Binary sequences with period N and nonlinear complexity $N-2$

Zibi Xiao [*], Xiangyong Zeng, Chaoyun Li [†], and Yupeng Jiang [‡]

Abstract: In this paper, periodic sequences with period N and nonlinear complexity $N-2$ are investigated. A necessary and sufficient condition for characterizing such sequences is established, and a recursive method is proposed to generate all possible binary sequences with period N and nonlinear complexity $N-2$. The exact number of such sequences is also determined.

Keywords: binary sequence, periodic sequence, nonlinear complexity.

1 Introduction

Pseudorandom sequences have been widely used in cryptography [13]. The complexity of a sequence is one of the important measures to assess the security level of the sequence. Sequences can be generated efficiently by employing feedback shift registers (FSRs). The most commonly used approach to measure complexity is henceforth by the length of the shortest feedback shift register that can generate a given sequence. When the feedback function of the FSR is restricted to be linear (resp. of degree at most k), the complexity is known as *linear complexity* (resp. *k-th order complexity*). When there is no restriction on the degree of the feedback function, it is referred to as *nonlinear complexity*, also called *maximum order complexity*.

Linear complexity of pseudorandom sequences has been extensively investigated in [2, 3, 7, 8, 9, 10, 14, 16], whereas k-th order complexity and nonlinear complexity have not been studied to the same extent due to its intractability. The problem of determining the nonlinear complexity of sequences was highlighted by Jansen [5] and Jansen and Boekee [6]. Chan and Games in [1]

[*]Z. Xiao and X. Zeng are with the Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, Hubei, China. Email: holly_xzb@126.com, xzeng@hubu.edu.cn

[†]C. Li is with imec-COSIC, Department of Electrical Engineering, KU Leuven, Leuven 3001, Belgium. Email: chaoyun.li@esat.kuleuven.be.

[‡]Y. Jiang is with State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 10009, China. Email: jiangyupeng@amss.ac.cn.

proposed an algorithm for computing the second-order complexity of a binary sequence. This algorithm has been further improved by Rizomiliotis et al in [19], and extended to the case of nonlinear complexity [18]. By applying Boolean algebra arguments, Limniotis et al. in [11] developed a recursive algorithm that computes the feedback function of the shortest nonlinear feedback shift register. The theoretical bounds and behavior of nonlinear complexity of random sequences have also received considerable attention. Erdmann and Murphy in [4] presented a way to approximate the distribution of the nonlinear complexity and constructed statistical tests for random sequences. Recently, Xing and Niederreiter in [15] improved lower bounds on nonlinear complexities of some pseudorandom sequences and showed probabilistic result on the behavior of nonlinear complexities of random sequences. Petrides and Mykkeltveit in [17] investigated the classification of periodic binary sequences into nonlinear complexity classes. They only determine the number of sequences with maximum nonlinear complexity and left the other cases as open problems. This motives us to study the other sequences with given nonlinear complexity.

The problem of designing sequences with large nonlinear complexity was first investigated by Rizomiliotis [20], where two methods for constructing period binary sequences with given linear complexity and maximum nonlinear complexity were proposed. The nonlinear complexity of a sequence of periodic N is upper bounded by $N-1$ [5]. Sun et al. in [21] proposed a recursive approach that generates all periodic sequences with maximum nonlinear complexity and analyzed the randomness properties of such sequences. Recently, Luo et al. presented a construction of sequences with high nonlinear complexity from function fields [12]. It is of interesting to construct new sequences with high nonlinear complexity.

The purpose of this paper is to study periodic sequences with period N and nonlinear complexity $N-2$, which will be called *near maximum nonlinear complexity sequences* accordingly. We first establish a necessary and sufficient condition for a sequence to achieve near maximum nonlinear complexity. This enables us to completely determine the structure of near maximum nonlinear complexity binary sequences. Based on the structural properties, we propose a recursive construction of all near maximum nonlinear complexity binary sequences with arbitrary period. We also determine the exact number of near maximum nonlinear complexity binary sequences of period N up to shift equivalence. Our results completely characterize a class of sequences with given nonlinear complexity, which resolves a special case in the classification of periodic binary sequences into nonlinear complexity classes [17]. Moreover, the near maximum nonlinear complexity sequences can be served as a basis in constructing new sequences with high nonlinear complexity. It is worth noting that the near maximum nonlinear complexity sequences have more complicated structures than those with maximum nonlinear complexity, which might be preferable in certain applications.

The main technique used in this paper is to divide a period into several disjoint subsets and then show that the items in each subset take identical values. Our methods are inspired by the previous work [21] in which one only needs to discuss two complementary subsets of a period. However, to analyze sequences in this paper we construct three disjoint subsets in three cases respectively, which means much more cases need to be treated.

The remainder of this paper is organized as follows. Section 2 first introduces some necessary notations and basic results. Then the aforementioned necessary and sufficient condition is proved. The construction of all binary near maximum nonlinear complexity sequences is described in Section 3. Moreover, the total number of the sequences is determined in Section 4. Finally, Section 5 concludes the study.

2 Preliminaries

First we introduce some basic notations that are needed throughout this paper.

- We denote a sequence $\mathbf{s}^\infty = s_0 s_1 \cdots s_i \cdots$ with least period N by $\mathbf{s}^N = s_0 s_1 \cdots s_{N-1}$ since it is completely specified by the elements of a single period.
- Given a sequence $\mathbf{s}^\infty = s_0 s_1 \cdots s_i \cdots$, we denote *the ith subsequence of length n* (or *the ith n-tuple*) by $\mathbf{s}_i^{i+n-1}$, that is, $\mathbf{s}_i^{i+n-1} = s_i s_{i+1} \cdots s_{i+n-1}$.
- We denote the concatenation of two finite sequences $\mathbf{s} = s_0 s_1 \cdots s_{k-1}$ and $\mathbf{t} = t_0 t_1 \cdots t_{n-1}$ by $\mathbf{st} = s_0 s_1 \cdots s_{k-1} t_0 t_1 \cdots t_{n-1}$, and denote the concatenation of m copies of the sequence $\mathbf{s}$ by $\mathbf{s}^m = (s_0 s_1 \cdots s_{k-1})^m$.
- $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ denotes the residue class ring modulo n for a positive integer n.
- Define that $A \bmod p = \{x \bmod p \,|\, x \in A\}$, where A is a set of integers and p is a positive integer.

Some definitions and useful properties of nonlinear complexity of a periodic sequence are characterized below.

Definition 1. *([5]) The nonlinear complexity $C(\boldsymbol{s}^N)$ of a periodic sequence $\boldsymbol{s}^N$ is defined as the smallest positive integer m for which there exists a polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ such that $s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1})$ for all $0 \le i \le N-1$, where $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is the ring of polynomials over the finite field $\mathbb{F}_q$ in the m variables $x_1, x_2, \ldots, x_m$.*

Definition 2. *Let L denote the cyclic left shift operation of a periodic sequence $\boldsymbol{s}^N$ which is defined by $L(\boldsymbol{s}^N) = s_1 s_2 \cdots s_{N-1} s_0$. And for any integer $e > 1$, $L^e(\boldsymbol{s}^N) = s_e s_{e+1} \cdots s_{N-1} s_0 \cdots s_{e-1}$. Let $\boldsymbol{s}^N$ and $\boldsymbol{s'}^N$ be two periodic sequences. If there exists an positive integer $e < N$ such that $\boldsymbol{s'}^N = L^e(\boldsymbol{s}^N)$, then we say that $\boldsymbol{s}^N$ and $\boldsymbol{s'}^N$ are shift equivalent. Otherwise, we say that $\boldsymbol{s}^N$ and $\boldsymbol{s'}^N$ are shift-distinct.*

Lemma 1. *([5]) Let $\boldsymbol{s}^N$ be a periodic sequence. Then*

(i) the nonlinear complexity of $\boldsymbol{s}^N$ is the smallest integer c such that all c-tuples $(s_i s_{i+1} \ldots s_{i+c-1})$ for $0 \le i \le N-1$ are different, where the subscripts i in s_i are taken modulo N.

(ii) the nonlinear complexity of $\boldsymbol{s}^N$ is equal to $l+1$, where l is the length of the longest tuple in $\boldsymbol{s}^N$ that occurs at least twice with different successors.

(iii) the shift equivalent sequences of $\boldsymbol{s}^N$ have the same nonlinear complexity.

(iv) the maximal nonlinear complexity of $\boldsymbol{s}^N$ is $N-1$.

Now we present a necessary and sufficient condition for a periodic sequence $\mathbf{s}^N$ to have nonlinear complexity $N-2$.

Lemma 2. *Let $\boldsymbol{s}^N$ be a periodic sequence with $N \ge 4$ and not shift equivalent to $(\alpha)^{N-1}\beta$, where α and β are two distinct elements of an arbitrary finite field $\mathbb{F}_q$. Then the nonlinear complexity $C(\boldsymbol{s}^N) = N-2$ if and only if there exist two integers h and c with $0 \le h < h+c \le N-1$ such that*

$$\boldsymbol{s}_h^{N+h-4} = \boldsymbol{s}_{h+c}^{N+h+c-4}, \ \ s_{N+h-3} \ne s_{N+h+c-3} \ \ and \ \ s_{N+h-1} \ne s_{N+h+c-1}, \tag{1}$$

Proof. If $C(\mathbf{s}^N) = N-2$, then by Lemma 1 (i) there exist two $(N-3)$-tuples, say $\mathbf{s}_h^{N+h-4}$ and $\mathbf{s}_{h+c}^{N+h+c-4}$, such that $\mathbf{s}_h^{N+h-4} = \mathbf{s}_{h+c}^{N+h+c-4}$ and $s_{N+h-3} \ne s_{N+h+c-3}$. Now suppose $s_{N+h-1} = s_{N+h+c-1}$, then we obtain two identical $(N-2)$-tuples with different successors in $\mathbf{s}^N$ due to the periodicity, i.e., $\mathbf{s}_{h-1}^{N+h-4} = \mathbf{s}_{h+c-1}^{N+h+c-4}$ and $s_{N+h-3} \ne s_{N+h+c-3}$ for $h \ge 1$, $\mathbf{s}_{c-1}^{N+c-4} = \mathbf{s}_{N-1}^{2N-4}$ and $s_{N+c-3} \ne s_{2N-3}$ for $h = 0$. It follows from Lemma 1 (ii) that $C(\mathbf{s}^N) = N-1$, which is a contradiction.

Conversely, since there exist two identical $(N-3)$-tuples $\mathbf{s}_h^{N+h-4}$ and $\mathbf{s}_{h+c}^{N+h+c-4}$ in $\mathbf{s}^N$, it follows from Lemma 1 (ii) that $C(\mathbf{s}) \ge N-2$. Thus, it suffices to show that $C(\mathbf{s}) \le N-2$. By Lemma 1 (i), this is equivalent to show N tuples of length $(N-2)$ in $\mathbf{s}^N$, i.e., $\mathbf{s}_i^{i+N-3}$ for $0 \le i \le N-1$ are all different.

Note that the nonlinear complexity of a periodic sequence remains unchanged up to a cyclic shift operation by Lemma 1 (iii). Therefore, we may assume without loss of generality that $h = 0$ and $1 \le c \le \lfloor \frac{N}{2} \rfloor$. That is to say, we suppose there exists an integer c with $1 \le c \le \lfloor \frac{N}{2} \rfloor$

such that

$$\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}, \ \ s_{N-3} \neq s_{N+c-3} \ \text{ and } \ s_{N-1} \neq s_{N+c-1}. \tag{2}$$

Furthermore, we suppose, on the contrary, that there are two $(N-2)$-tuples in $\mathbf{s}^N$ that are identical, say

$$\mathbf{s}_d^{d+N-3} = \mathbf{s}_{d+e}^{d+e+N-3} \ \text{ with } \ 0 \leq d < d+e \leq N-1. \tag{3}$$

Next we will show that it is impossible for a sequence of period $N \geq 4$ to satisfy both (2) and (3), other than those shift equivalent to $(\alpha)^{N-1}\beta$. According to the size of e, we divide the proof into three cases.

Case 1: $e = 1$. It follows from (3) that $s_d = s_{d+1} = \cdots = s_{d+N-2}$. That means the sequence $\mathbf{s}^N$ is shift equivalent to $(\alpha)^{N-1}\beta$. This contradicts the assumption that $\mathbf{s}^N$ is not shift equivalent to $(\alpha)^{N-1}\beta$.

Case 2: $e = 2$. In this case we distinguish the cases of even and odd N. If N is even, then it follows from (3) that for any nonnegative integers i, j, $s_i = s_j$ if and only if $i \equiv j \,(\mathrm{mod}\, 2)$. But we also have $s_0 = s_c$ and $s_{N-1} \neq s_{N+c-1}$ by (2), which imply $c \equiv 0 \,(\mathrm{mod}\, 2)$ and $N-1 \not\equiv N+c-1 \,(\mathrm{mod}\, 2)$, an obvious contradiction.

Now we assume N is odd. Then from (3) we get that for $i, j \in \{d, d+1, \ldots, N+d-1\}$,

$$s_i = s_j \ \text{ if and only if } \ i \equiv j \,(\mathrm{mod}\, 2). \tag{4}$$

When $d = 0$, we have $s_0 = s_c$ by (2), and hence c is even by (4). Since $N-3$ and $N+c-3$ are both even and $s_{N-3} \neq s_{N+c-3}$, we get $c \geq 4$, and then $N-c \leq N-4$. Therefore, $s_{N-c} = s_N = s_0$ by (2), which is a contradiction since $N - c \not\equiv 0 \,(\mathrm{mod}\, 2)$. It implies that $d \geq 1$. Then for even d, we have

$$\begin{aligned} s_d = s_{d+2} = \cdots = s_{N-1} = s_1 = s_3 = \cdots = s_{d-1}, \\ s_{d+1} = s_{d+3} = \cdots = s_{N-2} = s_0 = s_2 = \cdots = s_{d-2}, \end{aligned}$$

and for odd d, we have

$$\begin{aligned} s_d = s_{d+2} = \cdots = s_{N-2} = s_0 = s_2 = \cdots = s_{d-1}, \\ s_{d+1} = s_{d+3} = \cdots = s_{N-1} = s_1 = s_3 = \cdots = s_{d-2}. \end{aligned}$$

Note that $s_{N-1} \neq s_0$ whenever $d \geq 1$. Furthermore, we have $s_0 = s_c$ and $s_{N-1} \neq s_{c-1}$, and thus $s_0 = s_{c-1} = s_c$. This happens only if d is odd and $c = d$. Since both N and d are odd and $d + e \leq N-1$, we have $0 < d \leq N-4$. It follows from (2) that $s_d = s_{2d}$, which is impossible because $d < 2d < d+N-1$ and $d \not\equiv 2d \,(\mathrm{mod}\, 2)$.

Case 3: $e \geq 3$. Then we have $d+e \leq N-1 \leq N+d+e-3$, and since $\mathbf{s}_d^{N+d-3} = \mathbf{s}_{d+e}^{N+d+e-3}$, we get

$$s_{N-1} = s_{N-e-1}.$$

We also have $0 \leq N-e-1 \leq N-4$ in this case, and from $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$ we get then

$$s_{N-e-1} = s_{N+c-e-1}.$$

When $e+d-c \geq 2$, we have $d \leq N+c-e-1 \leq N+d-3$. It follows from $\mathbf{s}_d^{N+d-3} = \mathbf{s}_{d+e}^{N+d+e-3}$ that

$$s_{N+c-e-1} = s_{N+c-1}.$$

When $e+d-c < 0$, we have $d \leq c-e-1 < N+d-3$. Then with $\mathbf{s}_d^{N+d-3} = \mathbf{s}_{d+e}^{N+d+e-3}$ and the periodicity of the sequence we get

$$s_{N+c-e-1} = s_{c-e-1} = s_{c-1} = s_{N+c-1}.$$

Altogether, we have $s_{N-1} = s_{N+c-1}$ whenever $e+d-c \geq 2$ or $e+d-c < 0$, which is a contradiction.

In the remaining case we have $e+d-c = 0$ or 1. We note first that $c \neq \frac{N}{2}$ for even N with $N \geq 6$, for otherwise $c-1 = \frac{N}{2}-1 \leq N-4$ would imply that $S_{N+c-1} = s_{c-1} = s_{2c-1} = s_{N-1}$, a contradiction. Together with $e \geq 3$ and $1 \leq c \leq \lfloor \frac{N}{2} \rfloor$, we obtain $e+d \leq N-3$ except for two special cases where $N=5$, $e=3$, $d=0$, $c=2$ and $N=4$, $e=3$, $d=0$, $c=2$. One can verify that it is impossible for (2) and (3) to be satisfied at the same time in these two cases. Now we assume $e+d \leq N-3$, then from $\mathbf{s}_d^{N+d-3} = \mathbf{s}_{d+e}^{N+d+e-3}$, we get

$$s_{N-3} = s_{N-e-3}.$$

Moreover, we have $0 \leq N-e-3 < N-4$ and $d \leq N+c-e-3 \leq d+N-3$. It follows then from $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$ and $\mathbf{s}_d^{N+d-3} = \mathbf{s}_{d+e}^{N+d+e-3}$ that

$$s_{N-e-3} = s_{N+c-e-3} \text{ and } s_{N+c-e-3} = s_{N+c-3}.$$

Therefore, we obtain $s_{N-3} = s_{N+c-3}$, a contradiction.

The proof is completed. □

3 Binary near maximum nonlinear complexity sequences

In the present paper, we shall focus on the binary case. Specifically, we shall explore the structure of binary sequences $\mathbf{s}^N$ with period $N \geq 4$ and nonlinear complexity $N-2$. By Lemma

2, we can assume that there exists an integer c with $1 \le c \le N-1$ such that

$$\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}, \ \ s_{N-3} \ne s_{N+c-3} \ \text{ and } \ s_{N-1} \ne s_{N+c-1}. \tag{5}$$

For $N = 4$, it is easily to verify that there is, up to shift equivalence, only one binary sequence with nonlinear complexity $N-2$.

Proposition 1. *Up to shift equivalence, the unique binary periodic sequence with period $N = 4$ and nonlinear complexity $N-2$ is $\boldsymbol{s}^N = 0011$.*

3.1 Necessary conditions

For $N > 4$, we first characterize the property of the positive integer c in (5).

Proposition 2. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with $N > 4$ and $C(\boldsymbol{s}^N) = N-2$, and let c be the positive integer such that $\boldsymbol{s}^N$ satisfies the condition (5). Then:*

(i) If N is even, then $\gcd(N, c) \le 2$.

(ii) If N is odd, then $\gcd(N, c) = 1$ and $c \ne 2, N-2$.

Proof. Let $d = \gcd(N, c)$, $e = \frac{N}{d}$ and $f = \frac{c}{d}$. We first show that $d \le 2$ for any $N > 4$. Suppose, on the contrary, that $d \ge 3$. Define d sets

$$H_k = \{(c - k + tc) \mod N \mid t = 0, 1, \cdots, e-1\} \ \text{ for } \ k = 1, 2, \cdots, d.$$

Since $\gcd(e, f) = 1$, we have

$$\begin{aligned} H_d &= \{(c - d + tc) \mod N \mid t = 0, 1, \cdots, e-1\} \\ &= \{(fd - d + tfd) \mod ed \mid t = 0, 1, \cdots, e-1\} \\ &= \{td \mod N \mid t = 0, 1, \cdots, e-1\}. \end{aligned}$$

It is easily seen that H_d is an additive subgroup of $\mathbb{Z}_N$ and $H_k = H_d + d - k$ for all $k \in \{1, 2, \cdots, d-1\}$, so that

$$H_i \cap H_j = \varnothing \text{ for } i \ne j \text{ and } \bigcup_{i=1}^{d} H_i = \mathbb{Z}_N.$$

Furthermore, $c - k + (e-1)c = ec - k = \frac{c}{d}N - k \equiv N - k \,(\mathrm{mod}\, N)$, that is to say, $N - k \in H_k$ for all $k \in \{1, 2, \cdots, d\}$. Then neither of $N-2$ and $N-3$ is in H_1 since $d \ge 3$. Together with the condition $s_i = s_{(i+c) \bmod N}$ for $0 \le i \le N-4$ in (5), we obtain $s_i = s_j$ for any $i, j \in H_1$, which implies $s_{c-1} = s_{N-1}$, a contradiction to the condition $s_{N-1} \ne s_{(N+c-1) \bmod N}$ in (5).

Since for odd integer N, $\gcd(N,c) \leq 2$ implies $\gcd(N,c) = 1$, it remains to show that $c \neq 2$ and $c \neq N-2$ for odd N. If $c = 2$, then the condition $s_i = s_{(i+c) \bmod N}$ for $0 \leq i \leq N-4$ in (5) implies that $s_0 = s_2 = \cdots = s_{N-3}$ and $s_1 = s_3 = \cdots = s_{N-2}$. Together with $s_{N-3} \neq s_{N-1}$ and $s_{N-1} \neq s_1$, one obtains that the items of the binary sequence $\mathbf{s}^N$ must satisfy that $s_0 = s_1 = s_2 = \cdots = s_{N-2} \neq s_{N-1}$. Without loss of generality, by taking $s_{N-2} = \alpha$ and $s_{N-1} = \beta$, where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$, we obtain that $\mathbf{s}^N = (\alpha)^{N-1}\beta$. If $c = N-2$, we can similarly obtain from the condition (5) that $s_i = s_0$ if and only if $i \in \mathbb{Z}_N \backslash \{N-3\}$, and hence the binary sequence $\mathbf{s}^N$ is of the form $\mathbf{s}^N = (\alpha)^{N-3}\beta\alpha\alpha$, which is shift equivalent to $\mathbf{s}^N = (\alpha)^{N-1}\beta$. But the nonlinear complexity of the sequence $\mathbf{s}^N = (\alpha)^{N-1}\beta$ is $N-1$, which is a contradiction. □

We consider first two special cases, $c = 1$ and $c = 2$ for even N.

Proposition 3. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with $N > 4$ and nonlinear complexity $N-2$, and let c be the positive integer in (5). Then*

(i) for $c = 1$, the sequence $\boldsymbol{s}^N$, up to shift equivalence, has the form $(\alpha)^{N-2}\beta\beta$, where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$;

(ii) for even N and $c = 2$, the sequence $\boldsymbol{s}^N$, up to shift equivalence, has the form $(\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha$, where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$.

Proof. (i) For $c = 1$, the condition (5) is equivalent to $s_0 = s_1 = s_2 = \cdots = s_{N-4} = s_{N-3}$ and $s_{N-3} \neq s_{N-2}$, $s_{N-1} \neq s_0$. Since the sequence is binary, it follows that $s_0 = s_1 = s_2 = \cdots = s_{N-4} = s_{N-3} \neq s_{N-2} = s_{N-1}$. Without loss of generality, by taking $s_{N-3} = \alpha$ and $s_{N-2} = \beta$, where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$, then the sequence $\mathbf{s}^N$, up to shift equivalence, has the form $(\alpha)^{N-2}\beta\beta$.

(ii) For even N and $c = 2$, the conditions in (5) are equivalent to $s_0 = s_2 = \cdots = s_{N-4} = s_{N-2}$, $s_1 = s_3 = \cdots = s_{N-5} = s_{N-3}$, and $s_{N-3} \neq s_{N-1}$, $s_{N-1} \neq s_1$. For a binary sequence, that is to say, $s_0 = s_2 = \cdots = s_{N-2} = s_{N-1}$ and $s_1 = s_3 = \cdots = s_{N-3}$, or $s_0 = s_1 = \cdots = s_{N-2} \neq s_{N-1}$. In the former case, take $s_{N-1} = \alpha$ and $s_{N-3} = \beta$, where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$. then we get a binary sequence $(\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha$. In the latter case, take $s_{N-2} = \alpha$ and $s_{N-1} = \beta$, then we get another binary sequence $(\alpha)^{N-1}\beta$, which can be verified to have nonlinear complexity $N-1$, a contradiction. Thus the desired result follows. □

Next we shall investigate the general case, i.e., the case $c = p$, where p is an integer such that $3 \leq p \leq N-1$. By Proposition 2, p must satisfy $\gcd(N,p) \leq 2$. At this point it is convenient to divide the discussion into two subcases $\gcd(N,p) = 1$ and $\gcd(N,p) = 2$. We first define the following sets and discuss their properties.

For any two positive integers n and q with $3 \le q \le n-1$ and $\gcd(n,q)=1$, according to Bezout's Lemma, there exist uniquely determined positive integers $u \in \mathbb{Z}_n$ and $v \in \mathbb{Z}_q$ satisfying $uq - vn = 1$. When $u < \frac{n}{2}$, define three sets

$$\begin{aligned} H_1(n,q) &= \{(q-1+tq) \bmod n \mid t = 0,1,\cdots,n-2u-1\}, \\ H_2(n,q) &= \{(q-2+tq) \bmod n \mid t = 0,1,\cdots,u-1\}, \\ H_3(n,q) &= \{(q-3+tq) \bmod n \mid t = 0,1,\cdots,u-1\}. \end{aligned} \tag{6}$$

When $u > \frac{n}{2}$, define three sets

$$\begin{aligned} I_1(n,q) &= \{(q-1+tq) \bmod n \mid t = 0,1,\cdots,n-u-1\}, \\ I_2(n,q) &= \{(q-2+tq) \bmod n \mid t = 0,1,\cdots,n-u-1\}, \\ I_3(n,q) &= \{(q-3+tq) \bmod n \mid t = 0,1,\cdots,2u-n-1\}. \end{aligned} \tag{7}$$

For any two positive integers n and q with $3 \le q \le n-1$ and $\gcd(n,q)=2$, also by Bezout's Lemma, there exist uniquely determined positive integers $u \in \mathbb{Z}_{\frac{n}{2}}$ and $v \in \mathbb{Z}_{\frac{q}{2}}$ satisfying $u \cdot \frac{q}{2} - v \cdot \frac{n}{2} = 1$ since $\gcd(\frac{n}{2}, \frac{q}{2}) = 1$. Define three sets

$$\begin{aligned} D_1(n,q) &= \{(q-1+tq) \bmod n \mid t = 0,1,\cdots,\tfrac{n}{2}-u-1\}, \\ D_2(n,q) &= \{(q-2+tq) \bmod n \mid t = 0,1,\cdots,\tfrac{n}{2}-1\}, \\ D_3(n,q) &= \{(q-3+tq) \bmod n \mid t = 0,1,\cdots,u-1\}. \end{aligned} \tag{8}$$

The following properties of the defined sets are of great importance. The proofs will be given in Appendix A.

Lemma 3. *Let q be an integer with $3 \le q \le n-1$ and $\gcd(n,q)=1$. Let $u \in \mathbb{Z}_n$ and $v \in \mathbb{Z}_q$ be the integers satisfying $uq - vn = 1$. Then:*

(i) when $u < \frac{n}{2}$, $\{H_i(n,q) \mid i = 1,2,3\}$ forms a partition of $\mathbb{Z}_n$, and $n-1$, $n-2$, $n-3$ belong to $H_2(n,q)$, $H_3(n,q)$ and $H_1(n,q)$, respectively.

(ii) when $u > \frac{n}{2}$, $\{I_i(n,q) \mid i = 1,2,3\}$ forms a partition of $\mathbb{Z}_n$, and $n-1$, $n-2$ and $n-3$ belong to $I_3(n,q)$, $I_1(n,q)$ and $I_2(n,q)$, respectively.

Lemma 4. *Let q be an integer with $3 < q < n-1$ and $\gcd(n,q)=2$. Let $u \in \mathbb{Z}_{\frac{n}{2}}$ and $v \in \mathbb{Z}_{\frac{q}{2}}$ be the integers satisfying $u \cdot \frac{q}{2} - v \cdot \frac{n}{2} = 1$. Then $\{D_i(n,q) \mid i = 1,2,3\}$ forms a partition of $\mathbb{Z}_n$, and $n-1$, $n-2$, $n-3$ belong to $D_3(n,q)$, $D_2(n,q)$, $D_1(n,q)$, respectively.*

After the above preparations, we can now treat the case where c satisfies $3 \le c \le N-1$ and the necessary conditions in Proposition 2. We first show an equivalent expression of a binary periodic sequence $\mathbf{s}^N$ satisfying the condition (5). This expression is related to the sets defined in (6), (7) and (8).

Proposition 4. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with $N > 4$, c be the positive integer such that $\boldsymbol{s}^N$ satisfies the condition (5).*

(i) For $c = p$ with $\gcd(p, N) = 1$, $3 \le p \le N-1$ and $p \ne N-2$, let $a \in \mathbb{Z}_N$ and $b \in \mathbb{Z}_p$ be the uniquely determined integers satisfying $ap - bN = 1$. If $a < \frac{N}{2}$, then the condition (5) holds if and only if for $i \in \mathbb{Z}_N$,

$$s_i = \begin{cases} \alpha, & \text{if } i \in H_1(N,p); \\ \beta, & \text{if } i \in H_2(N,p) \cup H_3(N,p). \end{cases}$$

where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \ne \beta$. If $a > \frac{N}{2}$, then the condition (5) holds if and only if for $i \in \mathbb{Z}_N$,

$$s_i = \begin{cases} \alpha, & \text{if } i \in I_3(N,p); \\ \beta, & \text{if } i \in I_1(N,p) \cup I_2(N,p), \end{cases}$$

where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \ne \beta$.

(ii) For $c = p$ with $\gcd(p, N) = 2$ and $3 < p < N-2$, let $e \in \mathbb{Z}_{\frac{N}{2}}$ and $f \in \mathbb{Z}_{\frac{p}{2}}$ be the integers satisfying $e \cdot \frac{p}{2} - f \cdot \frac{N}{2} = 1$. Then the condition (5) holds if and only if for $i \in \mathbb{Z}_N$,

$$s_i = \begin{cases} \alpha, & \text{if } i \in D_1(N,p); \\ \beta, & \text{if } i \in D_2(N,p) \cup D_3(N,p). \end{cases}$$

or

$$s_i = \begin{cases} \alpha, & \text{if } i \in D_3(N,p); \\ \beta, & \text{if } i \in D_1(N,p) \cup D_2(N,p). \end{cases}$$

where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \ne \beta$.

Proof. (i) For $c = p$ with $\gcd(p, N) = 1$, $3 \le p \le N-1$ and $p \ne N-2$, we only prove the case $a < \frac{N}{2}$, and the case $a > \frac{N}{2}$ can be proved similarly, so we skip it here. When $a < \frac{N}{2}$, it follows from Lemma 3 and its proof that $\{H_i(N,p) \mid i = 1,2,3\}$ forms a partition of $\mathbb{Z}_N$ and $N-1 \equiv p-2+(a-1)p \pmod N$, $N-2 \equiv p-3+(a-1)p \pmod N$, $N-3 \equiv p-1+(N-2a-1)p \pmod N$. Thus we get

$$H_1(N,p) \setminus \{N-3\} \subset \mathbb{Z}_{N-3},\ H_2(N,p) \setminus \{N-1\} \subset \mathbb{Z}_{N-3} \text{ and } H_3(N,p) \setminus \{N-2\} \subset \mathbb{Z}_{N-3}.$$

Consequently, the condition $s_i = s_{(i+p) \bmod N}$ for each $i \in \mathbb{Z}_{N-3}$ in (5) is equivalent to

$$s_i = s_j \text{ for any two integers } i, j \in H_k(N,p),\ k = 1,2,3.$$

Furthermore, the conditions $s_{N-3} \ne s_{(N+p-3) \bmod N}$ and $s_{N-1} \ne s_{(N+p-1) \bmod N}$ in (5) are equivalent to $s_{N-3} \ne s_{p-3}$ and $s_{N-1} \ne s_{p-1}$ since $3 \le p \le N-1$. Hence, if we restrict to binary sequences, then the condition (5) is equivalent to

$$s_i = s_j \text{ if and only if either } i, j \in H_1(N,p) \text{ or } i, j \in H_2(N,p) \cup H_3(N,p),$$

because of the fact that $N-1 \in H_2(N,p)$ and $N-3 \in H_1(N,p)$. By taking $s_{p-1}=\alpha$, $s_{p-3}=\beta$, we get the desired result.

(ii) For $c=p$ with $\gcd(p,N)=2$ and $3<p<N-2$, it follows from Lemma 4 that $\{D_i(N,p) \mid i=1,2,3\}$ forms a partition of $\mathbb{Z}_N$ and $N-1 \equiv p-3+(e-1)p \pmod N$, $N-2 \equiv p-2+(\frac{N}{2}-1)p \pmod N$, $N-3 \equiv p-1+(\frac{N}{2}-e-1)p \pmod N$. Thus we have

$$D_1(N,p) \setminus \{N-3\} \subset \mathbb{Z}_{N-3},\ D_2(N,p) \setminus \{N-2\} \subset \mathbb{Z}_{N-3} \text{ and } D_3(N,p) \setminus \{N-1\} \subset \mathbb{Z}_{N-3}.$$

Therefore, the condition $s_i = s_{(i+p) \bmod N}$ for each $i \in \mathbb{Z}_{N-3}$ in (5) is equivalent to

$$s_i = s_j \text{ for any integers } i \text{ and } j \text{ belonging to the same set } D_k(N,P) \text{ with } k=1,2,3.$$

If we restrict to binary sequences, then by the same argument as in the proof of (i), the condition (5) is equivalent to

$$\begin{aligned} s_i = s_j \text{ if and only if either } i,j \in D_1(N,p) \text{ or } i,j \in D_2(N,p) \cup D_3(N,p), \\ \text{or } s_i = s_j \text{ if and only if either } i,j \in D_3(N,p) \text{ or } i,j \in D_1(N,p) \cup D_2(N,p). \end{aligned}$$

In the former case, take $s_{p-1}=\alpha$, $s_{p-3}=\beta$, and in the latter case, take $s_{p-3}=\alpha$, $s_{p-2}=\beta$, the desired results are obtained. □

3.2 Recursive characterizations

Throughout what follows, we let $\mathbf{s}^N(c)$ denote the periodic binary sequence satisfying the condition (5) for a given positive integer c, that is, the items of the sequence satisfy

$$s_i = s_{i+c} \ \text{ for } \ i=0,1,\cdots,N-4, \ \text{ and } \ s_{N-3} \neq s_{N+c-3}, \ \ s_{N-1} \neq s_{N+c-1}.$$

We observe that for $c=p$ with $3 \le p \le N-1$, the structure of $\mathbf{s}^N(p)$ is related to the remainder r of N divided by p. We first discuss the special cases $r=1$ and $r=2$.

Proposition 5. *(i) Let $N=mp+1$ with $3 \le p \le N-1$. Then $\boldsymbol{s}^N(p)$, up to shift equivalence, has the form*

$$\boldsymbol{s}^N(p) = ((\alpha)^{p-2}\beta\beta)^m\alpha,$$

where $\alpha,\beta \in \mathbb{F}_2$ and $\alpha \neq \beta$;

(ii) Let $N=mp+2$ with p odd, $3 \le p \le N-1$, and $p \neq N-2$. Then the sequence $\boldsymbol{s}^N(p)$, up to shift equivalence, has the form

$$\boldsymbol{s}^N(p) = ((\beta)^{p-1}\alpha)^m\beta\beta,$$

where $\alpha, \beta \in \mathbb{F}_2$ *and* $\alpha \neq \beta$*;*

(iii) Let $N = mp+2$ *with* p *even and* $3 < p < N-1$*. Then for even* $p = N-2$ *the sequence* $\boldsymbol{s}^N(p)$*, up to shift equivalence, has the form*

$$\boldsymbol{s}^N(p) = (\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha,$$

and for $p \neq N-2$ *the sequence* $\boldsymbol{s}^N(p)$*, up to shift equivalence, has the form*

$$\boldsymbol{s}^N(p) = ((\beta)^{p-1}\alpha)^m\beta\beta \ \ or \ \ ((\beta\alpha)^{\frac{p-2}{2}}\beta\beta)^m\beta\alpha,$$

where $\alpha, \beta \in \mathbb{F}_2$ *and* $\alpha \neq \beta$*.*

Proof. (i) Note that $N = mp+1$ implies $\gcd(N,p) = \gcd(p,1) = 1$ and $(N-m)p - N(p-1) = 1$. It is easily seen $\frac{N}{2} < N-m < N$, so that the items s_i for $i \in \mathbb{Z}_N$ in the binary sequence $\mathbf{s}^N(p)$ satisfy

$$s_i = \begin{cases} \alpha, & \text{if } i \in I_3(N,p); \\ \beta, & \text{if } i \in I_1(N,p) \cup I_2(N,p), \end{cases}$$

by Proposition 4 (i). Recall that $A \bmod p$ denotes $\{x \bmod p \,|\, x \in A\}$, where A is a set of some integers. Since $p-1+(m-1)p = mp-1 = N-2$ and $p-1+tp < N$ for $t = 0, 1, \cdots, m-1$, it follows that $I_1(N,p) \bmod p = \{p-1\}$. Similarly, we have $I_2(N,p) \bmod p = \{p-2\}$. Next we shall show that $I_3(N,p) \bmod p = \{0, 1, \cdots, p-3\}$. Let $x = (p-3+t_xp) \bmod N$ with $0 \leq t_x \leq N-2m-1$ be an arbitrary integer belonging to $I_3(N,p)$. Then there exists a unique nonnegative integer $j_x = \lfloor \frac{p-3+t_xp}{N} \rfloor$ such that $x = p-3+t_xp-j_xN$, so that

$$x = p-3+t_xp-j_x(mp+1) \equiv -3-j_x \,(\bmod p).$$

It is straightforward to verify that as t_x runs through the numbers $0, 1, \cdots, N-2m-1$, j_x runs through the numbers $0, 1, \cdots, p-3$, and so does $x \,(\bmod p)$. Thus we have $I_3(N,p) \bmod p = \{0, 1, \cdots, p-3\}$. By what we have already shown, the items s_i for $i \in \mathbb{Z}_N$ in the binary sequence $\mathbf{s}^N(p)$ satisfy

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in \{0, 1, \cdots, p-3\}; \\ \beta, & \text{if } (i \bmod p) \in \{p-1, p-2\}. \end{cases}$$

This indicates that the sequence has the form $((\alpha)^{p-2}\beta\beta)^m\alpha$.

(ii) Note that $N = mp+2$ and p odd imply that $\gcd(N,p) = \gcd(p,2) = 1$ and $\frac{N-m}{2}p - \frac{p-1}{2}N = 1$. Since $\frac{N-m}{2} < \frac{N}{2}$, it follows from Proposition 4 (i) that the items of the binary sequence $\mathbf{s}^N(p)$ satisfy

$$s_i = \begin{cases} \alpha, & \text{if } i \in H_1(N,p); \\ \beta, & \text{if } i \in H_2(N,p) \cup H_3(N,p). \end{cases}$$

We can prove that $H_1(N,p) \mod p = \{p-1\}$, $H_2(N,p) \mod p = \{1,3,\cdots,p-2\}$ and $H_3(N,p) \mod p = \{0,2,\cdots,p-3\}$ in a way similar to that in (i). Thus, the items s_i for $i \in \mathbb{Z}_N$ in the binary sequence $\mathbf{s}^N(p)$ satisfy

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in \{p-1\}; \\ \beta, & \text{if } (i \bmod p) \in \{0,1,\cdots,p-2\}. \end{cases}$$

Therefore we obtain that the sequence $\mathbf{s}^N(p)$ must be of the form $((\beta)^{p-1}\alpha)^m\beta\beta$.

(iii) Note that $N = mp+2$ and p even imply that $\gcd(N,p) = \gcd(p,2) = 2$ and $(\frac{N}{2} - m)\frac{p}{2} - (\frac{p}{2}-1)\frac{N}{2} = 1$. Then by Proposition 4 (ii), for p with $3 < p < N-2$, the items s_i with $i \in \mathbb{Z}_N$ in the sequence $\mathbf{s}^N(p)$ satisfy either

$$s_i = \begin{cases} \alpha, & \text{if } i \in D_1(N,p); \\ \beta, & \text{if } i \in D_2(N,p) \cup D_3(N,p). \end{cases}$$

or

$$s_i = \begin{cases} \alpha, & \text{if } i \in D_3(N,p); \\ \beta, & \text{if } i \in D_1(N,p) \cup D_2(N,p). \end{cases}$$

By similar arguments we can show that $D_1(N,p) \bmod p = \{p-1\}$, $D_2(N,p) \bmod p = \{0,2,\cdots,p-2\}$ and $D_3(N,p) \bmod p = \{1,3,\cdots,p-3\}$. Therefore, the items s_i for $i \in \mathbb{Z}_N$ in the sequence $\mathbf{s}^N(p)$ satisfy either

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in \{p-1\}; \\ \beta, & \text{if } (i \bmod p) \in \{0,1,2,\cdots,p-2\}. \end{cases}$$

or

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in \{1,3,\cdots,p-3\}; \\ \beta, & \text{if } (i \bmod p) \in \{0,2,\cdots,p-2\} \cup \{p-1\}. \end{cases}$$

Thus we obtain that the sequence $\mathbf{s}^N(p)$ has the form

$$((\beta)^{p-1}\alpha)^m\beta\beta \text{ or } ((\beta\alpha)^{\frac{p-2}{2}}\beta\beta)^m\beta\alpha.$$

For $p = N-2$, one can deduce from the conditions in (5) that $s_0 = s_2 = \cdots = s_{N-4} = s_{N-2}$, $s_1 = s_3 = \cdots = s_{N-5} = s_{N-1} \neq s_{N-3}$. This implies that $\mathbf{s}^N(p)$ has the form $((\alpha)^{N-3}\beta)\alpha\alpha$ or $((\alpha\beta)^{\frac{N-4}{2}}\alpha\alpha)\alpha\beta$. However, the former is a cyclic shift of $(\alpha)^{N-1}\beta$. It then follows from Proposition 3, the sequence $\mathbf{s}^N(p) = \mathbf{s}^N(N-2)$, up to shift equivalence, has the form $(\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha$. □

For the case $r \geq 3$, we need the following two lemmas, which will be proved in Appendix A.

Lemma 5. *Let $N = mp+r$ with $3 \le r < p < N-2$ and $\gcd(N,p) = 1$. Let $a \in \mathbb{Z}_N$ and $b \in \mathbb{Z}_p$ be the integers satisfying $ap - bN = 1$, $u \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_r$ be the integer satisfying $ur - vp = 1$.*

(i) If $a < \frac{N}{2}$, then $u > \frac{p}{2}$, and $H_1(N,p) \bmod p = I_3(p,r)$, $H_2(N,p) \bmod p = I_1(p,r)$, $H_3(N,p) \bmod p = I_2(p,r)$.

(ii) If $a > \frac{N}{2}$, then $u < \frac{p}{2}$, and $I_3(N,p) \bmod p = H_1(p,r)$, $I_2(N,p) \bmod p = H_3(p,r)$, $I_1(N,p) \bmod p = H_2(p,r)$.

Lemma 6. *Let $N = mp + r$ with $3 < r < p < N-1$ and $\gcd(N,p) = 2$. Let $e \in \mathbb{Z}_{\frac{N}{2}}$ and $f \in \mathbb{Z}_{\frac{p}{2}}$ be the integers satisfying $e \cdot \frac{p}{2} - f \cdot \frac{N}{2} = 1$, $u \in \mathbb{Z}_{\frac{p}{2}}$ and $v \in \mathbb{Z}_{\frac{r}{2}}$ be the integers satisfying $u \cdot \frac{r}{2} - v \cdot \frac{p}{2} = 1$. Then the sets defined in (8) satisfy $D_1(N,p) \bmod p = D_3(p,r)$, $D_2(N,p) \bmod p = D_2(p,r)$, $D_3(N,p) \bmod p = D_1(p,r)$.*

In the sequel, we let $F(\mathbf{s}^N, r) = (s_0 s_1 \cdots s_{r-1})$ with $1 \le r \le N-1$ denote the first r bits taking from the sequence $\mathbf{s}^N$. For the general case, i.e., the case $r \ge 3$, we arrive at the following result.

Proposition 6. *Let $N = mp + r$ with $3 \le r < p < N-2$ and $\gcd(N,p) \le 2$. Then*

$$\boldsymbol{s}^N(p) = F((\boldsymbol{s}^p(r))^{m+1}, N),$$

where $\boldsymbol{s}^p(r)$ is exactly the binary sequence with period p and nonlinear complexity $p-2$ corresponding to a given integer r.

Proof. Recall that $\mathbf{s}^N(p)$ denotes the binary sequences with period N and nonlinear complexity $N-2$ obtained by conditions in (5) for the given positive integer p. From the condition $s_i = s_{i+p}$ for $i \in \mathbb{Z}_{N-4}$, we derive that $s_i = s_{i+p} = \cdots = s_{i+(m-1)p}$ for all i with $0 \le i \le p-1$, and $s_{mp+j} = s_j$ for $j = 0, 1, \ldots, r-1$. That is to say the sequence $\mathbf{s}^N(p)$ must be of the form

$$(s_0 s_1 \ldots s_{p-1})^m s_0 s_1 \ldots s_{r-1}.$$

On the other hand, $\mathbf{s}^N(p)$ has one of the forms in Proposition 4 depending on the values of N and p. To determine further the concrete representation of the subsequence $s_0 s_1 \ldots s_{p-1}$, it is sufficient to determine the integers modulo p in various sets. We now distinguish the cases $\gcd(N,p) = 1$ and $\gcd(N,p) = 2$.

Case 1: $\gcd(N,p) = 1$. It is obvious that $\gcd(p,r) = 1$. Let $a \in \mathbb{Z}_N$ and $b \in \mathbb{Z}_p$ be the integers satisfying $ap - bN \equiv 1 \pmod N$, $u \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_r$ be the integers satisfying $ur - vp = 1$. If $a < \frac{N}{2}$, then by Proposition 4 (i), for $i \in \mathbb{Z}_N$,

$$s_i = \begin{cases} \alpha, & \text{if } i \in H_1(N,p); \\ \beta, & \text{if } i \in H_2(N,p) \cup H_3(N,p). \end{cases}$$

Furthermore, by Lemma 5 (i) we have $u > \frac{p}{2}$, and $H_1(N,p) \bmod p = I_3(p,r)$, $H_2(N,p) \bmod p = I_1(p,r)$, $H_3(N,p) \bmod p = I_2(p,r)$. That is to say, for $i \in \mathbb{Z}_N$,

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in I_3(p,r); \\ \beta, & \text{if } (i \bmod p) \in I_1(p,r) \cup I_2(p,r). \end{cases}$$

Then again by Proposition 4 (i), the subsequence $s_0 s_1 \cdots s_{p-1}$ is the binary sequence with period p and nonlinear complexity $p-2$ corresponding to a given positive integer $c = r$, and so $\mathbf{s}^N(p)$ has the form $(\mathbf{s}^p(r))^m F(\mathbf{s}^p(r), r)$, that is, $F((\mathbf{s}^p(r))^{m+1}, N)$.

The result for $a > \frac{N}{2}$ can be established by using the same arguments as for $a < \frac{N}{2}$.

Case 2: $\gcd(N,p) = 2$. It is obvious that $\gcd(p,r) = 2$. Then by Proposition 4 (ii), for $i \in \mathbb{Z}_N$, the items of the sequence $\mathbf{s}^N(p)$ satisfy that

$$s_i = \begin{cases} \alpha, & \text{if } i \in D_1(N,p); \\ \beta, & \text{if } i \in D_2(N,p) \cup D_3(N,p), \end{cases} \quad \text{or} \quad s_i = \begin{cases} \alpha, & \text{if } i \in D_3(N,p); \\ \beta, & \text{if } i \in D_1(N,p) \cup D_2(N,p). \end{cases}$$

Since $D_1(N,p) \bmod p = D_3(p,r)$, $D_2(N,p) \bmod p = D_2(p,r)$, $D_3(N,p) \bmod p = D_1(p,r)$ by Lemma 6, we get

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in D_3(p,r); \\ \beta, & \text{if } (i \bmod p) \in D_1(p,r) \cup D_2(p,r), \end{cases}$$

or

$$s_i = \begin{cases} \alpha, & \text{if } (i \bmod p) \in D_1(p,r); \\ \beta, & \text{if } (i \bmod p) \in D_2(p,r) \cup D_3(p,r). \end{cases}$$

This implies that the subsequence $s_0 s_1 \cdots s_{p-1}$ is a binary sequence with period p and nonlinear complexity $p-2$ obtained by conditions in (5) for a given positive integer $c = r$.

Conversely, let $\mathbf{s}^p(r)$ be the binary sequence with period p and nonlinear complexity $p-2$ corresponding a given integer $c = r$. Then we claim that the sequence $\mathbf{s}^N = F((\mathbf{s}^p(r))^{m+1}, N)$ must have nonlinear complexity $N-2$. For the sequence $\mathbf{s}^N$, we examine the following two subsequences of length $N-3$:

$$\mathbf{s}_0^{N-4} = (\mathbf{s}^p(r))^m F(\mathbf{s}^p(r), r-3) \text{ and } \mathbf{s}_p^{N+p-4} = (\mathbf{s}^p(r))^{m-1} F(\mathbf{s}^p(r), r) F(\mathbf{s}^p(r), p-3).$$

The first $(m-1)p + r = N - p$ bits of the two subsequences, i.e., $\mathbf{s}_0^{N-p-1}$ and $\mathbf{s}_p^{N-1}$ are identical obviously. The next $p-3$ bits in $\mathbf{s}_p^{N+p-4}$ are, in order, $s_0, s_1, s_2, \cdots, s_{p-4}$, and those in $\mathbf{s}_0^{N-4}$ are, in order, $s_r, s_{r+1}, \cdots, s_{p-1}, s_0, s_1, \cdots, s_{r-4}$ if $r \geq 4$ and $s_r, s_{r+1}, \cdots, s_{p-1}$ if $r = 3$. We note that the items of $\mathbf{s}^p(r)$ satisfy the conditions in (5). The condition $s_i = s_{(i+r) \bmod p}$ for $i \in \mathbb{Z}_{p-3}$ in (5) implies

$$(s_0, s_1, s_2, \cdots, s_{p-4}) = (s_r, s_{r+1}, \cdots, s_{p-1}, s_0, s_1, \cdots, s_{r-4}) \text{ for } r \geq 4,$$

$$(s_0, s_1, s_2, \cdots, s_{p-4}) = (s_r, s_{r+1}, \cdots, s_{p-1}) \text{ for } r = 3.$$

Together with $\mathbf{s}_0^{N-p-1} = \mathbf{s}_p^{N-1}$, we obtain that $\mathbf{s}_0^{N-4} = \mathbf{s}_p^{N+p-4}$. On the other hand, the conditions $s_{p-3} \neq s_{(p+r-3) \bmod p}$ and $s_{p-1} \neq s_{(p+r-1) \bmod p}$ imply that the $(N-2)$nd bit and the Nth bit of the sequence $\mathbf{s}^N$ satisfy

$$s_{N-3} \neq s_{(p+N-3) \bmod N} \text{ and } s_{N-1} \neq s_{(p+N-1) \bmod N}$$

due to $s_{N-3} = s_{r-3} = s_{(p+r-3) \bmod p}$ and $s_{N-1} = s_{r-1} = s_{(p+r-1) \bmod p}$, respectively. Altogether, the sequence $\mathbf{s}^N = F((\mathbf{s}^p(r))^{m+1}, N)$ has nonlinear complexity $N-2$ according to Lemma 2. □

Remark 1. *If we set $\boldsymbol{s}^p(1) = (\alpha)^{p-2}\beta\beta$ for $p \geq 3$, $\boldsymbol{s}^p(2) = (\beta)^{p-1}\alpha$ for odd number $p \geq 3$ and $\boldsymbol{s}^p(2) = (\beta)^{p-1}\alpha$ or $(\beta\alpha)^{\frac{p-2}{2}}\beta\beta$ for even number $p > 3$, then the results in Propositions 5 can be uniformly rewritten as $\boldsymbol{s}^N(p) = F((\boldsymbol{s}^p(r))^{m+1}, N)$ for $r = 1, 2$. Together with Proposition 6, we get that for any period $N > 4$ and integer $c = p$ with $3 \leq p \leq N-1$, $p \neq N-2$ and $\gcd(N, p) \leq 2$, if $N = mp + r$, then*

$$\boldsymbol{s}^N(p) = F((\boldsymbol{s}^p(r))^{m+1}, N).$$

It should be noted that $\boldsymbol{s}^p(r)$ denotes all the binary sequences with period p and nonlinear complexity $p-2$ for a given integer $c = r$ in general, but the cases $r = 2$ and $(p, r) = (3, 1)$ are exceptions.

With the preparations in Propositions 3, 5 and 6, we are now ready to present a recursive method to characterize all binary sequences with near maximum nonlinear complexity. It is convenient to distinguish the cases of odd and even period.

Theorem 1. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with N odd and $N > 4$. Then $\boldsymbol{s}^N$ has nonlinear complexity $N-2$ if and only if it can, up to shift equivalence, be represented as one of the following forms:*

(i) $\boldsymbol{s}^N(c) = (\alpha)^{N-2}\beta\beta$ for $c = 1$.

(ii) for $c = p$ with $3 \leq p \leq N-1$, $p \neq N-2$ and $\gcd(N, p) = 1$, let $N = r_0$, $p = r_1$ and $r_{i-1} = m_i r_i + r_{i+1}$ for $i = 1, 2, \cdots, k$, where $r_1 > r_2 > \cdots > r_{k+1} = 1$. Then $\boldsymbol{s}^N(p) = \boldsymbol{s}^{r_0}(r_1)$ with

$$\boldsymbol{s}^{r_{i-1}}(r_i) = F((\boldsymbol{s}^{r_i}(r_{i+1}))^{m_i+1}, r_{i-1}) \text{ for } i = 1, 2, \cdots, k-1,$$

where

$$\boldsymbol{s}^{r_{k-1}}(r_k) = \begin{cases} (\beta)^{r_{k-1}-1}\alpha, & \text{if } r_k = 2; \\ ((\alpha)^{r_k-2}\beta\beta)^{m_k}\alpha, & \text{if } r_k \neq 2. \end{cases}$$

Proof. The statement (i) is established by Proposition 3 (i). We thus only need to prove (ii). For $c = p$ with $3 \le p \le N-1$, $p \ne N-2$ and $\gcd(N,p) = 1$, by using the Euclidean algorithm on $N = r_0$ and $p = r_1$, we obtain that $r_{i-1} = m_i r_i + r_{i+1}$ for $i = 1, 2, \cdots, k$, and the final nonzero remainder $r_{k+1} = 1$. If $r_k \ne 2$, then by Proposition 5 (i),

$$\mathbf{s}^{r_{k-1}}(r_k) = ((\alpha)^{r_k-2}\beta\beta)^{m_k}\alpha.$$

Since $r_i \ge 3$ for all $i = k, k-1, \cdots, 2, 1$, by Proposition 6, we have,

$$\mathbf{s}^{r_{i-1}}(r_i) = F((\mathbf{s}^{r_i}(r_{i+1}))^{m_i+1}, r_{i-1}) \ for \ i = k-1, \cdots, 2, 1.$$

If $r_k = 2$, then by Proposition 5 (ii),

$$\mathbf{s}^{r_{k-2}}(r_{k-1}) = (\mathbf{s}^{r_{k-1}}(r_k))^{m_{k-1}} F(\mathbf{s}^{r_{k-1}}(r_k), r_k) = F((\mathbf{s}^{r_{k-1}}(r_k))^{m_{k-1}+1}, r_{k-2}),$$

where $\mathbf{s}^{r_{k-1}}(r_k) = \mathbf{s}^{r_{k-1}}(2) = (\beta)^{r_{k-1}-1}\alpha$. Again by Proposition 6, the desired result follows. □

Theorem 2. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with N even and $N > 4$. Then $\boldsymbol{s}^N$ has nonlinear complexity $N-2$ if and only if it can, up to shift equivalence, be represented as one of the following forms:*

(i) $\boldsymbol{s}^N(c) = (\alpha)^{N-2}\beta\beta$ for $c = 1$;

(ii) $\boldsymbol{s}^N(c) = (\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha$ for $c = 2$;

(iii) for $c = p$ with $3 \le p \le N-1$ and $\gcd(N,p) = 1$, let $N = r_0$, $p = r_1$ and $r_{i-1} = m_i r_i + r_{i+1}$ for $i = 1, 2, \cdots, k$, where $r_1 > r_2 > \cdots > r_{k+1} = 1$. Then $\boldsymbol{s}^N(p) = \boldsymbol{s}^{r_0}(r_1)$ with

$$\boldsymbol{s}^{r_{i-1}}(r_i) = F((\boldsymbol{s}^{r_i}(r_{i+1}))^{m_i+1}, r_{i-1}) \ for \ i = 1, 2, \cdots, k-1,$$

where

$$\boldsymbol{s}^{r_{k-1}}(r_k) = \begin{cases} (\beta)^{r_{k-1}-1}\alpha, & \text{if } r_k = 2; \\ ((\alpha)^{r_k-2}\beta\beta)^{m_k}\alpha, & \text{if } r_k \ne 2. \end{cases}$$

(iv) for $c = p$ with $3 < p < N-1$ and $\gcd(N,p) = 2$, if $p = N-2$, then $\boldsymbol{s}^N(p) = (\alpha\beta)^{\frac{N-2}{2}}\alpha\alpha$. If $p \ne N-2$, let $N = r_0$, $p = r_1$ and $r_{i-1} = m_i r_i + r_{i+1}$ for $i = 1, 2, \cdots, k$, where $r_1 > r_2 > \cdots > r_{k+1} = 2$. Then $\boldsymbol{s}^N(p) = \boldsymbol{s}^{r_0}(r_1)$ with

$$\boldsymbol{s}^{r_{i-1}}(r_i) = F((\boldsymbol{s}^{r_i}(r_{i+1}))^{m_i+1}, r_{i-1}) \ \ for \ \ i = 1, 2, \cdots, k,$$

and $\boldsymbol{s}^{r_k}(r_{k+1}) = (\beta)^{r_k-1}\alpha$ or $(\beta\alpha)^{\frac{r_k-2}{2}}\beta\beta$.

Proof. The statements (i) and (ii) are established by Proposition 3. One can obtain (iii) and (iv) by applying the Euclidean algorithm on $N = r_0$ and $p = r_1$ and the results in Propositions 5 and 6. □

4 Analyzing near maximum nonlinear complexity sequences

In this section we shall exactly determine the number of binary near maximum nonlinear complexity sequences of period N. By Theorems 1 and 2, we know that such sequences are determined by the values of the integer c. So we need to consider whether the sequences corresponding different values of the integer c are shift-distinct.

The following lemma shows a useful property of the periodic binary sequences $\mathbf{s}^N$ with nonlinear complexity $N-2$ which will be helpful. The proof will be included in Appendix A.

Lemma 7. *Let $\boldsymbol{s}^N$ be a periodic binary sequence with $N > 4$ and $C(\boldsymbol{s}^N) = N-2$. Then there is exactly one pair of $(N-3)$-tuples among $\boldsymbol{s}_i^{N+i-4}$ with $0 \le i \le N-1$ that are equal.*

With Lemma 7, we can characterize the shift equivalent relation between binary near maximum nonlinear complexity sequences as shown below.

Lemma 8. *For a given period $N > 4$, let c and c' be two distinct positive integers satisfying the condition (i) or (ii) in Proposition 2, and let $\boldsymbol{s}^N(c)$ and $\boldsymbol{s}^N(c')$ be periodic binary sequences with nonlinear complexity $N-2$ satisfying the conditions in (5) for the given positive integers c and c', respectively. Then $\boldsymbol{s}^N(c)$ and $\boldsymbol{s}^N(c')$ are shift equivalent if and only if $c + c' = N$.*

Proof. We first show the necessity. Suppose that

$$\mathbf{s}^N(c) = s_0 s_1 \cdots s_{N-1}, \text{ and } \mathbf{s}^N(c') = t_0 t_1 \cdots t_{N-1}.$$

Since $\mathbf{s}^N(c)$ and $\mathbf{s}^N(c')$ are shift equivalent, there exists an integer e with $1 \le e \le N-1$ such that

$$t_i = s_{(e+i) \bmod N}, \text{for } i \ge 0. \tag{9}$$

By (5), we have $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$. This together with (9) shows that $\mathbf{t}_{N-e}^{N-e+N-4} = \mathbf{t}_{(c-e) \bmod N}^{((c-e) \bmod N)+N-4}$. Again by (5), $\mathbf{t}_0^{N-4} = \mathbf{t}_{c'}^{N+c'-4}$. Then by Lemma 7,

$$(0, c') = ((c-e) \bmod N, N-e).$$

Since $1 \le c, e \le N-1$, we have $N = e + c' = c + c'$ as desired.

To prove the sufficiency, we assume, without loss of generality, that $c < N/2 < c'$. For the case $c = 1$, the periodic binary sequence $\mathbf{s}^N(c)$ with nonlinear complexity $N-2$ has the form $\mathbf{s}^N(1) = (\alpha)^{N-2}\beta\beta$ by Proposition 3 (i). For $c' = N-1$, it follows from Proposition 5 (i) that

$$\mathbf{s}^N(c') = \mathbf{s}^N(N-1) = (\alpha)^{N-3}\beta\beta\alpha,$$

which is easily seen to be shift equivalent to $\mathbf{s}^N(1)$. For the case N is even, $c = 2$ and $c' = N-2$, it follows from Proposition 3 (ii) and Proposition 5 (iii) that $\mathbf{s}^N(N-2)$ and $\mathbf{s}^N(2)$ are shift equivalent. For the case $c = p$ with $3 \le p < N/2 < c' = N-p$, let $N = mp + r$ with $0 < r < p$, then $m \ge 2$. By Propositions 5 and 6,

$$\mathbf{s}^N(p) = F((\mathbf{s}^p(r))^{m+1}, N) = (\mathbf{s}^p(r))^m F(\mathbf{s}^p(r), r).$$

For the integer $c' = N-p$, we have $N = c' + p$ and $c' = N-p = (m-1)p + r$, it follows from Proposition 6 that $\mathbf{s}^N(c') = \mathbf{s}^{c'}(p)F(\mathbf{s}^{c'}(p), p)$ and $\mathbf{s}^{c'}(p) = (\mathbf{s}^p(r))^{m-1}F(\mathbf{s}^p(r), r)$. Therefore,

$$\mathbf{s}^N(c') = \mathbf{s}^N(N-p) = (\mathbf{s}^p(r))^{m-1}F(\mathbf{s}^p(r), r)\,\mathbf{s}^p(r),$$

which is easily seen to be shift equivalent to $\mathbf{s}^N(p)$. □

Let $\mathcal{N}$ denote the number of all binary near maximum nonlinear complexity sequences of period $N \ge 4$. From the preceding discussion we get the following result.

Theorem 3. *Given a positive integer $N \ge 4$, the total number of binary near maximum nonlinear complexity sequences of period N, up to shift equivalence, is given by*

$$\mathcal{N} = \begin{cases} 1, & N = 4, \\ \varphi(N) - 2, & N \text{ is odd}, \\ \varphi(N) + 2\varphi(\frac{N}{2}) - 2, & N \text{ is even}, \end{cases}$$

where $\varphi(\cdot)$ is the Euler's totient function.

Proof. For the case $N = 4$, the result follows from Proposition 1.

For a given odd integer $N > 4$, by the recursive method in Theorem 1, the binary near maximum nonlinear complexity sequences of period N are determined by the choice of the integer c and the elements α, β in $\mathbb{F}_2$. Specifically, for a fixed integer c satisfying $\gcd(N, c) = 1$ and $c \ne 2, N-2$, there are two binary near maximum nonlinear complexity sequences of period N corresponding two different values of α and β. It then follows from Lemma 8 that there are, up to shift equivalence, in total $\varphi(N) - 2$ binary near maximum nonlinear complexity sequences of period N.

For a given even integer $N > 4$, by the recursive method in Theorem 2, there are two binary near maximum nonlinear complexity sequences of period N corresponding two different values of α and β for a fixed integer c satisfying either $\gcd(N, c) = 1$ or $c = 2, N-2$ and four such sequences for those c satisfying $\gcd(N, c) = 2$ and $c \ne 2, N-2$. Since the number of c with $\gcd(N, c) = 2$ is $\varphi(\frac{N}{2})$, it then follows from Lemma 7 that the total number of binary near maximum nonlinear complexity sequences of period N, up to shift equivalence, is $\varphi(N) + 2 + 2[\varphi(\frac{N}{2}) - 2] = \varphi(N) + 2\varphi(\frac{N}{2}) - 2$. □

Remark 2. *We denote by $nlin(N, C)$ the number of binary sequences of period N and nonlinear complexity C. In [17], only the value $nlin(N, N-1)$ is obtained. Theorem 3 completely determines $nlin(N, N-2)$. It remains open to give $nlin(N, N-i)$ for $i > 2$.*

Example 1. *By exhaustive search, for integer N with $4 \leq N \leq 18$, all binary sequences with period N and nonlinear $N-2$, up to equivalence, and the number $\mathcal{N}$ of such sequences are given in Table 2. It demonstrates the theoretical results in Theorems 1 and 2.*

To illustrate our recursive construction, we give the example for the case $N = 14$. By Theorem 2, for $c = 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13$, taking $\alpha = 0$ and $\beta = 1$, or $\alpha = 1$ and $\beta = 0$, we obtain the binary sequences with period 14 and nonlinear complexity 12. These sequences are exhibited in Table 1. It is readily seen that the sequences corresponding the integer c are shift equivalent to those corresponding $14 - c$. Moreover, by Theorem 3, the total number of the binary sequences with period 14 and nonlinear complexity 12 is $\varphi(14) + 2\varphi(7) - 2 = 16$, which is in accordance with the numerical result for $N = 14$ in Table 1.

Table 1: Binary sequences with period 14 and nonlinear complexity 12

c	$\alpha = 0,\ \beta = 1$	$\alpha = 1,\ \beta = 0$	c	$\alpha = 0,\ \beta = 1$	$\alpha = 1,\ \beta = 0$
1	$(0)^{12}11$	$(1)^{12}00$	13	$(0)^{12}11$	$(1)^{12}00$
2	$(01)^{6}00$	$(10)^{6}11$	12	$(01)^{6}00$	$(10)^{6}11$
3	$(001)^{4}00$	$(110)^{4}11$	11	$(001)^{4}00$	$(110)^{4}11$
4	$(1110)^{3}11$ $(1011)^{3}10$	$(0001)^{3}00$ $(0100)^{3}01$	10	$(1110)^{3}11$ $(1011)^{3}10$	$(0001)^{3}00$ $(0100)^{3}01$
5	$(00110)^{2}0011$	$(11001)^{2}1100$	9	$(00110)^{2}0011$	$(11001)^{2}1100$
6	$((1)^{5}0)^{2}11$ $(101011)^{2}10$	$((0)^{5}1)^{2}00$ $(010100)^{2}01$	8	$((1)^{5}0)^{2}11$ $(101011)^{2}10$	$((0)^{5}1)^{2}00$ $(010100)^{2}01$

We will present some experimental results on the linear and k-error linear complexity of near maximum nonlinear complexity sequences. From the definition of the nonlinear complexity of a sequence $\mathbf{s}^N$, we know that the linear complexity, denoted by $LC(\mathbf{s}^N)$, is no less than its nonlinear complexity $C(\mathbf{s}^N)$. Therefore, all near maximum nonlinear complexity sequences have maximum or near maximum high linear complexity.

The k-error linear complexity of a periodic sequence $\mathbf{s}^N$, denoted by $LC_k(\mathbf{s}^N)$, is defined as the smallest linear complexity that can be obtained by changing k or fewer bits of the sequence per period. A cryptographically strong sequence should have not only a large linear complexity, but also a large k-error linear complexity. This can insure that altering a few terms should not cause a significant decrease of the linear complexity. Given an integer N with $4 < N \leq 64$,

Table 2: Binary near maximum nonlinear complexity sequences of period $4 \le N \le 18$

N	Sequences	$\mathcal{N}$
4	0011	1
5	00011, 00111	2
6	000011, 000101, 010111, 001111	4
7	0000011, 0010011, 0011011, 0011111	4
8	00000011, 00001001, 00010101, 01010111, 01101111, 00111111	6
9	000000011, 000110011, 001100111, 001111111	4
10	0000000011, 0000010001, 0001000101, 0001010101, 0010010011 0011011011, 0101010111, 0101110111, 0111011111, 0011111111	10
11	00000000011, 00001001001, 00001100011, 00100110011 00110011011, 00111001111, 01101101111, 00111111111	8
12	000000000011, 000000100001, 000101010101 010101010111, 011110111111, 001111111111	6
13	0000000000011, 0000100001001, 0000011000011, 0010010010011, 0001100110011 0011001100111, 0011011011011, 0011110011111, 0110111101111, 0011111111111	10
14	00000000000011, 00000001000001, 00000100010001, 00001001001001 00010001000101, 00010100010101, 00010101010101, 00011000110011 00110011100111, 01010101010111, 01010111010111, 01011101110111 01101101101111, 01110111011111, 01111101111111, 00111111111111	16
15	000000000000011, 000000110000011, 001001100110011 001100110011011, 001111100111111, 001111111111111	6
16	0000000000000011, 0000000010000001, 0000010000010001, 0001000101000101 0000110001100011, 0010010010010011, 0001010101010101, 0101010101010111 0011011011011011, 0011100111001111, 0101110101110111, 0111011111011111 0111111011111111, 0011111111111111	14
17	00000000000000011, 00000001100000011, 00000010000100001, 00001001001001001 00001100001100011, 00100100110010011, 00011001100110011, 00110011001100111 00110110011011011, 00111001111001111, 01101101101101111, 00111111001111111 01111011110111111, 00111111111111111	14
18	000000000000000011, 000000000100000001, 000001000100010001, 000010000100001001 000100010001000101, 000101010001010101, 000101010101010101, 001001100100110011 001100110110011011, 010101010101010111, 010101011101010111, 010111011101110111 011011110111101111, 011101110111011111, 011111110111111111, 001111111111111111	16

we calculate the k-error linear complexity of all binary near maximum nonlinear complexity sequences $\mathbf{s}^N$ for small k, $1 \le k \le 3$. The numerical results show some regularity.

(i) For odd period N, $LC_1(\mathbf{s}^N) > \lfloor \frac{N}{2} \rfloor$ always holds, $LC_2(\mathbf{s}^N) > \lfloor \frac{N}{2} \rfloor$ holds except for two

sequences $\mathbf{s}^N = (0)^{N-2}11$ and $\mathbf{s}^N = (1)^{N-2}00$. Specially, if N is odd prime, then $LC_1(\mathbf{s}^N) = N - 1$.

(ii) For even period $N > 14$, $LC_1(\mathbf{s}^N) > \lfloor \frac{N}{2} \rfloor$ holds except for two sequences $\mathbf{s}^N = (01)^{\frac{N-2}{2}}00$ and $\mathbf{s}^N = (10)^{\frac{N-2}{2}}11$. Moveover, $LC_2(\mathbf{s}^N) > \lfloor \frac{N}{2} \rfloor$ holds for at least $\mathcal{N} - 10$ sequences, where $\mathcal{N}$ denotes the number of all binary near maximum nonlinear complexity sequences with period N.

We also make some comparisons between near maximum nonlinear complexity sequences and maximum nonlinear complexity sequences. Let N be the period. Some experimental results for N with $4 < N \leq 64$ are summarized in the following.

- All near maximum nonlinear complexity sequences of period N have two possible linear complexities. i.e., $N - 1$ and $N - 2$ while all maximum nonlinear complexity sequences have linear complexity $N - 1$.
- Let N be odd. Then each near maximum nonlinear complexity sequence shares the same k-error linear complexity profile with some maximum nonlinear complexity sequence of the same period.
- Let N be even. For any maximum nonlinear complexity sequence $\mathbf{s}^N$, we have $LC_1(\mathbf{s}^N) < LC(\mathbf{s}^N)$. However, For some near maximum nonlinear complexity sequences we have $LC_i(\mathbf{s}^N) = LC(\mathbf{s}^N)$ for all $i \leq 3$.

To sum up, near maximum nonlinear complexity sequences have almost the same linear complexities with maximum nonlinear complexity sequences. In some cases, they have more stable k-error linear complexity profile.

5 Conclusion

In this paper, we proceed with the theoretical investigation of periodic sequences with near maximum nonlinear complexity. Our main contribution is the establishment of an efficient recursive method for creating all binary near maximum nonlinear complexity sequences. The main results can be easily generalized to the nonbinary case. For future work, it is interesting to investigate sequences with high nonlinear complexity and other randomness properties.

Acknowledgements

The author would like to thank the anonymous referees for valuable comments and helpful suggestions. X. Zeng was supported by the National Natural Science Foundation of China (No.

61472120). C. Li was supported by European Union's Horizon 2020 research and innovation program under grant agreement No. H2020-MSCA-ITN-2014-643161 ECRYPT-NET.

Appendix A

Proof of Lemma 3. We only give a proof for (i). The result in (ii) can be proved similarly, so we skip it here. Since $uq - vn = 1$ implies $uq \equiv 1 \pmod{n}$, we have

$$\begin{aligned} H_2(n,q) &= \{(q-2+tq) \bmod n \mid t = 0, 1, \cdots, u-1\} \\ &= \{(q-2+(t-u)q) \bmod n \mid t = u, u+1, \cdots, 2u-1\} \\ &= \{(q-3+tq) \bmod n \mid t = u, u+1, \cdots, 2u-1\}, \end{aligned}$$

and

$$\begin{aligned} H_1(n,q) &= \{(q-1+tq) \bmod n \mid t = 0, 1, \cdots, n-2u-1\} \\ &= \{(q-1+(t-2u)q) \bmod n \mid t = 2u, 2u+1, \cdots, n-1\} \\ &= \{(q-3+tq) \bmod n \mid t = 2u, 2u+1, \cdots, n-1\}. \end{aligned}$$

Then it follows from the condition $\gcd(n,q) = 1$ that $H_i(n,q) \cap H_j(n,q) = \varnothing$ for $i, j = 1, 2, 3$ and $i \neq j$, and

$$\bigcup_{i=1}^{3} H_i(n,q) = \{(q-3+tq) \bmod n \mid t = 0, 1, \cdots, n-1\} = \mathbb{Z}_n.$$

Moreover, again by $uq \equiv 1 \pmod{n}$ we obtain $n-1 \equiv uq-2 \equiv q-2+(u-1)q \pmod{n}$, $n-2 \equiv uq-3 \equiv q-3+(u-1)q \pmod{n}$ and $n-3 \equiv nq-2uq-1 \equiv q-1+(n-2u-1)q \pmod{n}$, and so we have $n-1 \in H_2(n,q)$, $n-2 \in H_3(n,q)$ and $n-3 \in H_1(n,q)$. □

Proof of Lemma 4. Since $u \in \mathbb{Z}_{\frac{n}{2}}$ satisfies $u \cdot \frac{q}{2} \equiv 1 \pmod{\frac{n}{2}}$, it follows that $uq \equiv 2 \pmod{n}$. Then we have

$$\begin{aligned} D_1(n,q) &= \{(q-1+tq) \bmod n \mid t = 0, 1, \cdots, \frac{n}{2}-u-1\} \\ &= \{(q-1+(t-u)q) \bmod n \mid t = u, u+1, \cdots, \frac{n}{2}-1\} \\ &= \{(q-3+tq) \bmod n \mid t = u, u+1, \cdots, \frac{n}{2}-1\}. \end{aligned}$$

Then it follows from the condition $\gcd(\frac{n}{2}, \frac{q}{2}) = 1$ that $D_1(n,q) \cap D_3(n,q) = \varnothing$ and

$$\begin{aligned} D_1(n,q) \cup D_3(n,q) &= \{(q-3+tq) \bmod n \mid t = 0, 1, \cdots, \frac{n}{2}-1\} \\ &= \{(2 \cdot (\frac{q-4}{2} + t \cdot \frac{q}{2}) \bmod \frac{n}{2}) + 1 \mid t = 0, 1, \cdots, \frac{n}{2}-1\} \\ &= \{1, 3, 5, \cdots, n-1\}. \end{aligned}$$

In addition,

$$\begin{aligned} D_2(n,q) &= \{(q-2+tq) \bmod n \mid t = 0, 1, \cdots, \frac{n}{2} - 1\} \\ &= \{2 \cdot (\frac{q}{2} - 1 + t \cdot \frac{q}{2}) \bmod \frac{n}{2} \mid t = 0, 1, \cdots, \frac{n}{2} - 1\} \\ &= \{0, 2, 4, \cdots, n-2\}. \end{aligned}$$

It is easily seen that $D_i(n,q) \cap D_j(n,q) = \varnothing$ for $i, j \in \{1,2,3\}$ and $i \neq j$, and $\bigcup_{i=1}^{3} D_i(n,q) = \mathbb{Z}_n$. Furthermore, since $uq \equiv 2 \pmod n$ we obtain $n-1 \equiv -3 + uq \equiv q - 3 + (u-1)q \pmod n$, $n-2 \equiv \frac{q}{2} \cdot n - 2 \equiv q - 2 + (\frac{n}{2} - 1)q \pmod n$ and $n-3 \equiv \frac{q}{2} \cdot n - uq - 1 \equiv q - 1 + (\frac{n}{2} - u - 1)q \pmod n$, and so we have $n-1 \in D_3(n,q)$, $n-2 \in D_2(n,q)$ and $n-3 \in D_1(n,q)$. □

Proof of Lemma 5. (i) Substituting $N = mp + r$ in $ap - bN = 1$ yields $ap - b(mp + r) = 1$, and so $(p-b)r - (r - a + bm)p = 1$. Since $0 < a < \frac{N}{2}$, it follows that $0 < bN = ap - 1 < \frac{Np}{2}$, and thus $0 < b < \frac{p}{2}$. In addition, $0 < \frac{pr}{2} < (p-b)r - 1 < pr$, and so $0 < r - a + bm < r$. That is to say, $u = p - b > \frac{p}{2}$ and $v = r - a + bm$.

By the definition of the set $H_1(N,p)$, any element $x \in H_1(N,p)$ can be expressed uniquely as $x = p - 1 + t_x p - j_x N$, where $0 \leq t_x \leq N - 2a - 1$ and $0 \leq j_x = \lfloor \frac{t_x p + p - 1}{N} \rfloor \leq \lfloor \frac{p - 1 + (N - 2a - 1)p}{N} \rfloor = \lfloor \frac{(p-2b)N - 3}{N} \rfloor \leq p - 2b - 1$. As t_x runs through all nonnegtive integers $\leq N - 2a - 1$, then j_x runs through all nonnegtive integers $\leq p - 2b - 1$. Furthermore,

$$\begin{aligned} x &= p - 1 + t_x p - j_x(mp + r) \\ &\equiv (-1 - j_x r) \pmod p \\ &\equiv (r - 1 - 2(p-b)r + (p - 2b - 1 - j_x)r) \pmod p \\ &\equiv (r - 3 + (p - 2b - 1 - j_x)r) \pmod p. \end{aligned}$$

This implies,

$$H_1(N,p) \bmod p \subseteq I_3(p,r) \tag{10}$$

due to $0 \leq p - 2b - 1 - j_x \leq p - 2b - 1$. We next prove that $|H_1(N,p) \bmod p| = |I_3(p,r)|$. For any two elements $x, y \in H_1(N,p)$ with the expressions as $x = p - 1 + t_x p - j_x N$ and $y = p - 1 + t_y p - j_y N$, where $0 \leq t_x, t_y \leq N - 2a - 1$ and $0 \leq j_x, j_y \leq p - 2b - 1$, one has $x - y = (t_x - t_y)p - (j_x - j_y)N \equiv (j_y - j_x)r \pmod p$, which implies $x \equiv y \pmod p$ if and only if $j_y = j_x$. Therefore

$$|H_1(N,p) \bmod p| = |\{j_x \mid x \in H_1(N,p)\}| = p - 2b = |I_3(p,r)|.$$

Together with (10) we get the desired result. The statements $H_2(N,p) \bmod p = I_1(p,r)$ and $H_3(N,p) \bmod p = I_2(p,r)$ can be proved in a similar way. Hence we skip the proof here.

(ii) The assertion in (ii) can be proved by the same approach used in the proof of (i). So we omit the proof here as well. □

Proof of Lemma 6. Since $e\cdot\frac{p}{2}-f\cdot\frac{N}{2}=1$ and $N=mp+r$, it follows that $e\cdot\frac{p}{2}-f\cdot\frac{mp+r}{2}=1$, and so $(\frac{p}{2}-f)\frac{r}{2}-(fm-e+\frac{r}{2})\cdot\frac{p}{2}=1$. It is easily verify that $\frac{p}{2}-f\in\mathbb{Z}_{\frac{p}{2}}$ and $fm-e+\frac{r}{2}\in\mathbb{Z}_{\frac{r}{2}}$, so that $u=\frac{p}{2}-f$ and $v=fm-e+\frac{r}{2}$, and hence $D_1(p,r)=\{(r-1+tr)\bmod p \mid t=0,1,\cdots,f-1\}$, $D_2(p,r)=\{(r-2+tr)\bmod p \mid t=0,1,\cdots,\frac{p}{2}-1\}$, $D_3(p,r)=\{(r-3+tr)\bmod p \mid t=0,1,\cdots,\frac{p}{2}-f-1\}$. Since any integer $x\in D_2(N,p)$ can be expressed as $x=p-2+t_xp-j_xN$, where $0\le t_x\le\frac{N}{2}-1$ and $0\le j_x=\lfloor\frac{t_xp+p-2}{N}\rfloor\le\frac{p}{2}-1$. we obtain

$$\begin{aligned} x &= p-2+t_xp-j_x(mp+r)\\ &\equiv (-2-j_xr)\ (\mathrm{mod}\, p)\\ &\equiv (-2-\frac{pr}{2}+r-r+\frac{pr}{2}-j_xr)\ (\mathrm{mod}\, p)\\ &\equiv (r-2+(\frac{p}{2}-1-j_x)r)\ (\mathrm{mod}\, p). \end{aligned}$$

This implies $D_2(N,p)\bmod p\subseteq D_2(p,r)$ because of $0\le\frac{p}{2}-1-j_x\le\frac{p}{2}-1$. By using arguments analogous to those in the proof of Lemma 5 (i), one may show that $|D_2(N,p)\bmod p|=|D_2(p,r)|$. Therefore, $D_2(N,p)\bmod p=D_2(p,r)$. Similarly, the statements $D_1(N,p)\bmod p=D_3(p,r)$ and $D_3(N,p)\bmod p=D_1(p,r)$ can be proved. □

Proof of Lemma 7. Since $\mathbf{s}^N$ is a binary sequence with period $N>4$ and nonlinear complexity $N-2$, we may assume without loss of generality that there exists an positive integer $c<\frac{N}{2}$ such that

$$\mathbf{s}_0^{N-4}=\mathbf{s}_c^{N+c-4},\ \ s_{N-3}\ne s_{N+c-3}\ \text{ and }\ s_{N-1}\ne s_{N+c-1}.$$

We suppose that there exists another pair of $(N-3)$-tuples in $\mathbf{s}^N$ that are identical, say,

$$\mathbf{s}_d^{d+N-4}=\mathbf{s}_{d+e}^{d+e+N-4}\ \text{ with }\ 0\le d<d+e\le N-1\ \text{ and }\ (d,e)\ne(0,c).$$

If $d=0$, then we have $e\ne c$ and $\mathbf{s}_0^{N-4}=\mathbf{s}_c^{N+c-4}=\mathbf{s}_e^{N+e-4}$. Since $\mathbf{s}^N$ is a binary sequence, there must be two among the above three $(N-3)$-tuples with the same successor. Thus there exist two identical $(N-2)$-tuples in $\mathbf{s}^N$, which means $C(\mathbf{s}^N)>N-2$, a contradiction. Now we suppose $d\ne0$ and divide the proof into three cases according to the size of e.

Case 1: $e=1$. It follows from $\mathbf{s}_d^{d+N-4}=\mathbf{s}_{d+e}^{d+e+N-4}$ that $s_d=s_{d+1}=\cdots=s_{d+N-3}$. By using the same argument as in the proof of Lemma 2, we get $s_{d+N-3}\ne s_{d+N-2}$ and $s_{d+N-1}\ne s_{d+N+1}=s_{d+1}$. Since $\mathbf{s}^N$ is binary, we have $s_d=s_{d+1}=\cdots=s_{d+N-3}\ne s_{d+N-2}=s_{d+N-1}$. If $d=1$, it follows from $s_0=s_c$ that $c=N-1$, and hence $s_1=s_N=s_0$, a contradiction. If $d=2$, it follows from $s_0=s_c$ that $c=1$, and hence $s_1=s_2$, again a contradiction. If $d\ge3$, then $s_0=s_1=\cdots=s_{d-3}\ne s_{d-2}=s_{d-1}\ne s_d=s_{d+1}=\cdots=s_{N-1}$. When $c=1$, since

$0 \le d-3 < N-4$, it follows that $s_{d-3} = s_{d-2}$, an obvious contradiction. When $c > 1$, since $0 < d-2 \le N-4$, it follows that $s_{d-2} = s_{d+c-2}$, and hence $d+c-2 = d-1$ or $N+d-1$, which is impossible.

Case 2: $e = 2$. For odd N, we have

$$s_d = s_{d+2} = \cdots = s_{d+N-3},\ s_{d+1} = s_{d+3} = \cdots = s_{d+N-2}.$$

This implies that $\mathbf{s}^N$ is shift equivalent to $((\alpha\beta)^{\frac{N-1}{2}}\alpha)$ or $((\alpha\beta)^{\frac{N-1}{2}}\beta)$ where $\alpha, \beta \in \mathbb{F}_2$ and $\alpha \neq \beta$. It follows that $C(\mathbf{s}^N) > N-2$, a contradiction.

For even N, we have

$$s_d = s_{d+2} = \cdots = s_{d+N-2},\ s_{d+1} = s_{d+3} = \cdots = s_{d+N-3}.$$

It follows that $s_{d+N-3} \neq s_{d+N-2}$, since otherwise $\mathbf{s}^N$ is shift equivalent to $((\alpha)^{N-1}\beta)$, which is impossible. Further, we have

$$s_{d+N-2} = s_{d+N-1}.$$

Otherwise, $s_{d+N-1} = s_{d+N-3}$ since $\mathbf{s}^N$ is binary. This implies that $\mathbf{s}^N$ is shift equivalent to $((\alpha\beta)^{\frac{N}{2}})$, which is of period 2, a contradiction.

Since $0 \le d-1 \le N-4$, it follows from $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$ that $s_{d+N-1} = s_{d-1} = s_{d+c-1}$. Then we get c is odd due to that $d \le d+c-1 < d+N-1$. On the other hand, we get from $s_0 = s_c$ that c is even except for the only case that d is even and $c = d-1$. Consider s_2 and s_{c+2}. We have $s_2 = s_d$ since d is even and $s_{c+2} = s_{d+1}$ due to $c = d-1$. This yields that $s_2 \neq s_{c+2}$ since $s_d \neq s_{d+1}$. Note that N is even hence $N \ge 6$. Then $s_2 = s_{c+2}$ due to $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$. Thus, we arrive at a contradiction.

Case 3: $e \ge 3$. Then we have $d+e \le N-1 < N+d+e-4$, and since $\mathbf{s}_d^{N+d-4} = \mathbf{s}_{d+e}^{N+d+e-4}$, we get

$$s_{N-1} = s_{N-e-1}.$$

We also have $0 \le N-e-1 \le N-4$ in this case, and from $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$ we get then

$$s_{N-e-1} = s_{N+c-e-1}.$$

When $e+d-c \ge 3$, we have $d < N+c-e-1 \le N+d-4$. It follows from $\mathbf{s}_d^{N+d-4} = \mathbf{s}_{d+e}^{N+d+e-4}$ that

$$s_{N+c-e-1} = s_{N+c-1}.$$

When $e+d-c < 0$, we have $d \le c-e-1 < N+d-4$. Then with $\mathbf{s}_d^{N+d-4} = \mathbf{s}_{d+e}^{N+d+e-4}$ and the periodicity of the sequence we get

$$s_{N+c-e-1} = s_{c-e-1} = s_{c-1} = s_{N+c-1}.$$

Altogether, we have $s_{N-1} = s_{N+c-1}$ whenever $e + d - c \geq 3$ or $e + d - c < 0$, which is a contradiction. When $e + d - c = 0$, we obtain $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4} = \mathbf{s}_d^{N+d-4}$, which will lead to a contradiction by the same argument as in the case $d = 0$.

In the remaining case we have $e+d-c = 1$ or 2. Since $e \geq 3$ and $c < \frac{N}{2}$, we have $e+d \leq N-3$ except for two cases where $N = 7$, $c = 3$ and $N = 6$, $c = 2$. It is easily checked that there is only a pair of identical $(N-3)$-tuples in $\mathbf{s}^7(3)$ and $\mathbf{s}^6(2)$, so that we can assume $e + d \leq N - 3$. Then we get from $\mathbf{s}_d^{N+d-4} = \mathbf{s}_{d+e}^{N+d+e-4}$ that

$$s_{N-3} = s_{N-e-3}.$$

Moreover, we have $0 \leq N - e - 3 < N - 4$ and $d \leq N + c - e - 3 \leq d + N - 4$, it follows from $\mathbf{s}_0^{N-4} = \mathbf{s}_c^{N+c-4}$ and $\mathbf{s}_d^{N+d-4} = \mathbf{s}_{d+e}^{N+d+e-4}$ that

$$s_{N-e-3} = s_{N+c-e-3} \text{ and } s_{N+c-e-3} = s_{N+c-3}.$$

Therefore, we obtain $s_{N-3} = s_{N+c-3}$, a contradiction. □

References

[1] A.H. Chan, R.A. Games, On the quadratic spans of DeBruijn sequences, IEEE Trans. Inf. Theory 36(4), 822-829 (1990).

[2] C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl. 3, 159-174 (1997).

[3] C. Ding, T. Helleseth, W. Shan, On the linear complexity of Legendre sequences, IEEE Trans. Inf. Theory 44(3), 1276-1278 (1998).

[4] D. Erdmann, S. Murphy, An approximate distribution for the maximum order complexity, Des. Codes Cryptogr. 10(3), 325-339 (1997).

[5] C.J.A. Jansen, Investigations on nonlinear streamcipher systems: construction and evaluation methods, Ph.D. dissertation, 1989.

[6] C.J.A. Jansen, D.E. Boekee, The shortest feedback shift register that can generate a given sequence, in: Brassard G. (eds.) Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science, vol. 435, pp. 90-99, Springer-Verlag, New York (1989).

[7] J.H. Kim, H.Y. Song, On the linear complexity of Hall's sextic residue sequences, IEEE Trans. Inf. Theory 47(5), 2094-2096 (2001).

[8] N. Kolokotronis, N. Kalouptsidis, On the linear complexity of nonlinear filtered PN-sequences, IEEE Trans. Inf. Theory 49(11), 3047-3059 (2003).

[9] C. Lam, G. Gong, A lower bound for the linear span of filtering sequences, in State of the Art of Stream Ciphers (SASC), 220-233, 2004.

[10] N. Li, X. Tang, On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude, IEEE Trans. Inf. Theory 57(11), 7597-7604 (2011).

[11] K. Limniotis , N. Kolokotronis, N. Kalouptsidis, On the nonlinear complexity and Lempel-Ziv complexity of finite length sequences, IEEE Trans. Inf. Theory 53(11), 4293-4302 (2007).

[12] Y. Luo, C. Xing, L. You, Construction of sequences with high nonlinear complexity from function fields, IEEE Trans. Inf. Theory 63(12), 7646-7650 (2017).

[13] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, CRC press, 1996.

[14] H. Niederreiter, Linear complexity and related complexity measures for sequences, in Johansson T. and Maitra S. (eds.) International Conference on Cryptology in India, INDOCRYPT 2003. Lecture Notes in Computer Science, vol. 2904, pp. 1-17. Springer-Verlag, Berlin (2003).

[15] H. Niederreiter, C. Xing, Sequences with high nonlinear complexity, IEEE Trans. Inf. Theory 60(10), 6696-6701 (2014).

[16] K.G. Paterson, Root counting, the DFT and the linear complexity of nonlinear filtering, Des. Codes Cryptogr. 14(3), 247-259 (1998).

[17] G. Petrides, J. Mykkeltveit, Composition of recursions and nonlinear complexity of periodic binary sequences, Des. Codes Cryptogr. 49(1), 251-264 (2008).

[18] P. Rizomiliotis, N. Kalouptsidis, Results on the nonlinear span of binary sequences, IEEE Trans. Inf. Theory 51(4), 1555-1563 (2005).

[19] P. Rizomiliotis, N. Kolokotronis, N. Kalouptsidis, On the quadratic span of binary sequences, IEEE Trans. Inf. Theory 51(5), 1840-1848 (2005).

[20] P. Rizomiliotis, Constructing periodic binary sequences with maximum nonlinear span, IEEE Trans. Inf. Theory 52(9), 4257-4261 (2006).

[21] Z. Sun, X. Zeng, C. Li, T. Helleseth, Investigations on periodic sequences with maximum nonlinear complexity, IEEE Trans. Inf. Theory 63(10), 6188-6198 (2017).