}\left(\prod_{j_1\in U}(pq+n-k+j_1)\right)+|U|(p+q)\right|\\
&\ll \frac{(k+1)^2}{2^{k+1}}p^{1/2}q^{1/2}\log(pq)+\frac{(k+1)}{2^{k+1}}(p+q).
\end{aligned}
$$

Similarly, we have

$$
\sum_{3}\ll \frac{(k+1)^2}{2^{k+1}}p^{1/2}q^{1/2}\log(pq)+\frac{(k+1)}{2^{k+1}}(p+q).
$$

Hence, we obtain

$$
\left|N_{(\underline{a},\underline{b},k,\tau)}(S_{pq})-\frac{pq}{2^{2k+2}}\right|\ll (2k+2)^2p^{1/2}q^{1/2}\log(pq)+(2k+2)(p+q).
$$

This completes the proof of lemma. □

Lemma 3.7. *Let p and q be two distinct primes with $\gcd(p-1,q-1)=2$. Let S_{pq} be the binary sequence with period pq defined in* (3.8). *Let $1\le\tau\le k$ be integers. For any pattern $\underline{c}=\{c_0,c_1,\cdots,c_{k+\tau}\}\in\{0,1\}^{k+\tau+1}$, we know*

$$
N_{(\underline{c},k,\tau)}(S_{pq})=|\{n:\ pq\le n\le 2pq-1,(s_{n-k},s_{n-k+1},\cdots,s_{n+\tau})=(c_0,c_1,\cdots,c_{k+\tau})\}|,
$$

then

$$
\lambda_{k+\tau+1}(S_{pq})\ll (k+\tau+1)^2p^{1/2}q^{1/2}\log(pq)+(k+\tau+1)(p+q), \tag{3.11}
$$

for $1\le k<\frac{\log_2 p+\log_2 q}{4}$.

Proof. By (3.9) and Lemma 3.5, we have

$$
\begin{aligned}
N_{(\underline{c},k,\tau)}-\frac{pq}{2^{k+\tau+1}} &= \frac{1}{2^{k+\tau+1}}\sum_{n=pq}^{2pq-1}\prod_{j=0}^{k+\tau}(1+(-1)^{s_{n-k+j}+c_j})-\frac{pq}{2^{k+\tau+1}}\\
&\le \frac{2^{k+\tau+1}-1}{2^{k+\tau+1}}\max_{W\neq\emptyset}\left|\sum_{n=pq}^{2pq-1}\prod_{j\in W}(-1)^{s_{n-k+j}}\right|\\
&\le \frac{2^{k+\tau+1}-1}{2^{k+\tau+1}}\max_{W\neq\emptyset}\left|\sum_{n\in\mathbb{Z}_{pq}}\chi_{pq}\left(\prod_{j\in W}(pq+n-k+j)\right)+|W|(p+q)\right|\\
&\ll (k+\tau+1)^2p^{1/2}q^{1/2}\log(pq)+(k+\tau+1)(p+q).
\end{aligned}
$$

This concludes the proof of lemma. □

Substituting the results of Lemmas 3.6 and 3.7 into Theorem 1.2, we immediately have the arithmetic autocorrelation of the binary generalized cyclotomic sequence.

Theorem 3.8. *Let p and q be two distinct primes with* $\gcd(p-1, q-1) = 2$. *Let S_{pq} be the binary sequence with period pq defined by* (3.8). *The arithmetic autocorrelation of sequence S_{pq} satisfies*

$$A(\tau) \ll \min\left\{\sqrt{2}\, p^{\frac{3}{4}} q^{\frac{3}{4}} (\log(pq))^{\frac{3}{2}}, 2^{r+1} p^{\frac{1}{2}} q^{\frac{1}{2}} (\log(pq))^4\right\}, \tag{3.12}$$

where $r = \min\{\tau, p^2 - \tau\}$ *for* $1 \le \tau \le p^2 - 1$.

We enumerate some actual maximum arithmetic autocorrelation values and the upper bounds obtained from Theorem 3.8 for small periods of binary sequence S_{pq} in Figure 2. The graph shows that the upper bound is greater than the actual maximum value of arithmetic autocorrelation. Then the result derived from Theorem 3.8 indicates the arithmetic autocorrelation of the sequence S_{pq} is rather small for a sufficiently large period pq.

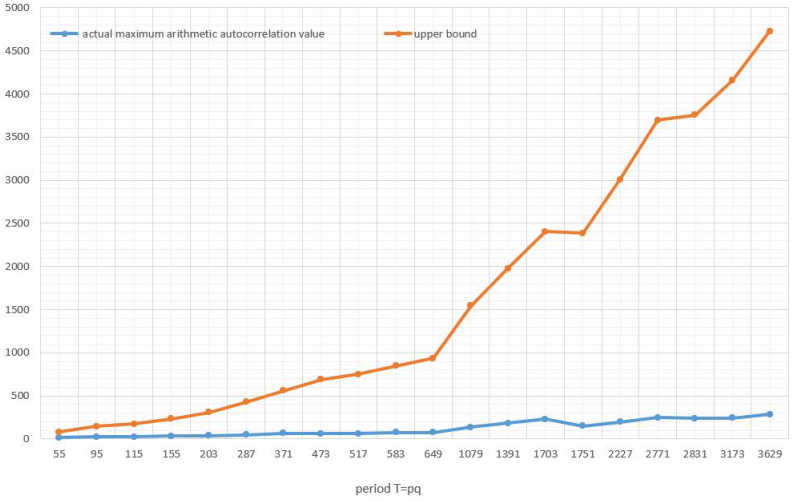

Figure 2. The actual maximum arithmetic autocorrelation values and the upper bounds of binary sequence S_{pq}.

Remark 3.9. *Rivat and Sárközy [35] studied the pseudorandom correlation measure of the binary Jacobi sequence of period pq defined with polynomial $f(n)$. For $f(n) = n$, their results imply*

$$\left|\sum_{n=1}^{pq-p-q} (-1)^{s_n s_{n+p} s_{n+q} s_{n+p+q}}\right| \ge pq - 35p^{1/2}q^{1/2},$$

that means "long term" correlation of order 4 of the generalized cyclotomic sequence S_{pq} in (3.8) is large. Then we cannot obtain the arithmetic autocorrelation of the sequence by Proposition 1.1. In contrast to this, we get a rather small "short term" pattern distribution, resulting in a small arithmetic autocorrelation of the binary sequence S_{pq}.

4. Final remarks

Let p, q and T be prime numbers, and d, n, and k be integers. We list the previously known and currently proposed arithmetic autocorrelation functions $A(\tau)$ as well as conditions with binary sequences in Table 1.

Table 1. Know arithmetic autocorrelation of binary sequences.

No.	$A(\tau) \ll$	period of sequence	conditions	reference
1	0	$p^{r-1}(p-1)$	2 is primitive root modulo p^r	[19]
2	$4p^{3/4}(\log_2 p)^{1/2}$	p		[26]
3	$d^{1/2}p^{3/4}$	p	$d < \frac{1}{2\log\log p}\log p$ or 2 is a primitive root modulo p	[25]
4	$p^{3n/4}$	$p^n - 1$		[25]
5	$d^{1/2}p^{1/4}T^{1/2}$	T	$d < \frac{\log p}{\log\log p}$ or 2 is a primitive root modulo T	[25]
6	$d^{1/2}2^{3k/4}$	$2^k - 1$(is prime)	$k \le d + 1$	[25]
	0	$p^{r-1}(p-1)/2$	$p \equiv 1 (\mathrm{mod}\ 8)$	
7	$p^{r-1/2}\ln p$	$p^{r-1}(p-1)/2$	$p \equiv -1 (\mathrm{mod}\ 8)$ $2^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2), ord_p(2) = \frac{p-1}{2}$	[8]
8	$2^{n-1} - 1$	$2^n - 1$		[10]
9	$\sqrt{2}p^{11/6}(\log p)^{1/2}$	p^2		Theorem 3.4
10	$\sqrt{2}\,(pq)^{3/4}(\log(pq))^{3/2}$	pq		Theorem 3.8

Goresky and Klapper [4, 5] presented the expected arithmetic autocorrelation over all binary sequences with period T, which is $\frac{T}{2^{T-\gcd(\tau,T)}}$ for fixed τ. Subsequently, Hofer, Mérai, and Winterhof [7] gave the upper bound of arithmetic autocorrelation for any pseudorandom binary sequence of period T with a small correlation measure, $A(\tau) = O(T^{\frac{3}{4}}(\log_2 T)^{\frac{1}{2}})$. They studied the arithmetic autocorrelation of several sequences, including binary sequences from the Legendre symbol, the Sidelnikov–Lempel–Cohn–Eastman sequence, and the sequence from the trace function, as in the 3–6-th row of Table 1. The arithmetic autocorrelation of these sequences is relatively small with respect to its period when the period is sufficiently large, but obtaining these results relies on a small correlation measure of high order. Moreover, Goresky and Klapper [3] proved ℓ-sequence have ideal arithmetic autocorrelation, as in the 1-th row of Table 1; however, the classical autocorrelation equals the period, which is not desired. Chen et al. [36] presented the arithmetic autocorrelation of the binary m-sequence, which amounts to half of the period, as in the 8-th row of Table 1. Compared with these sequences, the generalized cyclotomic sequence of order 2 studied in Theorem 3.8 has rather small arithmetic autocorrelation with upper bound of order of magnitude $O(p^{\frac{3}{4}}q^{\frac{3}{4}}(\log(pq))^{3/2})$ for sufficiently large period pq, although its correlation measure of order 4 is quite large. As well as binary sequence E_{p^2} studied in Theorem 3.4, which has a small upper bound of arithmetic autocorrelation relative to its large enough period, its f-correlation measure is also small.

5. Conclusions

In this paper we constructed the relation between arithmetic autocorrelation and pattern distribution of binary sequences. Based on this relation, we proved the arithmetic autocorrelation of the binary sequence defined in [15]; and pointed out that the generalized cyclotomic sequence defined in [25] has a small "short term" pattern distribution and gave an upper bound of arithmetic autocorrelation. Our results indicate that some pseudorandom sequences with large "long term" pseudorandom correlations of order k may have small arithmetic correlations; and therefore can also be used for research in certain cryptographic fields. It may be interesting to find and study these pseudorandom sequences.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors express their gratitude to the referees for their nice comments. This paper is supported by the National Natural Science Foundation of China under Grant No. 12071368, the Science and Technology Program of Shaanxi Province of China under Grant Nos. 2024JC-YBMS-040 and 2024JC-JCQN-04, and the Shaanxi Fundamental Science Research Project for Mathematics and Physics under Grant Nos. 23JSY025 and 22JSY017.

Conflict of interest

The authors declare there are no conflicts of interest.

References

1. D. Mandelbaum, Arithmetic codes with large distance, *IEEE Trans. Inf. Theory*, **13** (1967), 237–242. https://doi.org/10.1109/TIT.1967.1054015
2. R. Hofer, A. Winterhof, On the arithmetic autocorrelation of the legendre sequence, *Adv. Math. Commun.*, **11** (2017), 237–244. https://doi.org/10.3934/amc.2017015
3. M. Goresky, A. Klapper, Arithmetic crosscorrelation of feedback with carray shift register sequences, *IEEE Trans. Inf. Theory*, **43** (1997), 1342–1345. https://doi.org/10.1109/18.605605
4. M. Goresky, A. Klapper, Some results on the arithmetic correlation of sequences, in *Sequences and Their Applications-SETA 2008: 5th International Conference Lexington*, **5203** (2008), 71–80. https://doi.org/10.1007/978-3-540-85912-3_7
5. M. Goresky, A. Klapper, Statistical properties of the arithmetic correlation of sequences, *Int. J. Found. Comput. Sci.*, **22** (2011), 1297–1315. https://doi.org/10.1142/S0129054111008726
6. M. Goresky, A. Klapper, *Algebratic Shift Register Sequences*, Cambridge University Press, U.K., 2012. https://doi.org/10.1017/CBO9781139057448

7. R. Hofer, L. Mérai, A. Winterhof, "Measure of pseudorandomness: Arithmetic autocorrelation and correlation measure", in *Number Theory-Diophantine Problems, Uniform Distribution and Applications*, (eds. C. Elsholtz and P. Grabner), Spring, Cham (2017), 303–312. https://doi.org/10.1007/978-3-319-55357-3_15

8. C. Ding, Pattern distributions of Legendre sequences, *IEEE Trans. Inf. Theory*, **44** (1998), 1693–1698. https://doi.org/10.1109/18.681353

9. S. W. Golomb, G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*, Cambridge University Press, Cambridge, 2005. https://doi.org/10.1017/CBO9780511546907

10. H. Liu, Y. Ren, Balance, pattern distribution and linear complexity of M-ary sequences from Sidel'nikov sequences, *Appl. Algebra Engrg. Comm. Comput.*, **35** (2024), 667–682. https://doi.org/10.1007/s00200-022-00580-5

11. C. Mauduit, A. Sárközy, On finite pseudorandom sequences of k symbols, *Indag. Math.*, **13** (2002), 89–101. https://doi.org/10.1016/S0019-3577(02)90008-X

12. H. Aly, A. Winterhof, Boolean functions derived from Fermat quotients, *Cryptogr. Commun.*, **3** (2011), 165–174. https://doi.org/10.1007/s12095-011-0043-5

13. M. C. Chang, Short character sums with Fermat quotients, *Acta Arith.*, **152** (2012), 23–38. https://doi.org/10.4064/aa152-1-3

14. Z. Chen, A. Winterhof, Interpolation of Fermat quotients, *SIAM J. Discrete Math.*, **28** (2014), 1–7. https://doi.org/10.1137/130907951

15. D. Gómez, A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hungar.*, **64** (2012), 161–168. https://doi.org/10.1007/s10998-012-3747-1

16. A. Ostafe, I. E. Shparlinski, Pseudorandomness and dynamics of Fermat quotients, *SIAM J. Discrete Math.*, **25** (2011), 50–71. https://doi.org/10.1137/100798466

17. I. E. Shparlinski, Fermat quotients: exponential sums, value set and primitive roots, *Bull. Lond. Math. Soc.*, **43** (2011), 1228–1238. https://doi.org/10.1112/blms/bdr058

18. I. E. Shparlinski, Character sums with Fermat quotients, *Q. J. Math.*, **62** (2011), 1031–1043. https://doi.org/10.1093/qmath/haq028

19. I. E. Shparlinski, Bounds of multiplicative character sums with Fermat quotients of primes, *Bull. Aust. Math. Soc.*, **83** (2011), 456–462. https://doi.org/10.1017/S000497271000198X

20. Z. Chen, L. Hu, X. Du, Linear complexity of some binary sequences derived from Fermat quotients, *China Commun.*, **9** (2012), 105–108.

21. Z. Chen, Trace representation and linear complexity of binary sequences derived from Fermat quotients, *Sci. China Inf. Sci.*, **57** (2014), 112109:1–10. https://doi.org/10.1007/s11432-014-5092-x

22. Z. Chen, Z. Niu, C. Wu, On the k-error linear complexity of binary sequences derived from polynomial quotients, preprint, arXiv:1307.6626.

23. X. Du, A. Klapper, Z. Chen, Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations, *Inf. Process. Lett.*, **112** (2012), 233–237. https://doi.org/10.1016/j.ipl.2011.11.017

24. A. L. Whiteman, A family of difference sets, *Illinois J. Math.*, **6** (1962), 107–121. https://doi.org/10.1215/ijm/1255631810

25. C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, *Finite Fields Appl.*, **3** (1997), 159–174. https://doi.org/10.1006/ffta.1997.0181

26. T. W. Cusick, C. Ding, A. Renvall, *Stream Ciphers and Number Theory*, North-holland mathematical library, Amsterdam, The Netherlands: North-Holland, 1998. https://doi.org/10.1016/s0924-6509(98)x8001-3

27. C. Ding, Autocorrelation values of generalized cyclotomic sequences of order two, *IEEE Trans. Inf. Theory*, **44** (1998), 1699–1702. https://doi.org/10.1109/18.681354

28. N. Brandstätter, A. Winterhof, Some notes on the two-prime generator of order 2, *IEEE Trans. Inf. Theory*, **51** (2005), 3654–3657. https://doi.org/10.1109/TIT.2005.855615

29. Z. Dai, G. Gong, H. Y. Song, A trace representation of binary Jacobi sequences, *Discrete Math.*, **309** (2009), 1517–1527. https://doi.org/10.1016/j.disc.2008.02.024

30. R. Hofer, A. Winterhof, On the 2-adic complexity of the two-prime generator, *IEEE Trans. Inf. Theory*, **64** (2018), 5957–5960. https://doi.org/10.1109/TIT.2018.2811507

31. E. Bai, X. Fu, G. Xiao, On the linear complexity of generalized cyclotomic sequences of order four over $\mathbb{Z}_{pq}$, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, **E88-A** (2005), 392–395. https://doi.org/10.1093/ietfec/E88-A.1.392

32. E. Bai, X. Liu, G. Xiao, Linear complexity of new generalized cyclotomic sequences of order two of length pq, *IEEE Trans. Inf. Theory*, **51** (2005), 1849–1853. https://doi.org/10.1109/TIT.2005.846450

33. T. Yan, X. Du, G. Xiao, X, Huang, Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k, *Inf. Sci.*, **179** (2009), 1019–1023. https://doi.org/10.1016/j.ins.2008.11.006

34. L. Hu, Q. Yue, M. Wang, The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$, *IEEE Trans. Inf. Theory*, **58** (2012), 5534–5543. https://doi.org/10.1109/TIT.2012.2196254

35. J. Rivat, A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli, *Period. Math. Hungar.*, **51** (2005), 75–107. https://doi.org/10.1007/s10998-005-0031-7

36. Z. Chen, Z. Niu, Y. Sang, C. Wu, Arithmetic autocorrelation of binary m-sequences, *Cryptologia*, **47** (2023), 449–458. https://doi.org/10.1080/01611194.2022.2071116

37. Z. Chen, V. Edemskiy, Z. Niu, Y. Sang, Arithmetic correlation of binary half-ℓ-sequences, *IET Inf. Secur.*, **17** (2023), 289–293. https://doi.org/10.1049/ise2.12093

38. Z. Chen, Z. Niu, A. Winterhof, Arithmetic crosscorrelation of pseudorandom binary sequences of coprime periods, *IEEE Trans. Inf. Theory*, **68** (2022), 7538–7544. https://doi.org/10.1109/tit.2022.3184176

39. X. Jing, K. Feng, Arithmetic crosscorrelation of binary m-sequences with coprime periods, *Finite Fields Appl.*, **96** (2024), 102424. https://doi.org/10.1016/j.ffa.2024.102424

40. X. Jing, A. Zhang, K. Feng, Arithmetic Autocorrelation Distribution of Binary m-Sequences, *IEEE Trans. Inf. Theory*, **69** (2023), 6040–6047. https://doi.org/10.1109/tit.2023.3282229

AIMS Press