Binary Sequences Derived from Differences of Consecutive Primitive Roots

Arne Winterhof[1] and Zibi Xiao[2]

[1] Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
e-mail: arne.winterhof@oeaw.ac.at
[2] College of Science
Wuhan University of Science and Technology
Wuhan 430081, Hubei, China
e-mail: xiaozibi@wust.edu.cn

Abstract

Let $1 < g_1 < \ldots < g_{\varphi(p-1)} < p-1$ be the ordered primitive roots modulo p. We study the pseudorandomness of the binary sequence (s_n) defined by $s_n \equiv g_{n+1} + g_{n+2} \bmod 2$, $n = 0, 1, \ldots$. In particular, we study the balance, linear complexity and 2-adic complexity of (s_n). We show that for a typical p the sequence (s_n) is quite unbalanced. However, there are still infinitely many p such that (s_n) is very balanced. We also prove similar results for the distribution of longer patterns. Moreover, we give general lower bounds on the linear complexity and 2-adic complexity of (s_n) and state sufficient conditions for attaining their maximums. Hence, for carefully chosen p, these sequences are attractive candidates for cryptographic applications.

1 Introduction

For a prime $p \geq 11$, let $g_1, \ldots, g_{\varphi(p-1)}$ with

$$1 < g_1 < g_2 < \ldots < g_{\varphi(p-1)} < p-1$$

be all the primitive roots modulo p in increasing order, where $\varphi(n)$ is Euler's totient function. The sequence (s_n) derived from the parities of differences (or sums) between consecutive primitive roots modulo p is a binary sequence of period $T = \varphi(p-1) - 1$ and its first period is defined by

$$s_n \equiv g_{n+1} + g_{n+2} \bmod 2, \quad n = 0, 1, \ldots, T-1. \tag{1}$$

Caragiu et al. [2] calculated the linear complexity of this sequence for the first 1000 primes p showing that for 610 primes p the sequence has maximal linear complexity which may suggest this sequence for cryptography. This has motivated us to study theoretically properties of this sequence.

Balance and uniform *pattern distribution* are desirable features of a cryptographic sequence. In Section 2.1 we show that the sequence (s_n) is rather unbalanced if $\frac{\varphi(p-1)}{p}$ is large. For example, if $\frac{\varphi(p-1)}{p}$ is close to its supremum $1/2$, we have for sufficiently large p essentially $2T/3$ ones and $T/3$ zeros in a period of (s_n). This is the case for Fermat primes $p = 2^s + 1$ and safe primes, that is, $(p-1)/2$ is prime. The sequence (s_n) becomes more balanced with decreasing $\frac{\varphi(p-1)}{p}$. Note that for any $\varepsilon > 0$ there are infinitely many primes with $\frac{\varphi(p-1)}{p} < \varepsilon$. However, for a typical p we get unbalanced sequences. We also study the distribution of longer patterns in (s_n) in Section 2.2. Our results on balance and pattern distribution are based on a result of Cobeli and Zaharescu on the distribution of primitive roots [3]. Note that in the special case that p is either a Fermat prime or a safe prime, that is, the primitive roots coincide with the quadratic non-residues except -1 for the latter, the result of Ding [5] on the distribution of quadratic residues can be used to improve our error term, see [17] and the Remarks below Theorem 1.

The *linear complexity* of a sequence is the length of the shortest linear feedback shift register that generates the sequence. A large linear complexity is essential for cryptographic applications. For a periodic sequence (s_n) of period T we can calculate the linear complexity $L(s_n)$ by

$$L(s_n) = T - \deg(\gcd(X^T - 1, S(X))), \tag{2}$$

where

$$S(X) = \sum_{n=0}^{T-1} s_n X^n,$$

see for example [4, Lemma 8.2.1].

The *2-adic complexity* $C(s_n)$ of a T-periodic binary sequence is the length of the shortest feedback with carry shift register and can be calculated by

$$C(s_n) = \left\lfloor \log_2 \left(\frac{2^T - 1}{\gcd(2^T - 1, S(2))} \right) \right\rfloor, \tag{3}$$

where we denote by $\log_2(x)$ the binary logarithm of x.

For some periods T any non-constant sequence of period T has a large linear complexity and a large 2-adic complexity, respectively. In particular, we will

2

see in Section 3.1 that if $T = \varphi(p-1) - 1$ is a prime such that 2 is a primitive root modulo T and $p \equiv 1 \bmod 4$, then the linear complexity of (s_n) attains its maximum $L(s_n) = T$. Moreover, if $2^T - 1$ is a Mersenne prime, then the 2-adic complexity of (s_n) attains its maximum.

In Section 4 we provide some experimental data which indicates that it is not difficult to find large primes p such that the sequence (s_n) is balanced and has a desirable pattern distribution at least for short patterns, a large linear complexity and a large 2-adic complexity. Hence, for carefully chosen p our sequences are attractive candidates for cryptography.

For surveys and some recent articles on linear complexity, 2-adic complexity and related measures of pseudorandomness see [4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20].

We use the notation $f(n) = O(g(n))$ if $|f(n)| \leq c|g(n)|$ for some absolute constant $c > 0$ and the notation $f(n) = o(g(n))$ if $g(n) \neq 0$ for sufficiently large n and $\lim\limits_{n \to \infty} \frac{f(n)}{g(n)} = 0$.

2 Balance and Pattern Distribution

2.1 Balance

In this section we discuss the balance of the sequence (s_n) of parities of differences of primitive roots modulo p defined by (1).

Theorem 1. *Let p be a prime, and let $N(1)$ and $N(0)$ denote the number of 1s and 0s, respectively, in a period of the sequence (s_n) defined by (1) of period $T = \varphi(p-1) - 1$. Then we have*

$$N(1) = \left(\frac{1}{2 - \varphi(p-1)/p} + o(1) \right) T$$

and

$$N(0) = \left(\frac{1 - \varphi(p-1)/p}{2 - \varphi(p-1)/p} + o(1) \right) T,$$

where $p \to \infty$.

Proof. For $i \in \mathbb{F}_p^*$ let $c(i) = 1$ if i is a primitive root modulo p and $c(i) = -1$ otherwise. For $s \geq 1$ and $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s \in \{-1, 1\}$, set

$$M(\varepsilon_1, \cdots, \varepsilon_s) = |\{j = 1, 2, \ldots, p-s : c(j+i) = \varepsilon_{i+1}, \ i = 0, \ldots, s-1\}|. \quad (4)$$

Let $z = z(\varepsilon_1, \ldots, \varepsilon_s)$ be the number of i with $\varepsilon_i = 1$, $i = 1, \ldots, s$, and put

$$\eta = \eta(p) = \tfrac{\varphi(p-1)}{p}.$$

From [3, Theorem 1] we get

$$\left| M(\varepsilon_1, \ldots, \varepsilon_s) - p\eta^z (1-\eta)^{s-z} \right| \leq 2^{s-z+1} s \sqrt{p} \log p (\tau(p-1))^s, \quad (5)$$

3

where $\tau(p-1)$ is the number of divisors of $p-1$.

Note that $\tau(p-1) = p^{O(1/\log\log p)}$, see for example [1, Theorem 13.12]. Then for sufficiently small s with respect to p, (5) simplifies to

$$M(\varepsilon_1,\ldots,\varepsilon_s) = p\eta^z (1-\eta)^{s-z} + O\left(p^{1/2+o(1)}\right), \quad s = o(\log\log p). \quad (6)$$

For a non-negative integer k put

$$N_k = M(1,\underbrace{-1,\ldots,-1}_{k},1),$$

that is, $z = z(1,-1,\cdots,-1,1) = 2$. N_k contributes to $N(1)$ for even k and to $N(0)$ for odd k. Choosing

$$m = \left\lfloor \frac{\log\log p}{\log\log\log p} \right\rfloor = o(\log\log p)$$

and recall

$$\frac{p}{2} > \varphi(p-1) \gg \frac{p}{\log\log p}, \quad (7)$$

see for example [6, Section 18.4], we have by (6)

$$\begin{aligned}
N(1) &\geq \sum_{k=0}^{m} N_{2k} = p\eta^2 \sum_{k=0}^{m}(1-\eta)^{2k} + O\left(p^{1/2+o(1)}\right) \\
&= \left(\frac{1}{2-\eta} + o(1)\right) T
\end{aligned}$$

and

$$\begin{aligned}
N(0) &\geq \sum_{k=0}^{m} N_{2k+1} = p\eta^2(1-\eta) \sum_{k=0}^{m}(1-\eta)^{2k} + O\left(p^{1/2+o(1)}\right) \\
&= \left(\frac{1-\eta}{2-\eta} + o(1)\right) T.
\end{aligned}$$

The result follows from these inequalities and $N(0) + N(1) = T$. $\qquad\square$

Remarks. 1. Large $\varphi(p-1)$:
We have

$$\varphi(p-1) \leq \frac{p-1}{2}$$

which is attained for *Fermat primes* p, that is, p is of the form $p = 2^s + 1$. We may call $\varphi(p-1)$ *large* with respect to p if

$$\varphi(p-1) = \frac{p}{2} + o(p).$$

4

Safe primes p, that is, $(p-1)/2$ is also a *(Sophie Germain) prime*, are further examples of large $\varphi(p-1) = (p-3)/2$. For primes p with large $\varphi(p-1)$, a period of the sequence (s_n) consists of

$$N(0) = (1/3 + o(1))T$$

zeros and

$$N(1) = (2/3 + o(1))T$$

ones and is very unbalanced.

Note that for a Fermat prime p the primitive roots modulo p are exactly the quadratic non-residues and the proof of [17, Theorem 3.1] can be easily modified to get the Theorem with a more precise error term. The same applies to a safe prime p for which the primitive roots modulo p are the quadratic non-residues $\neq p-1$.

Since the sequence (s_n) is not balanced for large $\varphi(p-1)$, as in [17] we may consider the essentially balanced sequence (t_n) with $t_n = 1$ whenever $g_{n+1} = g_n + 1$ and $t_n = 0$ otherwise instead of (s_n).

2. Small $\varphi(p-1)$:

We have $\varphi(n) \gg n/\log\log n$ which is attained for infinitely many n, see for example [6]. We call $\varphi(p-1)$ of order of magnitude $p/\log\log p$ or more general with

$$\varphi(p-1) = o(p)$$

small. In this case, for sufficiently large p, the sequence (s_n) is essentially balanced, that is,

$$N(a) = \left(\frac{1}{2} + o(1)\right)T, \quad a = 0, 1.$$

3. Typical $\varphi(p-1)$:

For an even n the expected value of $\varphi(n)$ is $4n/\pi^2$. More precisely, the probability that a randomly chosen even number n and a random number k are both divisible by a prime $r > 2$ is $1/r^2$. Hence, the probability that n and k are co-prime is

$$\frac{1}{2}\prod_{r>2}\left(1 - \frac{1}{r^2}\right) = \frac{2}{3}\prod_r\left(1 - \frac{1}{r^2}\right) = \frac{2}{3\zeta(2)} = \frac{4}{\pi^2}.$$

Here, see for example [1, Chapters 11 and 12],

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad s \in \mathbb{C},$$

denotes the *Riemann zeta function*, by Euler's product formula [1, Theorem 11.7] we have

$$\frac{1}{\zeta(s)} = \prod_r\left(1 - \frac{1}{r^s}\right), \quad \mathrm{Re}(s) > 1,$$

and it is well-known, [1, Theorem 12.17], that

$$\zeta(2) = \frac{\pi^2}{6}.$$

We call $\varphi(p-1)$ *typical* if

$$\varphi(p-1) = \left(\frac{4}{\pi^2} + o(1)\right)p.$$

In this case we have

$$N(1) = \left(\frac{1}{2 - 4/\pi^2} + o(1)\right)T = (0.627\ldots + o(1))T$$

and

$$N(0) = \left(\frac{1 - 4/\pi^2}{2 - 4/\pi^2} + o(1)\right)T = (0.372\ldots + o(1))T.$$

2.2   Pattern Distribution

Now we extend Theorem 1 to longer patterns of fixed length ℓ and $p \to \infty$.

Theorem 2. *Let* $(a_0, \ldots, a_{\ell-1}) \in \mathbb{F}_2^\ell$ *be a pattern of fixed length* $\ell \geq 1$ *with* w *coordinates equal to* 1 *and* $\ell - w$ *coordinates equal to* 0. *Let* $N_\ell(w)$ *be the number of* $n = 0, 1, \ldots, T - \ell$ *with* $s_{n+i} = a_i$ *for* $i = 0, \ldots, \ell - 1$. *Then we have*

$$N_\ell(w) = \left(\left(\frac{1}{2 - \varphi(p-1)/p}\right)^w \left(\frac{1 - \varphi(p-1)/p}{2 - \varphi(p-1)/p}\right)^{\ell-w} + o(1)\right)T, \quad p \to \infty.$$

Proof. Without loss of generality we consider $(a_0, \ldots, a_{\ell-1}) = (\underbrace{1, \ldots, 1}_{w}, \underbrace{0, \ldots, 0}_{\ell-w})$.

Recall (4) and put

$$N_{k_1, \ldots, k_\ell} =$$
$$M(1, \underbrace{-1, \ldots, -1}_{2k_1}, 1, \ldots, 1, \underbrace{-1, \ldots, -1}_{2k_w}, 1, \underbrace{-1, \ldots, -1}_{2k_{w+1}+1}, 1, \ldots, 1, \underbrace{-1, \ldots, -1}_{2k_\ell+1}, 1).$$

Put

$$m = \left\lfloor \frac{\log\log p}{\log\log\log p} \right\rfloor.$$

Then we have

$$N_\ell(w) \geq \sum_{k_1, \ldots, k_\ell = 0}^{m} N_{k_1, \ldots, k_\ell}$$

$$\geq p\eta^{\ell+1}(1 - \eta)^{\ell-w} \sum_{k_1, \ldots, k_\ell = 0}^{m} (1 - \eta)^{2(k_1 + \ldots + k_\ell)} + O\left(p^{1/2 + o(1)}\right)$$

6

by (6), where $\eta = \frac{\varphi(p-1)}{p}$ and thus

$$
\begin{aligned}
N_\ell(w) \quad &\geq \quad T\eta^\ell(1-\eta)^{\ell-w} \left(\sum_{k=0}^{m} (1-\eta)^{2k} \right)^\ell + O\left(p^{1/2+o(1)} \right) \\
&= \quad T\eta^\ell(1-\eta)^{\ell-w} \left(\frac{1 - (1-\eta)^{2(m+1)}}{1 - (1-\eta)^2} \right)^\ell + O\left(p^{1/2+o(1)} \right) \\
&= \quad T(1-\eta)^{\ell-w} \left(\frac{1 + o(1)}{2 - \eta} \right)^\ell + O\left(p^{1/2+o(1)} \right) \\
&= \quad T\left((1-\eta)^{\ell-w} \left(\frac{1}{2 - \eta} \right)^\ell + o(1) \right).
\end{aligned}
$$

In the last step we used $T \gg p/\log\log p$ and $0 < \frac{1}{2-\eta} < 1$ since $0 < \eta < 1/2$, see the remark after Theorem 1. We recall that ℓ is fixed.

We have $\binom{\ell}{w}$ patterns $(a_0, \ldots, a_{\ell-1})$ with w coordinates equal to 1. Since

$$
\sum_{w=0}^{\ell} \binom{\ell}{w} \left(\frac{1}{2-\eta} \right)^w \left(\frac{1-\eta}{2-\eta} \right)^{\ell-w} = \left(\frac{1}{2-\eta} + \frac{1-\eta}{2-\eta} \right)^\ell = 1
$$

the main term of this lower bound is optimal and the result follows. $\qquad\square$

Remark. For large $\varphi(p-1) = \frac{p}{2} + o(p)$ we get

$$
N_\ell(w) = \left(\left(\frac{2}{3} \right)^w \left(\frac{1}{3} \right)^{\ell-w} + o(1) \right) T.
$$

For small $\varphi(p-1) = o(p)$ we get

$$
N_\ell(w) = \left(\left(\frac{1}{2} \right)^\ell + o(1) \right) T
$$

and for typical $\varphi(p-1) = \frac{4p}{\pi^2} + o(p)$ we have

$$
N_\ell(w) = \left((0.627\ldots)^w (0.372\ldots)^{\ell-w} + o(1) \right) T.
$$

3   Linear Complexity and 2-Adic Complexity

3.1   Linear Complexity

In this section, we estimate the linear complexity of the T-periodic sequence (s_n) defined by (1). In particular, we give a sufficient condition for attaining the maximal value $L(s_n) = T$.

For integers m and q with $\gcd(m, q) = 1$ we denote by $\text{ord}_m(q)$ the *order* of q modulo m. Note that $\varphi(p-1)$ is even for $p \geq 5$, that is, $T = \varphi(p-1) - 1$ is odd and $T \geq 3$ for $p \geq 11$.

Proposition 1. *Let p be a sufficiently large prime and $T = \varphi(p-1) - 1$. Let $T = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of T with pairwise distinct odd primes $p_1, \ldots, p_r$ and $e_i \geq 1$ for $i = 1, \ldots, r$. Then the linear complexity of the sequence (s_n) of period T defined by (1) satisfies*

$$L(s_n) \geq \min \{\mathrm{ord}_{p_1}(2), \ldots, \mathrm{ord}_{p_r}(2)\} + \varepsilon,$$

where

$$\varepsilon = \begin{cases} 1, & p \equiv 1 \bmod 4, \\ 0, & p \equiv 3 \bmod 4. \end{cases} \tag{8}$$

In particular, if T is a prime and 2 is a primitive root modulo T, then

$$L(s_n) \begin{cases} = T, & p \equiv 1 \bmod 4, \\ \geq T - 1, & p \equiv 3 \bmod 4. \end{cases}$$

The proof is based on a slightly more precise version of [4, Theorem 3.3.1].

Lemma 1. *Let $T = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of an odd integer $T \geq 3$ with pairwise distinct primes $p_1, \ldots, p_r$ and $e_i \geq 1$ for $i = 1, \ldots, r$. Then for each non-constant sequence (s_n) over $\mathbb{F}_2$ of period T we have*

$$L(s_n) \geq \min \{\mathrm{ord}_{p_1}(2), \ldots, \mathrm{ord}_{p_r}(2)\} + S(1),$$

where

$$S(1) = \sum_{n=0}^{T-1} s_n \in \mathbb{F}_2 = \{0, 1\}.$$

Proof. Since T is odd we have $\gcd(X - 1, X^{T-1} + \ldots + X + 1) = 1$ and thus

$$\gcd(X^T - 1, S(X)) = \gcd(X - 1, S(X)) \gcd(X^{T-1} + \ldots + X + 1, S(X)).$$

From the proof of [4, Theorem 3.3.1] we know that

$$T - \deg(\gcd(X^{T-1} + \ldots + X + 1, S(X))) \geq \min\{\mathrm{ord}_{p_1}(2), \ldots, \mathrm{ord}_{p_r}(2)\}.$$

Now $\gcd(X - 1, S(X)) = X - 1$ if $S(1) = 0$ and $\gcd(X - 1, S(X)) = 1$ if $S(1) = 1$ and the result follows from (2). $\qquad\square$

Now we study the value of $S(1)$.

Lemma 2. *For a prime $p \equiv 1 \bmod 4$ and the sequence (s_n) defined by (1) we have*
$$S(1) = 1.$$

Proof. By the definition of (s_n) we have

$$S(1) = \sum_{n=0}^{\varphi(p-1)-2} s_n = \sum_{n=0}^{\varphi(p-1)-2} (g_{n+1} + g_{n+2}) = g_1 + g_{\varphi(p-1)} \in \mathbb{F}_2.$$

For an arbitrary primitive root g modulo p we have $g^{(p+1)/2} \equiv -g \bmod p$. Since $\gcd((p+1)/2, p-1) = 1$ for $p \equiv 1 \bmod 4$, it follows that $-g$ is also a primitive root modulo p. This shows that if g_1 denotes the smallest primitive root modulo p, then $p - g_1$ is the largest primitive root modulo p, that is, $g_1 + g_{\varphi(p-1)} = p$ in $\mathbb{Z}$. Thus we have

$$g_1 + g_{\varphi(p-1)} = 1 \in \mathbb{F}_2,$$

which completes the proof. $\qquad\square$

Remark. For $p \equiv 3 \bmod 4$ both possible values of $S(1)$ can be attained. For example, $S(1) = 2+8 = 0 \in \mathbb{F}_2$ for $p = 11$ and $S(1) = 2+15 = 1 \in \mathbb{F}_2$ for $p = 19$.

For proving Proposition 1 it remains to verify that the sequence (s_n) defined by (1) is non-constant for a sufficiently large prime p. By (7) and Theorem 1 we have

$$N(1) \geq \left(\frac{1}{2} + o(1) \right) T \quad \text{and} \quad N(0) \geq \left(\frac{1}{3} + o(1) \right) T.$$

Hence, $N(1)$ and $N(0)$ are both positive for sufficiently large p and (s_n) is not constant. Hence, Lemma 1 is applicable and completes the proof of Proposition 1. $\qquad\square$

3.2   2-Adic Complexity

Now we estimate the 2-adic complexity of (s_n) defined by (1).

Proposition 2. *Let p be a sufficiently large prime and $T = \varphi(p-1) - 1$. Let q be the smallest prime divisor of $2^T - 1$. Then the 2-adic complexity of the sequence (s_n) of period T defined by (1) satisfies*

$$C(s_n) \geq \lfloor \log_2(q) \rfloor.$$

In particular, if $2^T - 1$ is a (Mersenne) prime, then

$$C(s_n) = \lfloor \log_2(2^T - 1) \rfloor.$$

Since (s_n) is not constant for sufficiently large p, by Theorem 1 it is enough to verify the following lemma, which may be of independent interest.

Lemma 3. *Let q be the smallest prime divisor of $2^T - 1$. Then for each non-constant sequence (s_n) over $\mathbb{F}_2$ of period T we have*

$$C(s_n) \geq \lfloor \log_2(q) \rfloor.$$

Proof. Put $d = \gcd(S(2), 2^T - 1)$. We have $d = 2^T - 1$ if and only if $S(2) \in \{0, 2^T - 1\}$, that is, (s_n) is constant.

Now assume that (s_n) is not constant and q denotes the smallest prime divisor of $2^T - 1$. Then we have $d \leq \frac{2^T - 1}{q}$ and thus

$$C(s_n) = \left\lfloor \log_2 \left(\frac{2^T - 1}{\gcd(S(2), 2^T - 1)} \right) \right\rfloor \geq \lfloor \log_2(q) \rfloor$$

by (3). □

Remark. Note that there are highly predictable sequences with both maximum linear complexity and maximum 2-adic complexity, for example, any sequence with only one non-zero entry in a period. Hence, studying the balance and pattern distribution is always a must to test a sequence for suitability in cryptography.

4   Heuristic

To guarantee a rather balanced sequence with large linear complexity and large 2-adic complexity we need primes p such that

- The ratio $\frac{\varphi(p-1)}{p}$ is small.

- The period $T = \varphi(p-1) - 1$ contains only large prime divisors q such that $\mathrm{ord}_q(2)$ is also large. This is guaranteed if T is prime and 2 is a primitive root modulo 2.

- The Mersenne number $2^T - 1$ contains only large prime divisors. This is guaranteed if $2^T - 1$ is a Mersenne prime.

In the following table we list primes T for which $2^T - 1$ is a Mersenne prime and the largest primes p with $T = \varphi(p-1) - 1$. For these primes we have $L(s_n) \geq \mathrm{ord}_T(2) + S(1)$ with $S(1)$ defined by (8), and $C(s_n)$ is maximal.

T	p	$\mathrm{ord}_T(2)$	$\frac{\varphi(p-1)}{p}$
3	13	2	$\frac{4}{13} = 0.307\ldots$
5	19	4	$\frac{6}{19} = 0.315\ldots$
7	31	3	$\frac{8}{31} = 0.258\ldots$
19	67	18	$\frac{20}{67} = 0.298\ldots$
31	103	**5**	$\frac{32}{103} = 0.310\ldots$
107	379	106	$\frac{108}{379} = 0.284\ldots$
127	409	**7**	$\frac{128}{409} = 0.312\ldots$
1279	5281	639	$\frac{1280}{5281} = 0.242\ldots$
2203	6619	734	$\frac{2204}{6619} = 0.331\ldots$

Now we also list some primes T for which $2^T - 1$ is not a prime. We denote by q the smallest prime divisor of $2^T - 1$ from which we can derive the lower bound $C(s_n) \geq \lfloor \log_2(q) \rfloor$ on the 2-adic complexity.

T	q	$\lfloor \log_2(q) \rfloor$	p	$\mathrm{ord}_T(2)$	$\frac{\varphi(p-1)}{p}$
11	23	4	43	10	$0.279\ldots$
23	47	5	79	11	$0.303\ldots$
43	431	8	139	14	$0.316\ldots$
47	2351	11	211	23	$0.227\ldots$
53	6361	12	163	52	$0.331\ldots$
59	179951	17	199	58	$0.301\ldots$
71	228479	17	271	35	$0.265\ldots$
79	2687	11	331	39	$0.209\ldots$
83	167	**7**	197	82	**0.426**$\ldots$
131	263	**8**	269	130	**0.490**$\ldots$
163	150287	17	499	162	$0.328\ldots$
167	2349023	21	523	83	$0.321\ldots$
179	359	**8**	419	178	**0.429**$\ldots$
191	383	**8**	673	95	$0.285\ldots$
199	164504919713	37	751	99	$0.255\ldots$

We may consider the following features undesirable and emphasized this in the tables (boldface):

- The value $\lfloor \log_2(q) \rfloor$ is small, say, smaller than $\frac{T}{10}$. Then a very large 2-adic complexity cannot be guaranteed.

- The order of 2 modulo T is small, say, smaller than $\frac{T}{4}$. Then a very large linear complexity cannot be guaranteed.

- The ratio $\frac{\varphi(p-1)}{p}$ is large, say, at least $\frac{1}{3}$. Then for sufficiently large p the sequence contains at least 60 percent ones and is rather unbalanced. Moreover, the frequency of the pair 11 is at least 36 percent whereas the frequency of 00 is at most 16 percent of the period.

Still it seems to be not difficult to find large primes T and p with $T = \varphi(p-1)-1$ without these undesirable features.

Acknowledgment

References

[1] T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[2] M. Caragiu, S. Tefft, A. Kemats, T. Maenle, A linear complexity analysis of quadratic residues and primitive roots spacings. Far East J. Math. Ed. 19 (2019), no. 1, 27–37.

[3] C. Cobeli, A. Zaharescu, On the distribution of primitive roots mod p. Acta Arith. 83 (1998), no. 2, 143–153.

[4] T. W. Cusick, C. Ding, A. Renvall, Stream Ciphers and Number Theory. Amsterdam, The Netherlands: Elsevier/North-Holland, 1998.

[5] C. Ding, Pattern distributions of Legendre sequences. IEEE Trans. Inform. Theory 44 (1998), no. 4, 1693–1698.

[6] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[7] R. Hofer, L. Mérai, A. Winterhof, Measures of pseudorandomness: arithmetic autocorrelation and correlation measure. Number theory – Diophantine problems, uniform distribution and applications, 303–312, Springer, Cham, 2017.

[8] R. Hofer, A. Winterhof, On the 2-adic complexity of the two-prime generator. IEEE Trans. Inform. Theory 64 (2018), no. 8, 5957–5960.

[9] H. Hu, Comments on "A new method to compute the 2-adic complexity of binary sequences". IEEE Trans. Inform. Theory 60 (2014), no. 9, 5803–5804.

[10] W. Meidl, A. Winterhof, Linear complexity of sequences and multisequences, in G. L. Mullen, D. Panario (eds.), Handbook of Finite Fields, CRC Press, Boca Raton, FL(2013), 324–336.

[11] L. Mérai, H. Niederreiter, A. Winterhof, Expansion complexity and linear complexity of sequences over finite fields. Cryptogr. Commun. 9 (2017), no. 4, 501–509.

[12] L. Mérai, A. Winterhof, On the pseudorandomness of automatic sequences. Cryptogr. Commun. 10 (2018), no. 6, 1013–1022.

[13] L. Mérai, A. Winterhof, On the Nth linear complexity of automatic sequences. J. Number Theory 187 (2018), 415–429.

[14] H. Niederreiter, A. Winterhof, Applied number theory. Springer, Cham, 2015.

[15] A. Topuzoğlu, A. Winterhof, Pseudorandom sequences. Topics in geometry, coding theory and cryptography, 135–166, Algebr. Appl., 6, Springer, Dordrecht, 2007.

[16] A. Winterhof, Linear complexity and related complexity measures. Selected topics in information and coding theory, 3–40, Ser. Coding Theory Cryptol., 7, World Sci. Publ., Hackensack, NJ, 2010.

[17] A. Winterhof, Z. Xiao, Binary sequences derived from differences of consecutive quadratic residues. Adv. Math. Commun., to appear, doi: 10.3934/amc.2020100.

[18] Z. Xiao, X. Zeng, C. Li, T. Helleseth, New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptogr. 86 (2018), no. 7, 1483–1497.

[19] Z. Xiao, X. Zeng, Z. Sun, 2-adic complexity of two classes of generalized cyclotomic binary sequences. Int. J. Found. Comput. Sci. 27 (2016), no. 7, 879–893.

[20] H. Xiong, L. Qu, C. Li, A new method to compute the 2-adic complexity of binary sequences. IEEE Trans. Inform. Theory 60 (2014), no. 4, 2399–2406.