# The ideal arithmetic correlations of $N$-ary sequences and related results

Feifei Yan[1], Pinhui Ke[2*], Chenhuang Wu[3]

[1]School of Mathematics and Statistics, Fujian Normal University, Fuzhou, 350117, Fujian, China.
[2*]Key Laboratory of Analytical Mathematics and Applications (Ministry of Education), Fujian Normal University, Fuzhou, 350117, Fujian, China.
[3]Provincial Key Laboratory of Applied Mathematics, Putian University, Putian, 351100, Fujian, China.

*Corresponding author(s). E-mail(s): keph@fjnu.edu.cn;
Contributing authors: ffyfjnu@139.com; ptuwch@163.com;

**Abstract**

Arithmetic correlations represent the extension of classical correlations into the with-carry setting and serve as a critical performance criterion for pseudorandom sequences constructed via feedback with carry shift registers. The arithemetic correlation values should be as small as possible for application perspective. This paper establishes a sufficient condition for $\boldsymbol{N}$-ary sequences to have ideal arithmetic correlation. Based on this characterization, it is demonstrated that $\boldsymbol{N}$-ary $\boldsymbol{\ell}$-sequences with a prime connection integer $\boldsymbol{p}$ satisfying $\boldsymbol{p \equiv 1 (\mathrm{mod}\ N)}$ exhibit ideal arithmetic correlation. Furthermore, under the condition $\boldsymbol{N^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)}$, this result is extended to the case where the connection integer is a prime power. Additionally, an upper bound is established for the arithmetic crosscorrelation of binary sequences derived from Fermat quotients with coprime periods.

**Keywords:** Binary sequence, $\boldsymbol{N}$-ary sequence, Arithmetic correlations, Feedback with carry shift registers

# 1 Introduction

Pseudorandom sequences are critically employed across multiple disciplines, including communications, software testing, and cryptography etc. [1]. Such sequences are generated by distinct shift registers and deterministic algorithms. Among various pseudorandom sequence generators, those based on linear feedback shift registers (LFSRs) are most prevalent. An alternative architecture, the feedback with carry shift register (FCSR), was introduced by Klapper and Goresky during the 1990s [2]. This design has an algebraic framework analogous to that of LFSRs.

The notion of arithmetic correlations was proposed to measure the pseudorandomness of two periodic sequences generated by FCSRs [3, 4]. This measure is important for applications such as synchronization and identification in multi-user environments and ID-based remote mutual authentication [4, 5].

It is desirable to minimize the absolute values of arithemetic correlations. A sequence is said to have ideal arithmetic correlations if all its nontrivial shift arithmetic correlations vanish (equal to zero). To date, among binary sequences, the class of $\ell$-sequences[1] consititutes the earliest known family achieving ideal arithmetic autocorrelation. Goresky and Klapper developed extensive families of sequences exhibiting ideal cross-correlation properties, derived from decimations of $\ell$-sequences, and they posed an open challenge for generating further families with ideal arithmetic correlations [4]. Chen et al. [6] established that, under specific conditions, for two binary half $\ell$-sequences[2], the arithmetic correlations vanish at all non-trivial shifts. Furthermore, their $d$-fold decimations, where $d$ is coprime with period, yield a collection of sequences exhibiting ideal arithmetic cross-correlations. Recently, Chen, Edemskiy, and Wu [7] generalized the construction of binary sequences with ideal arithmetic correlations to cases beyond odd prime power connection integers. For non-binary $\ell$-sequences, prior works [8, 9] indicate that if $p \equiv 1 (\mathrm{mod}\ N)$, then an $N$-ary (with $N \geq 2$) $\ell$-sequence defined over a prime connection integer $p$ has ideal arithmetic auto-correlation.

Recent work by Chen et al. [10] shows that the arithmetic crosscorrelation of two binary sequences with coprime periods is constant, thereby complementing the analogous classical crosscorrelation property. Nevertheless, the arithmetic crosscorrelation of binary sequences under coprime period conditions remains relatively unexplored. To date, results in this direction have been established primarily for Legendre sequences and m-sequences [10, 11]. Very recently, Liu et al. [12] established an upper bound for the arithmetic autocorrelation of binary sequences derived from Fermat quotients by analyzing their pattern distribution. This motivates the study of arithmetic cross-correlation of these sequences when their periods are coprime.

Inspired by the open problem of Goresky and Klapper and the complementary observation of Chen et al., this paper investigates ideal arithmetic correlations in $N$-ary sequences and the arithmetic crosscorrelation of binary sequences with coprime periods. The paper is structured as follows. Section 2 introduces some related concepts. In Sections 3 and 4, we establish a condition for $N$-ary sequences to have ideal

[1] An $N$-ary $\ell$-sequence is a the maximal-period FCSR sequence with prime power connection integer $q$ and period $\phi(q)$, where $\phi(\cdot)$ denotes Euler function and $\gcd(N, q) = 1$.

[2] Binary sequences with odd prime power connection integer $q$ and period $\phi(q)/2$ are referred to as half $\ell$-sequences.

arithmetic correlation and subsequently construct $N$-ary sequences with connection integers being odd prime powers that exhibit ideal arithmetic correlation. Section 5 establishes an upper bound for the arithmetic crosscorrelation of binary sequence pairs derived from Fermat quotients, under the condition that their periods are coprime. Section 6 presents the conclusions.

# 2 Preliminaries

## 2.1 Notations

• $\mathbb{Z}_M = \{0, 1, \cdots, M-1\}$ denotes the ring of residue classes modulo $M$ and $\mathbb{Z}_M^*$ denotes the multiplicative group of units in $\mathbb{Z}_M$, that is, the set of elements coprime to $M$.
• $M_j$ counts the occurrences of $j$ over the minimal period common to both sequences in a given pair, such as the pairs $(\mathcal{S}, \mathcal{T})$ and $(\mathcal{G}, \mathcal{H})$.
• $N_j$ is the number of $j$ appearing in the least period of sequence $\mathcal{U}$.
• We say that $h(n) = O(l(n))$ (also written as $h(n) \ll l(n)$) if there exists an absolute constant $C > 0$ such that $|h(n)| \leq Cl(n)$ for all $n$.
• The notation $V \subseteq U$ means that $V$ is a subset of $U$.
• log is the logarithm to base 10.

## 2.2 Arithmetic correlation

Let $N$ be an integer not less than 2 and $\mathcal{S} = (s_i)_{i\geq 0}$ denote a nonzero $T$-periodic $N$-ary sequence over $\mathbb{Z}_N$ generated by an $m$-stage FCSR, it uniquely associates with the formal power series

$$\alpha = \sum_{i=0}^{\infty} s_i N^i = -\frac{\sum_{i=0}^{T-1} s_i N^i}{N^T - 1} = -\frac{f}{q},$$

where $f$ and $q$ are coprime positive integers satisfying $f < q$, the denominator $q$, which is expressed in the form $q = q_0 + q_1 N + \cdots + q_m N^m$, is termed *the connection integer* of the FCSR. Now let $2 \leq N < q$ with $N$ and $q$ relatively prime. An equivalent definition of $\mathcal{S}$ is

$$s_i = A\left(N^{-i} f \pmod{q}\right) \pmod{N}, \tag{1}$$

where $N^{-i} f \pmod{q}$ represents the unique residue modulo $q$ in the range $[0, q-1]$ and $A = -q_0^{-1} (\mathrm{mod}\, N)$. And we have $T = \mathrm{ord}_q(N)$, which is the order of $N$ modulo $q$ [2].

Let $\mathcal{T} = (t_i)_{i\geq 0}$ be another $T$-period (nonzero) sequence with the connection integer $q$ over $\mathbb{Z}_N$. The sequence $\mathcal{T}^{(\tau)}$, representing a $\tau$-shift of $\mathcal{T}$, is associated with the formal power series

$$\beta^{(\tau)} = \sum_{i=0}^{\infty} t_{i+\tau} N^i = -\frac{\sum_{i=0}^{T-1} t_{i+\tau} N^i}{N^T - 1} = -\frac{y_\tau}{q},$$

where $y_\tau$ and $q$ are coprime positive integers satisfying $y_\tau < q$, then $\alpha - \beta^{(\tau)}$ uniquely corresponds to the (new) $N$-ary sequence $\mathcal{U} = (u_i)_{i\geq 0}$, that is

$$\alpha - \beta^{(\tau)} = \sum_{i=0}^{\infty}(s_i - t_{i+\tau})N^i \triangleq \sum_{i=0}^{\infty} u_i N^i,$$

which is eventually period over $\mathbb{Z}_N$, its pre-period is $\kappa$ and period divides $T$ [9, Definition 7]. For sequences $\mathcal{S}$ and $\mathcal{T}$, the *arithmetic cross-correlation* at lag $\tau$ can be expressed as $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)$, is

$$\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = \sum_{i=\kappa}^{\kappa+T-1} \xi_N^{u_i} = \sum_{j=0}^{N-1} M_j \xi_N^j, \tag{2}$$

where $\xi_N = e^{\frac{2\pi\sqrt{-1}}{N}}$ is a complex primitive $N$-th root of unity, and $M_j$ counts the occurrences of $j$ over a full period (of length $T$) of the sequence $\mathcal{U}$. When $\mathcal{S} = \mathcal{T}$, $\mathcal{C}^A_{\mathcal{S},\mathcal{S}}(\tau)$ is called the *arithmetic auto-correlation* of $\mathcal{S}$ and is simply written as $\mathcal{A}^A_{\mathcal{S}}(\tau)$.

If $\mathcal{A}^A_{\mathcal{S}}(\tau) = 0$ for $\tau \neq 0$ (resp. $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)$=0 when $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ for all $\tau$), we say that this pair of sequences has ideal arithmetic auto-(resp. cross-) correlation.

Specifically, consider two binary sequences $\mathcal{G} = (g_i)_{i=0}^{T-1}$ and $\mathcal{H} = (h_i)_{i=0}^{T-1}$ of period $T$, with each element $g_i, h_i \in \{0, 1\}$. Here, $T$ is the minimal period common to both sequences. Write

$$G(2) = \sum_{i=0}^{T-1} g_i 2^i,\ H^{(\tau)}(2) = \sum_{i=0}^{T-1} h_{i+\tau} 2^i.$$

The integer $\left|G(2) - H^{(\tau)}(2)\right| \geq 0$ can be expressed in 2-adic expansion $\left|G(2) - H^{(\tau)}(2)\right| = \sum_{i=0}^{T-1} w_i 2^i (w_i \in \{0, 1\})$. The arithmetic crosscorrelation of $\mathcal{G}$ and $\mathcal{H}$ at a shift $\tau$ is defined as

$$\mathcal{C}^A_{\mathcal{G},\mathcal{H}}(\tau) = \begin{cases} M_0 - M_1, & \text{if } G(2) \geq H^{(\tau)}(2), \\ M_1 - M_0, & \text{if } G(2) < H^{(\tau)}(2), \end{cases} \tag{3}$$

where for each $j \in \{0, 1\}$, $M_j$ is the cardinality of the set $\{i \in \{0, 1, \ldots, T-1\} \,|w_i = j\}$.

## 2.3 The Binary sequence related to the Fermat quotient

Consider an odd prime $p$ and an integer $n$ coprime to $p$. The Fermat quotient, denoted by $q_p(n)$, is defined by

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

and let $q_p(kp)$ be defined as 0 for $k \in \mathbb{Z}$.

A binary sequence $\mathcal{G}_{p^2} = \left\{g_0, g_1, \cdots, g_{p^2-1}\right\} \in \{0, 1\}^{p^2}$ combining Fermat quotient $q_p(n)$ with the Legendre symbol $\left(\frac{\cdot}{p}\right)$ was defined by Gomez and Winterhof [13] as

follows

$$g_n = \begin{cases} 0, & \text{if } \left(\frac{q_p(n)}{p}\right) = 1 \text{ or } q_p(n) = 0, \\ 1, & \text{otherwise .} \end{cases} \tag{4}$$

The binary sequence $\mathcal{G}_{p^2}$ has several desired features of pseudorandomness, see [13–15] for detail.

# 3 A sufficient condition of ideal arithmetic correlations

This section presents a sufficient condition for ideal arithmetic correlations that will be used later.

Let $q > N \geq 2$ be integers, where $q$ is odd and $\gcd(q, N) = 1$. Define

$$D(q) = \left\{N^i (\mathrm{mod}\, q) : 0 \leq i < \mathrm{ord}_q(N)\right\} \subseteq \{1, 2, \cdots, q-1\}. \tag{5}$$

The set $D(q)$ forms a multiplicative subgroup of $\mathbb{Z}_q^*$. And for an integer $g$, let

$$gD(q) = \left\{gN^i (\mathrm{mod}\, q) : 0 \leq i < \mathrm{ord}_q(N)\right\} \subseteq \{1, 2, \cdots, q-1\}. \tag{6}$$

Obviously, $\left\{N^{-i} g (\mathrm{mod}\, q) : 0 \leq i < \mathrm{ord}_q(N)\right\}$ also form the set $gD(q)$.

Let $\mathcal{U} = (u_i)_{i\geq 0}$ denote an $N$-ary sequence of period $\mathrm{ord}_q(N)$ associated with $-\frac{h}{q}$, where $h$ and $q$ are coprime positive integers with $h < q$. By Equation (1), $\mathcal{U}$ can defined as $u_i = A\left(N^{-i}h \pmod q\right) (\mathrm{mod}\ N)$ for all $i \geq 0$, where $1 \leq A \leq N-1$ and $\gcd(A, N) = 1$. Thus $u_i = j$ if and only if $A\left(N^{-i}h \pmod q\right) (\mathrm{mod}\, N)$ equals $j$. Then the number of every $j$ in a period of $\mathcal{U}$ equals the number of integers modulo $N$ equal $j$ in $A(hD(q))$ since all numbers $N^{-i}h \pmod q$ form the set $hD(q)$.

For $N$-ary periodic sequence $\mathcal{U} = (u_i)_{i\geq 0}$, $\xi_N = e^{\frac{2\pi\sqrt{-1}}{N}}$ is a complex primitive $N$-th root of unity and $N_j$ is the number of $j$ appearing in the least period of $\mathcal{U}$. If $N_j$ for all $j = 0, 1, 2, \cdots, N-1$ are equal, the periodic sequence $\mathcal{U}$ is called *balanced*. If $\sum_{j=0}^{N-1} N_j \xi_N^j = 0$, $\mathcal{U}$ is said to be *weakly balanced*.

Note

$$A\left(N^{-i}h \pmod q\right) (\mathrm{mod}\ N) = A\left((N^{-i}h \pmod q) \mathrm{mod}\ N\right) (\mathrm{mod}\ N).$$

holds for all $i \geq 0$. If the number of occurrences of each element in $(N^{-i}h \pmod q)(\mathrm{mod}\ N)$ is equal, then based on $A$ coprime with $N$, we have $\{A \cdot x \,(\mathrm{mod}\, N) | x \in \mathbb{Z}_N\} = \mathbb{Z}_N$. It follows that the frequency of each element appearing in $A\left((N^{-i}h \pmod q) \mathrm{mod}\ N\right) (\mathrm{mod}\, N)$ is also equal. Consequently, for the remainder of the paper, we can simplify the assessment by stating that the balanced of sequence $\mathcal{U}$ is indicated by the identical frequency of each element appearing in $hD(q) (\mathrm{mod}\, N)$.

*Lemma 1* [9, Lemma 1] A balanced $N$-ary sequence $\mathcal{U}$ is necessarily weakly balanced. Moreover, when $N$ is a prime, the properties of being balanced and weakly balanced are equivalent.

**Theorem 1** *Let $\mathcal{S} = (s_i)_{i\geq 0}$ and $\mathcal{T} = (t_i)_{i\geq 0}$ be two $N$-ary periodic sequences whose connection integer $q$ is an odd positive integer, where $N$ is an integer such that $2 \leq N < q$. Then $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ and $\tau \geq 0$ if the following holds: for every divisor $\bar{q} > 1$ of $q$, and for any integer $h$ coprime with $\bar{q}$, the number of integers modulo $N$ equal to $i\,(0 \leq i \leq N-1)$ in $hD(\bar{q})$ equals $\frac{\mathrm{ord}_{\bar{q}}(N)}{N}$.*

*Proof* Suppose the sequences $\mathcal{S}$ corresponds to $-\frac{f}{q}$ and $\mathcal{T}^{(\tau)}$ to $-\frac{y_\tau}{q}$, for positive integers $f$ and $y_\tau$ less than and coprime to $q$. Under the condition that $f \neq y_\tau$, we have $\gcd(f-y_\tau, q) = n$. Set $\bar{q} = \frac{q}{n}$. The arithmetic crosscorrelation at shift $\tau$ depends on the imbalance of the $N$-ary sequence $\mathcal{U}$ (with full period $\mathrm{ord}_q(N)$) associated with the rational number

$$\gamma = -\frac{1}{\bar{q}} \times \begin{cases} (f-y_\tau)/n, & \text{if } f - y_\tau > 0, \\ (f-y_\tau+q)/n, & \text{if } f - y_\tau < 0. \end{cases}$$

Hence $\mathcal{U}$ is balanced under the assumption with $hD(\bar{q})$ for $h = (f-y_\tau)/n$ or $h = (f-y_\tau+q)/n$. According to Equation (2), $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ when $\mathcal{S} \neq \mathcal{T}^{(\tau)}$. This is because $\xi_N$, the complex primitive $N$-th root of 1 satisfies $\xi_N^{N-1} + \xi_N^{N-2} + \cdots + 1 = 0$.

This completes the proof. □

*Remark 1* When $N$ is a prime, it follows from Lemma 1 that if $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ and $\tau \geq 0$ in Theorem 1, then, for these $\tau$, the number of integers congruent to $i$ modulo $N$ $(0 \leq i \leq N-1)$ in $hD(\bar{q})$ equals $\frac{\mathrm{ord}_{\bar{q}}(N)}{N}$ for $h = (f-y_\tau)/n$ or $h = (f-y_\tau+q)/n$, with $\bar{q} = \frac{q}{n}$.

# 4 Ideal arithmetic correlations

This section is devoted to the construction of sequences $\mathcal{S}$ and $\mathcal{T}$ with ideal arithmetic correlations, derived from their connection integers. First, we provide a relevant lemma here which will be used in the subsequent proof.

*Lemma 2* Let $p$ be an odd prime and $\gcd(p, N) = 1$. For $k \geq 1$, let $q = p^k$, if $N|\mathrm{ord}_q(N)$, then $p \equiv 1 (\mathrm{mod}\ N)$.

*Proof* Since $\gcd(p, N) = 1$ and $q = p^k$ $(k \geq 1)$, by Euler's theorem, it follows that $N^{\phi(q)} \equiv 1 (\mathrm{mod}\ q)$, where $\phi(q)$ denotes the Euler function. From $N^{\mathrm{ord}_q(N)} \equiv 1 (\mathrm{mod}\ q)$, then $\mathrm{ord}_q(N)|p^{k-1}(p-1)$. From $N|\mathrm{ord}_q(N)$, we get $N|p^{k-1}(p-1)$. Since $\gcd(p, N) = 1$, it follows that $N|p-1$, which completes the proof. □

*Remark 2* From Theorem 1 and Lemma 2, when $N$ is a prime, if two $N$-ary sequences with an odd prime power connection integer $p^k$ $(k \geq 1)$ have ideal arithmetic correlations, then we must have $p \equiv 1 (\mathrm{mod}\ N)$. Obviously, this congruence always holds when $N = 2$.

Two sequences have ideal arithmetic correlations in subsequent cases, we need the condition $p \equiv 1 (\mathrm{mod}\, N)$.

## 4.1 The connection integer is an odd prime $p$

*Lemma 3* Let $p$ be an odd prime and $p \equiv 1 (\mathrm{mod}\, N)$. We have the number of integers modulo $N$ equal $i$ in $\mathbb{Z}_p^*$ for $0 \leq i \leq N-1$ are equal.

*Proof* Let $a$ be any element in $\mathbb{Z}_p^*$, then the discussion can be divided into the following two cases based on the value of $a+N-1$.

**Case 1**: If $a+N-1 < p$, clearly, integers $a(\mathrm{mod}\, p)$, $a+1(\mathrm{mod}\, p)$, $\ldots$, $a+(N-1)(\mathrm{mod}\, p)$ are all appears in $\mathbb{Z}_p^*$, and they are $N$ different integers of modulo $N$ since $a+i \equiv a+j(\mathrm{mod}\, p)$ if and only if $i = j+pt$ for some $t$.

**Case 2**: If $a+N-1 \geq p$, there exists an integer $i$ $(i \geq 0)$ that makes $a+i = p$, then $a+i \notin \mathbb{Z}_p^*$. While integers $a(\mathrm{mod}\, p)$, $a+1(\mathrm{mod}\, p)$, $\ldots$, $a+(i-1)(\mathrm{mod}\, p)$, $a+(i+1)(\mathrm{mod}\, p)$, $\ldots$, $a+(N-1)(\mathrm{mod}\, p)$, $a+N(\mathrm{mod}\, p)$ are all appears in $\mathbb{Z}_p^*$, and they are $N$ different integers of modulo $N$.

Putting both cases together, we complete the proof. □

**Theorem 2** *Consider two $N$-ary periodic FCSR sequences $\mathcal{S} = (s_i)_{i\geq 0}$ and $\mathcal{T} = (t_i)_{i\geq 0}$ whose connection integer $p$ is an odd prime, where $2 \leq N < p$. If $N$ is a primitive root modulo $p$ and $p \equiv 1 (\mathrm{mod}\, N)$, then $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ and $\tau \geq 0$.*

*Proof* According to the proof of Theorem 1, since $p$ is prime, then $\gcd(f - y_\tau, p) = 1$, and the sequence $\mathcal{U}$ corresponds to the rational number $-\frac{h}{p}$. For any prime $p$ with $p \equiv 1 (\mathrm{mod}\, N)$, from Equation (5), we have $D(p) = \mathbb{Z}_p^*$ since $D(p)$ is a group under the multiplicative modulo $p$ and $\mathrm{ord}_p(N) = \phi(p) = p-1$. Then by Lemma 3, for $i$ ranging from 0 to $N-1$, the number of integers modulo $N$ equal $i$ in $D(p)$ all appear $\frac{p-1}{N} = \frac{\mathrm{ord}_p(N)}{N}$ times. By Equation (6), since this property holds for all $hD(p)$ where $h$ is coprime to $p$, we may apply Theorem 1 to obtain the desired result. □

*Remark 3* Theorem 2 shows that for an $N$-ary $\ell$ sequence $\mathcal{B}$ with a prime connection integer $p$ satisfying $p \equiv 1 (\mathrm{mod}\, N)$, we have $\mathcal{A}^A_{\mathcal{B}}(\tau) = 0$ for $\tau \neq 0$. The method of proof used here differs from that in [8, Theorem 5] and [9, Theorem 10].

## 4.2 The connection integer is an odd prime power $p^r$

We need Lemma 4 related to number theory to prove the following conclusion.

*Lemma 4* Let $p$ be an odd prime with $N^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$ and $\mathrm{ord}_p(N) = \lambda$. Then we get $\mathrm{ord}_{p^k}(N) = \lambda p^{k-1}$ for $k \geq 2$.

*Proof* Similar to the proof in [6, Lemma 2], we omit the details here. □

**Theorem 3** *Let $\mathcal{S} = (s_i)_{i\geq 0}$ and $\mathcal{T} = (t_i)_{i\geq 0}$ be two $N$-ary periodic FCSR sequences whose connection integer $q = p^r$ is a power of an odd prime $p$, with $N$ satisfying $2 \leq N < p$. If $N$ is a primitive root modulo $p$, $N^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$, and $p \equiv 1 (\mathrm{mod}\, N)$, then $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ and $\tau \geq 0$.*

*Proof* According to the proof of Theorem 1, since $q = p^r (r \geq 2)$, then $\gcd(f - y_\tau, p^r) = p^t$ for some $t$, and the sequence $\mathcal{U}$ corresponds to the rational number $-\frac{h}{\bar{q}}$. Let $\bar{q} \in \left\{p^k | 1 \leq k \leq r\right\}$.

A primitive root $N$ modulo a prime $p$ remains primitive modulo $p^m$ for all $m \geq 1$ provided that $N^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$ [17]. According to the proof of Theorem 2, each $i\,(0 \leq i \leq N-1)$ in $D(p)$ modulo $N$ appears $\frac{p-1}{N}$ times. It is clear that from Equation (5),

$$D(p^2) = \{x + jp : x \in D(p), 0 \leq j < p\}.$$

For each $x \in D(p)$, by Lemma 3, we see that $N$ different integers of modulo $N$ in $x + p$, $x + 2p, \ldots, x + (p-1)p$ all appear $\frac{p-1}{N}$ times since $p \equiv 1 (\mathrm{mod}\, N)$. Hence by Lemma 4, the elements of the set $D(p^2)$ are uniformly distributed modulo $N$, with each resides $i\,(0 \leq i \leq N-1)$ occurring with $\frac{p-1}{N}(p-1) + \frac{p-1}{N} = \frac{p(p-1)}{N} = \frac{\mathrm{ord}_{p^2}(N)}{N}$ times.

By induction on $k$ we get $D(p^k) = \left\{x + jp^{k-1} : x \in D(p^{k-1}), 0 \leq j < p\right\}$, $k \geq 2$, and the integers with modulo $N$ equal to $i\,(0 \leq i \leq N-1)$ in $D(p^k)$ all occur $\frac{p-1}{N}(p^{k-1} - p^{k-2}) + \frac{p^{k-1}-p^{k-2}}{N} = \frac{p^k - p^{k-1}}{N} = \frac{\mathrm{ord}_{p^k}(N)}{N}$ times. Since Equation (6) implies that every set $hD(\bar{q})$ (where $\gcd(h, \bar{q}) = 1$) also has the aforementioned property, applying Theorem 1 yields the desired result. □

For the case when $\mathrm{ord}_p(N)$ is not necessarily equal to $\phi(p)$, we have the following corollary.

*Corollary 1* Let $\mathcal{S} = (s_i)_{i\geq 0}$ and $\mathcal{T} = (t_i)_{i\geq 0}$ be two $N$-ary periodic FCSR sequences whose connection integer $q = p^r$ is a power of an odd prime $p$, with $N$ satisfying $2 \leq N < p$. Assume the following conditions hold:
(1) $p \equiv 1 (\mathrm{mod}\, N)$;
(2) $N^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$;
(3) for any integer $h$ such that $\gcd(h, p^k) = 1$ for all $1 \leq k \leq r$, the elements of the set $hD(p)$ are uniformly distributed modulo $N$. Specifically, each residue class $i \bmod N (0 \leq i \leq N-1)$ appears exactly $\frac{\mathrm{ord}_p(N)}{N}$ times.

Then, under these hypotheses, it follows that $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ and $\tau \geq 0$.

*Proof* Since from Equation (6), for $k \geq 1$,

$$hD(p^{k+1}) = \left\{x + jp^k : x \in hD(p^k), 0 \leq j < p\right\}.$$

Similar to Theorem 3, the results can be proved. □

Table 1 presents several examples computed using the Magma program to verify our main results.

**Table 1** Arithmetic autocorrelation of $\mathcal{S}$ with connection integer $q = p^r$

| $q = p^r$ | $N$ | $p \pmod N$ | $N^{p-1} \pmod{p^2}$ | $\mathrm{ord}_q(N)$ | $\mathcal{A}^A_{\mathcal{S}}(\tau)(\tau \neq 0)$ | Remarks |
|---|---|---|---|---|---|---|
| 7 | 3 | 1 | | 6 | 0 | Thm. 2 |
| $7^2$ | 3 | 1 | 43 | 42 | 0 | Thm. 3 |
| 13 | 6 | 1 | | 12 | 0 | Thm. 2 |
| $13^2$ | 6 | 1 | 144 | 156 | 0 | Thm. 3 |
| 17 | 2 | 1 | 222 | 8 | 0 | Cor. 1 |
| 17 | 4 | 1 | | 4 | $\not\equiv 0$ | Violation of Cor. 1(3) |

# 5 Arithmetic crosscorrelation of binary sequence related to Fermat quotient

In this section, we will prove upper bound on the arithmetic crosscorrelation for two binary sequence related to Fermat quotient of coprime periods.

The pattern distribution of two binary sequences defined in (4), which are associated with distinct primes $p$ and $r$, is given by the following lemma.

*Lemma 5* Consider odd primes $p$ and $r$ satisfying $p < r$. Let $\mathcal{G}_{p^2} = (g_i)_{i\geq 0}$ and $\mathcal{H}_{r^2} = (h_i)_{i\geq 0}$ denote binary sequences of periods $p^2$ and $r^2$ respectively, as defined in (4).
For an nonnegative integer $k$ and any pattern $\underline{e} \in \{0,1\}^{2k+2}$, if $k \leq (\frac{1}{3}\log p - \log\log p)/\log 2$, the quantity $\Sigma_k$ counts the number of indices $i = 0, 1, \ldots, p^2q^2 - 1$ such that

$$(g_{i-k}, g_{i-k+1}, \ldots, g_i, h_{i-k}, h_{i-k+1}, \ldots, h_i) = \underline{e}$$

satisfies $\Sigma_k = \frac{p^2r^2}{2^{2k+2}} + O\Big(2^{-k}\, k\, p^{\frac{5}{3}} r^2\Big)$.

*Proof* By [13, Theorem 2], we can obtain

$$\Sigma_k = (\frac{p^2}{2^{k+1}} + O(kp^{\frac{5}{3}})) \times (\frac{r^2}{2^{k+1}} + O(kr^{\frac{5}{3}})),$$

combining the result and after verifying that

$$\max\big\{2^{-k}k\,p^2 r^{\frac{5}{3}},\ 2^{-k}k\,p^{\frac{5}{3}}r^2,\ k^2(pr)^{\frac{5}{3}}\big\} = 2^{-k}k\,p^{\frac{5}{3}}r^2$$

holds for $k \leq (\frac{1}{3}\log p - \log\log p)/\log 2$, we arrive at the desired conclusion. □

The arithmetic crosscorrelation of these sequences follows from the aforementioned lemma.

**Theorem 4** *Let $\mathcal{G}_{p^2} = (g_i)_{i\geq 0}$ and $\mathcal{H}_{r^2} = (h_i)_{i\geq 0}$ be two binary sequences of prime power periods $p^2$ and $r^2$ defined by (4). For $2 < p < r$, the arithmetic crosscorrelation $C^A_{\mathcal{G},\mathcal{H}}(\tau)$ satisfies*

$$\mathcal{C}^A_{\mathcal{G},\mathcal{H}}(\tau) \ll\ p^{\frac{5}{3}}\, r^2 (\log p)^2, \qquad 0 \leq \tau < p^2 r^2.$$

*Proof* By [10, Theorem 1], the arithmetic crosscorrelation of two binary sequences with coprime periods is constant. Therefore, we may set $\tau = 0$. Furthermore, without loss of generality, we can assume $G(2) \geq H^{(0)}(2)$, where $G(2) = \sum_{i=0}^{p^2r^2-1} g_i 2^i$, $H^{(0)}(2) = \sum_{i=0}^{p^2r^2-1} h_i 2^i$. We write

$$G(2) - H^{(0)}(2) = \sum_{i=0}^{p^2r^2-1} (g_i - h_i)2^i = \sum_{i=0}^{p^2r^2-1} w_i\, 2^i$$

with $w_i \in \{0, 1\}$. Since the values $w_i$ are unique, it is necessary to estimate the number of indices $i$ for which $w_i = 1$.

Assume there exist integers $n \geq k \geq 1$ and $b \in \{0, 1\}$ such that

$$(g_{n-k}, h_{n-k}) = (b, 1-b),$$
$$g_{n-k+j} = h_{n-k+j}, \quad j \in \{1, 2, \ldots, k-1\},$$
$$(g_n, h_n) \in \{0, 1\}^2.$$

For $b = 1$, we have

$$2^{n-k+1} > \sum_{i=0}^{n-k} (g_i - h_i)2^i \geq 2^{n-k} - \sum_{i=0}^{n-k-1} 2^i > 0,$$

and thus $w_{n-k+1}$ depends only on $(g_{n-k+1}, h_{n-k+1})$. It follows that

$$w_{n-k+j} = g_{n-k+j} - h_{n-k+j} = 0 \text{ for } j \in \{1, 2, \ldots, k-1\}$$

and $w_n = 1$ iff $g_n \neq h_n$.

For $b = 0$, we have

$$0 < 2^{n-k+1} + \sum_{i=0}^{n-k} (g_i - h_i)2^i < 2^{n-k+1},$$

and thus for $j \in \{1, 2, \ldots, k-1\}$,

$$w_{n-k+j} = 1 + g_{n-k+j} - h_{n-k+j} = 1$$

and $w_n = 1$ iff $g_n = h_n$.

In total, there exist $2^{k+1}$ distinct patterns $\underline{e} \in \{0, 1\}^{2k+2}$ such that

$$(g_{n-k}, g_{n-k+1}, \ldots, g_n, h_{n-k}, h_{n-k+1}, \ldots, h_n) = \underline{e} \tag{7}$$

implies $w_n = 1$. According to Lemma 5, for each of these $2^{k+1}$ patterns $\underline{e}$, there exist $\frac{p^2r^2}{2^{2k+2}} + O\left(2^{-k}\, k\, p^{\frac{5}{3}} r^2\right)$ distinct integers $n \in \left[k, k + p^2r^2 - 1\right]$ satisfying equation (7). Therefore, for every $k = 1, 2, \ldots$, there exist at least

$$2^{k+1}\, \frac{p^2r^2}{2^{2k+2}} + O\left(\frac{2^{k+1}}{2^k} k\, p^{\frac{5}{3}} r^2\right) = \frac{p^2r^2}{2^{k+1}} + O\left(kp^{\frac{5}{3}} r^2\right)$$

distinct integers $n$ in every fixed interval of length $p^2r^2$ such that $w_n = 1$.

We choose $M = \left\lfloor \frac{\log p}{3 \log 2} - \frac{2 \log \log p}{\log 2} \right\rfloor \leq \log p$, which implies $p^{-1/3} (\log p)^2 \leq 2^{-M} \leq 2\, p^{-1/3} (\log p)^2$. Summing the contributions yields

$$M_1 \geq \sum_{k=1}^{M} \frac{p^2r^2}{2^{k+1}} + O\Big(\sum_{k=1}^{M} kp^{\frac{5}{3}} r^2\Big)$$

for the count of $n \in \left[0, p^2r^2 - 1\right]$ with $w_n = 1$. Given that

$$\begin{aligned}
&\sum_{k=1}^{M} \frac{p^2r^2}{2^{k+1}} + O\Big(\sum_{k=1}^{M} kp^{\frac{5}{3}}r^2\Big) \\
&= \frac{p^2r^2}{4} \sum_{k=0}^{M-1} 2^{-k} + O\big(M^2p^{\frac{5}{3}}r^2\big) \\
&= \frac{p^2r^2}{2}\left(1 - \left(\frac{1}{2}\right)^M\right) + O\big(p^{\frac{5}{3}}r^2(\log p)^2\big) \\
&= \frac{p^2r^2}{2} + O\big(p^{\frac{5}{3}}r^2(\log p)^2\big),
\end{aligned}$$

it follows that $M_1 \geq \frac{p^2r^2}{2} + O\big(p^{\frac{5}{3}}r^2(\log p)^2\big)$.

Analogously, the number $M_0$ of indices $n$ for which $w_n = 0$ satisfies the lower bound $M_0 \geq \frac{p^2r^2}{2} + O\big(p^{\frac{5}{3}}r^2(\log p)^2\big)$.

Since

$$M_0 = p^2r^2 - M_1 \leq \frac{p^2r^2}{2} + O\big(p^{\frac{5}{3}}r^2(\log p)^2\big),$$

then (3) yields the result. □

Set $T = p^2r^2$. If $p$ and $r$ are of comparable order of magnitude, then the bound is $O(T^{\frac{11}{12}}(\log T)^2)$.

Table 2 presents numerical values of the arithmetic crosscorrelation, as defined by (4), for the binary sequences $\mathcal{G}_{p^2}$ and $\mathcal{H}_{r^2}$ with coprime periods $p^2$ and $r^2$. The values of these arithmetic crosscorrelations are distributed between values close to zero and those approaching the theoretical upper bound.

**Table 2** Arithmetic crosscorrelation of two binary sequences $\mathcal{G}_{p^2}$ and $\mathcal{H}_{r^2}$ of coprime periods $p^2$ and $r^2$ defined by (4)

| $p$ | $r$ | $\mathcal{C}^A_{\mathcal{G},\mathcal{H}}(\tau)$ | $p^{\frac{5}{3}}r^2\,(\log\ p)^2$ (approximate value) |
|---|---|---|---|
| 3 | 13 | -1 | 240 |
| 3 | 73 | 23 | 7570 |
| 3 | 79 | -1407 | 8866 |
| 5 | 37 | 13 | 9778 |
| 5 | 43 | -1155 | 13207 |
| 7 | 11 | 317 | 2214 |

# 6 Conclusions

Arithmetic auto-/cross-correlation is an important measure of sequences generated by FCSRs. In practical applications, it is desirable that the arithmetic correlations should be as small as possible. This paper establishes the ideal arithmetic correlation of N-ary sequences with connection integers being prime powers. Additionally, it provides

an upper bound for the arithmetic cross-correlation of binary sequences constructed from Fermat quotients with coprime periods. An interesting future work would be designing $N$-ary FCSR sequences that have ideal arithmetic correlations and whose connection integer is the product of distinct prime powers.

## Declarations


- Funding
  This work is supported by the National Natural Science Foundation of China (No. 62272420), Natural Science Foundation of Fujian Province (No. 2023J01535).
- Conflict of interest
  The authors declare no competing interests.


## References


[1] Golomb, S.W., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. Cambridge University Press, Cambridge, UK (2005)

[2] Goresky, M., Klapper, A.: Algebraic Shift Register Sequences. Cambridge University Press, Cambridge, UK (2012)

[3] Mandelbaum, D.: Arithmetic codes with large distance. IEEE Transactions on Information Theory **13**(2), 237–242 (2003)

[4] Goresky, M., Klapper, A.: Arithmetic crosscorrelations of feedback with carry shift register sequences. IEEE Transactions on Information Theory **43**(4), 1342–1345 (2002)

[5] Wang, H.J., Wen, Q.Y., Zhang, J.: GLS: New class of generalized Legendre sequences with optimal arithmetic cross-correlation. RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications **47**(4), 371–388 (2013)

[6] Chen, Z.X., Edemskiy, V., Niu, Z.H., Sang, Y.Q.: Arithmetic correlation of binary half-$\ell$-sequences. IET Information Security **17**(2), 289–293 (2023)

[7] Chen, Z.R., Edemskiy, V., Wu, C.H.: Binary sequences with ideal and small arithmetic correlations. Cryptography and Communications **17**(2), 453–464 (2025)

[8] Goresky, M., Klapper, A.: Some results on the arithmetic correlation of sequences. In: International Conference on Sequences and Their Applications, pp. 71–80. Springer, Berlin, Heidelberg (2008)

[9] Goresky, M., Klapper, A.: Statistical properties of the arithmetic correlation of sequences. International Journal of Foundations of Computer Science **22**(06), 1297–1315 (2011)

[10] Chen, Z.X., Niu, Z.H., Winterhof, A.: Arithmetic crosscorrelation of pseudorandom binary sequences of coprime periods. IEEE Transactions on Information Theory **68**(11), 7538–7544 (2022)

[11] Jing, X.Y., Feng, K.Q.: Arithmetic crosscorrelation of binary $m$-sequences with coprime periods. Finite Fields and Their Applications **96**, 102424 (2024)

[12] Liu, X., Liu, H.N.: Arithmetic autocorrelation and pattern distribution of binary sequences. Electronic Research Archive **33**(2), 849–866 (2025)

[13] Gomez, D., Winterhof, A.: Multiplicative character sums of Fermat quotients and pseudorandom sequences. Periodica Mathematica Hungarica **64**(2), 161–168 (2012)

[14] Chen, Z.X., Hu, L., Du, X.N.: Linear complexity of some binary sequences derived from Fermat quotients. China Communications **9**(2), 105–108 (2012)

[15] Chen, Z.X.: Trace representation and linear complexity of binary sequences derived from Fermat quotients. Science China Information Sciences **57**(11), 1–10 (2014)

[16] Ireland, K., Rosen, M.I.: A Classical Introduction to Modern Number Theory. Springer, New York, NY (2013)

[17] Ribenboim, P.: The Book of Prime Number Records. Mathematical Gazette, Leicester, UK (1988)