BINARY SEQUENCES DERIVED FROM DIFFERENCES OF CONSECUTIVE QUADRATIC RESIDUES

ARNE WINTERHOF
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria

ZIBI XIAO
College of Science
Wuhan University of Science and Technology
Wuhan 430081, Hubei, China

Abstract. For a prime \( p \geq 5 \) let \( q_0, q_1, \ldots, q_{(p-3)/2} \) be the quadratic residues modulo \( p \) in increasing order. We study two \( (p-3)/2 \)-periodic binary sequences \((d_n)\) and \((t_n)\) defined by \( d_n = q_n + q_{n+1} \mod 2 \) and \( t_n = 1 \) if \( q_{n+1} = q_n + 1 \) and \( t_n = 0 \) otherwise, \( n = 0, 1, \ldots, (p-5)/2 \). For both sequences we find some sufficient conditions for attaining the maximal linear complexity \((p-3)/2\).

Studying the linear complexity of \((d_n)\) was motivated by heuristics of Caragiu et al. However, \((d_n)\) is not balanced and we show that a period of \((d_n)\) contains about \( 1/3 \) zeros and \( 2/3 \) ones if \( p \) is sufficiently large. In contrast, \((t_n)\) is not only essentially balanced but also all longer patterns of length \( s \) appear essentially equally often in the vector sequence \((t_n, t_{n+1}, \ldots, t_{n+s-1})\), \( n = 0, 1, \ldots, (p-5)/2 \), for any fixed \( s \) and sufficiently large \( p \).

1. Introduction

The linear complexity \( L(s_n) \) of a sequence \((s_n)\) over \( \mathbb{F}_2 \) is the length \( L \) of the shortest linear recurrence

\[
s_{n+L} = c_{L-1}s_{n+L-1} + \ldots + c_0s_n, \quad n = 0, 1, \ldots
\]

with coefficients \( c_0, \ldots, c_{L-1} \in \mathbb{F}_2 \). It is an important measure for the unpredictability and thus suitability of a sequence in cryptography. For surveys on linear complexity and related measures see [10, 11, 16, 17].

Caragiu et al. [2] suggested to study the linear complexity of the sequence of the parities of differences of consecutive quadratic residues modulo \( p \). In particular, they calculated the linear complexities for the first 1000 primes \( p \geq 5 \).

More precisely, for a prime \( p \geq 5 \) we identify the finite field \( \mathbb{F}_p \) of \( p \) elements with the set of integers \( \{0, 1, \ldots, p-1\} \). Let \( q_0, \ldots, q_{(p-3)/2} \) be the quadratic residues modulo \( p \) in increasing order \( 1 = q_0 < q_1 < \ldots < q_{(p-3)/2} \leq p-1 \). We consider
the sequence \((d_n)\) of parities of the differences (or sums) of consecutive quadratic residues modulo \(p\),
\begin{equation}
    d_n = q_n + q_{n+1} \mod 2, \quad n = 0, 1, \ldots, (p - 5)/2,
\end{equation}
and continue it with period \((p - 3)/2)\),
\begin{equation}
    d_{n+(p-3)/2} = d_n, \quad n = 0, 1, \ldots
\end{equation}

The heuristic of Caragiu et al. for the linear complexity of \((d_n)\) shows that among the first 1000 primes \(p \geq 5\) there are 671 sequences \((d_n)\) with maximal linear complexity \((p - 3)/2\)

In Section 2, we give some sufficient conditions on \(p\) for the maximality of \(L(d_n) = (p - 3)/2\).

Balancedness is another desirable feature of a cryptographic sequence, that is, each period should contain about the same numbers of zeros and ones. We show in Section 3 that the sequence \((d_n)\) contains asymptotically \(1/3\) zeros and \(2/3\) ones in each period and is very unbalanced.

Since \((d_n)\) is not balanced, we define a similar \((p - 3)/2\)-periodic sequence \((t_n)\) which is essentially balanced and defined by
\begin{equation}
    t_n = \begin{cases} 
    1, & q_{n+1} = q_n + 1, \\
    0, & q_{n+1} \neq q_n + 1,
    \end{cases} \quad n = 0, 1, \ldots, (p - 5)/2.
\end{equation}

In Section 4 we will show that \((t_n)\) is essentially balanced. Moreover, for fixed length \(s\) each pattern \((t_n, t_{n+1}, \ldots, t_{n+s-1}) = \neq \in \{0, 1\}^s\) appears for essentially the same number of \(n\) with \(0 \leq n \leq (p - 3)/2\) provided that \(p\) is sufficiently large with respect to \(s\).

Finally, we study the linear complexity of \((t_n)\) in Section 5 and provide a sufficient criterion for the maximality of \(L(t_n)\). We also prove a lower bound on the \(N\)th maximum order complexity of \((t_n)\) which implies a rather moderate but non-trivial and unconditional lower bound on the \(N\)th linear complexity of \((t_n)\).

We use the notation \(f(n) = O(g(n))\) if \(|f(n)| \leq cg(n)\) for some absolute constant \(c > 0\).

2. Linear complexity of \((d_n)\)

Our starting point to determine the linear complexity of a periodic sequence is [3, Lemma 8.2.1].

**Lemma 2.1.** Let \((s_n)\) be a \(T\)-periodic sequence over \(\mathbb{F}_2\) and

\[ S(X) = \sum_{n=0}^{T-1} s_n X^n. \]

Then the linear complexity \(L(s_n)\) of \((s_n)\) is

\[ L(s_n) = T - \deg(\gcd(X^T - 1, S(X))). \]

We write the period of the sequence \((d_n)\) in the form

\[ T = \frac{p - 3}{2} = 2^s r \]

with integers \(s \geq 0\) and odd \(r\). Then we have

\[ X^T - 1 = (X^r - 1)^{2^s}. \]
Sequences from differences of consecutive quadratic residues

We have to determine \( \gcd(X^T - 1, D(X)) \), where

\[
D(X) = \sum_{n=0}^{(p-5)/2} d_n X^n.
\]

First we study whether \( D(X) \) is divisible by \((X - 1)\), that is, we determine the value of \( D(1) \in \mathbb{F}_2 \). According to the definition of the sequence \((d_n)\), we get

\[
D(1) = \sum_{n=0}^{(p-5)/2} d_n \equiv q_0 + 2 \sum_{i=1}^{(p-5)/2} q_i + q_{(p-3)/2} \equiv 1 + q_{(p-3)/2} \mod 2.
\]

Since \(-1\) is a quadratic residue modulo \(p\) if and only if \(p \equiv 1 \mod 4\) and \(2\) is a quadratic residue modulo \(p\) if and only if \(p \equiv \pm1 \mod 8\), the largest quadratic residue \(q_{(p-3)/2}\) modulo \(p\) is

\[
q_{(p-3)/2} = \begin{cases} 
  p - 1, & p \equiv 1 \mod 4, \\
  p - 2, & p \equiv 3 \mod 8.
\end{cases}
\]

In the remaining case \(p \equiv 7 \mod 8\), both \(-1\) and \(-2\) are quadratic non-residues. Hence, the largest quadratic residue modulo \(p\) is \(p - u\) for some \(u > 2\). Assume \(u = 2m\) for some positive integer \(m\). Since \(-u\) and \(2\) are both quadratic residues modulo \(p\), \(-m \equiv p - m \mod p\) is quadratic residue modulo \(p\) as well, a contradiction to the maximality of \(p - u\). Hence, \(u\) is odd. So, the largest quadratic residue modulo \(p\) is

\[
q_{(p-3)/2} = \begin{cases} 
  p - 1 \equiv 0 \mod 2, & p \equiv 1 \mod 4, \\
  p - 2 \equiv 1 \mod 2, & p \equiv 3 \mod 8, \\
  p - u \equiv 0 \mod 2, & p \equiv 7 \mod 8.
\end{cases}
\]

Thus we have

\[
D(1) = \begin{cases} 
  0, & p \equiv 3 \mod 8, \\
  1, & p \not\equiv 3 \mod 8.
\end{cases}
\]

We return now to a general binary sequence \((s_n)\) of period \(T\). The following provides a necessary condition for \(S(\beta) = 0\) for a primitive \(r\)th root of unity \(\beta\) in some extension field of \(\mathbb{F}_2\).

**Lemma 2.2.** Let \(r\) be an odd prime divisor of \(T\) such that \(2\) is a primitive root modulo \(r\). Let \(\beta\) be any primitive \(r\)th root of unity in some extension field of \(\mathbb{F}_2\). If \(S(\beta) = 0\), then we have

\[
\sum_{j=0}^{T/r-1} s_{h+jr} = S(1), \quad h = 0, 1, \ldots, r - 1.
\]

**Proof.** Since \(2\) is a primitive root modulo \(r\), the cyclotomic polynomial

\[
1 + X + \ldots + X^{r-1}
\]

is irreducible over \(\mathbb{F}_2\), and thus the minimal polynomial of \(\beta\). In particular we have

\[
\beta^{r-1} = \sum_{h=0}^{r-2} \beta^h
\]
and $1, \beta, \ldots, \beta^{r-2}$ are linearly independent. Since $\beta^r = 1$ we get

$$S(\beta) = \sum_{n=0}^{T-1} s_n \beta^n = \sum_{h=0}^{r-1} \sum_{j=0}^{T/r-1} s_{h+jr} \beta^h = \sum_{h=0}^{r-2} \left( \sum_{j=0}^{T/r-1} s_{h+jr} - \sum_{j=0}^{T/r-1} s_{r-1+jr} \right) \beta^h.$$ 

Assume $S(\beta) = 0$. Then we get

$$\sum_{j=0}^{T/r-1} s_{h+jr} = \sum_{j=0}^{T/r-1} s_{r-1+jr}, \quad h = 0, 1, \ldots, r-2.$$ 

Hence, since $r$ is odd and

$$S(1) = \sum_{h=0}^{r-1} \sum_{j=0}^{T/r-1} s_{h+jr} = r \sum_{j=0}^{T/r-1} s_{r-1+jr} = \sum_{j=0}^{T/r-1} s_{r-1+jr},$$

the result follows.

Now we are ready to prove a sufficient condition on $p$ for $(d_n)$ having maximal linear complexity $L(d_n) = (p - 3)/2$.

**Theorem 2.3.** Let $p = 2s+1r + 3$ be a prime with $s \in \{0,1\}$ and either $r = 1$ or $r$ an odd prime such that 2 is a primitive root modulo $r$. Then the linear complexity of the sequence $(d_n)$ defined by (1) and (2) is maximal,

$$L(d_n) = \frac{p - 3}{2}.$$ 

**Proof.** Since $p = 2s+1r + 3$ with $s \in \{0,1\}$ and $r$ is odd, we have $p \neq 3 \mod 8$. It follows from (4) that $D(1) = 1$.

If $r = 1$, that is $T = (p-3)/2 = 2s$, we have $X^T - 1 = (X-1)^{2s}$, $\gcd(D(X), X^T - 1) = 1$ and $L(d_n) = \frac{p-3}{2}$ by Lemma 2.1.

Now let $r$ be an odd prime such that 2 is a primitive root modulo $r$. Next we prove that $D(\beta) \neq 0$ for any primitive $r$th root of unity $\beta$.

Assume $D(\beta) = 0$.

If $s = 0$, we get

$$d_0 = d_1 = \ldots = d_{r-1} = D(1) = 1$$

by Lemma 2.2. However, each $n$ with $1 \leq n \leq p - 3$ and

$$\left( \left( \frac{n}{p} \right), \left( \frac{n+1}{p} \right), \left( \frac{n+2}{p} \right) \right) = (1, -1, 1),$$

where $\left( \cdot \right)$ denotes the Legendre symbol, corresponds to some $(q_0, q_{i+1}) = (n, n+2)$ and thus $d_i \equiv n + n + 2 \equiv 0 \mod 2$. By [4, Proposition 2] there are at least

$$\frac{p}{8} - \frac{\sqrt{p}}{4} - \frac{15}{8} > 0, \quad p > 25,$$

such $n$, a contradiction for $p > 25$. The only remaining primes $p \leq 25$ of the form $p = 2r + 3$ with odd $r > 1$ are $p = 13$ and $17$. For $p = 13$ we have $q_0 = 1$ and $q_1 = 3$, that is, $d_0 = 0$, a contradiction. For $p = 17$ we get $r = 7$ but 2 is a quadratic residue modulo 7 and thus not a primitive root modulo 7.
If \( s = 1 \), we have \( p \equiv 7 \text{ mod } 8 \), \( p \geq 23 \), and we get from Lemma 2.2
\[
d_0 + d_r = d_1 + d_{r+1} = \ldots = d_{r-1} + d_{2r-1} = S(1) = 1.
\]
Hence, \((d_n)\) is balanced. However, the number of pairs of consecutive quadratic residues is \( (p - 3)/4 \), see for example [3, Proposition 4.3.2], and the number of \( n \) with \( 1 \leq n \leq p - 4 \) and
\[
\left( \frac{n}{p} \right), \left( \frac{n+1}{p} \right), \left( \frac{n+2}{p} \right), \left( \frac{n+3}{p} \right) = (1, -1, -1, 1)
\]
is at least
\[
\frac{p}{16} - \frac{5}{8} \sqrt{p} - \frac{39}{16} > 0, \quad p > 169,
\]
by [4, Proposition 2]. Hence we have at least
\[
\frac{p - 3}{4} + \frac{p}{16} - \frac{5}{8} \sqrt{p} - \frac{39}{16} > \frac{p - 3}{4}, \quad p > 169,
\]
different \( n \) with \( 0 \leq n \leq (p-5)/2 \) and \( d_n = 1 \), a contradiction for \( p > 169 \). It remains to check that there is an \( n \) satisfying (5) for any prime \( p \equiv 7 \text{ mod } 8 \) for which \( r = (p - 3)/4 \) is a prime and \( 23 \leq p < 169 \), that is, \( p \in \{23, 31, 47, 71, 79, 127, 151, 167\} \). We can delete \( p = 31, 71, 127, 167 \) from this list since for these values of \( r = (p-3)/4 \) it is easy to verify that 2 is not a primitive root modulo \( r \). We can choose \( n \) from the following table,
\[
\begin{array}{c|c|c|c|c}
 n & 23 & 47 & 79 & 151 \\
\hline
 p & 9 & 9 & 5 & 5 \\
\end{array}
\]
Thus, we obtain \( \gcd(X^T - 1, S(X)) = 1 \), and the result follows. \( \square \)

3. Imbalance of \((d_n)\)

In this section we show that, for sufficiently large \( p \), the sequence \((d_n)\) is imbalanced. More specifically, about \( 2/3 \) of the sequence elements are equal to 1.

**Theorem 3.1.** Let \( N(0) \) and \( N(1) \) denote the number of 0s and 1s in a period of the sequence \((d_n)\), respectively. Then we have
\[
N(0) = \frac{p}{6} + O \left( p^{1/2} \log p \right)^2
\]
and
\[
N(1) = \frac{p}{3} + O \left( p^{1/2} \log p \right)^2.
\]

**Proof.** We first prove a lower bound on \( N(1) \). We need a well known result about the pattern distribution of Legendre symbols.

For \( s \geq 1 \) and \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s \in \{-1, 1\} \), set
\[
N(\varepsilon_1, \ldots, \varepsilon_s) = \left| \left\{ j = 1, 2, \ldots, p - s : \left( \frac{j + i}{p} \right) = \varepsilon_{i+1}, \quad i = 0, \ldots, s - 1 \right\} \right|.
\]
From [4, Proposition 2] we get for \( s \geq 3 \),
\[
(6) \quad N(\varepsilon_1, \ldots, \varepsilon_s) = \frac{p}{2^s} + O \left( sp^{1/2} \right).
\]
Note that (6) is also true for \( s = 1 \), since we have each \((p - 1)/2\) quadratic residues and non-residues modulo \( p \), and for \( s = 2 \), see for example [3, Proposition 4.3.2].
For a non-negative integer \( k \), let \( N_k \) denote the number of \( j \) with \( 1 \leq j \leq p - 2 - k \) satisfying
\[
\left( \frac{j}{p} \right), \left( \frac{j + 1}{p} \right), \ldots, \left( \frac{j + k}{p} \right), \left( \frac{j + k + 1}{p} \right) = (1, -1, \ldots, -1, 1).
\]
Each pair \((j, k)\) satisfying (7) corresponds to an \( n \) with \((q_n, q_{n+1}) = (j, j + k + 1)\), that is, \( d_n \equiv q_n + q_{n+1} \equiv k + 1 \mod{2} \). Hence for any positive integer \( m \),
\[
N(1) \geq \sum_{k=0}^{m} N_{2k} = \frac{p}{4} \sum_{k=0}^{m} 4^{-k} + O \left( m^2 p^{1/2} \right)
\]
and
\[
N(0) \geq \sum_{k=0}^{m} N_{2k+1} = \frac{p}{8} \sum_{k=0}^{m} 4^{-k} + O \left( m^2 p^{1/2} \right)
\]
by (6). Choosing \( m = \lfloor \log p \rfloor \) we get
\[
N(1) \geq \frac{p}{3} \left( 1 - \left( \frac{1}{4} \right)^{m+1} \right) + O \left( m^2 p^{1/2} \right)
\]
\[
= \frac{p}{3} + O \left( p^{1/2} (\log p)^2 \right)
\]
and
\[
N(0) \geq \frac{p}{8} \sum_{k=1}^{m} 4^{-k} + O(m^2 p^{1/2}) = \frac{p}{6} + O \left( p^{1/2} (\log p)^2 \right).
\]
Now since \( N(0) + N(1) = (p - 3)/2 \) we get
\[
N(0) = \frac{p}{6} + O(p^{1/2} (\log p)^2) \text{ and } N(1) = \frac{p}{3} + O(p^{1/2} (\log p)^2).
\]
Therefore, the sequence \((d_n)\) is imbalanced for sufficiently large \( p \).

4. Pattern distribution of \((t_n)\)

The number \( N(1) \) of 1s in a period of the sequence \((t_n)\) defined by (3) is equal to the number of elements of the set
\[
\left\{ j = 1, 2, \ldots, p - 2 : \left( \frac{j}{p} \right) = \left( \frac{j+1}{p} \right) = 1 \right\}.
\]
Then it follows from [3, Proposition 4.3.2] that
\[
N(1) = \left\{ \begin{array}{ll}
(p - 3)/4, & p \equiv 3 \mod{4}, \\
(p - 5)/4, & p \equiv 1 \mod{4}.
\end{array} \right.
\]
So this sequence is balanced when \( p \equiv 3 \mod{4} \) and almost balanced when \( p \equiv 1 \mod{4} \).

Now we consider longer patterns.

**Theorem 4.1.** For a prime \( p \geq 5 \) let \((t_n)\) be the \((p - 3)/2\)-periodic sequence defined by (3). For any positive integer \( s \) and any pattern \( x = (x_0, \ldots, x_s-1) \in \{0, 1\}^s \) the number \( N_s(x) \) of \( n \) with \( 0 \leq n \leq (p - 5)/2 \) and
\[
(t_n, t_{n+1}, \ldots, t_{n+s-1}) = x
\]
satisfies
\[
N_s(x) = \frac{p}{2^{s+1}} + O \left( sp^{1/2} (\log p)^{s+1} \right).
\]
Proof. Each pattern of Legendre symbols
\[
\left( \left( \frac{j}{p} \right), \left( \frac{j+1}{p} \right), \ldots, \left( \frac{j+k_0 + \ldots + k_{s-1} + s}{p} \right) \right)
\]
\[= (1, -1, \ldots, -1, 1, -1, \ldots, -1, 1, \ldots, -1, 1),\]
j = 1, 2, \ldots, p - 1 - k_0 - \ldots - k_{s-1} - s, corresponds to a pattern \((t_n, \ldots, t_{n+s-1})\) with
\[t_{n+i} = \begin{cases} 1, & k_i = 0, \\ 0, & k_i > 0, \end{cases} \quad i = 0, \ldots, s - 1,
\]
for some \(n\) with \(0 \leq n \leq \frac{p-5}{2} - s\). Assume \(m \geq \max\{1, k_0, k_1, \ldots, k_{s-1}\}\).

Then the number of such \(j\) is
\[
\frac{p}{2^{s+1+k_0+\ldots+k_{s-1}}} + O(smp^{1/2})
\]
by (6).

Assume that the pattern \(x\) contains \(r\) zeros. Then for \(r \geq 1\) we have
\[
N_s(x) \geq \frac{p}{2^{s+1}} \sum_{\ell_1, \ldots, \ell_r = 1} 2^{-(\ell_1 + \ldots + \ell_r)} + O\left(sm^{r+1}p^{1/2}\right)
\]
\[= \frac{p}{2^{s+1}} (1 - 2^{-m})^r + O\left(sm^{r+1}p^{1/2}\right).
\]
Choosing \(m = \lceil \log p \rceil - 1\) we get
\[
N_s(x) \geq \frac{p}{2^{s+1}} + O\left(sp^{1/2}(-1 + \log p)^{r+1}\right).
\]
For \(r = 0\) we get
\[N_s(1, 1, \ldots, 1) = \frac{p}{2^{s+1}} + O\left(sp^{1/2}\right).
\]
Using
\[
N_s(x) \leq \frac{p-3}{2} - \sum_{y \in \mathbb{F}_2^s \backslash \{x\}} N_s(y)
\]
\[\leq \frac{p-3}{2} - (2^s - 1) \frac{p}{2^{s+1}} + O\left(sp^{1/2} \sum_{r=0}^{s} \binom{s}{r} (-1 + \log p)^{r+1}\right)
\]
\[= \frac{p}{2^{s+1}} + O\left(sp^{1/2} (\log p)^{s+1}\right)
\]
we get the result. \(\square\)

Using [9, Theorem 3] instead of [4, Proposition 2] we get a local analog of Theorem 4.1 exactly the same way.

Corollary 1. For a prime \(p \geq 5\) let \((t_n)\) be the \((p - 3)/2\)-periodic sequence defined by (3). For any positive integer \(s\), any \(N \) with \(1 \leq N \leq (p - 5)/2\) and any pattern \(x = (x_0, \ldots, x_{s-1}) \in \{0, 1\}^s\) the number \(N_s(x, N)\) of \(n \) with \(0 \leq n \leq N - 1\) and
\[(t_n, t_{n+1}, \ldots, t_{n+s-1}) = x\]
satisfies
\[ N_s(\overline{x}, N) = \frac{N}{2^{x+1}} + O \left( sp^{1/2}(\log p)^{r+2} \right). \]

We also get an analog of the lower bound (9),
\[ N_s(\overline{x}, N) \geq \frac{N}{2^{x+1}} + O \left( sp^{1/2}(\log p)^{r+2} \right), \]
where \( r \) is the number of zeros of \( x \in \{0, 1\}^8 \).

5. Linear complexity of \((t_n)\)

In this subsection we discuss the linear complexity of the sequence \((t_n)\). We now put
\[ T(X) = \sum_{n=0}^{(p-5)/2} t_n X^n. \]

According to (8), the number \( N(1) \) of 1s in a period of \((t_n)\) is equal to \((p-3)/4\) if \( p \equiv 3 \mod 4 \) and \((p-5)/4\) if \( p \equiv 1 \mod 4 \). Thus,
\[ T(1) = \sum_{n=0}^{(p-5)/2} t_n = \begin{cases} 1, & p \equiv \pm 1 \mod 8, \\ 0, & p \equiv \pm 3 \mod 8. \end{cases} \]

For the case \( p \equiv 1 \mod 4 \), the period \( T = r = (p-3)/2 \) of the sequence \((t_n)\) is an odd number. If we suppose that \( r \) is a prime such that 2 is a primitive root modulo \( r \), then Lemma 2.2 implies either \( T(\beta) \neq 0 \) or \( t_h = T(1) \) for all \( h \). Now 2 can be only a primitive root modulo \( r \) if it is not a square modulo \( r \), that is, \( r \equiv \pm 3 \mod 8 \), in particular, we have \( p \geq 13 \) and \((t_h)\) is not constant by (8). Hence, \( T(\beta) \neq 0 \) for any primitive \( r \)th root of unity \( \beta \). We obtain the following result.

**Theorem 5.1.** Let \( p \) be a prime with \( p \equiv 9 \) or \( 13 \mod 16 \) such that \( r = \frac{p-3}{2} \) is an odd prime and 2 is a primitive root modulo \( r \). Then the linear complexity \( L(t_n) \) of the sequence \((t_n)\) defined by (3) is
\[ L(t_n) = \begin{cases} \frac{p-3}{2}, & p \equiv 9 \mod 16, \\ \frac{p-5}{2}, & p \equiv 13 \mod 16. \end{cases} \]

The maximum order complexity \( M(s_n) \) of a binary sequence \((s_n)\) is the smallest positive integer \( M \) with
\[ s_{n+M} = f(s_{n+M-1}, \ldots, s_n), \quad n = 0, 1, \ldots, \]
for some mapping \( f : \mathbb{F}_2^M \rightarrow \mathbb{F}_2 \). Obviously, we have
\[ L(s_n) \geq M(s_n) \]
and each lower bound on \( M(t_n) \) is also a lower bound on \( L(t_n) \). In particular we have the trivial lower bound
\[ L(t_n) \geq M(t_n) \geq \frac{\log((p-3)/2)}{\log 2}, \]
see [7, Proposition 3.2].

For a positive integer \( N \) the \( N \)th maximum order complexity \( M(s_n, N) \) is the local analog of \( M(s_n) \), that is, the smallest \( M \) with
\[ s_{n+M} = f(s_{n+M-1}, \ldots, s_n), \quad n = 0, 1, \ldots, N-M-1, \]
for some $f$. We prove also a lower bound on $M(t_n, N)$ which is nontrivial for $N$ of order of magnitude at least $p^{1/2} \log^4 p$.

**Theorem 5.2.** For the $N$th maximum order complexity $M(t_n, N)$ of the sequence $(t_n)$ defined by (3) we have

$$M(t_n, N) \geq \frac{\log(N/p^{1/2})}{\log 2} - \frac{4 \log \log p}{\log 2} + O(1), \quad N = 1, 2, \ldots, (p - 5)/2.$$  

**Proof.** For $s \geq 1$ and $x \in \{0, 1\}$ the number $G_{s,x}(N)$ of $n$ with $0 \leq n \leq N - s$ satisfying

$$G_{s,x}(N) \geq \frac{N}{2^{s+1}} + O\left(sp^{1/2}(\log p)^3\right) = \frac{N}{2^{s+1}} + O\left(p^{1/2}(\log p)^3\right) \quad \text{for } s \leq \log p$$

by (10). Hence, there is a constant $c > 0$ such that for

$$s \leq \frac{\log(N/p^{1/2})}{\log 2} - \frac{4 \log \log p}{\log 2} - c$$

we have $G_{s,x} > 0$ for $x \in \{0, 1\}$ and both patterns in (11) of length $s$ appear at least once. Assume

$$M \leq \frac{\log(N/p^{1/2})}{\log 2} - \frac{4 \log \log p}{\log 2} - c$$

and that there is a recurrence of the form

$$t_{n+s} = f(t_{n+s-1}, \ldots, t_{n}), \quad n = 0, 1, \ldots, N - M - 1.$$  

However, there are $n_1$ and $n_2$ with $0 \leq n_1 < n_2 \leq N - 1 - M$ and

$$t_{n_1+i} = t_{n_2+i} = 1, \quad i = 0, 1, \ldots, M - 1, \quad t_{n_1+M} \neq t_{n_2+M},$$

a contradiction to (13). Hence, (12) is not true and the result follows. \qed

**Remark 1.** Theorem 5.2 is in good correspondence to the result of [7] that the maximum order complexity of a random sequence of length $N$ is of order of magnitude $\log N$.

For some recent papers on the maximum order complexity see [5, 6, 8, 12, 13, 14, 15, 18].

The correlation measure $C_2(s_n)$ of order 2 of a sequence $(s_n)$ of length $N$ is defined by

$$C_2(s_n) = \max_{M, d_1, d_2} \left| \sum_{n=0}^{M-1} (-1)^{s_n+d_1+s_{n+d_2}} \right|,$$

where the maximum is taken over all integers $M, d_1, d_2$ with $0 \leq d_1 < d_2 \leq N - M$. There exist $d_1$ and $d_2$ with $0 \leq d_1 < d_2$ with $s_{n+d_1} = s_{n+d_2}$ for $n = 0, 1, \ldots, M(s_n) - 2$ and we get

$$C_2(s_n) \geq M(s_n) - 1.$$  

A large correlation measure $C_2(s_n)$ of order 2 is undesirable for cryptographic applications since the expected value of $C_2(s_n)$ is of order of magnitude

$$N^{1/2}(\log N)^{1/2},$$
see [1], and a cryptographic sequence should not be distinguishable from a random sequence.

These results on expected values and (14) suggest that a good cryptographic sequence of length \( N \) should have maximum order complexity of order of magnitude between \( \log N \) and \( N^{1/2+\epsilon} \).

6. Conclusion

We showed that the sequence \((d_n)\) of the parities of differences of quadratic residues modulo \( p \) is very unbalanced. Hence, \((d_n)\) is, despite of a high linear complexity (at least in some cases), not suitable in cryptography. We introduced an alternative sequence \((t_n)\) which is not only balanced but also longer patterns appear essentially equally often. Moreover, we proved that \((t_n)\) has in some cases a very high linear complexity and obtained a moderate but nontrivial lower bound on the \(N\)th maximum order complexity of \((t_n)\). All these results indicate that \((t_n)\) is an attractive candidate for applications in cryptography.

Acknowledgments

We wish to thank the anonymous referees for their careful study of our paper and their very useful comments.

References

[1] N. Alon, Y Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, in Proc. Lond. Math. Soc., 95 (2007), 778–812.
[2] M. Caragiu, S. Tefft, A. Kemats and T. Maenle, A linear complexity analysis of quadratic residues and primitive roots spacings, Far East J. Math. Ed., 19 (2019), 27–37.
[3] T. W. Cusick, C. Ding and A. Renvall, Stream Ciphers and Number Theory, Elsevier Science B. V., Amsterdam, 2004.
[4] C. Ding, Pattern distributions of Legendre sequences, IEEE Trans. Inform. Theory, 44 (1998), 1693–1698.
[5] O. Geil, F. Özbudak and D. Ruano, Constructing sequences with high nonlinearity using the Weierstrass semigroup of a pair of distinct points of a Hermitian curve, Semigroup Forum, 98 (2019), 543–555.
[6] L. Işık and A. Winterhof, Maximum-order complexity and correlation measures, Cryptography, 1 (2017), 1–7.
[7] C. J. A. Jansen, Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods, Ph.D thesis, Delft University of Technology, the Netherlands, 1989.
[8] Y. Luo, C. Xing and L. You, Construction of sequences with high nonlinearity from function fields, IEEE Trans. Inform. Theory, 63 (2017), 7646–7650.
[9] C. Mauduit and A. Sárközy, On finite pseudorandom sequences of \( k \) symbols, Indag. Math., 13 (2002), 89–101.
[10] W. Meidl and A. Winterhof, Linear complexity of sequences and multisequences, In Handbook of Finite Fields, CRC Press, 2013, 324–336.
[11] H. Niederreiter, Linear complexity and related complexity measures for sequences, In Progress in Cryptology–INDOCRYPT 2003, Lecture Notes in Comput. Sci., volume 2004, Springer, Berlin, 2003, 1–17.
[12] J. Peng, X. Zeng and Z. Sun, Finite length sequences with large nonlinearity complexity, Adv. Math. Commun., 12 (2018), 215–230.
[13] Z. Sun and A. Winterhof, On the maximum order complexity of the Thue-Morse and Rudin-Shapiro sequence, Unif. Distr. Th., 14 (2019), 33–42.
[14] Z. Sun and A. Winterhof, On the maximum order complexity of subsequences of the Thue-Morse and Rudin-Shapiro sequence along squares, Int. J. Comput. Math. Comput. Syst. Theory, 4 (2019), 30–36.
[15] Z. Sun, X. Zeng, C. Li and T. Helleseth, Investigations on periodic sequences with maximum nonlinearity complexity, IEEE Trans. Inform. Theory, 63 (2017), 6188–6198.
Sequences from differences of consecutive quadratic residues

[16] A. Topuzo˘ glu and A. Winterhof, Pseudorandom sequences, in Topics in Geometry, Coding Theory and Cryptography, Algebr. Appl., volume 6, Springer, Dordrecht, (2007), 135–166.

[17] A. Winterhof, Linear complexity and related complexity measures, in Selected Topics in Information and Coding Theory, Ser. Coding Theory Cryptol., volume 7, World Sci. Publ., Hackensack, NJ, (2010), 3–40.

[18] Z. Xiao, X. Zeng, C. Li and Y. Jiang, Binary sequences with period $N$ and nonlinear complexity $N - 2$, Cryptogr. Commun., 11 (2019), 735–757.

Received March 2020; 1st revision May 2020.

E-mail address: arne.winterhof@oeaw.ac.at
E-mail address: xiaozibi@wust.edu.cn