Electronic Research Archive

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

ERA, 34(9): 6363–6381.
DOI: 10.3934/era.2026278
Received: 14 May 2026
Revised: 05 July 2026
Accepted: 10 July 2026
Published: 20 July 2026

Research article

On correlation measures of binary half-ℓ-sequences

Lingmei Xiao[1,*], Feifei Yan[2,3], Hezheng Lin[1] and Vladimir Edemskiy[4]

[1] Fujian Key Laboratory of Financial Information Processing, Putian University, Putian 351100, China
[2] School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China
[3] Provincial Key Laboratory of Applied Mathematics, Putian University, Putian 351100, China
[4] Department of Applied Mathematics and Informatics, Yaroslav-the-Wise Novgorod State University, Veliky Novgorod 173003, Russia

* **Correspondence:** Email: xiaolm1996@163.com.

Abstract: Half-ℓ-sequences as an extension of ℓ-sequences generated by feedback with carry shift registers (FCSRs) possess desirable pseudorandom properties. In this work, we focus on the arithmetic autocorrelation of binary half-ℓ-sequences with connection integers of the form $q = p_1^r p_2^s$. For this family of sequences, we establish a tight upper bound on the arithmetic autocorrelation and determine all possible values it can attain, which generalizes earlier results when the connection integer is a prime power. Our statements indicate that such sequences exhibit large arithmetic autocorrelation values yet can also demonstrate almost ideal arithmetic correlations for certain special forms of q. We reveal a profound connection between these values and the class numbers of imaginary quadratic fields. Numerical experiments further validate the theoretical findings.

Keywords: pseudorandom sequences; FCSR; half-ℓ-sequences; arithmetic correlation

1. Introduction

Pseudorandom sequences, though generated by deterministic algorithms and not truly random in the strict mathematical sense, play a vital role in communications and cryptography. From a broader mathematical perspective, the periodic behavior of such sequences can be linked to the theory of almost periodic functions. In particular, Lassoued et al. provided a systematic framework for studying periodic regularities in the continuous setting, which motivates analogous investigations in the discrete finite domain [1].

Such sequences are typically implemented in hardware using various types of shift registers. Among these, linear feedback shift registers (LFSRs) represent one of the most classical and widely deployed architectures. LFSRs generate eventually periodic sequences through linear recurrence relations, offering

advantages such as simple implementation and high operational speed. However, their algebraic structure also introduces certain vulnerabilities, making them susceptible to cryptographic attacks [2]. To address the inherent security limitations of LFSRs, Goresky and Klapper proposed a new register architecture known as feedback with carry shift registers (FCSRs), which introduced carry operations [2, 3]. FCSRs generate sequences with desirable pseudorandom properties, among which ℓ-sequences and half-ℓ-sequences have attracted particular attention due to their strong correlation characteristics. The arithmetic correlation property of sequences can be used for simultaneous synchronization and identification in a multiuser environment. Each client correlates its own signature sequence with the received signal. A matching sequence yields a significant peak, whereas a mismatched one results in only a small correlation value, thereby enabling identification and synchronization [4]. Moreover, this correlation metric can also be utilized for mutual authentication. Two communicating parties exchange their respective secret parameters to generate sequences. If the correlation value equals zero, authentication succeeds, and a shared secret key can be established; otherwise, the connection is rejected. This provides a feasible means for user authentication and channel synchronization prior to key distribution [5].

Research on the arithmetic correlation of sequences has yielded notable progress. For instance, Chen et al. explored the arithmetic autocorrelation of binary m-sequences [6]. Afterward, Jing et al. investigated the arithmetic autocorrelation distribution of binary m-sequences [7]. More recently, Liu and Liu established the relationship between arithmetic autocorrelation and pattern distributions of binary sequences [8].

Motivated by ℓ-sequences, Gu and Klapper introduced the *half-ℓ-sequence*, whose period satisfies $\mathrm{ord}_q(2) = \varphi(q)/2$, where q is the connection integer [9]. Various pseudorandom properties of these sequences have been widely investigated, mainly depending on the form of the connection integer q. For the case where q is an odd prime, early work by Gu and Klapper focused on the distributional properties [10], statistical properties, and imbalance properties [9]. Later, Wang and Tan improved upon their results by deriving two new bounds [11]. Niu and Sang provided upper and lower bounds on the linear complexity for primes satisfying $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$ [12]. When $q = p^r$ is an odd prime power, Chen et al. analyzed the arithmetic correlations of half-ℓ-sequences [13], proving ideal arithmetic autocorrelation when $p \equiv 1 \pmod 8$, and they established an upper bound of $p^{r-1/2}\ln(p)$ when $p \equiv -1 \pmod 8$. Recently, Zhang et al. proved that if q satisfies $2^{c-1} < q < 2^c$, then the maximum order complexity of half-ℓ-sequences is either $c-1$ or c [14]. When $q = p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t}$ is a product of distinct prime powers, Chen et al. investigated the behavior of small arithmetic correlations for connection integers of this form [15]. Xiao et al. [16] determined the arithmetic autocorrelation for the special cases $q = 3^3 5^s$ and $7^r p^s$ with $p \equiv \pm 3 \pmod 8$, showing that the correlation values attain half and one third of the period, respectively.

Building upon these works, this paper further investigates arithmetic correlations for binary half-ℓ-sequences whose connection integers are of the general form $q = p_1^r p_2^s$. Our main contributions include a complete classification of admissible connection integers for half-ℓ-sequences, sharp upper bounds for the arithmetic autocorrelation in all remaining cases, and an explicit link between these correlation values and class numbers of imaginary quadratic fields. These results extend the theory from prime-power moduli to composite moduli and provide a full characterization of the correlation behavior for this family.

2. Connection integers of half-ℓ-sequences

Let $\mathcal{S} = \{s_n\}_{n=0}^{\infty}$ be a T-periodic binary sequence. It uniquely corresponds to a rational number

$$\alpha := \sum_{n=0}^{\infty} s_n 2^n = -\frac{\sum_{n=0}^{T-1} s_n 2^n}{2^T - 1} = -\frac{f}{q},$$

where $0 < f < q$, and $\gcd(f, q) = 1$. Here, q is called a *connection integer* of $\mathcal{S}$, and the sequence can be expressed as

$$s_n = (f2^{-n} \bmod q) \bmod 2.$$

We first recall the definition of ℓ-sequences, as half-ℓ-sequences are derived from them. In particular, if q is an odd prime power, and 2 is a primitive root modulo q so that $T = \mathrm{ord}_q(2) = \varphi(q)$ (the Euler phi function), then $\mathcal{S}$ is called an ℓ-*sequence*, which possesses many desirable pseudorandom properties.

Let $\mathcal{S}_\tau = (s_{n+\tau})_{n=0}^{\infty}$ be the τ-shift of $\mathcal{S}$ with the corresponding rational number

$$\alpha_\tau := \sum_{n=0}^{\infty} s_{n+\tau} 2^n = -\frac{f_\tau}{q},$$

where $0 < f_\tau < q$, and $\gcd(f_\tau, q) = 1$. It is not difficult to check that $f_\tau = 2^{T-\tau} f \pmod q$. Compute

$$\alpha - \alpha_\tau = -\frac{f}{q} + \frac{f_\tau}{q} = c + \left(-\frac{\left(2^{T-\tau} - 1\right) f \bmod q}{q} \right) = c - \frac{f'}{q'} \tag{2.1}$$

for some integer c, where $0 < f' < q'$, and $\gcd(q', f') = 1$. The new (periodic) sequence $\mathcal{U}$ corresponding to the rational number $-f'/q'$ is exactly the periodic part of the sequence obtained from $\alpha - \alpha_\tau$, and it is clear that $q'|q$. Unlike classical autocorrelation, the *arithmetic autocorrelation* is defined as the number of zeros minus the number of ones in a complete period of length T of $\mathcal{U}$, that is,

$$\mathcal{A}^A_{\mathcal{S}}(\tau) = T - \frac{2T}{\mathrm{ord}_{q'}(2)} \cdot \lambda' = \frac{\mathrm{ord}_q(2)}{\mathrm{ord}_{q'}(2)} \left(\mathrm{ord}_{q'}(2) - 2\lambda' \right), \tag{2.2}$$

where λ' is the number of ones in a period of $\mathcal{U}$; see [4]. In other words, the arithmetic autocorrelation value at shift τ is completely determined by the Hamming weight of the periodic sequence corresponding to the reduced rational number $-f'/q'$ obtained from the difference $\alpha - \alpha_\tau$.

Ideally, the absolute values of the arithmetic autocorrelation should be as small as possible for all $1 \le \tau \le T - 1$. A sequence is said to have *ideal arithmetic autocorrelation* if all its arithmetic autocorrelations at nontrivial shifts equal zero. It is a known fact that ℓ-sequences exhibit ideal arithmetic autocorrelation [2, Chap.13].

However, when the connection integer q is not a prime power, the structure of sequences satisfying $\mathrm{ord}_q(2) = \varphi(q)/2$, namely *half-$\ell$-sequences*, becomes more complex, and the ideal arithmetic autocorrelation property may no longer hold in general. To systematically analyze arithmetic correlations for such sequences, it is therefore necessary to first characterize the possible forms of q for which a half-ℓ-sequence can exist.

Proposition 1. *Let $q > 1$ be an odd integer having at least two distinct prime factors and satisfying* $\mathrm{ord}_q(2) = \varphi(q)/2$. *Then, q is of the form*

$$q = p_1^r p_2^s, \quad r \geq 1, s \geq 1$$

with $\gcd(p_1 - 1, p_2 - 1) = 2$.

Proof. Suppose that q has the prime factorization $q = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ with $t \geq 2$. Then, the order of 2 modulo q satisfies

$$\mathrm{ord}_q(2) \leq l.c.m.\left(\varphi\left(p_1^{r_1}\right), \varphi\left(p_2^{r_2}\right), \cdots, \varphi\left(p_t^{r_t}\right)\right) \leq \frac{1}{2^{t-1}} \prod_{1 \leq i \leq t} \varphi\left(p_i^{r_i}\right) = \frac{\varphi(q)}{2^{t-1}}.$$

Hence, together with the assumption $\mathrm{ord}_q(2) = \varphi(q)/2$, we claim that $t = 2$, and $\gcd(p_1 - 1, p_2 - 1) = 2$. □

In the following, we will investigate the arithmetic autocorrelation of half-ℓ-sequences with the connection integer $q = p_1^r p_2^s$.

Proposition 2. *Let $q = p_1^r p_2^s$ be an odd integer, where $p_1,\ p_2$ are two distinct odd primes with* $\gcd(p_1 - 1,\ p_2 - 1) = 2$. *If* $\mathrm{ord}_q(2) = \varphi(q)/2$, *then $p_1,\ p_2$ only have three cases:*

- $p_1 \equiv p_2 \equiv 3 \pmod 8$;
- $p_1 \equiv \pm 3 \pmod 8$ *and* $p_2 \equiv 7 \pmod 8$;
- $p_1 \equiv 3 \pmod 8$ *and* $p_2 \equiv 5 \pmod 8$.

Proof. It is well-known that

$$\mathrm{ord}_{p^t}(2) \leq \frac{p^{t-1}(p-1)}{2}, \quad if\ p \equiv \pm 1 \pmod 8,$$

and

$$\mathrm{ord}_{p^t}(2) \leq p^{t-1}(p-1), \quad if\ p \equiv \pm 3 \pmod 8.$$

Because $\mathrm{ord}_q(2) = l.c.m.\left(\mathrm{ord}_{p_1^r}(2),\ \mathrm{ord}_{p_2^s}(2)\right)$, our analysis divides into three distinct cases as specified below:

Case 1. If $p_1 \equiv \pm 1 \pmod 8$, and $p_2 \equiv \pm 1 \pmod 8$, the order of 2 modulo q is

$$l.c.m.\left(\frac{p_1^{r-1}(p_1-1)}{2}, \frac{p_2^{s-1}(p_2-1)}{2}\right) = \frac{p_1^{r-1}p_2^{s-1}(p_1-1)(p_2-1)}{4} \neq \frac{\varphi(q)}{2}.$$

Case 2. If $p_1 \equiv \pm 3 \pmod 8$, and $p_2 \equiv \pm 1 \pmod 8$, it is not difficult to check that $2|(p_1 - 1)$. If $p_1 \equiv \pm 3 \pmod 8$, and $4|(p_2 - 1)/2$ if $p_2 \equiv 1 \pmod 8$, then the order of 2 modulo q is

$$l.c.m.\left(p_1^{r-1}(p_1-1), \frac{p_2^{s-1}(p_2-1)}{2}\right) = \frac{p_1^{r-1}p_2^{s-1}(p_1-1)(p_2-1)}{4} \neq \frac{\varphi(q)}{2}.$$

In this case, for the connection integer $q = p_1^r p_2^s$ with $p_1 \equiv \pm 3 \pmod 8$ and $p_2 \equiv 7 \pmod 8$, the binary sequences can be defined as half-ℓ-sequences.

Case 3. If $p_1 \equiv \pm 3 \pmod 8$, and $p_2 \equiv \pm 3 \pmod 8$, note that when $p_i \equiv 5 \pmod 8$, we have $4|(p_i - 1)$ for $i = 1, 2$. Consequently, $\gcd(p_1 - 1,\ p_2 - 1) = 4 \neq 2$. Hence, for the connection integer $q = p_1^r p_2^s$, we must take $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv \pm 3 \pmod 8$.

Putting everything together, we complete the proof. □

Throughout this work, $a \bmod m$ reduces to a number in $\{0, 1, \ldots, m-1\}$. Below, we will discuss the arithmetic autocorrelation of half-ℓ-sequences according to the three cases specified in Proposition 2.

3. Maximum arithmetic correlation of half-ℓ-sequences

In [13], Edemskiy et al. studied the arithmetic correlation of half-ℓ-sequences $\mathcal{S}$ with connection integers q being a prime-power. In this section, we consider the case where $q = p_1^r p_2^s$ with distinct odd primes $p_1,\ p_2$ and positive integers r, s. According to Proposition 2, there are three cases to consider. The first case, $p_1 \equiv p_2 \equiv 3 \pmod 8$, has been treated in [15], where it was shown that $\mathcal{A}^A_{\mathcal{S}}(\tau) = 0$ for all nontrivial shifts τ. We now turn to the remaining two cases.

For the reader's convenience, we summarize the main notions used throughout this paper as follows.

D_m	The set of powers of 2 modulo m: $\left\{2^l \pmod m : 0 \le l < \mathrm{ord}_m(2)\right\}$.
Δ	The difference between the number of even integers and the number of odd integers in D_{p_2}, the set of quadratic residues modulo p_2, where $p_2 \equiv 7 \pmod 8$.
Ω	The difference between the number of even integers and the number of odd integers in $D_{p_1p_2}$, where $p_1 \equiv 3 \pmod 8,\ p_2 \equiv 5 \pmod 8$.
$\lambda_{i,j}$	The number of odd integers in $D_{q'}$, where $q' = p_1^i p_2^j$.
$\lambda'_{i,j}$	The number of odd integers in the complement $\mathbb{Z}^*_{q'} \setminus D_{q'}$.

From Eqs (2.1) and (2.2), the arithmetic autocorrelation $\mathcal{A}^A_{\mathcal{S}}(\tau)$ is determined by the number of ones in $\mathcal{U}$, which in turn depends on the parity distribution of elements in $D_{q'}$. If $q' = p_1^i p_2^j$ for some $i,\ j > 0$, then by

$$u_n = (f' 2^{-n} \bmod q') \bmod 2,$$

we need to count the odd integers in $D_{q'}$ and its complement $\mathbb{Z}^*_{q'} \setminus D_{q'}$, denoted by $\lambda_{i,j}$ and $\lambda'_{i,j}$, respectively. Note that $\mathrm{ord}_{q'}(2) = \varphi(q')/2$, as $\mathcal{S}$ is a half-ℓ-sequence.

Lemma 1. *For $q' = p_1^i p_2^j$ with $i, j > 0$ and $\mathrm{ord}_{q'}(2) = \varphi(q')/2$, the quantity $\lambda_{i,j}$ (defined above) is given by*

$$\lambda_{i,j} = \lambda_{1,1} + \frac{\varphi\left(p_1^i p_2^j\right) - \varphi(p_1p_2)}{4}.$$

Proof. It is not difficult to check that $\mathrm{ord}_{p_1p_2}(2) = \varphi(p_1p_2)/2$. Write

$$I_{i,j} = \left\{x + p_1p_2k :\ x = 2^l \bmod p_1p_2, 0 \le l < \varphi(p_1p_2)/2, 0 \le k < p_1^{i-1}p_2^{j-1}\right\}.$$

Obviously, $D_{q'} = I_{i,j}$ because $D_{q'} \subseteq I_{i,j}$ and $\left|D_{q'}\right| = \left|I_{i,j}\right|$. Then, a number $x + p_1p_2k$ in $I_{i,j}$ is odd if and only if x is odd, and k is even, or x is even, and k is odd. Because the number of odd x is $\lambda_{1,1}$, one can easily get that the number of odd numbers in $D_{q'}$ satisfies

$$\lambda_{i,j} = \frac{p_1^{i-1}p_2^{j-1} + 1}{2} \cdot \lambda_{1,1} + \frac{p_1^{i-1}p_2^{j-1} - 1}{2} \cdot \left(\frac{\varphi(p_1p_2)}{2} - \lambda_{1,1}\right),$$

which completes the proof. □

By Lemma 1, we get

$$\lambda'_{i,j} = \frac{\varphi\left(p_1^i p_2^j\right) + \varphi(p_1p_2)}{4} - \lambda_{1,1},$$

which is exactly the number of even numbers in $D_{q'}$. We then have

$$\lambda_{i,j} - \lambda'_{i,j} = 2\lambda_{1,1} - \frac{\varphi(p_1p_2)}{2} = \lambda_{1,1} - \lambda'_{1,1}. \tag{3.1}$$

3.1. The case $q = p_1^r p_2^s$ with $p_1 \equiv \pm 3 \pmod 8$ and $p_2 \equiv 7 \pmod 8$

In this section, we first prove two lemmas.

Lemma 2. *Let p_2 be a prime with $p_2 \equiv 7 \pmod 8$, and let $\beta = \exp(2\pi\mathrm{i}/p_2)$. Then, for any integer x such that $p_2 \nmid x$, we have*

- $\sum\limits_{v\in D_{p_2}} \beta^{vx} = -\dfrac{1}{2} + \dfrac{\mathrm{i}\sqrt{p_2}}{2}\left(\dfrac{x}{p_2}\right)$;
- $\sum\limits_{v\in \mathbb{Z}_{p_2}^*\setminus D_{p_2}} \beta^{vx} = -\dfrac{1}{2} - \dfrac{\mathrm{i}\sqrt{p_2}}{2}\left(\dfrac{x}{p_2}\right)$;
- $\sum\limits_{v\in D_{p_2}} \dfrac{2}{1+\beta^v} = \mathrm{i}\sqrt{p_2}\Delta + \dfrac{p_2-1}{2}$.

Proof. To evaluate these sums, we introduce the Legendre symbol $\left(\frac{\cdot}{\cdot}\right)$ and use the standard identities for Gauss sums. By the definition of the Legendre symbol, we have $\left(\frac{k}{p_2}\right) = 1$ if $k \in D_{p_2}$ and $\left(\frac{k}{p_2}\right) = -1$ if $k \in \mathbb{Z}_{p_2}^* \setminus D_{p_2}$. Then, we have

$$\sum_{v\in D_{p_2}} \beta^{vx} = \frac{1}{2}\left[\sum_{k=1}^{p_2-1}\left(1+\left(\frac{k}{p_2}\right)\right)\beta^{kx}\right] = \frac{1}{2}\sum_{k=1}^{p_2-1}\beta^{kx} + \frac{1}{2}\sum_{k=1}^{p_2-1}\left(\frac{k}{p_2}\right)\beta^{kx}$$

and

$$\sum_{v\in \mathbb{Z}_{p_2}^*\setminus D_{p_2}} \beta^{vx} = \frac{1}{2}\left[\sum_{k=1}^{p_2-1}\left(1-\left(\frac{k}{p_2}\right)\right)\beta^{kx}\right] = \frac{1}{2}\sum_{k=1}^{p_2-1}\beta^{kx} - \frac{1}{2}\sum_{k=1}^{p_2-1}\left(\frac{k}{p_2}\right)\beta^{kx}.$$

Because $\sum\limits_{k=1}^{p_2-1}\beta^{kx} = -1$ for $p_2 \nmid x$, by the Gauss sums $G(x) = \sum\limits_{k=1}^{p_2-1}\left(\frac{k}{p_2}\right)\beta^{kx} = \left(\frac{x}{p_2}\right)G(1)$ and $G(1) = \mathrm{i}\sqrt{p_2}$, if $p_2 \equiv 3 \pmod 4$ (see Propositions 6.3.1 and 6.3.2 in [17]), we have

$$\sum_{k=1}^{p_2-1}\left(\frac{k}{p_2}\right)\beta^{kx} = \left(\frac{x}{p_2}\right)\cdot\sum_{k=1}^{p_2-1}\left(\frac{k}{p_2}\right)\beta^{k} = \mathrm{i}\left(\frac{x}{p_2}\right)\sqrt{p_2}.$$

Thus,

$$\sum_{v\in D_{p_2}} \beta^{vx} = -\frac{1}{2} + \frac{\mathrm{i}}{2}\left(\frac{x}{p_2}\right)\sqrt{p_2},\ \sum_{v\in \mathbb{Z}_{p_2}^*\setminus D_{p_2}} \beta^{vx} = -\frac{1}{2} - \frac{\mathrm{i}}{2}\left(\frac{x}{p_2}\right)\sqrt{p_2}, \tag{3.2}$$

which implies the first two results.

Now, we turn to show the third result. Let M_0 be the number of evens and M_1 the number of odds in D_{p_2}. That is, $\Delta = M_0 - M_1$. We note that D_{p_2} is exactly the set of quadratic residues modulo p_2. From the standard exponential sums

$$\sum_{x=0}^{p_2-1}\beta^{vx} = \begin{cases} p_2, & \text{if } v \equiv 0 \pmod{p_2}, \\ 0, & \text{if } v \not\equiv 0 \pmod{p_2}, \end{cases}$$

it follows that

$$M_0 = \sum_{v\in D_{p_2}} \frac{1}{p_2} \sum_{c=1}^{(p_2-1)/2} \sum_{x=0}^{p_2-1} \beta^{x(v-2c)} \text{ and } M_1 = \sum_{v\in D_{p_2}} \frac{1}{p_2} \sum_{c=0}^{(p_2-3)/2} \sum_{x=0}^{p_2-1} \beta^{x(v-2c-1)}.$$

If $x \neq 0$, then

$$\sum_{c=1}^{(p_2-1)/2} \beta^{-2xc} = \frac{\beta^{-x(p_2+1)} - \beta^{-2x}}{\beta^{-2x} - 1} = \frac{\beta^{-x} - \beta^{-2x}}{\beta^{-2x} - 1} = -\frac{1}{\beta^x + 1}. \tag{3.3}$$

Also,

$$\sum_{c=0}^{(p_2-3)/2} \beta^{-x(2c+1)} = -\frac{\beta^x}{\beta^x + 1}.$$

Hence,

$$p_2 M_0 = -\sum_{x=1}^{p_2-1} \sum_{v\in D_{p_2}} \frac{1}{\beta^x + 1} \beta^{vx} \text{ and } p_2 M_1 = -\sum_{x=1}^{p_2-1} \sum_{v\in D_{p_2}} \frac{\beta^x}{\beta^x + 1} \beta^{vx}.$$

Note that $\left(\frac{-1}{p_2}\right) = (-1)^{\frac{p_2-1}{2}}$ and $p_2 \equiv 7 \pmod 8$, so it follows that $p_2 - 1 \notin D_{p_2}$. Hence, the number of odd integers in D_{p_2} equals the number of even integers in $\mathbb{Z}_{p_2}^* \setminus D_{p_2}$. We therefore compute

$$\begin{aligned} p_2\Delta = p_2(M_0 - M_1) &= \sum_{x=1}^{p_2-1} \frac{1}{\beta^x + 1} \sum_{v\in\mathbb{Z}_{p_2}^*\setminus D_{p_2}} \beta^{vx} - \sum_{x=1}^{p_2-1} \frac{1}{\beta^x + 1} \sum_{v\in D_{p_2}} \beta^{vx} \\ &= -\mathrm{i}\sqrt{p_2} \sum_{v\in D_{p_2}} \frac{1}{\beta^v + 1} + \mathrm{i}\sqrt{p_2} \sum_{v\in\mathbb{Z}_{p_2}^*\setminus D_{p_2}} \frac{1}{\beta^v + 1} \\ &= -\mathrm{i}\sqrt{p_2} \sum_{v\in D_{p_2}} \frac{1}{\beta^v + 1} + \mathrm{i}\sqrt{p_2} \left(\frac{p_2 - 1}{2} - \sum_{v\in D_{p_2}} \frac{1}{\beta^v + 1} \right) \\ &= \frac{\mathrm{i}\sqrt{p_2}(p_2 - 1)}{2} - \mathrm{i}\sqrt{p_2} \sum_{v\in D_{p_2}} \frac{2}{\beta^v + 1}, \end{aligned}$$

as Eq (3.2) and

$$\sum_{v\in\mathbb{Z}_{p_2}^*\setminus D_{p_2}} \frac{1}{\beta^v + 1} = \sum_{v\in D_{p_2}} \frac{1}{\beta^{-v} + 1} = \frac{p_2 - 1}{2} - \sum_{v\in D_{p_2}} \frac{1}{\beta^v + 1}.$$

This completes the proof of Lemma 2.

□

Lemma 3. *Let p_1 and p_2 be primes with $p_1 \equiv \pm 3 \pmod 8$ and $p_2 \equiv 7 \pmod 8$ and with $\mathrm{ord}_{p_1p_2}(2) = \varphi(p_1p_2)/2$. Let $\lambda_{1,1}$ be the number of odds in $D_{p_1p_2} = \left\{2^l \pmod{p_1p_2} : l \geq 0\right\}$. Then,*

$$\lambda_{1,1} = \begin{cases} \dfrac{\varphi(p_1p_2)}{4}, & \text{if } \left(\dfrac{p_1}{p_2}\right) = 1, \\ \dfrac{\varphi(p_1p_2)}{4} - \Delta, & \text{if } \left(\dfrac{p_1}{p_2}\right) = -1. \end{cases}$$

Proof. Let $\xi = \alpha\beta$, where $\alpha = \exp(2\pi\mathrm{i}/p_1)$, and $\beta = \exp(2\pi\mathrm{i}/p_2)$. Because $p_2 \equiv 7 \pmod 8$, we have $\left(\frac{-1}{p_2}\right) = -1$; we shall use this fact repeatedly without further mention. From the standard exponential sum identity (see [17])

$$\sum_{t=0}^{p_1p_2-1} \xi^{tu} = \begin{cases} p_1p_2, & \text{if } u \equiv 0 \pmod{p_1p_2}, \\ 0, & \text{if } u \not\equiv 0 \pmod{p_1p_2} \end{cases}$$

and using Eq (3.3), the number of evens in $D_{p_1p_2}$ is given by

$$\begin{aligned} \frac{\varphi(p_1p_2)}{2} - \lambda_{1,1} &= \sum_{u\in D_{p_1p_2}} \frac{1}{p_1p_2} \sum_{c=1}^{(p_1p_2-1)/2} \sum_{t=0}^{p_1p_2-1} \xi^{t(u-2c)} \\ &= \frac{1}{p_1p_2} \sum_{u\in D_{p_1p_2}} \sum_{c=1}^{(p_1p_2-1)/2} 1 + \frac{1}{p_1p_2} \sum_{u\in D_{p_1p_2}} \sum_{c=1}^{(p_1p_2-1)/2} \sum_{t=1}^{p_1p_2-1} \xi^{t(u-2c)} \\ &= \frac{(p_1p_2-1)\left|D_{p_1p_2}\right|}{2p_1p_2} + \frac{1}{p_1p_2} \sum_{u\in D_{p_1p_2}} \sum_{t=1}^{p_1p_2-1} \xi^{tu} \sum_{c=1}^{(p_1p_2-1)/2} \xi^{-2tc} \\ &= \frac{(p_1p_2-1)\left|D_{p_1p_2}\right|}{2p_1p_2} + \frac{1}{p_1p_2} \sum_{u\in D_{p_1p_2}} \sum_{t=1}^{p_1p_2-1} \xi^{tu} \cdot \left(-\frac{1}{\xi^t+1}\right) \\ &= \frac{(p_1p_2-1)\left|D_{p_1p_2}\right|}{2p_1p_2} - \frac{1}{p_1p_2} \sum_{t=1}^{p_1p_2-1} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{tu}. \end{aligned} \tag{3.4}$$

Because the set $\{1, 2, \ldots, p_1p_2 - 1\}$ can be partitioned as

$$\{1, 2, \ldots, p_1p_2 - 1\} = P_1 \cup P_2 \cup \mathbb{Z}^*_{p_1p_2},$$

where $P_1 = \{p_1, 2p_1, \ldots, (p_2 - 1)p_1\}$, and $P_2 = \{p_2, 2p_2, \ldots, (p_1 - 1)p_2\}$, we compute the inner sums over $t \in P_1$, $t \in P_2$, and $t \in \mathbb{Z}^*_{p_1p_2}$, respectively.

Case 1: $t \in P_1$. For $t \in P_1$, we have $\alpha^t = 1$, and hence, $\xi^t = \beta^t$, where $t = p_1x$ for some $1 \le x \le p_2 - 1$. Thus,

$$\begin{aligned} \sum_{t\in P_1} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{ut} &= (p_1-1) \sum_{x=1}^{p_2-1} \frac{1}{\beta^x+1} \sum_{v\in D_{p_2}} \beta^{vx} \\ &= -\frac{(p_1-1)}{2} \sum_{x=1}^{p_2-1} \frac{1}{\beta^x+1} + \frac{\mathrm{i}\sqrt{p_2}(p_1-1)}{2} \sum_{x=1}^{p_2-1} \left(\frac{x}{p_2}\right) \frac{1}{\beta^x+1} \\ &= -\frac{\varphi(p_1p_2)}{4} + \frac{\mathrm{i}\sqrt{p_2}(p_1-1)}{2} \left(\sum_{v\in D_{p_2}} \frac{1}{\beta^v+1} - \sum_{v\in \mathbb{Z}^*_{p_2}\setminus D_{p_2}} \frac{1}{\beta^v+1} \right) \\ &= -\frac{\varphi(p_1p_2)}{4} + \frac{\mathrm{i}\sqrt{p_2}(p_1-1)}{2} \left(-\frac{p_2-1}{2} + \sum_{v\in D_{p_2}} \frac{2}{\beta^v+1} \right) \end{aligned}$$

$$= -\frac{\varphi(p_1p_2)}{4} - \frac{p_2(p_1-1)\Delta}{2}, \tag{3.5}$$

where we use Eq (3.2), Lemma 2, and the identity

$$\sum_{v\in\mathbb{Z}_{p_2}^*\setminus D_{p_2}} \frac{1}{\beta^v+1} = \sum_{v\in D_{p_2}} \frac{1}{\beta^{-v}+1} = \sum_{v\in D_{p_2}} \frac{\beta^v}{\beta^v+1} = \frac{p_2-1}{2} - \sum_{v\in D_{p_2}} \frac{1}{\beta^v+1}.$$

Case 2: $t \in P_2$. For $t \in P_2$, we have $\beta^t = 1$ and $\xi^t = \alpha^t$, where $t = p_2y$ for some $1 \le y \le p_1 - 1$. Because $D_{p_1p_2} \bmod p_1 = \left\{u \bmod p_1 : u \in D_{p_1p_2}\right\} = \mathbb{Z}_{p_1}^*$, and $\sum_{u\in\mathbb{Z}_{p_1}^*} \alpha^{uy} = -1$ for $p_1 \nmid y$, we have

$$\sum_{u\in D_{p_1p_2}} \xi^{ut} = \frac{p_2-1}{2} \sum_{u\in\mathbb{Z}_{p_1}^*} \alpha^{uy} = -\frac{p_2-1}{2}.$$

Also, using the identity $\frac{1}{\alpha^y+1} + \frac{1}{\alpha^{p_1-y}+1} = 1$, we get $\sum_{y=1}^{p_1-1} \frac{1}{\alpha^y+1} = \frac{p_1-1}{2}$. Therefore,

$$\begin{aligned}\sum_{t\in P_2} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{ut} &= \sum_{y=1}^{p_1-1} \frac{1}{\alpha^y+1} \cdot \frac{(p_2-1)}{2} \cdot \sum_{u\in\mathbb{Z}_{p_1}^*} \alpha^{uy} \\ &= -\frac{(p_2-1)}{2} \cdot \sum_{y=1}^{p_1-1} \frac{1}{\alpha^y+1} = -\frac{\varphi(p_1p_2)}{4}.\end{aligned} \tag{3.6}$$

Case 3: $t \in \mathbb{Z}_{p_1p_2}^*$. The reduction of $D_{p_1p_2}$ modulo p_1 is $\mathbb{Z}_{p_1}^*$, as $p_1 \equiv \pm 3 \pmod 8$, and $p_2 \equiv 7 \pmod 8$. Thus, for any $t \in \mathbb{Z}_{p_1p_2}^*$, by simple calculations, we get

$$\sum_{u\in D_{p_1p_2}} \xi^{ut} = \sum_{v\in D_{p_2}} \beta^{tv} \sum_{y=1}^{p_1-1} \alpha^{ty} = -\sum_{v\in D_{p_2}} \beta^{tv} = \frac{1}{2} - \frac{\mathrm{i}\sqrt{p_2}}{2}\left(\frac{t}{p_2}\right).$$

Note that $\left(\frac{t}{p_2}\right) = 1$ if $t \in D_{p_1p_2}$, and $\left(\frac{t}{p_2}\right) = -1$ if $t \in \mathbb{Z}_{p_1p_2}^* \setminus D_{p_1p_2}$. Hence,

$$\sum_{t\in\mathbb{Z}_{p_1p_2}^*\setminus D_{p_1p_2}} \frac{1}{\xi^t+1} = \sum_{t\in D_{p_1p_2}} \frac{1}{\xi^{-t}+1} = \sum_{t\in D_{p_1p_2}} \frac{\xi^t}{\xi^t+1} = \left|D_{p_1p_2}\right| - \sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1}.$$

Therefore,

$$\begin{aligned}\sum_{t\in\mathbb{Z}_{p_1p_2}^*} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{ut} &= \sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{ut} + \sum_{t\in\mathbb{Z}_{p_1p_2}^*\setminus D_{p_1p_2}} \frac{1}{\xi^t+1} \sum_{u\in D_{p_1p_2}} \xi^{ut} \\ &= \sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1}\left(\frac{1}{2} - \frac{\mathrm{i}\sqrt{p_2}}{2}\right) + \sum_{t\in\mathbb{Z}_{p_1p_2}^*\setminus D_{p_1p_2}} \frac{1}{\xi^t+1}\left(\frac{1}{2} + \frac{\mathrm{i}\sqrt{p_2}}{2}\right) \\ &= \left(\frac{1}{2} + \frac{\mathrm{i}\sqrt{p_2}}{2}\right)\left|D_{p_1p_2}\right| - \mathrm{i}\sqrt{p_2} \sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1}.\end{aligned} \tag{3.7}$$

It remains to evaluate $\sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1}$. Because each $u \in D_{p_1p_2}$ can be uniquely written as $u \equiv y \pmod{p_1}$ with $y \in \mathbb{Z}_{p_1}^*$ and $u \equiv v \pmod{p_2}$ with $v \in D_{p_2}$, we have

$$\begin{aligned}
\sum_{t\in D_{p_1p_2}} \frac{1}{\xi^t+1} &= \sum_{y=1}^{p_1-1}\sum_{v\in D_{p_2}} \frac{1}{1+\alpha^y\beta^v} \\
&= \sum_{y=1}^{p_1-1}\sum_{v\in D_{p_2}} \frac{1}{1+\alpha^y\beta^v}\cdot\frac{1+(\alpha^y\beta^v)^{p_1}}{1+\beta^{vp_1}} \\
&= \sum_{v\in D_{p_2}} \frac{1}{1+\beta^{vp_1}}\sum_{k=0}^{p_1-1}(-1)^k\beta^{kv}\sum_{y=1}^{p_1-1}\alpha^{ky} \\
&= \sum_{v\in D_{p_2}} \frac{1}{1+\beta^{vp_1}}\left(p_1-1-\sum_{k=1}^{p_1-1}(-1)^k\beta^{kv}\right) \\
&= p_1\sum_{v\in D_{p_2}} \frac{1}{1+\beta^{vp_1}} - \sum_{v\in D_{p_2}} \frac{1}{1+\beta^v} \\
&= \begin{cases} \dfrac{\varphi(p_1p_2)}{4} + \dfrac{\mathrm{i}\sqrt{p_2}(p_1-1)\Delta}{2}, & \text{if } \left(\dfrac{p_1}{p_2}\right)=1, \\ \dfrac{\varphi(p_1p_2)}{4} - \dfrac{\mathrm{i}\sqrt{p_2}(p_1+1)\Delta}{2}, & \text{if } \left(\dfrac{p_1}{p_2}\right)=-1. \end{cases}
\end{aligned} \tag{3.8}$$

Substituting Eq (3.8) into Eq (3.7), we obtain

$$\sum_{t\in\mathbb{Z}_{p_1p_2}^*} \frac{1}{\xi^t+1}\sum_{u\in D_{p_1p_2}} \xi^{ut} = \begin{cases} \dfrac{\varphi(p_1p_2)}{4} + \dfrac{p_2(p_1-1)\Delta}{2}, & \text{if } \left(\dfrac{p_1}{p_2}\right)=1, \\ \dfrac{\varphi(p_1p_2)}{4} - \dfrac{p_2(p_1+1)\Delta}{2}, & \text{if } \left(\dfrac{p_1}{p_2}\right)=-1. \end{cases} \tag{3.9}$$

Finally, combining the contributions from Cases 1–3 in Eqs (3.5), (3.6), and (3.9) and substituting into Eq (3.4), we obtain

$$\lambda_{1,1} = \begin{cases} \dfrac{\varphi(p_1p_2)}{4}, & \text{if } \left(\dfrac{p_1}{p_2}\right)=1, \\ \dfrac{\varphi(p_1p_2)}{4} - \Delta, & \text{if } \left(\dfrac{p_1}{p_2}\right)=-1. \end{cases}$$

This completes the proof. □

Theorem 1. *Let $\mathcal{S}$ be a binary half-ℓ-sequence with connection integer $q = p_1^r p_2^s$, where $p_1 \equiv \pm 3 \pmod 8$, $p_2 \equiv 7 \pmod 8$, and r, s are positive integers. Then,*

$$\max\left|\mathcal{A}_{\mathcal{S}}^A(\tau)\right| = |\Delta|\, p_1^{r-1}p_2^{s-1}(p_1-1).$$

In particular, $\max\left|\mathcal{A}_{\mathcal{S}}^A(\tau)\right| = 2$ *when* $q = 21$.

Proof. To compute $\mathcal{A}_{\mathcal{S}}^A(\tau)$, it suffices to compute the sequence $\mathcal{U}$ corresponding to the rational number

$$-\frac{(2^{T-\tau}-1)f \bmod q}{q} = -\frac{f'}{q'}, \quad 0 < f' < q', \ \gcd(f', q') = 1,$$

where q' is a divisor of q.

First of all, note that if $\frac{p_2-1}{2} \mid (p_1-1)$, or $(p_1-1) \mid (p_2-1)$, then $p_1 = 3,\ p_2 = 7$. It follows that $\max\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = 2$.

Suppose $q \neq 21$. Then, $p_2 \nmid (2^{p_1-1}-1)$, and $p_1 \nmid (2^{p_2-1}-1)$. In this case, we see that the possible values of q' belong to

$$\left\{p_1^i,\ p_2^j,\ p_1^i p_2^j : 1 \le i \le r,\ 1 \le j \le s\right\}.$$

For those τ with $q' = p_1^i$, we have $\mathcal{A}_{\mathcal{S}}^{A}(\tau) = 0$.

For those τ with $q' = p_1^i p_2^j$, we have $\max\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = 2\,|\Delta|\, p_1^{r-i} p_2^{s-j}$ or 0 by Eq (3.1) together with Lemmas 1 and 3.

For those τ with $q' = p_2^j$, by [13, Theorem 1], we get

$$\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| \le \left|\left(\frac{p_2-1}{2} - 2M_1\right) p_1^{r-1} p_2^{s-1}(p_1-1)\right| = |\Delta|\, p_1^{r-1} p_2^{s-1}(p_1-1).$$

Indeed, in this case, $\max\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = |\Delta|\, p_1^{r-1} p_2^{s-1}(p_1-1)$. One can confirm it by induction on j because there exists a τ such that $\gcd(2^{T-\tau}-1, p_2^j) > 1$.

If $j = 1$, then $q' = p_2$; by [13, Theorem 1] again,

$$\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = |\Delta|\, p_1^{r-1} p_2^{s-1}(p_1-1).$$

Now, we assume that it is true for $j \le k$, so we move to prove the case $j = k+1$. On one hand, for $0 \le m < k+1$, we have

$$\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| \le |\Delta|\, p_2^m p_2^{s-k-1} p_1^{r-1}(p_1-1) \le |\Delta|\, p_1^{r-1} p_2^{s-1}(p_1-1).$$

On the other hand, choosing $\tau = p_1^{r-1} p_2^{s-2}(p_1-1)(p_2-1)/2 (< T)$, we can get

$$2^{T-\tau} = 2^{p_1^{r-1} p_2^{s-1}(p_1-1)(p_2-1)/2-\tau} = 2^{p_1^{r-1} p_2^{s-2}(p_1-1)(p_2-1)^2/2} \equiv 1 \pmod{p_2},$$

which means that $\gcd(2^{T-\tau}-1, q) = p_2 > 1$. Then, there exists a τ such that $\max\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = |\Delta|\, p_1^{r-1} p_2^{s-1}(p_1-1)$. We thus complete the proof. □

Remark. From the proof of Theorem 1, we see that the possible values of the arithmetic autocorrelation are in the set

$$\left\{0,\ \pm 2\Delta p_1^{r-i} p_2^{s-j},\ \pm\Delta p_1^{r-i} p_2^{s-j+t}(p_1-1)\right\}.$$

Some concrete examples are given in Table 2 of Section 4.

3.2. The case $q = p_1^r p_2^s$ with $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv 5 \pmod 8$

In this section, let Ω be the number of odds minus the number of evens in $D_{p_1 p_2}$.

Theorem 2. *Let $\mathcal{S}$ be a binary half-ℓ-sequence with connection integer $q = p_1^r p_2^s$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$, and r, s are positive integers. Then,*

$$\max\left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = \begin{cases} |\Omega|, & \text{if } q = 3p_2^s, \\ |\Omega|\, p_1^{r-1} p_2^{s-1}, & \text{otherwise.} \end{cases}$$

Proof. First, we consider the special case of $q = 3p_2^s$. Because 3 divides $2^{p_2-1} - 1$, and q' divides q by Eq (2.1), the possible values of $q' = 3p_2^s$ or $q' \in \left\{p_2^j : j = 1, 2, \ldots, s\right\}$ follow. For those τ's when $q' = p_2^j$, we get $\mathcal{A}_S^A(\tau) = 0$, as we have an ℓ-sequence in this case. For those τ's when $q' = 3p_2^s$, by Eq (3.1),

$$\lambda_{i,j} - \lambda'_{i,j} = \lambda_{1,1} - \lambda'_{1,1},$$

so we have

$$\left|\mathcal{A}_S^A(\tau)\right| = |\Omega|.$$

Now, suppose that $p_1 \neq 3$ or $r > 1$. In this case, the period $T = p_1^{r-1}p_2^{s-1}(p_1 - 1)(p_2 - 1)/2$, and the possible values of q' belong to the set

$$\left\{p_1^i,\ p_2^j,\ p_1^i p_2^j : 1 \le i \le r,\ 1 \le j \le s\right\}.$$

We then obtain

$$\left|\mathcal{A}_S^A(\tau)\right| = \begin{cases} 0, & \text{if } q' = p_1^i \text{ or } p_2^j, \\ |\Omega|\, p_1^{r-i}p_2^{s-j}, & \text{if } q' = p_1^i p_2^j. \end{cases}$$

Choosing τ as follows:

- $\tau = p_1^{r-2}p_2^{s-2}(p_1 - 1)(p_2 - 1)(p_1p_2 - 2)/2$ if $r > 1$ and $s > 1$;
- $\tau = p_2^{s-2}(p_1 - 1)(p_2 - 1)(p_2 - 2)/2$ if $r = 1$ and $s > 1$;
- $\tau = p_1^{r-2}(p_1 - 1)(p_2 - 1)(p_1 - 2)/2$ if $r > 1$ and $s = 1$,

we can get $T - \tau = \varphi\left(p_1^{r-1}p_2^{s-1}\right)$. Hence,

$$2^{T-\tau} \equiv 2^{\varphi\left(p_1^{r-1}p_2^{s-1}\right)} \equiv 1 \pmod{p_1^{r-1}p_2^{s-1}}.$$

Under the given conditions, we have $\gcd\left(2^{T-\tau} - 1, p_1^r p_2^s\right) = p_1^{r-1}p_2^{s-1}$. Consequently, for a shift τ that attains the maximum of $\left|\mathcal{A}_S^A(\tau)\right|$, we obtain $q' = p_1p_2$ and $\max\left|\mathcal{A}_S^A(\tau)\right| = |\Omega|\, p_1^{r-1}p_2^{s-1}$, which completes the proof. □

Remark. From the proof of Theorem 2, we see that the possible values of the arithmetic autocorrelation are in the set $\{0, \pm\Omega\}$ when $q = 3p_2^s$ and otherwise in the set

$$\left\{0, \pm\Omega p_1^{r-i}p_2^{s-j} : 1 \le i \le r,\ 1 \le j \le s\right\}.$$

Some concrete examples are given in Table 3 of Section 4.

3.3. Related to imaginary quadratic fields

Interestingly, the computation of the arithmetic autocorrelation of half-ℓ-sequences leads directly to the class numbers of imaginary quadratic fields. It seems that there is a way to compute $\lambda_{1,1}$ with the help of the class number of imaginary quadratic fields $\mathbb{Q}\left(\sqrt{-d}\right)$ with $d > 0$. The analysis of the class number of a quadratic field is a classical problem in number theory and algebra, dating back to Gauss. Below, we introduce some facts about imaginary quadratic fields.

Let d be a positive, square-free integer. Because the polynomial $t^2 + d$ is irreducible over the field of rational numbers $\mathbb{Q}$, the field extension

$$\mathbb{Q}\left(\sqrt{-d}\right) = \left\{a + b\sqrt{-d} : a, b \in \mathbb{Q}\right\},$$

obtained by adjoining a root $\sqrt{-d}$ of this polynomial to $\mathbb{Q}$, is called an *imaginary quadratic field*; see [18, 19]. The order of the ideal class group of $\mathbb{Q}\left(\sqrt{-d}\right)$ is known as the *class number* and is denoted by $h(-d)$.

Lemma 4. *Let $p_2 \equiv 7 \pmod 8$ be a prime number. Then, the class number $h(-p_2)$ of imaginary quadratic fields $\mathbb{Q}\left(\sqrt{-p_2}\right)$ satisfies*

$$h(-p_2) = \Delta.$$

Proof. According to Theorem 4 in Section 5.4 in [19], we have

$$\begin{aligned} h(-p_2) &= \left|\left\{a \in D_{p_2} : 0 < a < p_2/2\right\}\right| - \left|\left\{a \in \mathbb{Z}^*_{p_2} \setminus D_{p_2} \ : \ 0 < a < p_2/2\right\}\right| \\ &= \left|\left\{2a : a \in D_{p_2}, 0 < a < p_2/2\right\}\right| - \left|\left\{2a : a \in \mathbb{Z}^*_{p_2} \setminus D_{p_2}, 0 < a < p_2/2\right\}\right|. \end{aligned}$$

As before, let M_0 be the number of even numbers and M_1 the number of odd integers in D_{p_2}, respectively. Because $p_2 \equiv 7 \pmod 8$, we have $2 \in D_{p_2}$ and $2a \in D_{p_2}$ if $a \in D_{p_2}$. That is,

$$M_0 = \left|\left\{2a : a \in D_{p_2}, 0 < a < p_2/2\right\}\right|.$$

By the fact that $-1 \pmod{p_2} \in \mathbb{Z}^*_{p_2} \setminus D_{p_2}$, the number of odd integers in D_{p_2} equals the number of even integers in $\mathbb{Z}^*_{p_2} \setminus D_{p_2}$; that is,

$$M_1 = \left|\left\{2a : a \in \mathbb{Z}^*_{p_2} \setminus D_{p_2}, 0 < a < p_2/2\right\}\right|.$$

Hence, we derive

$$h(-p_2) = M_0 - M_1 = \Delta,$$

which completes the proof. □

Corollary 1. *Let $\mathcal{S}$ be a binary half-ℓ-sequence with connection integer $q = p_1^r p_2^s$, where $p_1 \equiv \pm 3 \pmod 8$, $p_2 \equiv 7 \pmod 8$, and r, s are positive integers. Then,*

- $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 2\}$ *occurs only when $q = 21$;*
- $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 4\}$ *occurs only when $q = 35$;*
- $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 6\}$ *occurs only when $q = 69$.*

Proof. (i). If $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 2\}$, then $h(-p_2) = 1$. It is known that $h(-d) = 1$ only for $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$. Hence, $p_2 = 7$, and $p_1 = 3$.

(ii). If $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 4\}$, then $p_1 = 5$, and $h(-p_2) = 1$. Hence, $p_2 = 7$, and $q = 35$.

(iii). Here, $\mathcal{A}^A_{\mathcal{S}}(\tau) \in \{0, \pm 6\}$. Then, $h(-p_2) = 3$. If $h(-d) = 3$, then $d = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907, 1001$. Thus, $p_2 = 23, 31$, and $p_1 = 3$. However, we do not have a half-ℓ-sequence when $q = 93$. □

Lemma 5. *Let $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv 5 \pmod 8$ be prime numbers. Then, the class number $h(-p_1p_2)$ of imaginary quadratic fields $\mathbb{Q}\left(\sqrt{-p_1p_2}\right)$ satisfies*

$$h(-p_1p_2) = |\Omega|.$$

Proof. By conditions we have the Jacobi symbol $\left(\frac{2}{p_1p_2}\right) = 1$ because

$$\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = -1.$$

We therefore derive

$$\left(\frac{a}{p_1p_2}\right) = 1 \text{ for all } 0 < a \in D_{p_1p_2},$$
$$\left(\frac{b}{p_1p_2}\right) = -1 \text{ for all } b \in \mathbb{Z}^*_{p_1p_2} \setminus D_{p_1p_2}.$$

Further, $\left(\frac{-1}{p_1p_2}\right) = -1$. Thus, a Jacobi symbol is a nonprincipal, odd primitive character modulo p_1p_2 in this case.

We can show in the same way as in Lemma 4 that the number of odds in $D_{p_1p_2}$ is given by

$$\begin{aligned}\lambda_{1,1} &= \varphi(p_1p_2)/2 - \left|\left\{2a : a \in D_{p_1p_2}, a < p_1p_2/2\right\}\right| \\ &= \varphi(p_1p_2)/2 - \left|\left\{a \in D_{p_1p_2} \ : \ a < p_1p_2/2\right\}\right|,\end{aligned}$$

and the number of odds in $\mathbb{Z}^*_q \setminus D_{p_1p_2}$ is given by

$$\begin{aligned}\lambda'_{1,1} &= \varphi(p_1p_2)/2 - \left|\left\{2a : a \in \mathbb{Z}^*_q \setminus D_{p_1p_2}, a < p_1p_2/2\right\}\right| \\ &= \varphi(p_1p_2)/2 - \left|\left\{a \in \mathbb{Z}^*_q \setminus D_{p_1p_2} \ : \ a < p_1p_2/2\right\}\right|.\end{aligned}$$

Hence, we have

$$\Omega = \lambda_{1,1} - \lambda'_{1,1} = -\sum_{\substack{a \in \mathbb{Z}^*_{p_1p_2} \\ a < p_1p_2/2}} \left(\frac{a}{p_1p_2}\right).$$

According to [20, Corollary 3.4], we get

$$\sum_{\substack{a \in \mathbb{Z}^*_{p_1p_2} \\ a < p_1p_2/2}} \left(\frac{a}{p_1p_2}\right) = h(-p_1p_2)\left(2 - \left[\frac{-p_1p_2}{2}\right]\right),$$

where $\left[\frac{-p_1p_2}{2}\right]$ is the Kronecker symbol. In this case, $\left[\frac{-p_1p_2}{2}\right] = 1$, as $-p_1p_2 \equiv 1 \pmod 8$. Hence, we finish the proof. □

Corollary 2. *Let $\mathcal{S}$ be a binary half-ℓ-sequence with connection integer $q = p_1^r p_2^s$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$, and r, s are positive integers. Then,*

- *There exists only one family of sequences with* $\mathcal{A}_S^A(\tau) \in \{0, \pm 2\}$ *when* $q = 3 \times 5^s$*;*
- *There exist no half-*ℓ*-sequences with* $\mathcal{A}_S^A(\tau) \in \{0, \pm 4\}$ *except* $q = 39$ *or* 55*.*

Proof. The class number of an imaginary quadratic field is an important invariant in algebraic number theory. For the cases of $h(-d) = 2$ or 4, complete lists of d-values have been established in prior literature (see p. 636 in [21] or pp. 425–426 in [19]). However, under the specific conditions of our corollary, not all of these fields admit a half-ℓ-sequence. For clarity, we summarize these fields and their relevant properties in relation to the corollary in Table 1 below. Some detailed examples are given in Table 4 in Section 4.

Table 1. Values of d for imaginary quadratic fields $\mathrm{Q}\left(\sqrt{-d}\right)$ with class number 2 or 4.

Class number	$h(-d) = 2$	$h(-d) = 4$
Values of d	5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 133, 187, 235, 267, 403, 467	14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97, 102, 130, 133, 142, 155, 177, 190, 193, 195, 203, 219, 253, 259, 291, 323, 355, 435, 483, 555, 595, 627, 667, 715, 723, 763, 795, 955, 1003, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555

(i) For the fields with class number $h(-d) = 2$, the half-ℓ-sequence exists only when q takes the form $q = 3 \times 5^s$.
(ii) For the fields with class number $h(-d) = 4$ listed in the table, the half-ℓ-sequence exists only for $q = 39$ and $q = 55$.

□

4. Experimental analysis

In this section, we present some numerical examples to verify our theoretical results. The numerical computations were carried out using Python. For related computational approaches to sequence analysis, see [22].

For $q = p_1^r 7^s$, a simple calculation shows that the period $T = 3p_1^{r-1}7^{s-1}(p_1 - 1)$ and the set of quadratic residues modulo 7 is $D_7 = \{1, 2, 4\}$, so the difference between the numbers of even and odd integers in D_7 is 1; that is, $\Delta = 1$. With the known result of $h(-7) = 1$, we have

$$\max \left|\mathcal{A}_S^A(\tau)\right| = p_1^{r-1}7^{s-1}(p_1 - 1) = T/3. \tag{4.1}$$

In the following, we list some examples in Table 2 to confirm Eq (4.1).

Table 2. $\mathcal{A}^A_{\mathcal{S}}(\tau)$ of binary half-ℓ-sequence $\mathcal{S}$ with connection integer $q = p_1^r 7^s$.

$q = p_1^r 7^s$	**Period** T	$\mathcal{A}^A_{\mathcal{S}}(\tau) \in$
$1043 = 149 \times 7$	3×148	$\{0, \pm 148\}$
$1589 = 227 \times 7$	3×226	$\{0, \pm 2, \pm 226\}$
$2597 = 53 \times 7^2$	3×364	$\{0, \pm 52, \pm 364\}$
$2891 = 59 \times 7^2$	3×406	$\{0, \pm 2, \pm 14, \pm 58, \pm 406\}$
$5929 = 11^2 \times 7^2$	3×770	$\{0, \pm 110, \pm 770\}$
$6125 = 5^3 \times 7^2$	3×700	$\{0, \pm 2, \pm 10, \pm 14, \pm 50, \pm 70, \pm 100, \pm 350, \pm 700\}$

For $q = 15$, we have $T = 4$, $D_{15} = \{1, 2, 4, 8\}$, and $\mathbb{Z}^*_{15} \setminus D_{15} = \{7, 11, 13, 14\}$. Then, the number of odd elements in D_{15} is 1, and thus, $|\Omega| = \left|\lambda_{1,1} - \lambda'_{1,1}\right| = h(-15) = 2$. In Table 3, we examine several cases for $q = 3^r 5^s$ and derive the result

$$\max\left|\mathcal{A}^A_{\mathcal{S}}(\tau)\right| = \begin{cases} 2 \times 3^{r-1} 5^{s-1}, & \text{if } r > 1, \\ 2, & \text{if } r = 1. \end{cases}$$

Table 3. $\mathcal{A}^A_{\mathcal{S}}(\tau)$ of binary half-ℓ-sequence $\mathcal{S}$ with connection integer $q = 3^r 5^s$.

$q = 3^r 5^s$	**Period** T	$\mathcal{A}^A_{\mathcal{S}}(\tau) \in$
$1875 = 3 \times 5^4$	2×500	$\{0, \pm 2\}$
$9375 = 3 \times 5^5$	2×2500	$\{0, \pm 2\}$
$1215 = 3^5 \times 5$	2×162	$\{0, \pm 2, \pm 6, \pm 18, \pm 54, \pm 162\}$
$3645 = 3^6 \times 5$	2×486	$\{0, \pm 2, \pm 6, \pm 18, \pm 54, \pm 162, \pm 486\}$
$3375 = 3^3 \times 5^3$	2×450	$\{0, \pm 2, \pm 6, \pm 18, \pm 30, \pm 90, \pm 150, \pm 450\}$
$6075 = 3^5 \times 5^2$	2×810	$\{0, \pm 2, \pm 6, \pm 18, \pm 30, \pm 54, \pm 90, \pm 162, \pm 270, \pm 810\}$

For general cases, we list some examples in Table 4. The class number $h(-d)$ of imaginary quadratic fields $\mathbb{Q}\left(\sqrt{-d}\right)$ can be found in the tables in [19].

Table 4. $\mathcal{A}^A_{\mathcal{S}}(\tau)$ of binary half-ℓ-sequence $\mathcal{S}$ with connection integer $q = p_1^r p_2^s$.

$q = p_1^r p_2^s$	**Period** T	$(p_1 \bmod 8, p_2 \bmod 8)$	$h(\cdot)$	$\max\left\|\mathcal{A}^A_{\mathcal{S}}(\tau)\right\|$
$3^3 \times 71$	630	(3, 7)	$h(-71) = 7$	$126 = 7 \times 2 \times 3^2$
11×23^2	2530	(3, 7)	$h(-23) = 3$	$690 = 3 \times 10 \times 23$
$13^2 \times 47$	3588	(5, 7)	$h(-47) = 5$	$780 = 5 \times 12 \times 13$
29×79	1092	(5, 7)	$h(-79) = 5$	$140 = 5 \times 28$
11×37	180	(3, 5)	$h(-407) = 16$	16
3×13^2	156	(3, 5)	$h(-39) = 4$	4
$3^4 \times 29$	756	(3, 5)	$h(-87) = 6$	$162 = 6 \times 3^3$
19×5^3	900	(3, 5)	$h(-95) = 8$	$200 = 8 \times 5^2$

5. Conclusions and final remarks

In this work, we have determined the arithmetic autocorrelation of binary half-ℓ-sequences with connection integers of the form $q = p_1^r p_2^s$. Our result demonstrates that these sequences might have very large arithmetic autocorrelations in some cases while showing small arithmetic autocorrelations in others. For instance, when $q = 3 \times 5^s$ with $s \geq 1$ or $q = 3 \times 7 = 21$, we have $\max \left|\mathcal{A}_{\mathcal{S}}^{A}(\tau)\right| = 2$ for a nontrivial shift τ; that is, $\mathcal{A}_{\mathcal{S}}^{A}(\tau) \in \{0, \pm 2\}$. We call such $\mathcal{S}$ has *almost ideal arithmetic correlations*. It would be interesting to construct new binary sequences with this property in future work.

We also turn to the classical autocorrelation $C_{\mathcal{S}}(\tau)$ of half-ℓ-sequences. Gu and Klapper [10, Theorem 3] demonstrated that when q is an odd prime,

$$|C_{\mathcal{S}}(\tau)| \leq \left\lceil \frac{q}{6} \right\rceil - 1.$$

For $q = p_1^r p_2^s$ extensive numerical experiments (see examples in Table 5) suggest the following conjecture.

Conjecture 1. *Let $q = p_1^r p_2^s$ with $r,\ s \geq 1$, where either $p_1 \equiv \pm 3 \pmod 8$, and $p_2 \equiv 7 \pmod 8$, or $p_1 \equiv 3 \pmod 8$, and $p_2 \equiv 5 \pmod 8$. Then, the classical autocorrelation of corresponding half-ℓ-sequence $\mathcal{S}$ satisfies*

$$|C_{\mathcal{S}}(\tau)| \leq \left\lceil \frac{\varphi(q)}{6} \right\rceil + 1.$$

We leave the proof of this conjecture for further investigation. For further results on sequences with small classical autocorrelation, see [23]; for related work on the correlation properties of interleaved Legendre sequences and Ding–Helleseth–Lam sequences, see [24].

Table 5. $C_{\mathcal{S}}(\tau)$ of binary half-ℓ-sequence $\mathcal{S}$ with connection integer $q = p_1^r p_2^s$.

$q = p_1^r p_2^s$	**period** T	$(p_1 \bmod 8, p_2 \bmod 8)$	$\max \lvert C_{\mathcal{S}}(\tau)\rvert$	$\lceil \varphi(q)/6 \rceil$
5×47	92	(5, 7)	32	31
5×23^2	1012	(5, 7)	336	338
37×47	828	(5, 7)	276	276
11×23	110	(3, 7)	38	37
3×1511	1510	(3, 7)	502	504
$3^2 \times 23^2$	1518	(3, 7)	506	506
947×5	1892	(3, 5)	632	631
3×101	100	(3, 5)	32	34
$19^2 \times 5^2$	3420	(3, 5)	1140	1140

Use of AI tools declaration

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

Acknowledgments

L. Xiao was supported in part by the Co-innovation Platform Project of Fuzhou-Xiamen-Quanzhou National Independent Innovation Demonstration Zone under Grant No. 2025E3006, by the Science and Technology Project of Putian City of China under Grant No. 2024SZ3001PTXY02, and by the Fujian Provincial Education and Research Project for Middle-aged and Young Teachers under Grant No. JAT251122. F. Yan was supported by the Fujian Key Laboratory of Financial Information Processing (Putian University) under Grant No. JXJS202502. V. Edemskiy was supported by Novgorod University in carrying out the research project "Mathematical modeling of natural processes".

Conflict of interest

The authors declare there are no conflicts of interest.

References

1. D. Lassoued, R. Shah, T. Li, Almost periodic and asymptotically almost periodic functions: part I, *Adv. Differ. Equations*, **47** (2018), 1–19. https://doi.org/10.1186/s13662-018-1487-0
2. M. Goresky, A. Klapper, *Algebraic Shift Register Sequences*, Cambridge University Press, 2012.
3. A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, *J. Cryptol.*, **10** (1997), 111–147. https://doi.org/10.1007/s001459900024
4. M. Goresky, A. Klapper, Arithmetic crosscorrelations of feedback with carry shift register sequences, *IEEE Trans. Inf. Theory*, **43** (1997), 1342–1345. https://doi.org/10.1109/18.605605
5. H. Wang, Q. Wen, J. Zhang, GLS: New class of generalized Legendre sequences with optimal arithmetic cross-correlation, *RAIRO-Theor. Inf. Appl.*, **47** (2013), 371–388. https://doi.org/10.1051/ita/2013043
6. 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
7. 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
8. X. Liu, H. Liu, Arithmetic autocorrelation and pattern distribution of binary sequences, *Electron. Res. Arch.*, **33** (2025), 849–866. https://doi.org/10.3934/era.2025038
9. T. Gu, A. Klapper, Distribution properties of half-ℓ sequences, in *Sequences and Their Applications - SETA 2014* (eds. K. U. Schmidt, A. Winterhof), Lecture Notes in Computer Science, **8865** (2014), 234–245. https://doi.org/10.1007/978-3-319-12325-7_20
10. T. Gu, A. Klapper, Statistical properties of half-ℓ-sequences, *Cryptogr. Commun.*, **8** (2016), 383–400. https://doi.org/10.1007/s12095-015-0152-7
11. Q. Wang, C. H. Tan, New bounds on the imbalance of a half-ℓ-sequence, in *IEEE International Symposium on Information Theory-ISIT 2015*, (2015), 2688–2691. https://doi.org/10.1109/ISIT.2015.7282944

12. Z. Niu, Y. Sang, On the linear complexity of binary half-ℓ-sequences, *Int. J. Network Secur.*, **24** (2022), 444–449. https://doi.org/10.6633/IJNS.202205_24(3).07
13. 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
14. J. Zhang, Z. Niu, L. Xiao, V. Edemskiy, On the maximum order complexity of ℓ-sequences and related sequences, *Int. J. Network Secur.*, **27** (2025), 1139–1145. https://doi.org/10.6633/IJNS.202511_27(6).04
15. Z. Chen, V. Edemskiy, C. Wu, Binary sequences with ideal and small arithmetic correlations, *Cryptogr. Commun.*, **17** (2025), 453–464. https://doi.org/10.1007/s12095-024-00770-7
16. L. Xiao, V. Edemskiy, Arithmetic autocorrelation of certain binary half-ℓ-sequences, in *Information Security and Cryptology-Inscrypt 2025*, Lecture Notes in Computer Science, **16408** (2026), 388–397. https://doi.org/10.1007/978-981-95-6206-0_20
17. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, **84**, (1990).
18. S. Arno, M. L. Robinson, F. S. Wheeler, Imaginary quadratic fields with small odd class number, *Acta Arith.*, **83** (1998), 295–330. https://doi.org/10.4064/aa-83-4-295-330
19. Z. I. Borevich, I. R. Shefarevich, *Number Theory*, Academic Press, Orlando, FL, 1966. https://doi.org/10.1201/9781351137621-2
20. B. Berndt, Classical theorems on quadratic residues, *Enseign. Math.*, **22** (1976), 261–304.
21. P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, New York, 2001.
22. A. Shahid, H. L. Huang, M. M. Bhatti, M. Marin, Numerical computation of magnetized bioconvection nanofluid flow with temperature-dependent viscosity and Arrhenius kinetic, *Math. Comput. Simul.*, **200** (2022), 377–392. https://doi.org/10.1016/j.matcom.2022.04.032
23. Y. Cai, C. Ding, Binary sequences with optimal autocorrelation, *Theor. Comput. Sci.*, **410** (2009), 2316–2322. https://doi.org/10.1016/j.tcs.2009.02.021
24. Y. Ren, C. Hou, H. Liu, Correlation properties of interleaved Legendre sequences and Ding-Helleseth-Lam sequences, *Electron. Res. Arch.*, **31** (2023), 4549–4556. https://doi.org/10.3934/era.2023232

AIMS Press