The Linear Complexity and 2-Error Linear Complexity Distribution of 2^n-Periodic Binary Sequences with Fixed Hamming Weight

Wenlun Pan[1,2], Zhenzhen Bao[3(✉)], Dongdai Lin[1], and Feng Liu[1,2]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
wylbpwl@gmail.com, {ddlin,liufeng}@iie.ac.cn
[2] University of Chinese Academy of Sciences, Beijing 100049, China
[3] Shanghai Jiao Tong University, Shanghai 200240, China
baozhenzhen10@gmail.com

Abstract. The linear complexity and k-error linear complexity of sequences are important measures of the strength of key-streams generated by stream ciphers. Based on the characters of the set of sequences with given linear complexity, people get the characterization of 2^n-binary sequences with given k-error linear complexity for small k recently. In this paper, we put forward this study to get the distribution of linear complexity and k-error linear complexity of 2^n-periodic binary sequences with fixed Hamming weight. First, we give the counting function of the number of 2^n-periodic binary sequences with given linear complexity and fixed Hamming weight. Provide an asymptotic evaluation of this counting function when n gets large. Then we take a step further to study the distribution of 2^n-periodic binary sequences with given 2-error linear complexity and fixed Hamming weight. Through an asymptotic analysis, we provide an estimate on the number of 2^n-periodic binary sequences with given 2-error linear complexity and fixed Hamming weight.

Keywords: Sequence · Linear complexity · k-error linear complexity · Counting function · Hamming weight · Asymptotic analysis

1 Introduction

The linear complexity of an N-periodic sequence is defined by the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. By Berlekamp-Massey algorithm [7], we only need the first $2L$ elements of the sequence to recover the whole sequence, where L is the linear complexity of the sequence. For this reason, a secure key stream must has high linear complexity. But this is not sufficient. If altering a few elements in the sequence can result in greatly decrease its linear complexity, then the sequence is not cryptographically strong. This observation gives rise to the study of the stability of sequence [1] and develops to the concept of k-error linear complexity [11] which is defined

K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 107–123, 2016.
DOI: 10.1007/978-3-319-50011-9_9

as the minimum linear complexity of the sequence altering not more than k elements from the original sequence. A cryptographically strong sequence must both have larger linear complexity and k-error linear complexity.

Let $S = (s_0 s_1 \cdots s_{N-1})^\infty$ be an N-periodic sequence with the terms in finite field $\mathbb{F}_2$. And we denote S^N the set of all N-periodic binary sequences. For a given sequence $S \in S^N$, we denote the support set of S by $supp(S)$, which is the positions of nonzero elements in S, that is, $supp(S) = \{i : \ s_i \neq 0, \ 0 \leq i < N\}$. For $i, j \in supp(S)$, we define the distance between i and j as $d(i, j) = 2^t$ where $|i - j| = 2^t b$ and $2 \not| b$. Let $w_H(S)$ denote the Hamming weight of sequence S which is the number of nonzero elements of S in one period.

The linear complexity of S, denoted by $LC(S)$, is given by [1]

$$LC(S) = N - \deg(\gcd(x^N - 1, S(x))) \tag{1}$$

where $S(x) = s_0 + s_1 x + s_2 x^2 + ... + s_{N-1} x^{N-1}$ and is called the corresponding polynomial to S. According to Eq. (1), we can get the following two lemmas:

Lemma 1 [8]**.** *Let S be a 2^n-periodic binary sequence. Then $LC(S) = 2^n$ if and only if the Hamming weight of the sequence S is odd.*

Lemma 2 [8]**.** *Let S and S' be two 2^n-periodic binary sequences. Then we have $LC(S + S') = \max\{LC(S), \ LC(S')\}$ if $LC(S) \neq LC(S')$, and $LC(S + S') < LC(S)$ for otherwise.*

In this paper, we focus on 2^n-periodic binary sequences. Based on the observation $x^{2^n} - 1 = (x - 1)^{2^n}$, we have

$$\begin{aligned}\gcd(x^{2^n} - 1, S(x)) &= \gcd((x-1)^{2^n}, S_L(x) + x^{2^{n-1}} S_R(x)) \\ &= \gcd((x-1)^{2^n}, (S_L(x) + S_R(x)) + (x+1)^{2^{n-1}} S_R(x)),\end{aligned}$$

and according to Eq. (1), we get

$$LC(S) = \begin{cases} 2^{n-1} + LC(S_L + S_R) & \text{if } S_L \neq S_R, \\ LC(S_L) & \text{otherwise,} \end{cases} \tag{2}$$

where S_L, S_R are the left and right half part of the sequence S respectively and $S_L(x) = s_0 + s_1 x + \cdots + s_{2^{n-1}-1} x^{2^{n-1}-1}$, $S_R(x) = s_{2^{n-1}} + s_{2^{n-1}+1} x + \cdots + s_{2^n-1} x^{2^{n-1}-1}$. And the summation of two sequences $S = (s_0 s_1 \cdots s_{N-1})$, $S' = (s'_0 s'_1 \cdots s'_{N-1})$ is defined as $S + S' = (u_0 u_1 \cdots u_{N-1})$ where $u_i = s_i + s'_i$ for $0 \leq i < N$.

Iterating Eq. (2) on the length of sequence, one can immediately get the linear complexity of the 2^n-periodic binary sequence (note that, for sequence of length 1, $LC((1)) = 1$ and $LC((0)) = 0$). This iteration algorithm is known as Games-Chan Algorithm developed in [3].

For $0 \leq k \leq N$, the k-error linear complexity of S, denoted by $LC_k(S)$, is definable by

$$LC_k(S) = \min_{w_H(E) \leq k, \ E \in S^N} LC(S + E), \tag{3}$$

where E is called the error sequences.

For a given sequence $S \in S^N$, denote $merr(S) = \min\{k : LC_k(S) < LC(S)\}$, which is called the first descend point of linear complexity of S. Kurosawa et al. in [6] derived a formula for the exact value of $merr(S)$.

Lemma 3 [6]**.** *Let S be a nonzero 2^n-periodic binary sequence, then the first descend point of S is*

$$merr(S) = 2^{w_H(2^n - LC(S))}. \tag{4}$$

The counting function of a sequence complexity measure depicts the distribution of the sequences with given complexity. It is useful to determine the expected value and variance of a given complexity measure of a family of sequences. Besides, the exact number of available good sequences with high complexity measure value in a family of sequences can be known. Rueppel [10] determined the counting function of linear complexity for 2^n-periodic binary sequences as follows:

Lemma 4 [10]**.** *Let $\mathcal{N}(L)$ and $\mathcal{A}(L)$ respectively denote the number of and the set of 2^n-periodic binary sequences with given linear complexity L, where $0 \leq L \leq 2^n$. Then*

$$\mathcal{N}(0) = 1, \qquad \mathcal{A}(0) = \{(00\cdots0)\}, \text{ and}$$
$$\mathcal{N}(L) = 2^{L-1}, \quad \mathcal{A}(L) = \{S \in S^{2^n} : S(x) = (1-x)^{2^n - L}a(x),\ a(1) \neq 0\} \text{ for } 1 \leq L \leq 2^n.$$

Let $\mathcal{A}_k(L)$ and $\mathcal{N}_k(L)$ denote the set of and the number of 2^n-periodic binary sequences with k-error linear complexity L, $\mathcal{A}^w(L)$ and $\mathcal{N}^w(L)$ denote the set of and the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L, and $\mathcal{A}_k^w(L)$ and $\mathcal{N}_k^w(L)$ denote the set of and the number of 2^n-periodic binary sequences with Hamming weight w and k-error linear complexity L respectively, which can be formally defined as

$$\mathcal{A}_k(L) = \{S \in S^{2^n} : LC_k(S) = L\} \quad \text{and} \quad \mathcal{N}_k(L) = |\mathcal{A}_k(L)|,$$

$$\mathcal{A}^w(L) = \{S \in S^{2^n} : LC(S) = L \text{ and } w_H(S) = w\} \quad \text{and} \quad \mathcal{N}^w(L) = |\mathcal{A}^w(L)|,$$

$$\mathcal{A}_k^w(L) = \{S \in S^{2^n} : LC_k(S) = L \text{ and } w_H(S) = w\} \quad \text{and} \quad \mathcal{N}_k^w(L) = |\mathcal{A}_k^w(L)|.$$

By Lemma 4, one can get fully knowledge of the distribution of 2^n-periodic binary sequences with given linear complexity. Based on the characters of $\mathcal{A}(L)$ and using algebraic, combinatorial or decomposing method [2,5,9,13], people get the counting function $\mathcal{N}_k(L)$ for small k. However, under the current state of art, distribution of 2^n-periodic binary sequences with given linear complexity when fixed Hamming weight remains unclear. In this paper we first provide a solution to this interesting problem. And then get the distribution of 2-error linear complexity with fixed Hamming weight which is a more difficult question to answer. In other words, we study the counting function for the number of balanced 2^n-periodic binary sequences with given values of complexity measure. As a contribution, we provide asymptotic evaluations as well as the explicit formulas of the counting functions.

2 The Characterization of $\mathcal{A}^w(L)$

In this section we discuss the linear complexity distribution of 2^n-periodic binary sequences with fixed Hamming weight.

2.1 Counting Functions for $\mathcal{N}^w(L)$

Let us first review the Games-Chan Algorithm. For a 2^n-periodic binary sequence S, one can use Eq. (2) recurrently on the length of sequence to get the linear complexity of S. Now to counting the sequences, we reverse this process, namely, we use a short sequence to construct the long. In this reversed process, we make the linear complexity of the constructed sequence equal to L step by step. Simultaneously, we restrict the Hamming weight of constructed sequences to w to get the number of sequences which meet the requirements. We begin with a simple case that is less general than what can actually be said.

Lemma 5. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L, then one have*

$$\mathcal{N}^w(2^r+1) = \begin{cases} 2^{2^r} & \text{if } w = 2^{n-1}, \\ 0 & \text{otherwise}, \end{cases} \tag{5}$$

$$\mathcal{N}^w(2^{r_1}+2^{r_2}+1) = \begin{cases} 2^{2^{r_2}+2^{r_1-1}}\binom{2^{r_1-1}}{m} & \text{if } w = 2^{n-2}+m\cdot 2^{n-r_1} \text{ and } 0 \le m \le 2^{r_1-1}, \\ 0 & \text{otherwise}, \end{cases} \tag{6}$$

where $0 \le r < n$ and $0 \le r_2 < r_1 < n$.

Proof. Let $S = (s_0 s_1 \cdots s_{N-1})$ be binary sequence of linear complexity 2^r+1 and length N with $N = 2^{r+1}$. According to Eq. (2), we have $S_L \neq S_R$ and $LC(S_L + S_R) = 1$ and then we get $s_i + s_{i+N/2} = 1$ for $0 \le i < N/2$ where S_L and S_R denote the left and right half part of S respectively. Therefore, the number of 2^{r+1}-periodic binary sequences of linear complexity 2^r+1 is 2^{2^r} and we denote the set of all those sequence by $\mathcal{A}$.

For any sequence S in $\mathcal{A}$, we can construct a sequence S_1 of length 2^{r+2} preserving linear complexity by connecting two S, i.e. $S_1 = S||S$. In the same way, we can construct a serial sequences S_i, $1 < i \le n-i$, preserving the linear complexity where the length of S_i is 2^{r+i+1}. As a result, we can construct 2^{2^r} sequences of periodic 2^n and linear complexity 2^r+1. From Games-Chan Algorithm we can know that there does not exist sequences of linear complexity 2^r+1 except for those constructed above. Thus, the number of 2^n-periodic binary sequences of linear complexity 2^r+1 is 2^{2^r} and the Hamming weight of the sequence must be $(2^r)^{n-r-1} = 2^{n-1}$.

Similarly, there are $2^{2^{r_2}}$ binary sequences of length 2^{r_2+1} having linear complexity $2^{r_2}+1$. We can extend those sequences to sequences of length 2^{r_1} using the same method. It is clear that the Hamming weight of those extended sequences are 2^{r_1-1} and we denote the set of those sequences by $\mathcal{A}_1$.

For any sequence S in $\mathcal{A}_1$, suppose the support set of S is $supp(S) = \{i_1, i_2, \cdots, i_{N_1}\}$ where $N_1 = 2^{r_1-1}$ and $0 \le i_1 < i_2 < \cdots < i_{N_1} < 2^{r_1}$. Denote $U_s = \{0, 1, \cdots, 2^{r_1}-1\}$ and $U'_r = U_r - supp(S)$. Choose m points $j_1, j_2, \cdots, j_m$ from the set U'_r where $0 \le m \le 2^{r_1-1}$ and construct a sequence $S_1 = (s_0 s_1 \cdots s_{N_2})$ where $N_2 = 2^{r_1+1}$ and $s_{i_u} + s_{i_u+2^{r_1}} = 1$, $s_{j_v} + s_{j_v+2^{r_1}} = 2$ for $1 \le u \le N_1$, $1 \le v \le m$ and $s_t = 0$ for $t \notin \{i_1, \cdots, i_{N_1}, i_1 + 2^{r_1}, \cdots, i_{N_1} + 2^{r_1}, j_1, \cdots, j_m, j_1 + 2^{r_1}, \cdots, j_m + 2^{r_1}\}$. It can be confirmed that the linear complexity of S_1 is $2^{r_1} + 2^{r_2} + 1$ and the Hamming weight of S_1 is $2^{r_1-1} + 2m$. We use the same method to extend the length of S_1 to 2^n preserving the linear complexity. And the Hamming weight of constructed sequences are $(2^{r_1-1} + 2m) \cdot 2^{n-r_1-1} = 2^{n-2} + m \cdot 2^{n-r_1}$. Because for each sequence S we can construct $2^{2^{r_1-1}} \cdot \binom{2^{r_1-1}}{m}$ different sequences S_1, then we can construct $2^{2^{r_2}} \cdot 2^{2^{r_1-1}} \cdot \binom{2^{r_1-1}}{m}$ different sequences with Hamming weight $2^{n-2} + m \cdot 2^{n-r_1}$ and linear complexity $2^{r_1} + 2^{r_2} + 1$. Consequently, we get the counting function for $\mathcal{N}^w(2^{r_1} + 2^{r_2} + 1)$ as shown above. □

This argument readily extends to general cases in which binary representation of L involves an arbitrary number of ones.

Theorem 1. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L. Then when $L = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t} + 1$ and w is even, we have*

$$\mathcal{N}^w(L) = \sum_{\sum_{j=1}^{t-1} m_j \cdot 2^{n-r_j-j+1} = w - 2^{n-t},\ m_j \ge 0} 2^{2^{r_t}} \prod_{j=1}^{t-1} 2^{u_j} \cdot \binom{2^{r_j} - u_j}{m_j} \tag{7}$$

where $0 \le r_t < r_{t-1} < \cdots < r_1 < n$, $2 \le t < n$ and $u_{t-1} = 2^{r_{t-1}-1}$, $u_j = (2m_{j+1} + u_{j+1}) \cdot 2^{r_j - r_{j+1} - 1}$ for $1 \le j < t-1$.

Proof. The proof of Lemma 5 applies verbatim here.

First we construct $2^{2^{r_t}}$ sequences of length 2^{r_t+1} and linear complexity $2^{r_t}+1$, and at the same time all those sequences have Hamming weight 2^{r_t}. Denote the set of those sequences by $\mathcal{A}_t$. For any sequence S_t in $\mathcal{A}_t$, we extend the length of it to $2^{r_{t-1}}$ in the same way as we did in the previous proof, and denote the extended sequence by S'_t. It is apparent that the Hamming weight of S'_t is $2^{r_{t-1}-1}$.

Suppose the support set of S'_t is $supp(S'_t) = \{i_1, i_2, \cdots, i_{N_{t-1}}\}$ where $N_{t-1} = 2^{r_{t-1}-1}$. Denote $U_{t-1} = \{0, 1, \cdots, 2^{r_{t-1}} - 1\}$ and $U'_{t-1} = U_{t-1} - supp(S'_t)$. By choosing m_{t-1} points $j_1, j_2, \cdots, j_{m_{t-1}}$ from U'_{t-1}, we can construct a sequence $S_{t-1} = (s_0 s_1 \cdots s_{N_{t-1}})$ where $N_{t-1} = 2^{r_{t-1}+1}$ and $s_{i_u} + s_{i_u+2^{r_{t-1}}} = 1$, $s_{j_v} + s_{j_v+2^{r_{t-1}}} = 2$ for $1 \le u \le N_{t-1}$, $1 \le v \le m_{t-1}$ and $s_k = 0$ for $k \notin \{i_1, \cdots, i_{N_{t-1}}, i_1+2^{r_1}, \cdots, i_{N_{t-1}}+2^{r_{t-1}}, j_1, \cdots, j_{m_{t-1}}, j_1+2^{r_{t-1}}, \cdots, j_{m_{t-1}}+2^{r_{t-1}}\}$. We can confirm that the constructed sequence has linear complexity $2^{r_{t-1}} + 2^{r_t} + 1$ and Hamming weight $2^{r_{t-1}-1} + 2 \cdot m_{t-1}$. For each S'_t we can construct $2^{2^{r_{t-1}-1}} \binom{2^{r_{t-1}-1}}{m_{t-1}}$ different S_{t-1} of linear complexity $2^{r_{t-1}} + 2^{r_t} + 1$ and

the same Hamming weight by choosing different m_{t-1} points from the set U'_{t-1}. Denote the set of those constructed sequences by $\mathcal{A}_{t-1,m_{t-1}}$.

For any sequence S_{t-1} in $\mathcal{A}_{t-1,m_{t-1}}$, we extend the length of it to $2^{r_{t-2}}$ and preserving the linear complexity at the same time, which results in a sequence S'_{t-1}. It can be verified that Hamming weight of S'_{t-1} is $u_{t-2} = (2^{r_{t-1}-1} + 2m_{t-1}) \cdot 2^{r_{t-2}-r_{t-1}-1}$.

Suppose the support set of S'_{t-1} is $supp(S'_{t-1}) = \{i_1, i_2, \cdots, i_{u_{t-2}}\}$. Denote $U_{t-2} = \{0, 1, \cdots, 2^{r_{t-2}} - 1\}$ and $U'_{t-2} = U_{t-2} - supp(S'_{t-1})$. In the same vein, by choosing m_{t-2} points $j_1, j_2, \cdots, j_{m_{t-2}}$ from the set U'_{t-2}, we can construct a sequence $S_{t-2} = (s_0 s_1 \cdots s_{2^{r_{t-2}+1}})$ where $s_{i_u} + s_{i_u+2^{r_{t-2}}} = 1$, $s_{j_v} + s_{j_v+2^{r_{t-2}}} = 2$ and $s_k = 0$ for $1 \le u \le u_{t-2}$, $1 \le v \le m_{t-2}$ and $k \notin \{i_1, \cdots, i_{u_{t-2}}, i_1 + 2^{r_{t-2}}, \cdots, i_{u_{t-2}} + 2^{r_{t-2}}, \cdots, j_1, \cdots, j_{m_{t-2}}, j_1 + 2^{r_{t-2}}, \cdots, j_{m_{t-2}} + 2^{r_{t-2}}\}$. For each S'_{t-1} we can construct $2^{u_{t-2}} \cdot \binom{2^{r_{t-2}} - u_{t-2}}{m_{t-2}}$ different S_{t-2} of linear complexity $2^{r_{t-2}} + 2^{r_{t-1}} + 2^{r_t} + 1$ and Hamming weight $u_{t-2} + 2m_{t-2}$ by choosing different m_{t-2} points from U'_{t-2}. Denote the set of those constructed sequences by $\mathcal{A}_{t-2,m_{t-2}}$.

For each sequence S_{t-2} in $\mathcal{A}_{t-2,m_{t-2}}$, we extend it length to $2^{r_{t-3}}$ and preserving its linear complexity, which results in a sequence S'_{t-2}.

Proceeding in precisely the same manner as the previous process by recurrence, we can eventually extend the length of a sequence S_t in $\mathcal{A}_t$ to 2^n and make the final constructed sequence have linear complexity $2^{r_1} + 2^{r_2} + \cdots + 2^{r_t} + 1$ step by step. For each S_t in $\mathcal{A}_t$ we can get the set $\mathcal{A}_{t-1,m_{t-1}}$ by adding m_{t-1} points to S'_t and similarly for each sequence S_{t-1} in $\mathcal{A}_{t-1,m_{t-1}}$ we can get the set $\mathcal{A}_{t-2,m_{t-2}}$ by adding m_{t-2} points to S'_{t-1}. In this way, we can construct $2^{2^{r_t}} \cdot \prod_{j=t-1}^{1} 2^{u_j} \binom{2^{r_j} - u_j}{m_j}$ sequences of linear complexity L and Hamming weight $(u_1 + 2m_1) \cdot 2^{n-r_1-1}$ where $u_{t-1} = 2^{r_{t-1}-1}$ and $u_j = (u_{j+1} + 2m_{j+1}) \cdot 2^{r_j - r_{j+1}-1}$ for $1 \le j < t-1$.

As a result, for given linear complexity L and Hamming weight w, the number of sequences of linear complexity L and Hamming weight w is the summation of $2^{2^{r_t}} \cdot \prod_{j=t-1}^{1} 2^{u_j} \binom{2^{r_j} - u_j}{m_j}$ for all $m_1, m_2, \cdots, m_{t-1}$ such that $w = (u_1 + 2m_1) \cdot 2^{n-r_1-1} = \sum_{i=1}^{t-1} m_i \cdot 2^{n-r_i-i+1} + 2^{n-t}$ and from here, we achieve Eq. (7). □

Furthermore, we observe that when $r_t = 0$ the linear complexity $L = 2^{r_1} + 2^{r_2} + \cdots 2^{r_t} + 1$ has the form $L = 2^{r_1} + 2^{r_2} + \cdots 2^{r_{t'}+1}$ where $0 \le r_t < r_{t-1} < \cdots < r_1 < n$, $t < n$, and $r_{t'-1} - r_{t'} > 1$, $r_j - r_{j+1} = 1$ for $t' < j \le t$. In this case, we can use a similar method to construct sequences with linear complexity L and length 2^n from sequences with linear complexity $2^{r_{t'}}$ and length $2^{r_{t'}}$.

Corollary 1. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L. When $L = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t}$, we have*

$$\mathcal{N}^w(L) = \sum_{m=1, m \text{ is odd}}^{2^{r_t}} \sum_{\sum_{j=1}^{t-1} m_j \cdot 2^{n-r_j-j+1} = w - m \cdot 2^{n-r_t-t+1}} \binom{2^{r_t}}{m} \cdot \prod_{j=1}^{t-1} 2^{u_{m,j}} \cdot \binom{2^{r_j} - u_{m,j}}{m_j} \tag{8}$$

where $0 < r_t < r_{t-1} < \cdots < r_1 < n$, $2 \le t < n$ *and* $u_{m,t-1} = m \cdot 2^{r_{t-1}-r_t}$, $u_{m,j} = (2m_{j+1} + u_{j+1}) \cdot 2^{r_j - r_{j+1}-1}$ *for* $1 \le j < t-1$.

Proof. This corollary can be derived from Eq. (7) by exchanging the order of summations. We can also give a constructive proof similar to the one used for Theorem 1 and get the equation directly. Firstly, the number of sequences with length 2^{r_t}, linear complexity 2^{r_t} and Hamming weight m is $\binom{2^{r_t}}{m}$ where m must be odd. And denote the set of those sequences by $\mathcal{A}_{m,t}$. For sequence S_t in $\mathcal{A}_{m,t}$ we can extend the length to 2^n and make the linear complexity to be L using a similar method to the one in the proof for Theorem 1 step by step. And we can get the number of 2^n-periodic binary sequences with linear complexity L and Hamming weight $w = (u_{m,1} + 2m_1) \cdot 2^{n-r_1-1}$ which is $\binom{2^{r_t}}{m} \sum_{u_{m,1}+2m_1=w} \prod_{i=1}^{t-1} 2^{u_{m,i}} \binom{2^{r_i}-u_{m,i}}{m_i}$ where $u_{m,t-1} = m \cdot 2^{r_{t-1}-r_t}$ and $u_{m,i} = (u_{m,i+1} + 2m_{i+1}) \cdot 2^{r_i - r_{i+1}-1}$ for $1 \le i < t-1$. Then by enumerating all possible value of m and we can get Eq. (8). □

Because $w = \sum_{i=1}^{t-1} m_i \cdot 2^{n-r_i-i+1} + 2^{n-t}$ and $2^{n-r_1} \le 2^{n-r_j-j+1}$ for $1 < j \le t-1$, thus $2^{n-r_1} | w$. Combine with the fact that w is in range from 2^{n-t} to $2^n - 1$, we have

Corollary 2. *Let* S *be a* 2^n*-periodic binary sequence, if the linear complexity of* S *is* $L = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t} + 1$, *where* $0 \le r_t < r_{t-1} < \cdots < r_1 < n$ *and* $t < n$, *then the Hamming weight of* S *only can be* $2^{n-1} + l \cdot 2^{n-r_1}$ *and* $2^{r_1-t} - 2^{r_1-1} \le l \le 2^{r_1-1} - 2^{r_1-t}$.

To get the exact value of $\mathcal{N}^w(L)$, we need to get all solutions of equation $\sum_{j=1}^{t-1} m_j \cdot 2^{n-r_j-j+1} = 2^{n-1} - 2^{n-t}$. This may turns out to be impossible to solve when n is large. Thus, the result for $\mathcal{N}^w(L)$ in this subsection is perhaps not too useful for grasping the number of the sequence when n gets large, so that asymptotic analysis is called for.

To this end, we make asymptotic analysis of $\mathcal{N}^w(L)$, provide lower bound and upper bound of its value in the following subsection.

2.2 Asymptotic Analysis for $\mathcal{N}^w(L)$

Suppose $L = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t} + 1$ with $0 \le r_t < r_{t-1} < \cdots < r_1 < n$ in the sequel.

Let us begin with a simple case in which $t = 3$, and $w = 2^{n-1}$. According to Eq. (7), when $L = 2^{r_1} + 2^{r_2} + 2^{r_3} + 1$, $0 \le r_3 < r_2 < r_1 < n$ and $w = 2^{n-1}$, we have

$$\mathcal{N}^w(L) = 2^{2^{r_3}+2^{r_2-1}+2^{r_1-2}} \cdot \sum_{m=0}^{2^{r_2-1}} 2^{m \cdot 2^{r_1-r_2}} \binom{2^{r_2-1}}{m} \binom{3 \cdot 2^{r_1-2} - m \cdot 2^{r_1-r_2}}{3 \cdot 2^{r_1-3} - m \cdot 2^{r_1-r_2-1}}. \tag{9}$$

The following lemma provides an asymptotic estimate for this case.

Lemma 6. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L. Then when $L = 2^{r_1} + 2^{r_2} + 2^{r_3} + 1$ where $0 \le r_3 < r_2 < r_1 < n$ and $w = 2^{n-1}$, we have*

$$\begin{aligned} \mathcal{N}^w(L) &\ge 2^{2^{r_3}+2^{r_2-1}+2^{r_1}-0.5r_1-0.9107}(1+2^{\frac{0.7213}{3\cdot 2^{r_2-2}}})^{2^{r_2-1}}, \\ \mathcal{N}^w(L) &\le 2^{2^{r_3}+2^{r_2-1}+2^{r_1}-0.5r_1-0.9107}(1+2^{\frac{1.1887}{3\cdot 2^{r_2-2}}})^{2^{r_2-1}}. \end{aligned} \tag{10}$$

Proof. From Stirling's formula

$$n! = \sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{\theta_n}{12n}}, \quad 0 < \theta_n < 1, \tag{11}$$

it implies that

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{\sqrt{2\pi\cdot 2n}(\frac{2n}{e})^{2n} e^{\frac{\theta_{2n}}{24n}}}{(\sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{\theta_n}{12n}})^2} = 2^{2n-0.5\log n-0.5\log\pi+\frac{\theta}{3n}} = 2^{2n-0.5\log n-0.8257+\frac{\theta}{3n}}, \tag{12}$$

where $-0.7214 < \theta < 0.1084$.

Accordingly, the logarithmic transformation of the number of combinations $\binom{3\cdot 2^{r_1-2}-m\cdot 2^{r_1-r_2}}{3\cdot 2^{r_1-3}-m\cdot 2^{r_1-r_2-1}}$ yields:

$$\begin{aligned} &\log\binom{3\cdot 2^{r_1-2}-m\cdot 2^{r_1-r_2}}{3\cdot 2^{r_1-3}-m\cdot 2^{r_1-r_2-1}} \\ &= 3\cdot 2^{r_1-2} - m\cdot 2^{r_1-r_2} - 0.5\log(3\cdot 2^{r_1-2} - m\cdot 2^{r_1-r_2}) - 0.3257 + \varepsilon \\ &= 3\cdot 2^{r_1-2} - m\cdot 2^{r_1-r_2} - 0.5r_1 + \frac{\log e}{2}\frac{m}{3\cdot 2^{r_2-2}}(1+\sum_{i=2}^{\infty}\frac{1}{i}(\frac{m}{3\cdot 2^{r_2-2}})^{i-1}) - 0.9107 + \varepsilon \end{aligned}$$

where $\varepsilon = \frac{\theta}{3(3\cdot 2^{r_1-2}-m\cdot 2^{r_1-r_2})}$ and $-0.7214 < \theta < 0.1084$.

By observing that $0 \le \frac{m}{3\cdot 2^{r_2-2}} \le \frac{2}{3}$, and $\frac{\theta}{9\cdot 2^{r_1-2}} < \varepsilon < \frac{\theta}{3\cdot 2^{r_1-2}}$, we have

$$\begin{aligned} \log\binom{3\cdot 2^{r_1-2}-m\cdot 2^{r_1-r_2}}{3\cdot 2^{r_1-3}-m\cdot 2^{r_1-r_2-1}} &\ge 3\cdot 2^{r_1-2} - 0.5r_1 + (\frac{0.7213}{3\cdot 2^{r_2-2}} - 2^{r_1-r_2})\cdot m - 0.9107, \\ \log\binom{3\cdot 2^{r_1-2}-m\cdot 2^{r_1-r_2}}{3\cdot 2^{r_1-3}-m\cdot 2^{r_1-r_2-1}} &\le 3\cdot 2^{r_1-2} - 0.5r_1 + (\frac{1.1887}{3\cdot 2^{r_2-2}} - 2^{r_1-r_2})\cdot m - 0.9107. \end{aligned}$$

Altogether, the asymptotic evaluation of $\mathcal{N}^w(L)$ is well summarized by Lemma 6. □

By completing a similar yet much harder analytic task, we next provide the asymptotic form of $\mathcal{N}^w(L)$ for more general case.

Theorem 2. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L. Then when $L = 2^{r_1}+2^{r_2}+\cdots+2^{r_t}+1$ with $0 \le r_t < r_{t-1} < \cdots < r_1 < n$, $3 < t < n$ and $w = 2^{n-1}$, we have*

$$\begin{aligned} \mathcal{N}^w(L) &\ge 2^{2^{r_t}+2^{r_1}-0.5r_1-0.3257+\frac{0.7213}{2^{t-1}}}\prod_{j=2}^{t-1} b_j^{2^{r_j}}(\frac{2}{b_j})^{2^{r_j-t+j}} \\ \mathcal{N}^w(L) &\le 2^{2^{r_t}+2^{r_1}-0.5r_1-0.3257+\frac{1.2203}{2^{t-1}}}\prod_{j=2}^{t-1} a_j^{2^{r_j}}(\frac{2}{a_j})^{2^{r_j-t+j}} \end{aligned} \tag{13}$$

where $a_1 = 2^{1-\frac{1.2203}{2^{r_1}}}$, $b_1 = 2^{1-\frac{0.7213}{2^{r_1}}}$ *and* $a_j = 1 + \prod_{i=1}^{j-1}(\frac{2}{a_i})^{2^{r_i - r_j + i - j + 1}}$, $b_j = 1 + \prod_{i=1}^{j-1}(\frac{2}{b_i})^{2^{r_i - r_j + i - j + 1}}$ *for* $1 < j < t$.

Proof. Recall that $u_{t-1} = 2^{r_{t-1}} - 1$ and $u_j = (2m_{j+1} + u_{j+1}) \cdot 2^{r_j - r_{j+1} - 1}$ *for* $1 \leq j < t-1$, there follows:

$$\begin{aligned} u_1 &= (u_2 + 2m_2) \cdot 2^{r_1 - r_2 - 1} \\ &= \cdots \\ &= \sum_{j=2}^{t-1} m_j \cdot 2^{r_1 - r_j - j + 2} + u_{t-1} \cdot 2^{r_1 - r_{t-1} - t + 2} \\ &= \sum_{j=2}^{t-1} m_j \cdot 2^{r_1 - r_j - j + 2} + 2^{r_1 - t + 1}. \end{aligned}$$

Compared with $\sum_{j=1}^{t-1} m_j \cdot 2^{n - r_j - j + 1} = 2^{n-1} - 2^{n-t}$, we get

$$m_1 = 2^{r_1 - 1} - u_1/2.$$

It is evident that the value of u_1 can take the maximum only when all m_j take the maximum value $2^{r_j} - u_j$. Let $m_j = 2^{r_j} - u_j$ for $1 \leq j \leq t-1$, then

$$\begin{aligned} u_j &= (2m_{j+1} + u_{j+1}) \cdot 2^{r_j - r_{j+1} - 1} \\ &= (2(2^{r_{j+1}} - u_{j+1}) + u_{j+1}) \cdot 2^{r_j - r_{j+1} - 1} \\ &= 2^{r_j} - u_{j+1} \cdot 2^{r_j - r_{j+1} - 1}, \end{aligned}$$

thus

$$u_j \cdot 2^{-r_j} = 1 - \frac{1}{2} u_{j+1} \cdot 2^{-r_{j+1}}.$$

Then by recursive substitutions, we obtain

$$u_1 \cdot 2^{-r_1} = 1 - \frac{1}{2} u_2 \cdot 2^{-r_2} = \cdots = \sum_{j=0}^{t-3} (-\frac{1}{2})^j + (-\frac{1}{2})^{t-2} u_{t-1} \cdot 2^{-r_{t-1}} = \frac{2}{3}(1 - (-2)^{-t})$$

which provides the maximum value of u_1:

$$\max\{u_1\} = \frac{1}{3}(1 - (-2)^{-t}) \cdot 2^{r_1 + 1}.$$

Obviously, $u_1 \geq 2^{r_1 - t + 1}$, and consequently we have

$$\frac{1}{2^{t-1}} \leq \frac{u_1}{2^{r_1}} \leq \frac{2}{3}(1 - (-2)^{-t}). \tag{14}$$

Again, utilizing Stirling's formula, we obtain

$$\begin{aligned} \log \binom{2^{r_1} - u_1}{m_1} &= 2^{r_1} - u_1 - 0.5 \log(2^{r_1} - u_1) - 0.3257 + \varepsilon \\ &= 2^{r_1} - 0.5 r_1 - u_1 + \frac{0.7213 u_1}{2^{r_1}} (1 + \sum_{i=2}^{\infty} \frac{1}{i} (\frac{u_1}{2^{r_1}})^{i-1}) - 0.3257 + \varepsilon \end{aligned}$$

where $\varepsilon = \frac{\theta}{3(2^{r_1} - u_1)}$ and $-0.7214 < \theta < 0.1084$.

We only consider the cases in which $t > 3$ and r_1 is large, say $r_1 > 12$. In these cases, $0 \le \frac{u_1}{2^{r_1}} \le \frac{11}{16}$ and $\varepsilon < 0.0001$. Thus

$$\begin{aligned} \log \binom{2^{r_1} - u_1}{m_1} &\ge 2^{r_1} - 0.5r_1 + (\frac{0.7213}{2^{r_1}} - 1)u_1 - 0.3257, \\ \log \binom{2^{r_1} - u_1}{m_1} &\le 2^{r_1} - 0.5r_1 + (\frac{1.2203}{2^{r_1}} - 1)u_1 - 0.3257. \end{aligned} \tag{15}$$

From here, we are ready to evaluate the upper bound of $\mathcal{N}^w(L)$. The derivations are as follows:

$$\begin{aligned} \mathcal{N}^w(L) &= \sum_{\sum_{j=1}^{t-1} m_j \cdot 2^{n-r_j-j+1} = 2^{n-1} - 2^{n-t}} 2^{2^{r_t}} \prod_{j=1}^{t-1} 2^{u_j} \cdot \binom{2^{r_j} - u_j}{m_j} \\ &= 2^{\sum_{j=1}^{t} 2^{r_j - t + j}} \sum_{m_{t-1}=0}^{2^{r_{t-1}} - u_{t-1}} \cdots \sum_{m_2=0}^{2^{r_2} - u_2} \binom{2^{r_1} - u_1}{m_1} \\ &\quad \cdot \prod_{j=2}^{t-1} (2^{\sum_{k=1}^{j-1} 2^{r_j - k - r_j - k + 1}})^{m_j} \binom{2^{r_j} - u_j}{m_j} \\ &\le 2^{\sum_{j=2}^{t} 2^{r_j - t + j} + 2^{r_1} - 0.5r_1 - 0.3257 + \frac{1.2203}{2^{t-1}}} \sum_{m_{t-1}=0}^{2^{r_{t-1}} - u_{t-1}} \\ &\quad \cdots \sum_{m_2=0}^{2^{r_2} - u_2} a_1^{-(\sum_{i=2}^{t-1} m_i 2^{r_1 - r_i - i + 2})} \cdot \prod_{j=2}^{t-1} (2^{\sum_{k=1}^{j-1} 2^{r_j - k - r_j - k + 1}})^{m_j} \binom{2^{r_j} - u_j}{m_j} \\ &= 2^{\sum_{j=2}^{t} 2^{r_j - t + j} + 2^{r_1} - 0.5r_1 - 0.3257 + \frac{1.2203}{2^{t-1}}} \sum_{m_{t-1}=0}^{2^{r_{t-1}} - u_{t-1}} \\ &\quad \cdots \sum_{m_3=0}^{2^{r_3} - u_3} a_1^{-(\sum_{i=3}^{t-1} m_i 2^{r_1 - r_i - i + 2})} a_2^{2^{r_2} - u_2} \cdot \prod_{j=3}^{t-1} (2^{\sum_{k=1}^{j-1} 2^{r_j - k - r_j - k + 1}})^{m_j} \\ &\quad \binom{2^{r_j} - u_j}{m_j} \\ &= 2^{\sum_{j=2}^{t} 2^{r_j - t + j} + 2^{r_1} - 0.5r_1 - 0.3257 + \frac{1.2203}{2^{t-1}}} a_2^{2^{r_2} - 2^{r_2 - t + 2}} \sum_{m_{t-1}=0}^{2^{r_{t-1}} - u_{t-1}} \cdots \sum_{m_3=0}^{2^{r_3} - u_3} \\ &\quad a_1^{-(\sum_{i=3}^{t-1} m_i 2^{r_1 - r_i - i + 2})} a_2^{-(\sum_{i=3}^{t-1} m_i 2^{r_2 - r_i - i + 3})} \cdot \prod_{j=3}^{t-1} (2^{\sum_{k=1}^{j-1} 2^{r_j - k - r_j - k + 1}})^{m_j} \\ &\quad \binom{2^{r_j} - u_j}{m_j} \\ &= \cdots\cdots \\ &= 2^{2^{r_t} + 2^{r_1} - 0.5r_1 - 0.3257 + \frac{1.2203}{2^{t-1}}} \prod_{j=2}^{t-1} a_j^{2^{r_j}} (\frac{2}{a_j})^{2^{r_j - t + j}}. \end{aligned}$$

Estimate of the lower bound can be obtained via a similar derivation, and we finally achieve that

$$\mathcal{N}^w(L) \geq 2^{2^{r_t}+2^{r_1}-0.5r_1-0.3257+\frac{0.7213}{2^{t-1}}} \prod_{j=2}^{t-1} b_j^{2^{r_j}} (\frac{2}{b_j})^{2^{r_j-t+j}}$$

where $a_1 = 2^{1-\frac{1.2203}{2^{r_1}}}$, $b_1 = 2^{1-\frac{0.7213}{2^{r_1}}}$ and $a_j = 1 + \prod_{i=1}^{j-1} (\frac{2}{a_i})^{2^{r_i-r_j+i-j+1}}$, $b_j = 1 + \prod_{i=1}^{j-1} (\frac{2}{b_i})^{2^{r_i-r_j+i-j+1}}$ for $1 < j < t$. □

Denote the upper and lower bounds of $\mathcal{N}^w(L)$ by $\text{Upper}(\mathcal{N}^w(L))$ and $\text{Lower}(\mathcal{N}^w(L))$ respectively. Then we find

$$\frac{\text{Upper}(\mathcal{N}^w(L))}{\text{Lower}(\mathcal{N}^w(L))} \leq \frac{\binom{2^{r_1}-u_1}{m_1}_{max}}{\binom{2^{r_1}-u_1}{m_1}_{min}} = 2^{(1.2203-0.7213)u_1/2^{r_1}} \leq 2^{0.4990\cdot\frac{11}{16}} = 1.2684.$$

This implies that the upper and lower bounds of $\mathcal{N}^w(L)$ are larger and smaller than $\mathcal{N}^w(L)$ at most 26.84% and $1 - 1/1.2684 = 21.16\%$ respectively.

We next turn our attention to the cases in which w takes other values.

According to Corollary 2, it is effortless to see that the Hamming weight of sequence of linear complexity $L = 2^{r_1} + 2^{r_2} + \cdots 2^{r_t} + 1$ must be $w = 2^{n-1} + l \cdot 2^{n-r_1}$. This leads to $m_1 = \frac{w}{2^{n-r_1}} - \frac{u_1}{2} = \frac{1}{2}(2^{r_1} - u_1) + l$. For small l we can easily transform the binomial coefficient $\binom{2^{r_1}-u_1}{m_1}$ to $\binom{2^{r_1}-u_1}{\frac{1}{2}(2^{r_1}-u_1)}$. For instance, when $l = \pm 1$, we get $m_1 = \frac{1}{2}(2^{r_1} - u_1) \pm 1$ and $\binom{2^{r_1}-u_1}{m_1} = \frac{2^{r_1}-u_1}{2^{r_1}-u_1+2}\binom{2^{r_1}-u_1}{\frac{1}{2}(2^{r_1}-u_1)}$. Utilizing Eq. (14), we get

$$\binom{2^{r_1}-u_1}{m_1} \geq \frac{(1-(-2)^{1-t})\cdot 2^{r_1}}{(1-(-2)^{1-t})\cdot 2^{r_1}+6}\binom{2^{r_1}-u_1}{\frac{1}{2}(2^{r_1}-u_1)},$$
$$\binom{2^{r_1}-u_1}{m_1} \leq \frac{(1-2^{1-t})\cdot 2^{r_1}}{(1-2^{1-t})\cdot 2^{r_1}+2}\binom{2^{r_1}-u_1}{\frac{1}{2}(2^{r_1}-u_1)}.$$

Adopting a calculation analogous the one used for deriving Theorem 2, we can get the bounds of $\mathcal{N}^w(L)$ for the cases in which $w = 2^{n-1} \pm 2^{n-t}$ as follows.

Corollary 3. *Let $\mathcal{N}^w(L)$ be the number of 2^n-periodic binary sequences with Hamming weight w and linear complexity L. Then when $L = 2^{r_1}+2^{r_2}+\cdots+2^{r_t}+1$ with $0 \leq r_t < r_{t-1} < \cdots < r_1 < n$, $3 < t < n$ and $w = 2^{n-1} \pm 2^{n-r_1}$, we have*

$$\mathcal{N}^w(L) \leq \frac{(1-2^{1-t})\cdot 2^{r_1}}{(1-2^{1-t})\cdot 2^{r_1}+2} \cdot 2^{2^{r_t}+2^{r_1}-0.5r_1-0.3257+\frac{1.2203}{2^{t-1}}} \prod_{j=2}^{t-1} a_j^{2^{r_j}} (\frac{2}{a_j})^{2^{r_j-t+j}},$$
$$\mathcal{N}^w(L) \geq \frac{(1-(-2)^{1-t})\cdot 2^{r_1}}{(1-(-2)^{1-t})\cdot 2^{r_1}+6} \cdot 2^{2^{r_t}+2^{r_1}-0.5r_1-0.3257+\frac{0.7213}{2^{t-1}}} \prod_{j=2}^{t-1} b_j^{2^{r_j}} (\frac{2}{b_j})^{2^{r_j-t+j}}, \tag{16}$$

where $a_1 = 2^{1-\frac{1.2203}{2^{r_1}}}$, $b_1 = 2^{1-\frac{0.7213}{2^{r_1}}}$ and $a_j = 1 + \prod_{i=1}^{j-1} (\frac{2}{a_i})^{2^{r_i-r_j+i-j+1}}$, $b_j = 1 + \prod_{i=1}^{j-1} (\frac{2}{b_i})^{2^{r_i-r_j+i-j+1}}$ for $1 < j < t$.

From here, the counting problem for the number of 2^n-periodic binary sequences of given linear complexity and with fixed Hamming weight is solved.

3 The Characterization of $\mathcal{A}_2^w(L)$

In this section, we turn our attention to the counting problem for the number of 2^n-periodic binary sequences of 2-error linear complexity and with fixed Hamming weight.

Let $\mathcal{A}_2'(L)$ denote the set of 2^n-periodic binary sequences of 2-error linear complexity L and linear complexity smaller than 2^n, and let $\mathcal{N}_2'(L)$ denote the size of set $\mathcal{A}_2'(L)$, which can be formally defined as

$$\mathcal{A}_2'(L) = \{S \in S^{2^n} : LC_2(S) = L \text{ and } LC(S) < 2^n\} \quad \text{and} \quad \mathcal{N}_2'(L) = |\mathcal{A}_2'(L)|. \tag{17}$$

Let us first briefly introduce how to get $\mathcal{N}_2'(L)$. It is clear that, if there is a sequence S with 2-error linear complexity L then there must be another sequence S' of linear complexity L which satisfy that the Hamming distance between S and S' being no more than 2. According to Lemma 1, which states that the linear complexity of sequences with odd Hamming weight are 2^n, we get

$$\mathcal{A}_2'(L) \subseteq \mathcal{A}(L) \bigcup \mathcal{A}(L) + \mathbf{E}_2 \tag{18}$$

where $\mathbf{E}_2 = \{E \in S^{2^n} : \ w_H(E) = 2\}$.

From Lemma 4, it is apparent that for any sequence S in $\mathcal{A}(L)$, the corresponding polynomial of S satisfies that $S(x) = (x-1)^{2^n-L}a(x)$ and $a(1) \neq 0$. Combined with Eq. (1): $LC(S) = N - \deg(\gcd(x^N - 1, S(x)))$, we can easily verify the following two lemmas.

Lemma 7 [4]**.** *Let $\mathcal{A}(L)$ be the set of 2^n-periodic binary sequences of linear complexity L and E, E' be two error sequences, then we have*

$$\mathcal{A}(L) + E = \mathcal{A}(L) + E' \text{ or } (\mathcal{A}(L) + E) \bigcap (\mathcal{A}(L) + E') = \emptyset. \tag{19}$$

Lemma 8. *Let E, E' be two error sequences in $\mathbf{E}$, then $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$ if and only if there exist two sequences S, S' in $\mathcal{A}(L)$ such that $S + E = S' + E'$.*

Next, we devote to characterize the set $\mathcal{A}_2'(L)$ and evaluate its size $\mathcal{N}_2'(L)$ based on the properties provided in the above two lemmas. This problem has already received a treatment in [5,12], here we provide a more concise formula and proof.

Lemma 9. *Let $\mathcal{A}_2'(L)$ and $\mathcal{N}_2'(L)$ denote the set of and the number of 2^n-periodic binary sequences with 2-error linear complexity L and linear complexity less than 2^n respectively, then we have*

- *if* $L = 2^n - 2^r$, $0 \le r < n$, *then* $\mathcal{A}'_2(L) = \emptyset$ and $\mathcal{N}'_2(L) = 0$.
- *if* $L = 2^n - (2^{r_1} + 2^{r_2})$, $0 \le r_2 < r_1 < n$, *then*

$$\begin{aligned} \mathcal{A}'_2(L) &= \mathcal{A}(L) \bigcup (\mathcal{A}(L) + \mathbf{E}) \quad \text{and} \\ \mathcal{N}'_2(L) &= (1 + 2^{r_1}(2^{r_1+1} - 3 \cdot 2^{r_1-r_2-1} - 1)) \cdot 2^{L-1} \end{aligned} \tag{20}$$

where $\mathbf{E} = \{\{i, j\} : 0 \le i < j < 2^{r_1+1}, 2^{r_2} < d(i, j) < 2^{r_1}$ and $i + j < 2^{r_1+1}$ or $0 < d(i, j) < 2^{r_2}\}$.

- *if* $L = 2^n - (2^{r_1} + 2^{r_2} + x)$, $0 < r_2 < r_1 < n$ *and* $0 < x < 2^{r_2}$ *then*

$$\begin{aligned} \mathcal{A}'_2(L) &= \mathcal{A}(L) \bigcup (\mathcal{A}(L) + \mathbf{E}) \quad \text{and} \\ \mathcal{N}'_2(L) &= (1 + 2^{r_1}(2^{r_1+1} - 2^{r_1-r_2-1} + 2^{r_2-r_1+1} - 1)) \cdot 2^{L-1} \end{aligned} \tag{21}$$

where $\mathbf{E} = \{\{i, j\} : 0 \le i < j < 2^{r_1+1}$, $d(i, j) = 2^{r_1}$ and $0 \le i < 2^{r_2+1}$ or $2^{r_2} < d(i, j) < 2^{r_1}$ and $i + j < 2^{r_1+1}$ or $0 < d(i, j) \le 2^{r_2}\}$.

Proof. According to Lemma 7, to get the size of $\mathcal{A}'_2(L)$, it is sufficient to get the maximum subset of error sequences set $\mathbf{E}_0 \bigcup \mathbf{E}_2$ in which for any pair of error sequences E, E' it satisfies that $\mathcal{A}(L) + E \subseteq \mathcal{A}'_2(L)$ and $(\mathcal{A}(L) + E) \bigcap (\mathcal{A}(L) + E') = \emptyset$. Next, we proceed the proof case by case.

- Case 1. $L = 2^n - 2^r$, $0 \le r < n$. In this case, it can be observed that $merr(S) = 2$ for any sequence S in $\mathcal{A}(L)$, which follows $\mathcal{A}(L) \bigcap \mathcal{A}'_2(L) = \emptyset$. Suppose the support set of error sequence E in $\mathbf{E}_2$ is $supp(E) = \{i, j\}$. For each E in $\mathbf{E}_2$, we can construct an error sequence E' of which the support set is $supp(E') = \{i, j'\}$ and $d(j, j') = 2^r$. Then we have $LC(E + E') = 2^n - 2^r = L$, that is to say $LC_2(S + E) \le LC(S + E + E') < L$. Therefore we have $(\mathcal{A}(L) + \mathbf{E}_2) \bigcap \mathcal{A}'_2(L) = \emptyset$. As a result, we have $\mathcal{A}'_2(L) = \emptyset$ and $\mathcal{N}'_2(L) = 0$.
- Case 2. $L = 2^n - (2^{r_1} + 2^{r_2})$, $0 \le r_2 < r_1 < n$. In this case, one can observe that $merr(S) = 4$, which follows $\mathcal{A}(L) \subseteq \mathcal{A}'_2(L)$. For any error sequence E in $\mathbf{E}_2$, suppose the support set of E is $supp(E) = \{i, j\}$. If $d(i, j) > 2^{r_1}$, for any sequence S in $\mathcal{A}(L)$ we have $LC(S + E) = L$ that is to say $S + E \in \mathcal{A}(L)$. According to Lemma 8, we have $\mathcal{A}(L) + E = \mathcal{A}(L)$. If $d(i, j) = 2^{r_1}$ then we can construct an error sequence E' of which the support set is $supp(E') = \{i', j'\}$ such that $d(i, i') = d(j, j') = 2^{r_2}$. Then $LC(E + E') = L$ and $LC_2(S + E) \le LC(S + E + E') < L$, thus we have $(\mathcal{A}(L) + E) \bigcap \mathcal{A}'_2(L) = \emptyset$. Similarly, when $d(i, j) = 2^{r_2}$, we also have $(\mathcal{A}(L) + E) \bigcap \mathcal{A}'_2(L) = \emptyset$. Suppose $2^{r_2} < d(i, j) < 2^{r_1}$ or $0 < d(i, j) < 2^{r_2}$. We construct an error sequence E' of which the support set is $supp(E') = \{i', j'\}$ where $i' = i \mod 2^{r_1+1}$ and $j' = j \mod 2^{r_1+1}$. Then we have $(E + E')(x) = x^i + x^j + x^{i'} + x^{j'} = (x + 1)^{2^{r_1+1}} b(x)$ or 0 and $(S + E + E')(x) = (x + 1)^{2^{r_1+1}+2^{r_2}} a(x) + (x + 1)^{2^{r_1+1}} b(x) = (x + 1)^{2^n - L}((x + 1)^t b'(x) + a(x))$ or equal to $S(x)$ itself where $b(x) \ne 0$ and $t > 0$. Thus $S' = S + E + E' \in \mathcal{A}(L)$ and $S + E = S + E'$. According to Lemma 8, we have $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$. Therefore we only need to consider those error sequences in $\mathbf{E}_2$ with support set $\{i, j\}$ where $0 < i < j < 2^{r_1+1}$ and $2^{r_2} < d(i, j) < 2^{r_1}$ or $0 < d(i, j) < 2^{r_2}$. If $2^{r_2} < d(i, j) < 2^{r_1}$, we construct error

sequence E' with support set $supp(E') = \{i', j'\}$ where $|i' - i| = |j' - j| = 2^{r_1}$. Similarly we have $S' = S + E + E' \in \mathcal{A}(L)$ and thus $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$. Consequently, there are half of those error sequences in the set $\{\{i, j\} : 0 \leq i < j < 2^{r_1+1}, 2^{r_2} < d(i, j) < 2^{r_1}\}$ satisfying the requirements and we can choose this half part of the set which denoted by $Sub\mathbf{E}_1 = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}, 2^{r_2} < d(i, j) < 2^{r_1}$ *and* $i+j < 2^{r_1+1}\}$. Denote $Sub\mathbf{E}_2 = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}, 0 < d(i, j) < 2^{r_2}$. It is easy to verify that for any error sequences E and E' in $Sub\mathbf{E}_1 \bigcup Sub\mathbf{E}_2$ they satisfy that $(\mathcal{A}(L) + E') \bigcap (\mathcal{A}(L) + E') = \emptyset$ and $\mathcal{A}(L) + E \subseteq \mathcal{A}'_2(L)$. By combinatorial theory, we can state that the size of $Sub\mathbf{E}_1$ and $Sub\mathbf{E}_2$ are $\binom{2^{r_2+1}}{1}\binom{2^{r_1-r_2-1}}{2} \cdot 2^2/2 = 2^{r_1}(2^{r_1-r_2-1} - 1)$ and $\binom{2^{r_2}}{2}\binom{2^{r_1-r_2+1}}{1}^2 = 2^{2r_1-r_2+1}(2^{r_2} - 1)$ respectively. As a consequence, we obtain that

$$\mathcal{A}'_2(L) = \mathcal{A}(L) \bigcup (\mathcal{A}(L) + \mathbf{E}) \text{ and } \mathcal{N}'_2(L) = (1 + 2^{r_1}(2^{r_1+1} - 3 \cdot 2^{r_1-r_2-1} - 1)) \cdot 2^{L-1}$$

where $\mathbf{E} = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}, 2^{r_2} < d(i, j) < 2^{r_1}$ and $i + j < 2^{r_1+1}$ or $0 < d(i, j) < 2^{r_2}\}$.

– Case 3. $L = 2^n - (2^{r_1} + 2^{r_2} + x)$ where $0 < r_2 < r_1 < n$ and $0 < x < 2^{r_2}$. Similar to the analysis for Case 2, we can get $\mathcal{A}(L) \subseteq \mathcal{A}'_2(L)$ and only need to consider those error sequences in $\mathbf{E}_2$ with support set $\{i, j\}$ which satisfy that $0 \leq i < j < 2^{r_1+1}$. If $d(i, j) = 2^{r_1}$, we construct an error sequence E' with support set $supp(E') = \{i', j'\}$ where $i' = i \mod 2^{r_2+1}$ and $j' = j \mod 2^{r_2+1}$. It can be verified that $S' = S + E + E' \in \mathcal{A}(L)$ and then $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$. Thus, for the error sequences set $\mathbf{E} = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}$ and $d(i, j) = 2^{r_1}\}$ we only need to consider its subset $Sub\mathbf{E}_3 = \{\{i, j\} : 0 \leq i < 2^{r_2+1}$ and $j = i + 2^{r_1}\}$. Denote $Sub\mathbf{E}_4 = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}$ and $d(i, j) = 2^{r_2}\}$. Similar to the analysis for Case 2, it can be verify that for any error sequences E and E' in $Sub\mathbf{E}_1 \bigcup Sub\mathbf{E}_2 \bigcup Sub\mathbf{E}_3 \bigcup Sub\mathbf{E}_4$ they satisfy that $(\mathcal{A}(L) + E') \bigcap (\mathcal{A}(L) + E') = \emptyset$ and $\mathcal{A}(L) + E \subseteq \mathcal{A}'_2(L)$, where $Sub\mathbf{E}_1$ and $Sub\mathbf{E}_2$ are mentioned in the analysis for Case 2. By combinatorial theory, we can state that the size of $\mathbf{E}_3$ and $\mathbf{E}_4$ are 2^{r_2+1} and $\binom{2^{r_2}}{1}\binom{2^{r_1-r_2}}{1}^2 = 2^{2r_1-r_2}$ respectively. As a consequence, we obtain that

$$\mathcal{A}'_2(L) = \mathcal{A}(L) \bigcup (\mathcal{A}(L) + \mathbf{E}) \text{ and}$$
$$\mathcal{N}'_2(L) = (1 + 2^{r_1}(2^{r_1+1} - 2^{r_1-r_2-1} + 2^{r_2-r_1+1} - 1)) \cdot 2^{L-1}$$

where $\mathbf{E} = \{\{i, j\} : 0 \leq i < j < 2^{r_1+1}, d(i, j) = 2^{r_1}$ and $0 \leq i < 2^{r_2+1}$ or $2^{r_2} < d(i, j) < 2^{r_1}$ and $i + j < 2^{r_1+1}$ or $0 < d(i, j) \leq 2^{r_2}\}$. □

From Corollary 2, we can know that the Hamming weight w of sequence S in $\mathcal{A}(L)$ satisfy that $2^{n-r_1}|w$ where $L = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t} + 1$, $t < n$ and $0 \leq r_t < r_{t-1} < \cdots < r_1 < n$ (Notice that, in Lemmas 9 and 10, we used a different expression form of L, which is actually determined by the binary representation of $n - L$). Thus, when $r_1 \neq n - 1$, the Hamming weight of S in $\mathcal{A}(L)$ can be 2^{n-1} but must not be $2^{n-1} \pm 2$. Now, let us first consider a simple

case: $r_1 \neq n-1$ and $w = 2^{n-1}$ and try to get the value of $\mathcal{A}_2^w(L)$ based on the properties of $\mathcal{A}_2'(L)$.

Lemma 10. *Let $\mathcal{N}_2^w(L)$ be the number of 2^n-periodic binary sequences with 2-error linear complexity L and Hamming weight w, then we have*

- *if $L = 2^n - 2^t$, $0 \leq t < n$, then $\mathcal{N}_2^w(L) = 0$.*
- *if $L = 2^{n-1} - 2^t, 0 \leq t < n-1$ and $w = 2^{n-1}$, then*

$$(2^{2n-2} - 3 \cdot 2^{2n-t-3} + 1)\mathcal{N}^w(L) \leq \mathcal{N}_2^w(L) \leq (2^{2n-2} + 1)\mathcal{N}^w(L).$$

- *if $L = 2^{n-1} - 2^t - x, 0 \leq t < n-1, 0 < x < 2^t$ and $w = 2^{n-1}$, then*

$$(2^{2n-2} - 2^{2n-t-3} + 2^{t+1} + 1)\mathcal{N}^w(L) \leq \mathcal{N}_2^w(L) \leq (2^{2n-2} + 1)\mathcal{N}^w(L).$$

Proof. It is obvious that $\mathcal{A}_2^w(L) = \emptyset$, and $\mathcal{N}_2^w(L) = 0$ when $L = 2^n - 2^t$ and $0 \leq t < n$. According to Corollary 2, the Hamming weight of sequences in $\mathcal{A}(L)$ can not be $2^{n-1} \pm 2$, then $\mathcal{A}_2^w(L) \subseteq \mathcal{A}^w(L) \bigcup (\mathcal{A}^w(L) + \mathbf{E})$ based on Eq. (20) where $\mathbf{E}$ is defined in Eq. (20). Then the main problem of getting $\mathcal{A}^w(L)$ is how to eliminate those sequences with Hamming weight $w \pm 2$ or preserving the Hamming weight when adding an sequence E to S where $E \in \mathbf{E}$ and $S \in \mathcal{A}$. For any sequence S in $\mathcal{A}^w(L)$, there are at most $\binom{w}{1}\binom{2^n-w}{1} = 2^{2n-2}$ possibilities when we adding a sequence E in $\mathbf{E}$ to it and preserving the Hamming weight of S. And it is clear that there are at most $\binom{w}{2} = \binom{2^{n-1}}{2}$ and $\binom{2^n-w}{2} = \binom{2^{n-1}}{2}$ possibilities when we adding a sequence E in $\mathbf{E}$ to S and changing the Hamming weight of S to $w-2$ and $w+2$ respectively. Therefore there are at most $2^{2n-2}\mathcal{N}^w(L)$ and at least $(|\mathbf{E}| - 2\binom{2^{n-1}}{2})\mathcal{N}^w(L)$ sequences with Hamming weight w in the set $\mathcal{A}^w(L) + \mathbf{E}$. Thus we get

$$(2^{2n-2} - 3 \cdot 2^{2n-t-3} + 1)\mathcal{N}^w(L) \leq \mathcal{N}_2^w(L) \leq (2^{2n-2} + 1)\mathcal{N}^w(L).$$

if $L = 2^{n-1} - 2^t - x, 0 \leq t < n-1, 0 < x < 2^t$ follows an analysis analogous the one used for the previous case and we thus omit it here. □

Let $L = 2^n - (2^{r_1} + 2^{r_2} + \cdots 2^{r_t})$ and $w = 2^{n-1}$ where $0 \leq r_t < r_{t-1} < \cdots < r_1 < n$, when $r_1 < n-1$, according to $\mathcal{A}_2(L) \subseteq \mathcal{A}(L) \bigcup (\mathcal{A}(L) + \mathbf{E}_2)$ we have

$$\mathcal{A}_2^w(L) \subseteq \mathcal{A}^w(L) \bigcup (\mathcal{A}^w(L) + \mathbf{E}_2) \bigcup (\mathcal{A}^{w-2}(L) + \mathbf{E}_2) \bigcup (\mathcal{A}^{w+2}(L) + \mathbf{E}_2). \quad (22)$$

A similar analysis to the one in Lemma 10 provides the following theorem.

Theorem 3. *Let $\mathcal{N}_2^w(L)$ denote the number of 2^n-periodic binary sequences with 2-error linear complexity L and Hamming weight w, then we have*

- *if $L = 2^n - 2^r$, $0 \leq r < n$, then $\mathcal{N}_2^w(L) = 0$.*
- *if $L = 2^n - (2^{r_1} + 2^{r_2})$, $0 \leq r_2 < r_1 < n$ and $w = 2^{n-1}$, then*

$$\begin{aligned}\mathcal{N}_2^w(L) \geq & (2^{2r_1} - 3 \cdot 2^{2r_1 - r_2 - 1} + 1)\mathcal{N}^w(L) + \\ & (2^{2r_1} - 3 \cdot 2^{2r_1 - r_2 - 1} - 4)(\mathcal{N}^{w+2}(L) + \mathcal{N}^{w-2}(L)), \\ \mathcal{N}_2^w(L) \leq & (2^{2r_1} + 1)\mathcal{N}^w(L) + (2^{2r_1} - 4)(\mathcal{N}^{w+2}(L) + \mathcal{N}^{w-2}(L)).\end{aligned}$$

– *if* $L = 2^n - (2^{r_1} + 2^{r_2} + x)$, $0 < r_2 < r_1 < n$, $0 < x < 2^{r_2}$ *and* $w = 2^{n-1}$, *then*

$$\begin{aligned}\mathcal{N}_2^w(L) \geq & (2^{2r_1} - 2^{2r_1-r_2-1} + 2^{r_2+1} + 1)\mathcal{N}^w(L) + \\ & (2^{2r_1} - 2^{2r_1-r_2-1} + 2^{r_2+1} - 4)(\mathcal{N}^{w+2}(L) + \mathcal{N}^{w-2}(L)) \\ \mathcal{N}_2^w(L) \leq & (2^{r_1} + 1)\mathcal{N}^w(L) + (2^{2r_1} - 4)(\mathcal{N}^{w+2}(L) + \mathcal{N}^{w-2}(L)).\end{aligned}$$

Based on the above theorem and combining the bounds of $\mathcal{N}^w(L)$, $\mathcal{N}^{w\pm2}(L)$ provided in inequalities (13) and (16), we can get the bounds of $\mathcal{N}_2^w(L)$.

4 Conclusions

In this paper, we devote to get the distribution of linear complexity and k-error linear complexity of 2^n-periodic binary sequences with fixed Hamming weight. First, we use short sequence to construct special longer sequence in a manner similar to the reversed process of the Games-Chan algorithm. And we get the explicit formula of the number of sequences with given linear complexity L and Hamming weight w. Besides, we provide an asymptotic evaluation of this counting function when n gets large. Particularly, we analyze the bounds of counting function of the number of balance sequences with given linear complexity. And extend those bounds to the case of some special Hamming weight. Secondly, we characterize the 2-error linear complexity of 2^n-periodic binary sequences using a simple method. And then based on those characters we get the bounds of the number of 2^n-periodic balance binary sequence with fixed 2-error linear complexity. By further analyzing the bounds of the number of sequences with given Hamming weight, using our method can get the bounds of the counting functions of the k-error linear complexity of 2^n-periodic binary sequences with special Hamming weight and for some large k. Along this line of study, one can get evaluations on the number of sequences of other period or/and of other values of complexity measures and with fixed Hamming weight.

Acknowledgments. Many thanks go to the anonymous reviewers for their detailed comments and suggestions. This work was supported by the National Key R&D Program of China with No. 2016YFB0800100, CAS Strategic Priority Research Program with No. XDA06010701, National Key Basic Research Project of China with No. 2011CB302400 and National Natural Science Foundation of China with No. 61671448, No. 61379139.

References

1. Ding, C., Xiao, G., Shan, W.: The Stability Theory of Stream Ciphers. LNCS, vol. 561. Springer, Heidelberg (1991)
2. Fu, F.-W., Niederreiter, H., Su, M.: The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity. In: Gong, G., Helleseth, T., Song, H.-Y., Yang, K. (eds.) SETA 2006. LNCS, vol. 4086, pp. 88–103. Springer, Heidelberg (2006). doi:10.1007/11863854_8

3. Games, R., Chan, A.: A fast algorithm for determining the complexity of a binary sequence with period 2^n (corresp.). IEEE Trans. Inf. Theory **29**(1), 144–146 (1983)
4. Kavuluru, R.: 2^n-periodic binary sequences with fixed k-error linear complexity for $k = 2$ or 3. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 252–265. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85912-3_23
5. Kavuluru, R.: Characterization of 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity. Des. Codes Cryptogr. **53**(2), 75–97 (2009)
6. Kurosawa, K., Sato, F., Sakata, T., Kishimoto, W.: A relationship between linear complexity and k-error linear complexity. IEEE Trans. Inf. Theory **46**(2), 694–698 (2000)
7. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inf. Theory **15**(1), 122–127 (1969)
8. Meidl, W.: On the stability of 2^n-periodic binary sequences. IEEE Trans. Inf. Theory **51**(3), 1151–1155 (2005)
9. Ming, S.: Decomposing approach for error vectors of k-error linear complexity of certain periodic sequences. IEICE Trans. Fundam. Electr. Commun. Comput. Sci. **E97-A**(7), 1542–1555 (2014)
10. Rueppel, A.R.: Analysis and Design of Stream Ciphers. Communications and Control Engineering Series. Springer, Heidelberg (1986)
11. Stamp, M., Martin, C.F.: An algorithm for the k-error linear complexity of binary sequences with period 2^n. IEEE Trans. Inf. Theory **39**(4), 1398–1401 (1993)
12. Zhou, J.: A counterexample concerning the 3-error linear complexity of 2^n-periodic binary sequences. Des. Codes Cryptogr. **64**(3), 285–286 (2012)
13. Zhou, J., Liu, W.: The k-error linear complexity distribution for 2^n-periodic binary sequences. Des. Codes Cryptogr. **73**(1), 55–75 (2014)