Notes on the ideal arithmetic correlations of N-ary sequences

Feifei Yan[1] and Pinhui Ke[2*]

[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.

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

Abstract

In this paper, we investigate the nonexistence of $\boldsymbol{N}$-ary sequences with ideal arithmetic correlation. We prove that there exist no ternary, quaternary, or $\mathbf{6}$-ary sequences with ideal arithmetic autocorrelation when the connection integer is an odd prime power $\boldsymbol{p^t}$ and $\mathbf{ord}_{\boldsymbol{p^t}}(\boldsymbol{N}) = \boldsymbol{\phi(p^t)/4}$, where $\boldsymbol{\phi}$ denotes Euler's totient function. Furthermore, if $\mathrm{ord}_{\boldsymbol{p^t}}(\boldsymbol{N}) = \boldsymbol{\phi(p^t)/6}$ or $\boldsymbol{\phi(p^t)/8}$, then no such ternary, quaternary, or $\mathbf{6}$-ary sequence families with connection integer $\boldsymbol{p^t}$ exist. This includes in particular the case $\boldsymbol{p \equiv 7 (\mathrm{mod}\, 12)}$, for which $\mathrm{ord}_{\boldsymbol{p^t}}(\boldsymbol{N}) = \boldsymbol{\phi(p^t)/6}$; we further show that no $\boldsymbol{N}$-ary sequence families with ideal arithmetic autocorrelation exist for any prime $\boldsymbol{N > 2}$. These results provide further evidence that ideal arithmetic correlation is highly restrictive in the $\boldsymbol{N}$-ary setting. We also establish an upper bound on the arithmetic correlation of $\boldsymbol{N}$-ary sequences.

Keywords: FCSR sequences, Arithmetic correlation, Nonbinary sequence, Connection integer

1 Introduction

Pseudorandom sequences produced by feedback shift registers (FSR) are widely used in communication systems and stream ciphers [1–3]. Among the various shift-register models, the feedback with carry shift register (FCSR), introduced by Goresky, Klapper, and Xu in the 1990s, has received considerable attention [3–5]. The FCSR can be

viewed as an analogue of the linear feedback shift register (LFSR) with an additional carry mechanism. Among the parameters used to evaluate FCSR sequences, the N-adic complexity and the arithmetic correlation are of particular importance. The concept of arithmetic autocorrelation was originally proposed by Mandelbaum in connection with arithmetic codes [6]. Subsequently, Goresky and Klapper extended this concept to FCSR sequences and established its relevance in their analysis [3, 7]. These quantities provide useful criteria for assessing the randomness and cryptographic suitability of such sequences.

Let $N \geq 2$ be an integer. Let $\mathcal{S} = (s_i)_{i\geq 0}$ be a T-periodic N-ary sequence. According to the FCSR theory [3], $\mathcal{S}$ corresponds uniquely to a N-adic number

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

where $0 < f < q$ and $\gcd(f, q) = 1$. The integer q is referred to as the *connection number* of $\mathcal{S}$. Equivalently, $\mathcal{S}$ can also be given by [3]

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

for $i = 0, 1, 2, \ldots$, where $A \equiv -q^{-1} \pmod{N}$. Here and subsequently, $x \bmod q$ denotes the least nonnegative residue of x modulo q.

Let μ_j denote the frequency of occurrence of symbol j within one full period of $\mathcal{S}$, for each $j = 0, 1, \ldots, N-1$. Also, let $\xi_N = e^{2\pi i/N}$ be a primitive Nth root of unity, and define $i = \sqrt{-1}$. Then,

$$Z(\mathcal{S}) = Z\left(-\frac{f}{q}\right) = \sum_{j=0}^{N-1} \mu_j \xi_N^j, \tag{2}$$

is termed the *imbalance* of $\mathcal{S}$. The sequence $\mathcal{S}$ is said to be *balanced* if $\mu_k = \mu_l$ for all $k, l = 0, 1, \ldots, N-1$; it is *weakly balanced* if $Z(\mathcal{S}) = 0$.

Now let $\mathcal{T} = (t_i)_{i\geq 0}$ be another N-ary sequence with the same period T and the same connection integer q. For any shift τ, denote the τ-shift of $\mathcal{T}$ by $\mathcal{T}^{(\tau)}$. $\mathcal{T}$ and $\mathcal{T}^{(\tau)}$ are associate with $\beta = -g/q$ and $\beta^{(\tau)} = -g_\tau/q$, respectively, where $0 < g < q$ and $\gcd(g, q) = 1$. And $g_\tau \equiv N^{-\tau} g \pmod{q}$. Then, we may consider the sequence of coefficients associated with $\alpha - \beta^{(\tau)}$. This resulting sequence is eventually periodic, and its period divides T.

The *arithmetic crosscorrelation* of $\mathcal{S}$ and $\mathcal{T}$ at shift τ, denoted $C^A_{\mathcal{S},\mathcal{T}}(\tau)$ equals the imbalance of $\alpha - \beta_\tau$ over a complete period of length T [3]. We have

$$C^A_{\mathcal{S},\mathcal{T}}(\tau) = Z\left(-\frac{(f - gN^{-\tau}) \bmod q}{q}\right). \tag{3}$$

Sequence $\mathcal{S}$ and $\mathcal{T}$ exhibits *ideal arithmetic crosscorrelation* if $C^A_{\mathcal{S},\mathcal{T}}(\tau) = 0$ when $\mathcal{S} \neq \mathcal{T}^{(\tau)}$ for all τ. In particular, when $\mathcal{S} = \mathcal{T}$, $\mathcal{C}^A_{\mathcal{S},\mathcal{S}}(\tau)$ is called the *arithmetic autocorrelation* of $\mathcal{S}$ at τ, denoted $\mathcal{A}^A_{\mathcal{S}}(\tau)$.

Recently, the arithmetic correlation of FCSR sequences has received renewed attention. Studies have addressed the arithmetic correlation of m-sequences [8–11] and half-ℓ-sequences [12–14], as well as the concept of ideal arithmetic correlation [14–16].

The main purpose of this paper is to study the nonexistence of N-ary sequences with ideal arithmetic correlation, that is, sequences whose arithmetic correlation are equal to zero at every nontrivial shift. Motivated by Edemskiy's results on the imbalance and ideal arithmetic autocorrelation of N-ary half-ℓ-sequences [14], we establish several nonexistence results. Our approach is based on the partial sums of Legendre symbols and the imbalance property of the sequences. More precisely, we rule out the existence of 3-ary, 4-ary, and 6-ary sequences with ideal arithmetic autocorrelation in the cases of odd prime-power connection integers p^t with $\mathrm{ord}_{p^t}(N) = \phi(p^t)/4$ for single sequence, and odd prime-power connection integers p^t with $\mathrm{ord}_{p^t}(N) = \phi(p^t)/6$ or $\mathrm{ord}_{p^t}(N) = \phi(p^t)/8$ for sequence families; moreover, if $p \equiv 7 \pmod{12}$, no such sequence exists for any prime $N > 2$ and $\mathrm{ord}_{p^t}(N) = \phi(p^t)/6$ for sequence families. We further derive an upper bound for the arithmetic correlation of N-ary sequences, generalizing the existing binary case.

The remainder of this paper is organized as follows. In Section 2, we recall the necessary preliminaries on arithmetic correlation. Section 3 considers the case $\mathrm{ord}_{p^t}(N) = \phi(p^t)/4$ and proves the nonexistence of 3-ary, 4-ary, and 6-ary sequences with ideal arithmetic autocorrelation. Section 4 treats the cases $\mathrm{ord}_{p^t}(N) = \phi(p^t)/6$ and $\mathrm{ord}_{p^t}(N) = \phi(p^t)/8$ for sequence families. Section 5 is devoted to deriving an upper bound on the arithmetic correlation of N-ary sequences. Section 6 concludes the paper.

2 Preliminaries

We assume $N > 2$, primarily because the ideal arithmetic correlation properties of binary sequences were considered in [15]. To investigate the ideal arithmetic correlations, Legendre symbol sums will be employed. The results of sums of Legendre symbols can see references [17, 18].

Let $\left(\frac{a}{p}\right)$ denote a Legendre symbol and define

$$S_{k,j} = \sum_{(j-1)p/k<a<jp/k} \left(\frac{a}{p}\right), \quad k = 1, \ldots, p-1;\ j = 1, 2, \ldots, k.$$

When $p \equiv 1 \pmod 4$, then

$$S_{2,1} = 0, \quad S_{4,1} > 0. \tag{4}$$

$$S_{6,1} = -2S_{6,3} \neq 0, \quad \text{if } p \equiv 1 \pmod{24}, \tag{5}$$

$$S_{6,1} = 0, S_{6,3} \neq 0, \quad \text{if } p \equiv 13 \pmod{24}. \tag{6}$$

When $p \equiv 3 \pmod 4$, we obtain

$$S_{2,1} > 0, \tag{7}$$

along with

$$S_{6,1} = S_{6,2} = -S_{6,3} \neq 0, \quad \text{if } p \equiv 7 \pmod{24}, \tag{8}$$

$$3S_{6,1} = -3S_{6,3} = -S_{6,2} \neq 0, \quad \text{if } p \equiv 19 \pmod{24}. \tag{9}$$

To compute the arithmetic correlation of the sequence, we have the following equivalent formula.

Define $y_n = fN^{-n} \pmod{q}$, from Eq. (1), $s_n = Ay_n \bmod N$. Since $y_n \equiv Ny_{n+1} \pmod{q}$, there exists a unique integer $k_n \in \{0, 1, \ldots, N-1\}$ such that $Ny_{n+1} = y_n + k_n q$. Since $\gcd(q, N) = 1$, it follows that $k_n \equiv -q^{-1}y_n \bmod N$. Therefore, from $A \equiv -q^{-1} \pmod{N}$, we obtain $s_n = k_n$. Then

$$s_n = \frac{Ny_{n+1} - y_n}{q} = \left\lfloor \frac{Ny_{n+1}}{q} \right\rfloor.$$

For example, set $q = 7$, $N = 5$, and $f = 2$. Since $\mathrm{ord}_7(5) = 6$, we calculate: $5^{-1} \equiv 3 \pmod 7$, $5^{-2} \equiv 2 \pmod 7$, $5^{-3} \equiv 6 \pmod 7$, $5^{-4} \equiv 4 \pmod 7$, $5^{-5} \equiv 5 \pmod 7$. Hence $y_0 = 2$, $y_1 = 6$, $y_2 = 4$, $y_3 = 5$, $y_4 = 1$, $y_5 = 3$. Calculated by Eq. (1), we have $s_0 = 2 \times 2 \pmod 5 = 4$, $s_1 = 2 \times 6 \pmod 5 = 2$, $s_2 = 2 \times 4 \pmod 5 = 3$, $s_3 = 2 \times 5 \pmod 5 = 0$, $s_4 = 2 \times 1 \pmod 5 = 2$, $s_5 = 2 \times 3 \pmod 5 = 1$. On the other hand, $s_0 = \left\lfloor \frac{5\times 6}{7} \right\rfloor = 4$, $s_1 = \left\lfloor \frac{5\times 4}{7} \right\rfloor = 2$, $s_2 = \left\lfloor \frac{5\times 5}{7} \right\rfloor = 3$, $s_3 = \left\lfloor \frac{5\times 1}{7} \right\rfloor = 0$, $s_4 = \left\lfloor \frac{5\times 3}{7} \right\rfloor = 2$, $s_5 = \left\lfloor \frac{5\times 2}{7} \right\rfloor = 1$. The sequence calculated by these two methods are consistent.

Therefore, $s_n = j - 1$ if and only if $\frac{(j-1)q}{N} \leq y_{n+1} < \frac{jq}{N}$ for $j = 1, 2, \ldots, N$. Since $\gcd(f, q) = 1$, we have $y_{n+1} \neq 0$. Moreover, $\gcd(N, q) = 1$ implies that $\frac{(j-1)q}{N}$ is non-integer for $j \geq 2$. Consequently, for all $j = 1, 2, \ldots, N$,

$$s_n = j - 1 \iff \frac{(j-1)q}{N} < y_{n+1} < \frac{jq}{N}. \tag{10}$$

We now consider the case where q is an odd prime p. Let $H = \langle N \rangle$ denote the cyclic subgroup generated by N, that is

$$H = \langle N \rangle = \left\{ N^i \pmod p : 0 \leq i < \mathrm{ord}_p(N) \right\},$$

where $\mathrm{ord}_p(N)$ denote the multiplicative order of N modulo p. And for integer x, $xH = \left\{ xN^i \pmod p : 0 \leq i < \mathrm{ord}_p(N) \right\}$. And define

$$I_{N,j} = \left\{ x : \frac{(j-1)p}{N} < x < \frac{jp}{N} \right\}, j = 1, 2, \ldots, N.$$

Then by Eq. (2),

$$Z\left(-\frac{f}{p}\right) = \sum_{j=1}^{N} |fH \cap I_{N,j}| \, \xi_N^{j-1}. \tag{11}$$

In the sequel, let $\mathbb{F}_p^*$ denote the multiplicative group modulo p, $\mathbb{Q}$ the set of quadratic residues modulo p, and $\mathbb{NQ}$ the set of quadratic non-residues modulo p. Let g be a primitive root modulo p, m be an integer such that $m \mid p - 1$, and let $\mathrm{ord}_p(N) = \frac{p-1}{m}$. Since $\langle N \rangle = \langle g^m \rangle$ has index m in $\mathbb{F}_p^*$, we obtain the coset decomposition $\mathbb{F}_p^* = \bigcup_{i=0}^{m-1} g^i \langle N \rangle$. For convenience, we write $D_l^{(m)} = g^l H$ for $l = 0, 1, \ldots, m-1$.

Since $D_l^{(m)} D_j^{(m)} = D_{(l+j) \pmod m}^{(m)}$, it follows from Eq. (11) that if $f \in D_l^{(m)}$, then $Z\left(-\frac{f}{p}\right) = \sum_{j=1}^{N} \left|D_l^{(m)} \cap I_{N,j}\right| \xi_N^{j-1}$. For brevity, we write $M_{l,j}^{(m,N)} = \left|D_l^{(m)} \cap I_{N,j}\right|$ and $z_l^{(m,N)} = \sum_{j=1}^{N} M_{l,j}^{(m,N)} \xi_N^{j-1}$.

3 On the non-existence of ideal arithmetic correlations when $\mathbf{ord}_q(N) = \frac{\phi(q)}{4}$

Let p be an odd prime, when $\mathrm{ord}_p(N) = \frac{p-1}{4}$, let g be a primitive root modulo p. In this case, we have $\mathbb{F}_p^* = D_0^{(4)} \cup D_1^{(4)} \cup D_2^{(4)} \cup D_3^{(4)}$, $\mathbb{Q} = D_0^{(4)} \cup D_2^{(4)}$ and $\mathbb{NQ} = D_1^{(4)} \cup D_3^{(4)}$.

Denote by $(l, f)_4$ the cyclotomic numbers of order four, that is $(\ell, f)_4 = \left|(D_\ell^{(4)} + 1) \cap D_f^{(4)}\right|$.

Lemma 1 Let the N-adic number corresponding to the sequences $\mathcal{S}$ and $\mathcal{T}$ are $-\frac{f}{p}$ and $-\frac{g}{p}$, where $0 < f < p$ and $0 < g < p$. Suppose $-1 \in D_\varepsilon^{(4)}$, $f \in D_a^{(4)}$, $gf^{-1} \in D_h^{(4)}$ and $1 - gf^{-1}N^{-\tau} \in D_\ell^{(4)}$. Then the nontrivial arithmetic crosscorrelation value of the corresponding two sequences belongs to $\left\{z_0^{(4,N)}, z_1^{(4,N)}, z_2^{(4,N)}, z_3^{(4,N)}\right\}$, and the value $z_{a+\ell}^{(4,N)}$ occurs exactly $(\ell - \varepsilon, h)_4$ times, where all subscripts are taken modulo 4.

Proof Frome Eq. (3), we have

$$C_{\mathcal{S},\mathcal{T}}^{A}(\tau) = Z\left(-\frac{f\left(1 - gf^{-1}N^{-\tau}\right) \bmod p}{p}\right).$$

Since $f \in D_a^{(4)}$ and $1 - gf^{-1}N^{-\tau} \in D_\ell^{(4)}$, it follows that $f\left(1 - gf^{-1}N^{-\tau}\right) \in D_{a+\ell}^{(4)}$. As τ runs through a full period, every nontrivial arithmetic crosscorrelation value belongs to $\left\{z_0^{(4,N)}, z_1^{(4,N)}, z_2^{(4,N)}, z_3^{(4,N)}\right\}$. Varying τ yields precisely the elements of $D_h^{(4)} \setminus \{1\}$ via $gf^{-1}N^{-\tau}$, that is $\left|\left\{\tau : 1 - gf^{-1}N^{-\tau} \in D_\ell^{(4)}\right\}\right| = \left|\left\{x \in D_h^{(4)} \setminus \{1\} : 1 - x \in D_\ell^{(4)}\right\}\right|$. Let $y = x - 1$. Then the above equality becomes $\left|\left\{y \in D_{\ell-\varepsilon}^{(4)} : y + 1 \in D_h^{(4)}\right\}\right| = \left|(D_{\ell-\varepsilon}^{(4)} + 1) \cap D_h^{(4)}\right| = (\ell - \varepsilon, h)_4$. □

Corollary 1 Let the N-adic number corresponding to the sequence $\mathcal{S}$ be $-\frac{f}{p}$, where $0 < f < p$. Suppose $-1 \in D_\varepsilon^{(4)}$, $f \in D_a^{(4)}$, and $1 - N^{-\tau} \in D_\ell^{(4)}$. Then, at nontrivial shifts, the arithmetic autocorrelation value of $\mathcal{S}$ equals $z_{a+\ell}^{(4,N)}$ exactly $(\ell - \varepsilon, 0)_4$ times, with all subscripts taken modulo 4.

For every prime p satisfying $p \equiv 1 \pmod 4$, it is guaranteed that $p = x^2 + 4y^2$ for some integers x and y, with $x \equiv 1 \pmod 4$ and y is two-valued. The result for cyclotomic numbers of order four is given in Ref. [19].

For $p \equiv 1 \pmod 8$, we have

$$(0,0)_4 = \frac{p-11-6x}{16};\ \ (1,0)_4 = \frac{p-3+2x+8y}{16};$$
$$(2,0)_4 = \frac{p-3+2x}{16};\ \ (3,0)_4 = \frac{p-3+2x-8y}{16}.$$

For $p \equiv 5 \pmod 8$, we have

$$(0,0)_4 = \frac{p-7+2x}{16};\ \ (1,0)_4 = \frac{p-3-2x}{16};$$
$$(2,0)_4 = \frac{p-7+2x}{16};\ \ (3,0)_4 = \frac{p-3-2x}{16}.$$

Simple computations show that for $p \equiv 1 \pmod 8$, $(2,0)_4 > 0$ always holds. Moreover, $(1,0)_4 = 0$ and $(3,0)_4 = 0$ exclusively at $p = 17$, while $(0,0)_4 = 0$ if and only if $p = 17$ or $p = 41$. When $p \equiv 5 \pmod 8$, $(0,0)_4 = (2,0)_4 = 0$ is possible only if $p = 5$ or $p = 13$; the only prime with $(1,0)_4 = (3,0)_4 = 0$ is $p = 5$. When $(1,0)_4$, $(2,0)_4$, $(3,0)_4$, and $(4,0)_4$ are all positive, the arithmetic autocorrelation values of the sequence take all the values in $\left\{z_0^{(4,N)}, z_1^{(4,N)}, z_2^{(4,N)}, z_3^{(4,N)}\right\}$. In particular, when the prime $p \equiv 1 \pmod 4$ and $p > 41$, all four cyclotomic numbers are positive.

Lemma 2 Let p be an odd prime with $p \equiv 1 \pmod 4$, and let $\mathrm{ord}_p(N) = \frac{p-1}{4}$. Let $N \mid p-1$, then $z_0^{(4,N)} + z_2^{(4,N)} = \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$ and $z_1^{(4,N)} + z_3^{(4,N)} = -\frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$.

Proof Fix a $j \in \{1, 2, \ldots, N\}$. Since $\mathbb{Q} = D_0^{(4)} \cup D_2^{(4)}$ and $\mathbb{NQ} = D_1^{(4)} \cup D_3^{(4)}$, on the interval $I_{N,j}$, we have $M_{0,j}^{(4,N)} + M_{2,j}^{(4,N)} = \left|\mathbb{Q} \cap I_{N,j}\right|$ and $M_{1,j}^{(4,N)} + M_{3,j}^{(4,N)} = \left|\mathbb{NQ} \cap I_{N,j}\right|$. By definition of $S_{N,j}$, $S_{N,j} = \left|\mathbb{Q} \cap I_{N,j}\right| - \left|\mathbb{NQ} \cap I_{N,j}\right|$. As $N \mid p-1$, we have $\left|I_{N,j}\right| = \frac{p-1}{N}$, and hence $\left|\mathbb{Q} \cap I_{N,j}\right| + \left|\mathbb{NQ} \cap I_{N,j}\right| = \left|I_{N,j}\right| = \frac{p-1}{N}$. It follows that $\left|\mathbb{Q} \cap I_{N,j}\right| = \frac{1}{2}(\frac{p-1}{N} + S_{N,j})$, $\left|\mathbb{NQ} \cap I_{N,j}\right| = \frac{1}{2}(\frac{p-1}{N} - S_{N,j})$. Thus

$$z_0^{(4,N)} + z_2^{(4,N)} = \sum_{j=1}^{N} (M_{0,j}^{(4,N)} + M_{2,j}^{(4,N)}) \xi_N^{j-1} = \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} \frac{p-1}{N} + \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j},$$

since $1 + \xi_N + \cdots + \xi_N^{N-1} = 0$, it follows that $z_0^{(4,N)} + z_2^{(4,N)} = \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$. Similarly, $z_1^{(4,N)} + z_3^{(4,N)} = -\frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$. □

Lemma 3 Let $\mathrm{ord}_p(N) = \frac{p-1}{4}$.
(i) When $N = 4$, we have $z_0^{(4,4)} + z_2^{(4,4)} = (1-i)S_{4,1} \neq 0$ and $z_1^{(4,4)} + z_3^{(4,4)} = -(1-i)S_{4,1} \neq 0$.
(ii) When $N = 6$ and $6 \mid p-1$, we have $z_0^{(4,6)} + z_2^{(4,6)} = \frac{1}{2}(1 + \xi_6^5)(S_{6,1} - S_{6,3}) \neq 0$ and $z_1^{(4,6)} + z_3^{(4,6)} = -\frac{1}{2}(1 + \xi_6^5)(S_{6,1} - S_{6,3}) \neq 0$.
(iii) When $N = 3$, we have $z_0^{(4,3)} + z_2^{(4,3)} = \frac{3}{2}\xi_3 S_{6,3} \neq 0$ and $z_1^{(4,3)} + z_3^{(4,3)} = -\frac{3}{2}\xi_3 S_{6,3} \neq 0$.

Proof (i) When $N=4$, by Lemma 2, $z_0^{(4,4)}+z_2^{(4,4)}=\frac{1}{2}\sum_{j=1}^{4} i^{j-1}S_{4,j}$ and $z_1^{(4,4)}+z_3^{(4,4)}=-\frac{1}{2}\sum_{j=1}^{4} i^{j-1}S_{4,j}$. Since $p\equiv 1 \pmod 4$ implies $\left(\frac{-a}{p}\right)=\left(\frac{a}{p}\right)$, it follows that $S_{4,4}=S_{4,1}$ and $S_{4,3}=S_{4,2}$. Since $\sum_{j=1}^{4} S_{4,j}=0$, it follows that $S_{4,2}=-S_{4,1}$ and $S_{4,3}=-S_{4,1}$. Therefore, $z_0^{(4,4)}+z_2^{(4,4)}=(1-i)S_{4,1}$. By Eq. (4), $z_0^{(4,4)}+z_2^{(4,4)}\neq 0$. Similarly, $z_1^{(4,4)}+z_3^{(4,4)}=-(1-i)S_{4,1}\neq 0$.

(ii) When $N=6$ and $6\mid p-1$, we have $p\equiv 1 \pmod{24}$ or $p\equiv 13 \pmod{24}$. Since $p\equiv 1 \pmod 4$, we have $S_{6,6}=S_{6,1}$, $S_{6,5}=S_{6,2}$, and $S_{6,4}=S_{6,3}$. By Lemma 2,

$$z_0^{(4,6)}+z_2^{(4,6)}=\frac{1}{2}\left[(1+\xi_6^5)S_{6,1}+(\xi_6+\xi_6^4)S_{6,2}+(\xi_6^2+\xi_6^3)S_{6,3}\right].$$

Noting that $\xi_6+\xi_6^4=0$ and $\xi_6^2+\xi_6^3=-(1+\xi_6^5)$, we have $z_0^{(4,6)}+z_2^{(4,6)}=\frac{1}{2}(1+\xi_6^5)(S_{6,1}-S_{6,3})$. Eqs. (5) and (6) yields $z_0^{(4,6)}+z_2^{(4,6)}\neq 0$, and similarly $z_1^{(4,6)}+z_3^{(4,6)}\neq 0$.

(iii) Since $\mathrm{ord}_p(3)=\frac{p-1}{4}$, we have $3^{\frac{p-1}{2}}\equiv 1 \pmod p$. By Euler's criterion, $\left(\frac{3}{p}\right)=1$. On the other hand, by quadratic reciprocity, when $p\equiv 1 \pmod 4$, we have $\left(\frac{p}{3}\right)=\left(\frac{3}{p}\right)=1$, and thus $p\equiv 1 \pmod 3$. Hence $p\equiv 1 \pmod{12}$. Since $I_{3,1}=I_{6,1}\cup I_{6,2}$, $I_{3,2}=I_{6,3}\cup I_{6,4}$, and $I_{3,3}=I_{6,5}\cup I_{6,6}$, it follows that $S_{3,1}=S_{6,1}+S_{6,2}$, $S_{3,2}=S_{6,3}+S_{6,4}$, and $S_{3,3}=S_{6,5}+S_{6,6}$. By Lemma 2, we obtain

$$\begin{aligned} z_0^{(4,3)}+z_2^{(4,3)} &= \frac{1}{2}\left[(S_{6,1}+S_{6,2})+\xi_3(S_{6,3}+S_{6,4})+\xi_3^2(S_{6,5}+S_{6,6})\right] \\ &= \frac{1}{2}\left[(S_{6,1}+S_{6,2})+2\xi_3 S_{6,3}+\xi_3^2(S_{6,1}+S_{6,2})\right]. \end{aligned}$$

Since $\sum_{j=1}^{6} S_{6,j}=2(S_{6,1}+S_{6,2}+S_{6,3})=0$, we obtain $z_0^{(4,3)}+z_2^{(4,3)}=\frac{S_{6,3}}{2}(-1+2\xi_3-\xi_3^2)$. Using $1+\xi_3+\xi_3^2=0$, we obtain $z_0^{(4,3)}+z_2^{(4,3)}=\frac{3}{2}\xi_3 S_{6,3}$. From Eqs. (5) and (6), we obtain $z_0^{(4,3)}+z_2^{(4,3)}\neq 0$. A similar argument shows that $z_1^{(4,3)}+z_3^{(4,3)}\neq 0$. □

Theorem 1 *Let $p\equiv 1 \pmod 4$ be an odd prime and suppose $T=\mathrm{ord}_{p^t}(N)=\frac{p^{t-1}(p-1)}{4}$. Then there exist no N-ary sequences with ideal arithmetic autocorrelation for the connection integer p^t in any of the following cases:*
(i) *$p>17$ and $N=4$;*
(ii) *$6\mid p-1$ and $N=6$;*
(iii) *$N=3$.*

Proof When $t\geq 2$, taking the shift $\tau'=\phi(p^{t-1})=p^{t-2}(p-1)$, since $\frac{\tau'}{\mathrm{ord}_{p^t}(N)}=\frac{4}{p}<1$, we have $0<\tau'<T$. Then there exists an integer ω with $0<\omega<p$ such that $-\frac{f(1-N^{-\tau'})\bmod p^t}{p^t}=-\frac{\omega}{p}$. Thus, it suffices to prove the case where the connection integer is p.

(i) When $N=4$, since $\mathrm{ord}_p(4)=\frac{p-1}{4}$, we have $2^{\frac{p-1}{2}}\equiv 1 \pmod p$. By Euler's criterion, $\left(\frac{2}{p}\right)=1$, thus $p\equiv 1 \pmod 8$. By Corollary 1 and Lemma 3 (i), it suffices to consider only the cases $p=17$ and $p=41$, as all other cases fail to exhibit ideal arithmetic autocorrelation. When $p=41$, by Eq. (11), calculations yield $z_0^{(4,4)}=1-i$, $z_1^{(4,4)}=-3+3i$, $z_2^{(4,4)}=3-3i$ and $z_3^{(4,4)}=-1+i$. Consequently, the sequence also fails to exhibit ideal arithmetic autocorrelation at this value.

(ii) When $N = 6$ and $6 \mid p-1$, we have $p \equiv 1 (\mathrm{mod}\, 12)$. By Corollary 1 and Lemma 3 (ii), it suffices to consider only the case $p = 13$, as all other cases fail to exhibit ideal arithmetic autocorrelation. However, since $\mathrm{ord}_{13}(6) = 12$, $p = 13$ is excluded from our consideration.

(iii) When $N = 3$, we have $p \equiv 1 (\mathrm{mod}\, 12)$. By Corollary 1 and Lemma 3 (iii), it suffices to consider only the case $p = 13$, as all other cases fail to exhibit ideal arithmetic autocorrelation. When $p = 13$, by Eq. (11), calculations yield $z_0^{(4,3)} = \frac{3}{2} - \frac{\sqrt{3}}{2}i$, $z_1^{(4,3)} = \sqrt{3}i$, $z_2^{(4,3)} = -\sqrt{3}i$ and $z_3^{(4,3)} = -\frac{3}{2} + \frac{\sqrt{3}}{2}i$. Consequently, the sequence also fails to exhibit ideal arithmetic autocorrelation at this value.

This completes the proof. □

Corollary 2 Let q be an odd composite integer, and let $p \mid q$ be an odd prime divisor. Assume that $\mathrm{ord}_q(N) = \frac{\phi(q)}{4}$ and $\mathrm{ord}_p(N) = \frac{p-1}{4}$. If there exists a nontrivial shift τ such that $\frac{q}{p} \mid (N^{-\tau} - 1)$ and $q \nmid (N^{-\tau} - 1)$, then there exist no N-ary sequences with ideal arithmetic autocorrelation for the connection integer q satisfying the condition in Theorem 1.

Corollary 3 Let $p \equiv 1 \pmod 4$ be an odd prime, and suppose $\mathrm{ord}_p(N) = \frac{p-1}{4}$. If $p > 41$, then whenever $N = 3$, $N = 4$, or $N = 6$ with $6 \mid p-1$, the corresponding N-ary sequences with connection integer p fail to have ideal arithmetic crosscorrelation.

Example 1 When $p = 17$ and $N = 4$, $\mathrm{ord}_{17}(4) = 4$. Taking $g = 3$ as a primitive root modulo 17, the cyclotomic classes of order four modulo 17 are:

$$D_0^{(4)} = \{1, 4, 13, 16\}, \qquad D_1^{(4)} = \{3, 5, 12, 14\},$$
$$D_2^{(4)} = \{2, 8, 9, 15\}, \qquad D_3^{(4)} = \{6, 7, 10, 11\}.$$

According to Eq. (11), $z_0^{(4,4)} = 2-2i$, $z_1^{(4,4)} = 0$, $z_2^{(4,4)} = 0$, and $z_3^{(4,4)} = 2i-2$ are calculated. And $1 - 4^{-1} \equiv 5 \in D_1^{(4)}$, $1 - 4^{-2} \equiv 2 \in D_2^{(4)}$, $1 - 4^{-3} \equiv 14 \in D_1^{(4)}$. Thus, the arithmetic autocorrelation values at $\tau = 1, 2, 3$ are:

$$(z_1^{(4,4)}, z_2^{(4,4)}, z_1^{(4,4)}) = (0, 0, 0) \quad \text{if} \quad f \in D_0^{(4)};$$
$$(z_2^{(4,4)}, z_3^{(4,4)}, z_2^{(4,4)}) = (0, 2i-2, 0) \quad \text{if} \quad f \in D_1^{(4)};$$
$$(z_3^{(4,4)}, z_0^{(4,4)}, z_3^{(4,4)}) = (2i-2, 2-2i, 2i-2) \quad \text{if} \quad f \in D_2^{(4)};$$
$$(z_0^{(4,4)}, z_1^{(4,4)}, z_0^{(4,4)}) = (2-2i, 0, 2-2i) \quad \text{if} \quad f \in D_3^{(4)}.$$

Hence, for $p = 17$, the sequence has ideal arithmetic autocorrelation if and only if $f \in D_0^{(4)} = \{1, 4, 13, 16\}$. However, this does not imply that sequences whose connection integer is a power of 17 have ideal arithmetic autocorrelation.

4 On the non-existence of ideal arithmetic correlations for sequence families when $\mathrm{ord}_q(N) = \frac{\phi(q)}{6}$ or $\frac{\phi(q)}{8}$

Let p be an odd prime, when $\mathrm{ord}_p(N) = \frac{p-1}{6}$, let g be a primitive root modulo p. In this case, we have $\mathbb{F}_p^* = D_0^{(6)} \cup D_1^{(6)} \cup D_2^{(6)} \cup D_3^{(6)} \cup D_4^{(6)} \cup D_5^{(6)}$, $\mathbb{Q} = D_0^{(6)} \cup D_2^{(6)} \cup D_4^{(6)}$

and $\mathbb{NQ} = D_1^{(6)} \cup D_3^{(6)} \cup D_5^{(6)}$. Here we consider the arithmetic correlations of a family of sequences with the connection integer p.

Lemma 4 Let the N-adic numbers associated with the sequences $\mathcal{S}$ and $\mathcal{T}$ be $-\frac{f}{p}$ and $-\frac{g}{p}$, respectively, where $0 < f < p$ and $0 < g < p$. Then, for $\mathcal{S} \neq \mathcal{T}^{(\tau)}$, the set of possible values of the arithmetic correlations of $\mathcal{S}$ and $\mathcal{T}$ is $\left\{z_0^{(6,N)}, z_1^{(6,N)}, z_2^{(6,N)}, z_3^{(6,N)}, z_4^{(6,N)}, z_5^{(6,N)}\right\}$, and each of these values is attained.

Proof As f and g run through all values satisfying $0 < f, g < p$, it is clear that $\left(f - gN^{-\tau}\right) \bmod p$ exhausts the set $D_i^{(6)}$ for $i = 0, 1, \ldots, 5$. □

Lemma 5 Let p be an odd prime with $p \equiv 1 \pmod 6$, and let $\mathrm{ord}_p(N) = \frac{p-1}{6}$. Let $N \mid p-1$, then $z_0^{(6,N)} + z_2^{(6,N)} + z_4^{(6,N)} = \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$ and $z_1^{(6,N)} + z_3^{(6,N)} + z_5^{(6,N)} = -\frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$.

Proof Fix a $j \in \{1, 2, \ldots, N\}$. Since $\mathbb{Q} = D_0^{(6)} \cup D_2^{(6)} \cup D_4^{(6)}$ and $\mathbb{NQ} = D_1^{(6)} \cup D_3^{(6)} \cup D_5^{(6)}$, on the interval $I_{N,j}$. By definition of $S_{N,j}$, $S_{N,j} = (M_{0,j}^{(6,N)} + M_{2,j}^{(6,N)} + M_{4,j}^{(6,N)}) - (M_{1,j}^{(6,N)} + M_{3,j}^{(6,N)} + M_{5,j}^{(6,N)})$. On the other hand, $\left|I_{N,j}\right| = (M_{0,j}^{(6,N)} + M_{2,j}^{(6,N)} + M_{4,j}^{(6,N)}) + (M_{1,j}^{(6,N)} + M_{3,j}^{(6,N)} + M_{5,j}^{(6,N)})$. Then we have $M_{0,j}^{(6,N)} + M_{2,j}^{(6,N)} + M_{4,j}^{(6,N)} = \frac{S_{N,j} + |I_{N,j}|}{2}$ and $M_{1,j}^{(6,N)} + M_{3,j}^{(6,N)} + M_{5,j}^{(6,N)} = \frac{|I_{N,j}| - S_{N,j}}{2}$. As $N \mid p-1$, we have $\left|I_{N,j}\right| = \frac{p-1}{N}$. Since $1 + \xi_N + \cdots + \xi_N^{N-1} = 0$, it follows that $z_0^{(6,N)} + z_2^{(6,N)} + z_4^{(6,N)} = \frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$ and $z_1^{(6,N)} + z_3^{(6,N)} + z_5^{(6,N)} = -\frac{1}{2}\sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}$. □

Lemma 6 Let $\mathrm{ord}_p(N) = \frac{p-1}{6}$.
(i) When $N = 6$, we have $z_0^{(6,6)} + z_2^{(6,6)} + z_4^{(6,6)} \neq 0$.
(ii) When $N = 4$ and $4 \mid p-1$, we have $z_0^{(6,4)} + z_2^{(6,4)} + z_4^{(6,4)} \neq 0$.

Proof (i) Let $N = 6$.
Case 1: When $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $S_{6,6} = S_{6,1}$, $S_{6,5} = S_{6,2}$, and $S_{6,4} = S_{6,3}$. In this case, $p \equiv 1 \pmod{24}$ or $p \equiv 13 \pmod{24}$ and $\sum_{j=1}^{6} \xi_6^{j-1} S_{6,j} = (1 + \xi_6^5) S_{6,1} + (\xi_6 + \xi_6^4) S_{6,2} + (\xi_6^2 + \xi_6^3) S_{6,3}$. Since $\xi_6 + \xi_6^4 = 0$ and $\xi_6^2 + \xi_6^3 = -(1 + \xi_6^5)$, Eqs. (5) and (6) yields $\sum_{j=1}^{6} \xi_6^{j-1} S_{6,j} \neq 0$. By Lemma 5, we have $z_0^{(6,6)} + z_2^{(6,6)} + z_4^{(6,6)} \neq 0$.
Case 2: When $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $S_{6,6} = -S_{6,1}$, $S_{6,5} = -S_{6,2}$, and $S_{6,4} = -S_{6,3}$. In this case, $p \equiv 7 \pmod{24}$ or $p \equiv 19 \pmod{24}$ and $\sum_{j=1}^{6} \xi_6^{j-1} S_{6,j} = (1 - \xi_6^5) S_{6,1} + (\xi_6 - \xi_6^4) S_{6,2} + (\xi_6^2 - \xi_6^3) S_{6,3}$. Since $1 - \xi_6^5 = \xi_6$, $\xi_6 - \xi_6^4 = 2\xi_6$ and $\xi_6^2 - \xi_6^3 = \xi_6$,

we have $\sum_{j=1}^{6}\xi_6^{j-1}S_{6,j}=\xi_6(S_{6,1}+S_{6,3}+2S_{6,2})$. Eqs. (8) and (9) yields $\sum_{j=1}^{6}\xi_6^{j-1}S_{6,j}\neq 0$. By Lemma 5, we have $z_0^{(6,6)}+z_2^{(6,6)}+z_4^{(6,6)}\neq 0$.

(ii) When $N=4$ and $4\mid p-1$, by Lemma 5, $z_0^{(6,4)}+z_2^{(6,4)}+z_4^{(6,4)}=\frac{1}{2}(S_{4,1}+iS_{4,2}-S_{4,3}-iS_{4,4})$. Since $p\equiv 1 \pmod 4$, it follows that $S_{4,4}=S_{4,1}$ and $S_{4,3}=S_{4,2}$, then $z_0^{(6,4)}+z_2^{(6,4)}+z_4^{(6,4)}=\frac{1-i}{2}(S_{4,1}-S_{4,2})$. On the other hand, $S_{2,1}=S_{4,1}+S_{4,2}$. By Eq. (4), $S_{4,2}=-S_{4,1}$. Again by Eq. (4), we have $z_0^{(6,4)}+z_2^{(6,4)}+z_4^{(6,4)}\neq 0$.

The proof is complete. □

Lemma 7 Let p be an odd prime, $N>2$ be an integer, and $p\equiv 1 \pmod N$. If $S_{N,j}=0$ for $j=1,\ldots,N$, then the following cases cannot occur:
(i) $p\equiv 3 \pmod 4$ and $N>2$;
(ii) $p\equiv 1 \pmod 4$ and $3\mid N$;
(iii) $p\equiv 1 \pmod 4$ and $4\mid N$.

Proof The proof can be seen in Theorem 1 of [14]. □

Theorem 2 *Let $p\equiv 1 \pmod 6$ be an odd prime and $\mathrm{ord}_p(N)=\frac{p-1}{6}$. Then there exist no N-ary sequences with ideal arithmetic correlations for the connection integer p in any of the following cases:*
(i) $4\mid p-1$ *and* $N=4$;
(ii) $N=6$;
(iii) $N=3$;
(iv) $p\equiv 7 \pmod{12}$ *and* $N>2$ *is a prime.*

Proof It follows from Lemmas 4 and 6 that (i)(ii) hold.

When $N>2$ is a prime, suppose the sequences whose connection integer is p have ideal arithmetic correlation properties. Then by Lemma 4, $z_0^{(6,4)}=z_1^{(6,4)}=z_2^{(6,4)}=z_3^{(6,4)}=z_4^{(6,4)}=z_5^{(6,4)}=0$. That is $\sum_{j=1}^{N}M_{l,j}^{(6,N)}\xi_N^{j-1}=0$ for $l=0,1,2,3,4,5$. Since N is prime, the minimal polynomial of ξ_N is $\Phi(x)=1+x+x^2+\cdots+x^{N-1}$ [20]. Since $\Phi(x)$ has degree $N-1$, $P_l(x)=\sum_{j=1}^{N}M_{l,j}^{(6,N)}x^{j-1}$ has degree at most $N-1$, and $\Phi(x)\mid P_l(x)$, it follows that $P_l(x)=c_l\Phi(x)$ for some constant c_l. Hence

$$M_{l,1}^{(6,N)}=M_{l,2}^{(6,N)}=\cdots=M_{l,N}^{(6,N)}.$$

Moreover, since $\sum_{j=1}^{N}M_{l,j}^{(6,N)}=\left|D_l^{(6)}\right|=\frac{p-1}{6}$, we obtain $M_{l,j}=\frac{p-1}{6N}$ for $0\le l\le 5$ and $1\le j\le N$. For each interval $I_{N,j}$, we have

$$\left|\mathbb{Q}\cap I_{N,j}\right|=\left|(D_0^{(6)}+D_2^{(6)}+D_4^{(6)})\cap I_{N,j}\right|=M_{0,j}^{(6,N)}+M_{2,j}^{(6,N)}+M_{4,j}^{(6,N)}=\frac{p-1}{2N},$$

and

$$\left|\mathbb{NQ}\cap I_{N,j}\right|=\left|(D_1^{(6)}+D_3^{(6)}+D_5^{(6)})\cap I_{N,j}\right|=M_{1,j}^{(6,N)}+M_{3,j}^{(6,N)}+M_{5,j}^{(6,N)}=\frac{p-1}{2N},$$

Thus

$$S_{N,j}=\sum_{a\in I_{N,j}}\left(\frac{a}{p}\right)=\left|\mathbb{Q}\cap I_{N,j}\right|-\left|\mathbb{NQ}\cap I_{N,j}\right|=0$$

for $j = 1, 2, \ldots, N$. By Lemma 7, when $p \equiv 7 \pmod{12}$ and $N > 2$, or $p \equiv 1 \pmod{12}$ and $N = 3$, this is impossible, leading to a contradiction. This completes the proof. □

Using a similar method, we rule out the existence of such sequences when $\mathrm{ord}_p(N) = \frac{p-1}{8}$.

Theorem 3 *Let $p \equiv 1 \pmod 8$ be an odd prime and suppose $\mathrm{ord}_p(N) = \frac{p-1}{8}$. Then there exist no N-ary sequences with ideal arithmetic correlations for the connection integer p in any of the following cases:*
(i) $N = 4$;
(ii) $6 \mid p-1$ *and* $N = 6$;
(iii) $N = 3$.

Proof Let

$$E = z_0^{(8,N)} + z_2^{(8,N)} + z_4^{(8,N)} + z_6^{(8,N)}.$$

Since $D_0^{(8)} \cup D_2^{(8)} \cup D_4^{(8)} \cup D_6^{(8)}$ is exactly the set of quadratic residues modulo p, when $N \mid p-1$, we have

$$E = \frac{1}{2} \sum_{j=1}^{N} \xi_N^{j-1} S_{N,j}.$$

Similar to the proofs of Lemma 3, combined with Lemma 4, this yields the desired result. □

By Lemma 4 and considering the arithmetic autocorrelation of the sequence family, we obtain similar results.

Corollary 4 Let $d = 6$ or 8, let $t \geq 2$, and assume that $\mathrm{ord}_{p^t}(N) = p^{t-1} \times \frac{p-1}{d}$. Then the sequence family with connection integer p^t and satisfying the conditions in Theorems 2 and 3 cannot have ideal arithmetic autocorrelation.

For composite q, let $d \in \{6, 8\}$, and let $p \mid q$ be an odd prime divisor. Assume that $\mathrm{ord}_q(N) = \frac{\phi(q)}{d}$ and $\mathrm{ord}_p(N) = \frac{p-1}{d}$. If there exists a nontrivial shift τ such that $\frac{q}{p} \mid (N^{-\tau} - 1)$ and $q \nmid (N^{-\tau} - 1)$, then the corresponding sequence families with connection integer q fails to have ideal arithmetic autocorrelation, provided that the corresponding families with connection integer p is already ruled out by Theorems 2 or 3.

5 Arithmetic correlation bounds for N-ary FCSR sequences

Let $N \geq 2$ be a fixed integer, q be a positive integer, and assume $\gcd(N, q) = 1$. Let $T = \mathrm{ord}_q(N)$, that is the multiplicative order of N modulo q.

Let $\mathcal{S} = (s_i)_{i \geq 0}$ and $\mathcal{T} = (t_i)_{i \geq 0}$ be two periodic N-ary FCSR sequences with entries in $\{0, 1, \ldots, N-1\}$ and with the same connection integer q, and correspond to the rational numbers $\alpha = -\frac{f}{q}$ and $\beta = -\frac{g}{q}$, respectively, where $0 < f, g < q$ and

$\gcd(f,q) = \gcd(g,q) = 1$. For a shift $\tau \geq 0$, denote $\mathcal{T}^{(\tau)} = (t_{i+\tau})_{i\geq 0}$, and associate with $\beta^{(\tau)} = -\frac{g_\tau}{q}$. Then $g_\tau \equiv N^{-\tau} g \pmod{q}$. By Eq. (3), when $\mathcal{S} \neq \mathcal{T}^{(\tau)}$, we have $f \neq g_\tau$, let

$$d = \gcd(f - g_\tau, q), \qquad m = \frac{q}{d}, \qquad h = \frac{f - g_\tau}{d}.$$

Take $\widetilde{h}$ as the positive representative of h modulo m, that is,

$$\widetilde{h} \equiv h \pmod{m}, \qquad 0 < \widetilde{h} < m.$$

Then $\gcd(\widetilde{h}, m) = 1$, and the periodic part of the difference sequence corresponds to the rational number $-\frac{\widetilde{h}}{m}$. Its minimal period is $L = \mathrm{ord}_m(N)$. Since $m \mid q$, we have $L \mid T$. Therefore, the arithmetic correlation of length T consists of $\frac{T}{L}$ repetitions of a periodic difference sequence of length L. Let $A_m \equiv -m^{-1} \pmod{N}$. From Eq. (1), the coefficient sequence $\mathcal{U}$ of the rational number $-\frac{\widetilde{h}}{m}$ satisfies

$$u_i \equiv A_m\big(\widetilde{h}N^{-i} \bmod m\big) \pmod{N}, \qquad 0 \leq i < L. \tag{12}$$

Here $\widetilde{h}N^{-i} \bmod m$ takes the unique representative modulo m satisfying $1 \leq x \leq m-1$.

Assume $\gcd(N, m) = 1$, let

$$H_m = \big\{N^i (\bmod m) : 0 \leq i < \mathrm{ord}_m(N)\big\} \subseteq \mathbb{Z}_m^*,$$

where $\mathbb{Z}_m$ denotes the ring of residue classes modulo m and $\mathbb{Z}_m^*$ denotes the set of elements coprime to m. And

$$\widetilde{h}H_m = \Big\{\widetilde{h}N^i (\bmod m) : 0 \leq i < \mathrm{ord}_m(N)\Big\} \subseteq \mathbb{Z}_m^*.$$

In the sequel, for functions $f(m)$ and $g(m)$, we write

$$f(m) \ll_N g(m) \quad \text{or} \quad f(m) = O_N(g(m))$$

to indicate that $|f(m)| \leq C(N)g(m)$ for some constant $C(N)$ depending only on the fixed integer N.

Define

$$\Lambda_E = \Big|\Big\{0 \leq i < L : A_m\big(\widetilde{h}N^{-i} \bmod m\big) \bmod N \in E\Big\}\Big|.$$

Lemma 8 Assume $0 < \widetilde{h} < m$ and $\gcd(\widetilde{h}, m) = 1$, and let $A_m \in \mathbb{Z}_N^*$ be an arbitrary invertible coefficient. For any set $E \subseteq \mathbb{Z}_N$, we have

$$\left|\Lambda_E - \frac{|E|L}{N}\right| \ll_N \frac{m(1 + \ln m)}{\sqrt{p_m}},$$

where p_m be the smallest prime factor of m.

Proof As i ranges over $0 \le i < L$, N^{-i} traverse H_m, hence $\widetilde{h}N^{-i} \bmod m$ traverses the coset $\widetilde{h}H_m$. Let $E' = A_m^{-1}E \subseteq \mathbb{Z}_N$. Since $A_m \in \mathbb{Z}_N^*$, multiplication by A_m is a permutation on $\mathbb{Z}_N$, so $|E'| = |E|$. Thus

$$\Lambda_E = \left|\{x \in \widetilde{h}H_m : x \bmod N \in E'\}\right|.$$

Define in the integer interval

$$I(E') = \{1 \le x \le m-1 : x \bmod N \in E'\},$$

then

$$\Lambda_E = \sum_{x \in I(E')} \mathbf{1}_{\widetilde{h}H_m}(x),$$

where $\mathbf{1}_{\widetilde{h}H_m}$ denotes the indicator function of the coset $\widetilde{h}H_m$, so that $\mathbf{1}_{\widetilde{h}H_m}(x) = 1$ if $x \in \widetilde{h}H_m$ and 0 otherwise. Using additive character orthogonality,

$$\mathbf{1}_{\widetilde{h}H_m}(x) = \frac{1}{m}\sum_{y=0}^{L-1}\sum_{c=0}^{m-1} e_m(c(x - \widetilde{h}N^y)),$$

where $e_m(z) = \exp(2\pi iz/m)$. Therefore,

$$\Lambda_E = \frac{1}{m}\sum_{c=0}^{m-1}\left(\sum_{x \in I(E')} e_m(cx)\right)\left(\sum_{y=0}^{L-1} e_m(-c\widetilde{h}N^y)\right).$$

Denote $A_E(c) = \sum_{x \in I(E')} e_m(cx)$ and $B_{\widetilde{h}}(c) = \sum_{y=0}^{L-1} e_m(-c\widetilde{h}N^y)$.

When $c = 0$, we have $A_E(0) = |I(E')|$ and $B_{\widetilde{h}}(0) = L$, then $\frac{1}{m}A_E(0)B_{\widetilde{h}}(0) = \frac{|I(E')|L}{m}$. Since $I(E')$ is the set of integers in $1, \ldots, m-1$ falling into $|E|$ residue classes modulo N, and N is fixed, we have

$$|I(E')| = \frac{|E|m}{N} + O_N(1).$$

Therefore $\frac{|I(E')|L}{m} = \frac{|E|L}{N} + O_N\left(\frac{L}{m}\right)$. As $L \le \phi(m) \le m$, it follows that $\frac{L}{m} = O(1)$, so $O_N\left(\frac{L}{m}\right) = O_N(1)$. Thus,

$$\Lambda_E - \frac{|E|L}{N} = \frac{1}{m}\sum_{c=1}^{m-1} A_E(c)B_{\widetilde{h}}(c) + O_N(1). \tag{13}$$

For $1 \le c \le m-1$, by the subgroup exponential sum estimate [21], we have

$$|B_{\widetilde{h}}(c)| = \left|\sum_{y=0}^{L-1} e_m(-c\widetilde{h}N^y)\right| \le (\nu m)^{\frac{1}{2}}, \tag{14}$$

where $\nu = \frac{m}{p_m}$ and p_m is the smallest prime divisor of m. Since $\nu = \frac{m}{p_m}$, we have

$$(\nu m)^{1/2} = \frac{m}{\sqrt{p_m}}. \tag{15}$$

On the other hand, write E' as $E' = \{r_1, \ldots, r_s\}$, then $s = |E|$. Then

$$A_E(c) = \sum_{r \in E'} A_r(c),$$

where

$$A_r(c) = \sum_{\substack{1 \le x \le m-1 \\ x \equiv r \pmod N}} e_m(cx).$$

By geometric series estimation [21], we have

$$\sum_{c=1}^{m-1} |A_r(c)| \le m(1+\ln m).$$

Therefore,

$$\sum_{c=1}^{m-1} |A_E(c)| \le \sum_{r\in E'} \sum_{c=1}^{m-1} |A_r(c)| \le |E| m(1+\ln m). \tag{16}$$

Combining (13), (14), (15), and (16), we get

$$\begin{aligned}\left|\Lambda_E - \frac{|E|L}{N}\right| &\le \frac{1}{m}\sum_{c=1}^{m-1} |A_E(c)||B_{\widetilde{h}}(c)| + O_N(1)\\ &\le \frac{1}{m}\frac{m}{\sqrt{p_m}}\sum_{c=1}^{m-1} |A_E(c)| + O_N(1)\\ &\le \frac{1}{m}\frac{m}{\sqrt{p_m}}|E|m(1+\ln m) + O_N(1)\\ &= |E|\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1).\end{aligned}$$

Since $|E| \le N$ and N is fixed, we obtain

$$\left|\Lambda_E - \frac{|E|L}{N}\right| \ll_N \frac{m(1+\ln m)}{\sqrt{p_m}}.$$

This completes the proof. □

By Lemma 8, setting $E = E_k = \{0, 1, \ldots, k-1\}$ with $1 \le k \le N-1$ yields

$$\left|\Lambda_{E_k} - \frac{kL}{N}\right| \le k\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1), \tag{17}$$

Combining this with the fact that $k \le N-1$ implies

$$\left|\Lambda_{E_k} - \frac{kL}{N}\right| \le (N-1)\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1), \qquad 1 \le k \le N-1. \tag{18}$$

Let $\xi_N = e^{2\pi i/N}$. Let $M_0, M_1, \ldots, M_{N-1}$ be the frequencies of occurrence of symbols $j = 0, 1, \ldots, N-1$ in the difference sequence of the periodic part, where the periodic part has length $L = \mathrm{ord}_m(N)$. We have $\sum_{j=0}^{N-1} M_j = L$. Define

$$C_L = \sum_{j=0}^{N-1} M_j \xi_N^j.$$

For $1 \le k \le N-1$, we have

$$\Lambda_{E_k} = \sum_{j=0}^{k-1} M_j.$$

Define the deviation of each M_j as

$$\delta_j = M_j - \frac{L}{N}, \qquad 0 \le j \le N-1,$$

and let the total deviation of the first k values be

$$\Delta_k = \sum_{j=0}^{k-1} \delta_j.$$

The following lemma shows that taking $E = E_k = \{0, \dots, k-1\}$ is natural.

Lemma 9 Assume $\Delta_0 = \Delta_N = 0$. If $|\Delta_k| \le D$ for all $1 \le k \le N-1$ with some $D \ge 0$, then

$$|C_L| \le 2(N-1) \sin \frac{\pi}{N} D.$$

Proof By the definition of δ_j, we have $\sum_{j=0}^{N-1} \delta_j = \sum_{j=0}^{N-1} M_j - L = 0$. Since $\sum_{j=0}^{N-1} \xi_N^j = 0$, we have

$$C_L = \sum_{j=0}^{N-1} M_j \xi_N^j = \sum_{j=0}^{N-1} \left(\frac{L}{N} + \delta_j \right) \xi_N^j = \sum_{j=0}^{N-1} \delta_j \xi_N^j.$$

On the other hand, $\Delta_k = \sum_{j=0}^{k-1} \delta_j$, so $\delta_j = \Delta_{j+1} - \Delta_j$. Therefore,

$$C_L = \sum_{j=0}^{N-1} (\Delta_{j+1} - \Delta_j) \xi_N^j = \sum_{j=0}^{N-1} \Delta_{j+1} \xi_N^j - \sum_{j=0}^{N-1} \Delta_j \xi_N^j.$$

For the first term, let $r = j+1$, yielding $\sum_{j=0}^{N-1} \Delta_{j+1} \xi_N^j = \sum_{r=1}^{N} \Delta_r \xi_N^{r-1}$. Thus,

$$C_L = \sum_{r=1}^{N} \Delta_r \xi_N^{r-1} - \sum_{r=0}^{N-1} \Delta_r \xi_N^r.$$

Since $\Delta_0 = \Delta_N = 0$, the boundary terms vanish, giving

$$C_L = \sum_{r=1}^{N-1} \Delta_r \left(\xi_N^{r-1} - \xi_N^r \right).$$

Hence,

$$\begin{aligned} |C_L| &\le \sum_{r=1}^{N-1} |\Delta_r| \left| \xi_N^{r-1} - \xi_N^r \right| \\ &= \sum_{r=1}^{N-1} |\Delta_r| \left| \xi_N^{r-1} (1 - \xi_N) \right| \\ &= |1 - \xi_N| \sum_{r=1}^{N-1} |\Delta_r|. \end{aligned}$$

Moreover, $|1-\xi_N| = 2|\sin\frac{\pi}{N}| = 2\sin\frac{\pi}{N}$, hence

$$|C_L| \le 2\sin\frac{\pi}{N}\sum_{r=1}^{N-1}|\Delta_r|.$$

If $|\Delta_r| \le D$ for all $1 \le r \le N-1$, then

$$|C_L| \le 2(N-1)\sin\frac{\pi}{N}D.$$

This completes the proof. □

Since the arithmetic correlation is summed over the original period $T = \mathrm{ord}_q(N)$, while the reduced difference sequence has period $L = \mathrm{ord}_m(N)$, we need to compare T/L.

Lemma 10 Assume $m \mid q$ and $\gcd(N,q) = 1$. Let $T = \mathrm{ord}_q(N)$ and $L = \mathrm{ord}_m(N)$. Then $L \mid T$ and

$$\frac{T}{L} \le \frac{q}{m}.$$

Proof The proof is similar to that of Lemma 3 in [15] and is omitted here. □

Next, we present an upper bound on the arithmetic correlation of N-ary sequences, which generalizes Theorem 1 in [15].

Theorem 4 *Let $N \ge 2$ be fixed, q be a positive integer, and $\gcd(N,q) = 1$. Let p_q be the smallest prime factor of q. Let $\mathcal{S} = (s_i)_{i\ge 0}$ and $\mathcal{T} = (t_i)_{i\ge 0}$ be two N-ary periodic FCSR sequences with the same connection integer q, then the N-ary arithmetic correlation of $\mathcal{S}$ and $\mathcal{T}$ at shift τ satisfies*

$$\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| \ll_N \frac{q\ln q}{\sqrt{p_q}}.$$

More explicitly, it can be written as

$$\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| \le 2(N-1)^2\sin\frac{\pi}{N}\frac{q(1+\ln q)}{\sqrt{p_q}} + O_N\left(\frac{q}{p_q}\right).$$

Proof Since the trivial bound gives $\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| \le \mathrm{ord}_q(N)$, we may assume $\frac{q\ln q}{\sqrt{p_q}} \ll_N \mathrm{ord}_q(N)$. Let $\mathcal{S}$ and $\mathcal{T}^{(\tau)}$ be associated with rational numbers $\alpha = -\frac{f}{q}$ and $\beta^{(\tau)} = -\frac{g_\tau}{q}$, respectively, where $0 < f, g_\tau < q$ and $\gcd(fg_\tau, q) = 1$. When $\mathcal{S} \ne \mathcal{T}^{(\tau)}$, set $d = \gcd(f-g_\tau, q)$, $m = \frac{q}{d}$ and $h = \frac{f-g_\tau}{d}$. Then the periodic part of the difference sequence corresponds to $-\frac{\widetilde{h}}{m}$, where $\widetilde{h} \equiv h \pmod m$ and $0 < \widetilde{h} < m$.

Define $\Delta_0 = 0$. For $1 \le k \le N-1$, since

$$\Delta_k = \sum_{j=0}^{k-1}\delta_j = \sum_{j=0}^{k-1}M_j - \frac{kL}{N} = \Lambda_{E_k} - \frac{kL}{N},$$

Eq. (18) gives

$$|\Delta_k| \le (N-1)\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1),$$

where p_m be the smallest prime factor of m. When $k = N$, we have $E_N = \{0, 1, \ldots, N-1\}$ and the corresponding count $\Lambda_{E_N} = L$; hence $\Delta_N = \Lambda_{E_N} - L = 0$. Therefore, by Lemma 9, we have

$$\begin{aligned} |C_L| &\le 2(N-1)\sin\frac{\pi}{N}\left((N-1)\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1)\right) \\ &= 2(N-1)^2\sin\frac{\pi}{N}\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1). \end{aligned} \tag{19}$$

But $\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)$ is summed over the full period $T = \mathrm{ord}_q(N)$, while the period of the difference sequence is $L = \mathrm{ord}_m(N)$. Since $L \mid T$, the arithmetic correlation sum of length T is exactly T/L repetitions of the period sum of length L. Thus,

$$\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| = \frac{T}{L}\left|C_L\right|.$$

From Lemma 10 and Eq. (19), we obtain

$$\begin{aligned} \left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| &\le \frac{q}{m}\left(2(N-1)^2\sin\frac{\pi}{N}\frac{m(1+\ln m)}{\sqrt{p_m}} + O_N(1)\right) \\ &= 2(N-1)^2\sin\frac{\pi}{N}\frac{q(1+\ln m)}{\sqrt{p_m}} + O_N\left(\frac{q}{m}\right). \end{aligned}$$

Since $m \mid q$, then $p_m \ge p_q$. So $\frac{1}{\sqrt{p_m}} \le \frac{1}{\sqrt{p_q}}$. Also, $m \le q$ implies $1+\ln m \le 1+\ln q$. Therefore, since $m = \frac{q}{\gcd(f-g_\tau, q)}$ and $m > 1$, we have

$$\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| \le 2(N-1)^2\sin\frac{\pi}{N}\frac{q(1+\ln q)}{\sqrt{p_q}} + O_N\left(\frac{q}{p_q}\right).$$

Thus

$$\left|\mathcal{C}^A_{\mathcal{S},\mathcal{T}}(\tau)\right| \ll_N \frac{q\ln q}{\sqrt{p_q}}.$$

This completes the proof. □

Since $\mathrm{ord}_q(N) \le \phi(q) < q$, if q has a very small prime factor, the estimate is usually greater than the trivial bound and thus cannot be called non-trivial. Therefore, the method is truly effective when q is prime, or when the smallest prime factor p_q of q is large and $\mathrm{ord}_q(N)$ is sufficiently large.

6 Conclusion

In this paper, we studied the nonexistence of N-ary sequences with ideal arithmetic correlations. We obtained several nonexistence results in the cases $\mathrm{ord}_{p^t}(N) = \phi(p^t)/4$, $\mathrm{ord}_{p^t}(N) = \phi(p^t)/6$ and $\mathrm{ord}_{p^t}(N) = \phi(p^t)/8$, excluding in particular the 3-ary, 4-ary, and 6-ary cases, and we also proved a nonexistence result for prime $N > 2$ when $p \equiv 7 \pmod{12}$ and $\mathrm{ord}_{p^t}(N) = \phi(p^t)/6$. These results highlight the strong constraints imposed by ideal arithmetic correlation in the N-ary setting. We have also established a non-trivial upper bound on the arithmetic correlation of N-ary sequences, generalizing the result for binary sequences and showing that it applies when the smallest prime factor p_q of q is sufficiently large. It would be of interest to investigate whether similar nonexistence phenomena hold under other order conditions or for more general classes of connection integers.

Declarations

- Funding
  This work is supported by the National Natural Science Foundation of China (No. 62272420), Natural Science Foundation of Fujian Province (No. 2023J01535), Fujian Key Laboratory of Financial Information Processing (Putian University) (NO. JXJS202502).
- 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] Golomb, S.W.: Shift Register Sequences. Aegean Park Press, Laguna Hills, CA (1967)

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

[4] Klapper, A., Goresky, M.: Feedback shift registers, 2-adic span, and combiners with memory. Journal of Cryptology **10**(2), 111–147 (1997)

[5] Klapper, A., Xu, J.Z.: Algebraic feedback shift registers. Theoretical Computer Science **226**(1-2), 61–92 (1999)

[6] Mandelbaum, D.: Arithmetic codes with large distance. IEEE Transactions on Information Theory **13**(2), 237–242 (1967)

[7] Goresky, M., Klapper, A.: Arithmetic crosscorrelations of feedback with carry shift register sequences. IEEE Transactions on Information Theory **43**(4), 1342–1345 (1997)

[8] Chen, Z.X., Niu, Z.H., Sang, Y.Q., Wu, C.H.: Arithmetic autocorrelation of binary m-sequences. Cryptologia **47**(5), 449–458 (2023)

[9] Jing, X.Y., Zhang, A.X., Feng, K.Q.: Arithmetic autocorrelation distribution of binary m-sequences. IEEE Transactions on Information Theory **69**(9), 6040–6047 (2023)

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

[11] Jing, X.Y., Chen, Z.X., Feng, K.Q.: On arithmetic autocorrelation of p-ary m-sequences. Advances in Mathematics of Communications **19**(5), 1518–1538 (2025)

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

[13] Xiao, L.M., Edemskiy, V.: Arithmetic Autocorrelation of Certain Binary Half-ℓ-Sequences. In: International Conference on Information Security and Cryptology. Springer, Singapore (2025)

[14] Edemskiy, V.: Notes about imbalance and arithmetic autocorrelation of N-ary half-ℓ-sequences. Cryptologia **50**(1), 81–93 (2026)

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

[16] Edemskiy, V.: On the ideal arithmetic autocorrelation of binary FCSR sequences. Problems of Information Transmission **61**(2), 211–218 (2025)

[17] Berndt, B.C.: Classical theorems on quadratic residues. Enseignement Mathématique **22**(3-4), 261–304 (1976)

[18] Johnson, W., Mitchell, K.J.: Symmetries for sums of the Legendre symbol. Pacific Journal of Mathematics **69**(1), 117–124 (1977)

[19] Cusick, T.W., Ding, C.S., Renvall, A.R.: Stream Ciphers and Number Theory. Elsevier, Amsterdam (2004)

[20] Dummit, D.S., Foote, R.M.: Abstract Algebra. John Wiley & Sons, Hoboken, NJ (2004)

[21] Shparlinski, I.E.: Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. Birkhäuser, Basel (2003)