New Results on the 2-Adic Complexity of Binary Sequences

Longjiang Qu

College of Science
National University of Defense Technology

ljqu_happy@hotmail.com

(Joint work with Xiong Hai and Chao Li)

June 21, 2014
Overview

1. Motivation
2. Preliminaries
   - LFSR and Linear Complexity
   - FCSR and 2-adic Complexity
   - Optimal Autocorrelation Sequences
3. A New Method
   - A Key Lemma
   - The New Method
4. Applications of the New Method
   - Known Binary Sequences with Ideal Autocorrelation
   - Legendre Sequences and Ding-Helleseth-Lam Sequences
5. Two Classes of Binary Sequences with Interleaved Structure
6. Conclusions
Motivation

- Linear feedback shift registers (LFSRs) and feedback with carry shift registers (FCSRs) are two kinds of pseudo-random sequence generators.
- Linear complexity and 2-adic complexity are two of the most important security criteria of binary sequences.
- It is of interest to investigate the relationship between linear complexity and 2-adic complexity.
- Until now, there are only a few classes of pseudo-random sequences whose linear complexity and 2-adic complexity both are clear.
Binary sequences with optimal autocorrelation have played a significant role in many applications such as communications, cryptography, coding theory, etc.

However, no result about the 2-adic complexities of these sequences other than $m$-sequences is known yet.

Our Aim: To determine the 2-adic complexities of more sequences, especially those with optimal autocorrelation.
Notations

- Let \( s = (s_0, s_1, \cdots, s_{N-1}) \) be a binary sequence with period \( N \);
- \( D_s = \{0 \leq i \leq N - 1 | s_i = 1 \} \) is the support set of \( s \);
- \( P_s(x) = s_0 + s_1x + \cdots + s_{N-1}x^{N-1} \) is the sequence polynomial of \( s \);
Notations

- Let $s = (s_0, s_1, \cdots, s_{N-1})$ be a binary sequence with period $N$;
- $D_s = \{0 \leq i \leq N - 1 | s_i = 1\}$ is the support set of $s$.
- $P_s(x) = s_0 + s_1x + \cdots + s_{N-1}x^{N-1}$ is the sequence polynomial of $s$;
- $A_s = (a_{i,j})_{N \times N}$, where $a_{i,j} = s_{(i-j)} \mod N$.

$$A_s = \begin{pmatrix}
    s_0 & s_{N-1} & \cdots & s_2 & s_1 \\
    s_1 & s_0 & \cdots & s_3 & s_2 \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    s_{N-2} & s_{N-3} & \cdots & s_0 & s_{N-1} \\
    s_{N-1} & s_{N-2} & \cdots & s_1 & s_0
\end{pmatrix}.$$
Linear feedback shift registers

We call \( f(x) = \sum_{i=1}^{r} q_i x^i - 1 \) the connection polynomial of this LFSR.
Linear complexity

- For a binary sequence $s$, its linear complexity $LC(s)$ is the length of the shortest LFSR which can produce it.
- It is one of the most important security criteria since a periodic sequence $s$ can be completely determined by the Berlekamp-Massey algorithm [15] with $2LC(s)$ consecutive bits.
Lemma 1

(1) Let \( s = (s_0, s_1, \cdots) \) be a sequence of period \( N \) generated by the LFSR with connection polynomial \( f(x) \). Then \( \sum_{i=0}^{\infty} s_i x^i = \frac{g(x)}{f(x)} \). Further, the minimal polynomial of \( s \) is

\[
\frac{x^N - 1}{\gcd(x^N - 1, P_s(x))}
\]

and \( \text{LC}(s) = N - \deg(\gcd(x^N - 1, P_s(x))) \).

(2) Conversely, let \( s = (s_0, s_1, \cdots) \) be a periodic sequence over \( \mathbb{F}_q \). If \( \sum_{i=0}^{\infty} s_i x^i = \frac{g(x)}{f(x)} \), then \( s \) can be produced by the LFSR with connection polynomial \( f(x) \).
Feedback with carry shift register

We call $q = \sum_{i=1}^{r} q_i2^i - 1$ the *connection number* of this FCSR.
2-adic complexity

- We denote by \( \phi(s) \) the 2-adic complexity of \( s \), which is defined to be the length of the shortest FCSR which can produce \( s \).
- Let \( q(s) \) denote the connection number of that shortest FCSR. Then

\[
\phi(s) = \lceil \log_2(q(s) + 1) \rceil.
\]

- For binary sequences, 2-adic complexity is one of the most important security criteria. Because a periodic sequence \( s \) can be completely determined by the rational approximation algorithm [5] with \( 2\phi(s) \) consecutive bits.
2-adic complexity

The following result about 2-adic complexity of binary sequences was firstly presented by Klapper et. al. [1].

Lemma 2

1. Let \( s = (s_0, s_1, \cdots) \) be a periodic sequence generated by the FCSR with connection number \( q \). Then, in \( \mathbb{Q}_2 \), \( \sum_{i=0}^{\infty} s_i 2^i = \frac{p}{q} \), where \( p \) is an integer such that \(-q \leq p \leq 0\). Particularly, if \( \gcd(p, q) = 1 \), then \( \phi_2(s) = \lfloor \log_2(q + 1) \rfloor \).
2. Conversely, let \( s = (s_0, s_1, \cdots) \) be a binary periodic sequence. If \( \sum_{i=0}^{\infty} s_i 2^i = \frac{p}{q} \) in \( \mathbb{Q}_2 \), then \( s \) can be produced by the FCSR with connection number \( q \).
Similarly as the linear complexity, Klapper et. al. [1] got the following result.

**Lemma 3**

Let $s$ be a binary sequence of period $N$. Then

$$q(s) = \frac{2^N - 1}{\gcd(2^N - 1, P_s(2))}.$$
Definition 4

The autocorrelation function of $s$ is defined as follows.

$$C_s(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i + \tau + s_i}, \quad (0 \leq \tau \leq N - 1).$$
Definition 5

We say that $s$ is an **optimal autocorrelation sequence** if for any $\tau \neq 0$,

1. $C_s(\tau) = -1$ and $N \equiv -1 \pmod{4}$; or
2. $C_s(\tau) \in \{1, -3\}$ and $N \equiv 1 \pmod{4}$; or
3. $C_s(\tau) \in \{2, -2\}$ and $N \equiv 2 \pmod{4}$; or
4. $C_s(\tau) \in \{0, -4\}$ and $N \equiv 0 \pmod{4}$.

Please see [2] for a recent survey.  

---

Optimal autocorrelation sequences

Sequences in Class (1) are also said to have *ideal 2-level autocorrelation*. They are equivalent to cyclic difference sets.

**Definition 6**

We call subset $D$ of $\mathbb{Z}/(N)$ an $(N, k, \lambda)$ cyclic difference set if $|D| = k$ and $|D \cap (D + \tau)| = \lambda$ for any $\tau \neq 0$, where $D + \tau = \{x + \tau | x \in D\}$ and $\tau \in \mathbb{Z}/(N)$. 
Optimal autocorrelation sequences

Lemma 7

Let $s$ be a binary ideal 2-level autocorrelation sequence with period $N$. Then $D_s$, the support set of $s$, is an $(N, \frac{N+1}{2}, \frac{N+1}{4})$ or $(N, \frac{N-1}{2}, \frac{N-3}{4})$ cyclic difference set.

Based on their periods, all the known ideal 2-level autocorrelation sequences can be divided into three classes:

1. $N = 2^n - 1$;
2. $N = p$, where $p \equiv 3 \mod 4$ is a prime number;
3. $N = p(p + 2)$, where both $p$ and $p + 2$ are prime numbers.

It is generally conjectured that every such difference set has parameters as in one of the three series above.
Optimal autocorrelation sequences

The other three classes of optimal autocorrelation sequences are equivalent to almost cyclic difference sets.

**Definition 8**

We call subset $D$ of $\mathbb{Z}/(N)$ an $(N, k, \lambda, t)$ almost cyclic difference set if $|D| = k$ and $|D \cap (D + \tau)| = \lambda$ for $t$'s $\tau \neq 0$ while $|D \cap (D + \tau)| = \lambda + 1$ for the other $(N - 1 - t)$'s $\tau \neq 0$, where $D + \tau = \{x + \tau | x \in D\}$ and $\tau \in \mathbb{Z}/(N)$. 
Known results about linear complexity and 2-adic complexity of optimal autocorrelation sequences

- Linear complexity of most of optimal autocorrelation sequences is determined, such as $m$ sequences, Legendre sequences [6], Twin-prime sequences [7], Hall’s sextic sequences [16] and some other optimal autocorrelation sequences with interleaved structure [8-10].
- In contrast, before 2013, only 2-adic complexity of $m$ sequences is clear [11-12].
Lemma 9

Let \( s = (s_0, s_1, \cdots, s_{N-1}) \) be a binary sequence with period \( N \) and let \( P_s(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x] \). Let \( A = (a_{i,j})_{N \times N} \) be the matrix defined by \( a_{i,j} = s(i-j) \mod N \), and let us view \( A \) as a matrix over \( \mathbb{Q} \). If \( \det(A) \neq 0 \), then there exist \( u(x), v(x) \in \mathbb{Z}[x] \) such that

\[
u(x) P_s(x) + v(x)(1 - x^N) = \det(A), \tag{1}\]

where \( \deg u \leq N - 1, \ \deg v \leq N - 2 \).
A proof of Lemma 9

Note that Eq. (1) is equivalent to the following linear equation systems:

\[
\begin{aligned}
\begin{cases}
  s_0 u_0 + v_0 &= \det(A) \\
  s_1 u_0 + s_0 u_1 + v_1 &= 0 \\
  \cdots &= \cdots \\
  \sum_{i=0}^{N-2} s_{N-2-i} u_i + v_{N-2} &= 0 \\
  \sum_{i=0}^{N-1} s_{N-1-i} u_i &= 0 \\
  \sum_{i=1}^{N-1} s_{N-i} u_i - v_0 &= 0 \\
  \cdots &= \cdots \\
  s_{N-1} u_{N-1} - v_{N-2} &= 0
\end{cases}
\end{aligned}
\]

(2)
Let $C$ denote the coefficient matrix of Eq. (2).

$$
C = \begin{pmatrix}
    s_0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
    s_1 & s_0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\
    \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
    s_{N-2} & s_{N-3} & \cdots & 0 & 0 & 0 & \cdots & 1 \\
    s_{N-1} & s_{N-2} & \cdots & s_0 & 0 & 0 & \cdots & 0 \\
    0 & s_{N-1} & \cdots & s_1 & -1 & 0 & \cdots & 0 \\
    \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
    0 & 0 & \cdots & s_{N-1} & 0 & 0 & \cdots & -1 \\
\end{pmatrix}.
$$
A proof of Lemma 9

Adding the last \((N - 1)\) rows of \(C\) on the first \((N - 1)\) rows, we get

\[
D = \begin{pmatrix}
s_0 & s_{N-1} & \ldots & s_1 & 0 & 0 & \ldots & 0 \\
s_1 & s_0 & \ldots & s_2 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
s_{N-2} & s_{N-3} & \ldots & s_{N-1} & 0 & 0 & \ldots & 0 \\
s_{N-1} & s_{N-2} & \ldots & s_0 & 0 & 0 & \ldots & 0 \\
0 & s_{N-1} & \ldots & s_1 & -1 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & s_{N-1} & 0 & 0 & \ldots & -1 \\
\end{pmatrix}.
\]
A proof of Lemma 9

Then one can verify that

\[ \det(C) = \det(D) = \pm \det(A) \neq 0. \]  (3)

Hence Equation (2) has a unique solution

\[ \alpha = (u_0, \cdots, u_{N-1}, v_0, \cdots, v_{N-2})^T = C^{-1} \beta \in \mathbb{Z}^{2^N-1}, \] where
\[ \beta = (\det(A), 0, \cdots, 0)^T. \]
A general theorem

Theorem 10

Let the symbols be defined as in Lemma 9. If \( \gcd(1 - 2^N, \det(A)) = 1 \), then \( \phi_2(s) = N \).

Substituting \( x = 2 \) into the Eq. (2) and letting \( M = P_s(2) \), we have

\[
u(2)M + v(2)(1 - 2^N) = \det(A).
\]

(4)

Hence we have \( \gcd(M, 1 - 2^N) = 1 \) since \( \gcd(1 - 2^N, \det(A)) = 1 \). Then the theorem holds.
Two Remarks

Let \( d_1 = \gcd(M, 1 - 2^N) \) and \( d_2 = \gcd(1 - 2^N, \det(A)) \). Then it follows from (4) that \( d_1 | d_2 \). Hence \( q(s) = \frac{2^N - 1}{d_1} \geq \frac{2^N - 1}{d_2} \). Thus one can get a lower bound on \( q(s) \) and consequently a lower bound on \( \pi(s) \) if \( d_2 = \gcd(1 - 2^N, \det(A)) \neq 1 \).
Two Remarks

Let $d_1 = \gcd(M, 1 - 2^N)$ and $d_2 = \gcd(1 - 2^N, \det(A))$. Then it follows from (4) that $d_1|d_2$. Hence $q(s) = \frac{2^N-1}{d_1} \geq \frac{2^N-1}{d_2}$. Thus one can get a lower bound on $q(s)$ and consequently a lower bound on $\pi(s)$ if $d_2 = \gcd(1 - 2^N, \det(A)) \neq 1$.

It is clear that Theorem 10 can be naturally generalized to $p$-ary sequences.
Theorem 10 provides a new method to compute the 2-adic complexity of binary sequences. The key point of this method is to compute $\det(A)$ and then verify whether $\gcd(2^N - 1, \det(A)) = 1$, where $A$ is the circulant matrix constructed from the sequence.
Lemma 11

Let $s$ be a sequence with period $N$ and let $A = (a_{k,j})_{N \times N}$ be the matrix defined by $a_{k,j} = s_{(k-j) \mod N}$. Then $\det(A) = \prod_{j=0}^{N-1} P_s(w_j^j)$, where \( w_N = e^{\frac{2\pi i}{N}} \) is a primitive $N$-th root of unity of $\mathbb{C}$.

It is clear that $P_s(1) = \sum_{k=0}^{N-1} s_k = |D_s|$. For $1 \leq j \leq N - 1$, we have

$$P_s(w_j^j) = \sum_{k=0}^{N-1} s_k (w_j^j)^k = \sum_{k \in D_s} (w_j^j)^k.$$

Hence computing $P_s(w_j^j)$ is related to some exponential sums.
Two Cases

- If the corresponding exponential sums can be computed, then one can compute $\det(A)$ and check whether $\gcd(2^N - 1, \det(A)) = 1$. This is the case of Legendre sequences, Ding-Helleseth-Lam sequences and Ding-Helleseth-Martinsen sequences.
Two Cases

- If the corresponding exponential sums can be computed, then one can compute $\det(A)$ and check whether $\gcd(2^N - 1, \det(A)) = 1$. This is the case of Legendre sequences, Ding-Helleseth-Lam sequences and Ding-Helleseth-Martinsen sequences.

- If the exponential sums can not be easily computed, we may use other methods to compute $\det(A)$. This is the case of all the known binary sequences with ideal 2-level autocorrelation.
2-adic complexity of ideal two level autocorrelation sequence

**Theorem 12**

Let $s$ be any known ideal 2-level autocorrelation sequence with period $N$. Then its 2-adic complexity is $N$. 
A proof of Theorem 12

Clearly, according to Theorem 10, it suffice to prove that $\gcd(2^N - 1, \det(A)) = 1$. 
A proof of Theorem 12

- Clearly, according to Theorem 10, it suffice to prove that $\gcd(2^N - 1, \det(A)) = 1$.
- According to the properties of ideal two level autocorrelation sequences, we find it is easy to compute $\det(B)$, where $B = A^T A$. In fact, we can get $\det(B) = \left(\frac{N+1}{2}\right)^2 \left(\frac{N+1}{4}\right)^{N-1}$. 
A proof of Theorem 12

- Clearly, according to Theorem 10, it suffice to prove that $\gcd(2^N - 1, \det(A)) = 1$.

- According to the properties of ideal two level autocorrelation sequences, we find it is easy to compute $\det(B)$, where $B = A^T A$. In fact, we can get $\det(B) = (\frac{N+1}{2})^2(\frac{N+1}{4})^{N-1}$.

- Since there are only three cases of $N$, one can verify that $\gcd(2^N - 1, \det(A)) = 1$ by each of cases.
Conjecture 13

If there exists a binary ideal 2-level autocorrelation sequence with period $N$, or equivalently, if there exists an $(N, \frac{N+1}{2}, \frac{N+1}{4})$ or $(N, \frac{N-1}{2}, \frac{N-3}{4})$ cyclic difference set, then $\gcd(2^N - 1, N + 1) = 1$. 
Theorem 12 gives a unified proof that all the known binary sequences with ideal 2-level autocorrelation have the maximum 2-adic complexities.
Theorem 12 gives a unified proof that all the known binary sequences with ideal 2-level autocorrelation have the maximum 2-adic complexities.

Now we can say more about the relation of linear complexity and 2-adic complexity.

**Table:** Examples of Binary Sequence with Period $N$

<table>
<thead>
<tr>
<th>Sequence Type</th>
<th>2-adic complexity</th>
<th>Linear complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l$ sequences</td>
<td>minimum</td>
<td>$\leq \frac{N+1}{2}$</td>
</tr>
<tr>
<td>$m$ sequences</td>
<td>maximum</td>
<td>minimum</td>
</tr>
<tr>
<td>Legendre sequences</td>
<td>maximum</td>
<td>maximum</td>
</tr>
<tr>
<td>Hall’s sextic sequences</td>
<td>maximum</td>
<td>maximum</td>
</tr>
</tbody>
</table>
In this subsection, we will use Theorem 10 to determine 2-adic complexities of Legendre sequences and Ding-Helleseth-Lam sequences.

According to Theorem 10 and the analysis followed, we need to compute $P_s(w^j)$, which is related to some exponential sums.

A Legendre sequence is related to a quadratic Gauss sum, while a Ding-Helleseth-Lam sequence is related to a quartic Gauss sum.
Gauss sums

Let $p$ be a prime number and let $\psi$ be a multiplicative character of $\mathbb{F}_p$. Define

$$G(\psi; \alpha) = \sum_{x \in \mathbb{F}_p^*} \psi(x) w_p^{\alpha x}$$

and

$$g(k; \alpha) = \sum_{x \in \mathbb{F}_p} w_p^{\alpha x^k},$$

where $k$ is an integer, $w_p = e^{\frac{2\pi i}{p}}$ is a primitive $p$-th root of unity of $\mathbb{C}$ and $\alpha \in \mathbb{F}_p$. 
Gauss sums

Both the above sums are called *Gauss sums* and they are connected by the following results [4].

**Lemma 14**

Let $\psi$ be a multiplicative character of $\mathbb{F}_p$ with order $k$. Then

$$g(k; \alpha) = \sum_{j=1}^{k-1} G(\psi^j; \alpha) = \sum_{j=1}^{k-1} \psi^j(\alpha^{-1})G(\psi^j; 1).$$
**Lemma 15**

Assume that $p \equiv 1 \mod 4$. Then the following statements hold.

1. If $\psi$ is the quadratic character of $\mathbb{F}_p$, then $G(\psi; 1) = g(2; 1) = \sqrt{p}$;
2. If $\psi$ is a character of order 4, then
   \[
   G(\psi; 1) + G(\psi^3; 1) = \pm \left\{ 2 \left( \frac{2}{p} \right) (p + a\sqrt{p}) \right\}^{1/2},
   \]
   where \( \left( \frac{2}{p} \right) \equiv 2^{p-1}/2 \mod p \) is the Legendre symbol, $a$, $b$ are two integers such that $a^2 + b^2 = p$ and $a \equiv - \left( \frac{2}{p} \right) \mod 4$;
3. If $\psi$ is a nontrivial character, then $|G(\psi; 1)| = \sqrt{p}$. 

Longjiang Qu

New Results on the 2-Adic Complexity of Binary Sequences
2-adic complexity of Legendre sequences

**Legendre Sequences**: Let \( p \equiv 1 \mod 4 \) be a prime number. Let \( s \) be a binary sequence defined by

\[
    s_i = \begin{cases} 
        1, & \text{if } i \in D_0^{(2,p)}; \\
        0, & \text{otherwise}.
    \end{cases}
\]

Then \( s \) has optimal out-of-phase autocorrelation values \( \{1, -3\} \).

**Theorem 16**

*Let \( s \) be a Legendre sequence with period \( p \equiv 1 \mod 4 \). Then \( \phi_2(s) = p \).*
A proof of Theorem 16

By Theorem 10, it suffices to prove that \( \gcd(1 - 2^p, \det(A)) = 1 \), where \( A = (a_{k,j})_{p \times p} \) is the matrix defined by \( a_{k,j} = s(k-j) \mod p \).

\[
P_s(w^j_p) = \sum_{k \in D_0^{(2,p)}} w^{kj}_p = \begin{cases} \frac{p-1}{2}, & \text{if } j = 0; \\ B_0, & \text{if } j \in D_0^{(2,p)}; \\ B_1, & \text{if } j \in D_1^{(2,p)}. \end{cases}
\]

Let \( w_p = e^{\frac{2\pi i}{p}} \), \( B_0 = \sum_{x \in D_0^{(2,p)}} w^x_p \) and \( B_1 = \sum_{x \in D_1^{(2,p)}} w^x_p \).
A proof of Theorem 16

\[
\det(A) = \prod_{j=0}^{p-1} P_s(w^j_p)
\]

\[
= \frac{p-1}{2} \left( \frac{\sqrt{p}-1}{2} \right)^{\frac{p-1}{2}} \left( \frac{-\sqrt{p}-1}{2} \right)^{\frac{p-1}{2}}
\]

\[
= \frac{p-1}{2} \left( \frac{p-1}{4} \right)^{\frac{p-1}{2}}
\]

Hence we have that \( \gcd(1 - 2^p, \det(A)) = 1 \).
2-adic complexity of Ding-Helleseth-Lam sequences

**Ding-Helleseth-Lam Sequences**: Let \( p \equiv 1 \mod 4 \) be a prime number. Let \( s \) be a binary sequence defined by

\[
s_i = \begin{cases} 
1, & \text{if } i \in D_0^{(4,p)} \cup D_1^{(4,p)}; \\
0, & \text{otherwise}.
\end{cases}
\]

Then \( s \) has optimal out-of-phase autocorrelation values \( \{1, -3\} \).

**Theorem 17**

Let \( s \) be a Ding-Helleseth-Lam sequence with period \( p \equiv 1 \mod 4 \). Then \( \phi_2(s) = p \).
Binary Sequences with Interleaved Structure

Assume that $s$ is a sequence with period $NT$ where $N$, $T$ both are positive integers. Then it can be arranged as a matrix $M_s$ of the form

$$M_s = \begin{pmatrix}
  s_0 & s_1 & \cdots & s_{T-1} \\
  s_T & s_{T+1} & \cdots & s_{2T-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  s_{(N-1)T} & s_{(N-1)T+1} & \cdots & s_{NT-1}
\end{pmatrix}.$$
And we say that $s$ has an $N \times T$ interleaved structure. We usually denote it by $s = I(a^0, a^1, \cdots, a^{T-1})$, where $a^i = (s_i, s_{i+T}, \cdots, s_{i+(N-1)T})$. We also call $\{a^i | 0 \leq i \leq T - 1\}$ the base sequences of $s$.

In particular, if there exist a sequence $a$ and a set of integers $\{e_i | 0 \leq i \leq T - 1\}$ such that $a^i = L^{e_i}a$, then we call $(e_0, e_1, \cdots, e_{T-1})$ a shift sequence of $s$ with respect to base sequence $a$. 
Zhou-Tang-Gong sequences

Construction A: Let $a$ be an optimal autocorrelation sequence with period $N(\equiv 3 \mod 4)$. Randomly choose a positive integer $L$ such that $2 < L < N$.

(1) If $L$ is an even integer, let $M = \lfloor \frac{N-2}{L} \rfloor$. Define shift sequences $(e_{i,0}, e_{i,1})(0 \leq i < M)$ as

$$(e_{i,0}, e_{i,1}) = \begin{cases} \left( \frac{L}{2} i, N - 1 - \frac{L}{2} (i + 1) \right), & \text{if } L | (N - 1); \\ \left( \frac{L}{2} i, N - \frac{L}{2} (i + 1) \right), & \text{otherwise.} \end{cases}$$
(2) If $L$ is an odd integer, let $M = \lfloor \frac{N-1}{L} \rfloor$. Define shift sequences $(e_{i,0}, e_{i,1})(0 \leq i < M)$ as

$$(e_{i,0}, e_{i,1}) = \begin{cases} 
\left( \frac{i}{2} L, N - \frac{L - 1}{2} - \frac{i}{2} L \right), & \text{if } L | N, \ i \ \text{even}; \\
\left( N - 1 - \frac{i + 1}{2} L, \frac{iL + 1}{2} \right), & \text{if } L | N, \ i \ \text{odd}; \\
\left( \frac{i}{2} L, N - \frac{L - 1}{2} - \frac{i}{2} L \right), & \text{if } L \not| N, \ i \ \text{even}; \\
\left( N - \frac{i + 1}{2} L, \frac{iL + 1}{2} \right), & \text{if } L \not| N, \ i \ \text{odd}.
\end{cases}$$
Zhou-Tang-Gong sequences

Let $U_1 = \{s^i | 0 \leq i < M, s^i = I(L^{e_i,0} a, L^{e_i,1} a)\}$ and $U_2 = \{s^{i+M} | 0 \leq i < M, s^{i+M} = I(L^{e_i,0} a, L^{e_i,1} a + 1)\}$ be two sequence sets. Then $U = U_1 \cup U_2$ is a $(2N, 2M, L, 2)$-LCZ sequence set.
Tang-Ding sequences

Construction: Let \( a, b \) be two optimal autocorrelation sequences with period \( N(\equiv 3 \mod 4) \). Let \( s = l(a, b, L^{\frac{N+1}{2}} a, L^{\frac{N+1}{2}} b + 1) \). Then \( s \) is an almost balanced optimal autocorrelation sequence with period \( 4N \).
Two Lemmas

Lemma 18

Let \( u = I(a^0, a^1, \ldots, a^{T-1}) \), where \( a^i(0 \leq i \leq T - 1) \) are binary sequences with the same period \( N \). Then

\[
P_u(2) = P_{a^0}(2^T) + 2P_{a^1}(2^T) + \cdots + 2^{T-1}P_{a^{T-1}}(2^T).
\]

Particularly, if there exists a sequence \( s \) such that \( a^i = L^{e_i}s \) for \( 0 \leq i \leq (T - 1) \), then

\[
P_u(2) = P_s(2^T)(\sum_{i=0}^{T-1} 2^{(N-e_i)T+i}) \pmod{2^{NT} - 1}.
\]
Two Lemmas

Lemma 19

Let $s$ be any binary ideal 2-level autocorrelation sequence with known period $N > 15$. Then

1. $\gcd(P_s(2^2), 2^{2N} - 1) = \gcd(3, N + 1)$;
2. $\gcd(P_s(2^4), 2^{4N} - 1) = \gcd(15, N + 1)$. 
2-adic complexity of Zhou-Tang-Gong sequences

**Theorem 20**

Let \( a \) be any ideal 2-level autocorrelation sequence with known period \( N \). For any sequence \( s^i \in \mathcal{U}_1 \), we have

\[
q(s^i) = \frac{2^{2N} - 1}{2^{\gcd(N, 2e_i - 1)} + 1}.
\]

Besides, one can get \( \phi(s^i) = 2N - \gcd(N, 2e_i - 1) - 1 \).
Theorem 21

Let \( a \) be any ideal 2-level autocorrelation sequence with known period \( N \). For any sequence \( s^{i+M} \in \mathcal{U}_2 \), we have

\[
q(s^{i+M}) = \frac{2^{2N} - 1}{2^{\gcd(N, 2e_i - 1)} - 1}.
\]

Besides, one can get

\[
\phi(s^{i+M}) = \begin{cases} 
2N, & \text{if } \gcd(N, 2e_i - 1) = 1; \\
2N - \gcd(N, 2e_i - 1), & \text{otherwise}.
\end{cases}
\]
2-adic complexity of Tang-Ding sequences

Theorem 22

Let \( s = l(a, b, L^{N+1/2}a, L^{N+1/2}b + 1) \), where \( a \) and \( b \) are ideal 2-level autocorrelation sequences with known period \( N \). Then \( q(s) = 2^{4N} - 1 \), and thus \( \phi(s) = 4N \).
Our Contributions

- A new method is presented to compute the 2-adic complexity of binary sequences.
- All the known binary sequences with ideal 2-level autocorrelation are uniformly proved to have the maximum 2-adic complexities, i.e. their 2-adic complexities equal their periods.
- We also investigated the 2-adic complexities of two classes of optimal autocorrelation sequences with period $N \equiv 1 \mod 4$.
- 2-Adic complexities of two classes of binary sequences with interleaved structure are determined.
Future Work

- Can this new method be used to determine the 2-adic complexities of more binary sequences?
- In classes (2)-(4) of optimal autocorrelation sequences, there are still some sequences whose 2-adic complexity is unclear.
- For sequences in Class (1), we determine their 2-adic complexity only by using the properties of cyclic difference sets. While for other sequences, can we determine their 2-adic complexity only by using the properties of almost cyclic difference sets?
- To prove/disprove the conjecture about the length of a binary sequence with ideal 2-level autocorrelation.
References


References


References


Thanks for your attention!