Characterization of 2^n-Periodic Binary Sequences with Fixed 2-error or 3-error Linear Complexity*

Ramakanth Kavuluru

Department of Computer Science, University of Kentucky,
Lexington, KY 40506, USA.

Abstract

The linear complexity of sequences is an important measure of the cryptographic strength of key streams used in stream ciphers. The instability of linear complexity caused by changing a few symbols of sequences can be measured using k-error linear complexity. In their SETA 2006 paper, Fu, Niederreiter, and Su [3] studied linear complexity and 1-error linear complexity of 2^n-periodic binary sequences to characterize such sequences with fixed 1-error linear complexity. In this paper we study the linear complexity and the k-error linear complexity of 2^n-periodic binary sequences in a more general setting using a combination of algebraic, combinatorial, and algorithmic methods. This approach allows us to characterize 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity. Using this characterization we obtain the counting function for the number of 2^n-periodic binary sequences with fixed k-error linear complexity for $k = 2$ and 3. Using the characterization we also show that there many 2^n-periodic binary sequences with high linear complexity and high 2-error or 3-error linear complexity.

1 Introduction

The linear complexity of a sequence is the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. The LFSR that generates a given sequence can be determined using the Berlekamp-Massey [6] algorithm using only the first $2L$ elements of the sequence, where L is the linear complexity of the sequence. Hence for cryptographic purposes sequences with high linear complexity are essential as an adversary would then need large initial segments of the sequences to recover the LFSRs that generate them using the Berlekamp-Massey algorithm.

*A portion of this paper has appeared in the proceedings of the 5th international conference on Sequences and their Applications (SETA 2008).This material is based upon work supported by the National Science Foundation under Grant No. CCF-0514660. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

A system is insecure if all but a few symbols of the key stream can be extracted. Hence for a cryptographically strong sequence, the linear complexity should not decrease drastically if a few symbols are changed. If it did, an attacker could modify the known prefix of the key stream and try to decrypt the result using the Berlekamp-Massey algorithm. If the resulting sequence differed from the actual key stream by only a few symbols, the attacker could extract most of the message. This observation gives rise to k-error linear complexity of sequences introduced in [13] based on the earlier concepts of sphere complexity and weight complexity, see [2]. The k-error linear complexity of a periodic sequence is the smallest linear complexity achieved by making k or fewer changes per period. Besides having large linear complexity, cryptographically strong sequences should, thus, also have large k-error linear complexity at least for small k.

Let $\mathbf{S} = (s_0, \cdots, s_{T-1})^\infty$ be a periodic binary sequence with period T. We associate the polynomial $\mathbf{S}(x) = s_0 + s_1 x + \cdots + s_{T-1}x^{T-1}$ and the corresponding T-tuple $\mathbf{S}^{(T)} = (s_0, \cdots, s_{T-1})$ to $\mathbf{S}$. The relationship between the linear complexity, denoted $L(\mathbf{S})$, of $\mathbf{S}$ and the associated polynomial $\mathbf{S}(x)$ is given by

$$L(\mathbf{S}) = T - \deg(\gcd(x^T - 1, \mathbf{S}(x))), \tag{1}$$

see e.g. [1], Lemma 8.2.1. Let $w_H(\mathbf{S})$ denote the Hamming weight of the T-tuple $\mathbf{S}^{(T)}$. For $0 \le k \le T$, the k-error linear complexity of $\mathbf{S}$, denoted $L_k(\mathbf{S})$, is given by

$$L_k(\mathbf{S}) = \min_{\mathbf{E}} L(\mathbf{S} + \mathbf{E}),$$

where the minimum is taken over all T-periodic binary sequences $\mathbf{E}$ with $w_H(\mathbf{E}) \le k$. Since we consider only 2^n-periodic sequences, we use $T = 2^n$ and the observation

$$x^T - 1 = x^{2^n} - 1 = (x-1)^{2^n} \tag{2}$$

for the rest of the paper.

Let $merr(\mathbf{S})$ denote the minimum value k such that the k-error linear complexity of a 2^n-periodic sequence $\mathbf{S}$ is strictly less than its linear complexity. That is

$$merr(\mathbf{S}) = \min\{k : L_k(\mathbf{S}) < L(\mathbf{S})\}.$$

Kurosawa et al. [5] derived a formula for the exact value of $merr(\mathbf{S})$.

Lemma 1.1. *For any nonzero 2^n-periodic sequence $\mathbf{S}$, we have*

$$merr(\mathbf{S}) = 2^{w_H(2^n - L(\mathbf{S}))},$$

where $w_H(j)$, $0 \le j \le 2^n - 1$, denotes the Hamming weight of the binary representation of j.

The counting function of a sequence measure gives the number of sequences with a given measure value. Rueppel [12] determined the counting function of linear complexity for 2^n-periodic binary sequences. Using equations (1) and (2) it is straightforward to characterize the 2^n-periodic sequences with fixed linear complexity.

Lemma 1.2 ([3]). *Let $\mathcal{N}(L)$ and $\mathcal{A}(L)$ denote, respectively, the number of and the set of 2^n-periodic binary sequences with given linear complexity L, $0 \le L \le 2^n$. Then*

$$\mathcal{N}(0) = 1 \text{ and } \mathcal{N}(L) = 2^{L-1} \text{ for } 1 \le L \le 2^n. \tag{3}$$

Also, $\mathcal{A}(0) = \{(0, 0, \cdots)\}$ and $\mathcal{A}(L)$, where $1 \le L \le 2^n$, is equal to the set of 2^n-periodic binary sequences $\mathbf{S}$ with the corresponding polynomials

$$\mathbf{S}(x) = (1 - x)^{2^n - L} a(x),$$

where $a(x)$ is a binary polynomial with $\deg(a(x)) \le L - 1$ and $a(1) \neq 0$.

Counting functions and expected values for linear complexity and k-error linear complexity were extensively explored by Meidl and Niederreiter [8, 9, 10]. Using efficient algorithms to compute the linear complexity of p^n-periodic sequences over $\mathbb{F}_p$, Meidl [7] obtained the counting function and the expected value for the 1-error linear complexity of 2^n-periodic binary sequences. Meidl and Venkateswarlu [11] extended these results to p^n-periodic sequences over $\mathbb{F}_p$.

Recently, using algebraic and combinatorial methods Fu et al. [3] characterized 2^n-periodic binary sequences with fixed 1-error linear complexity. They derived some properties of the set $\mathcal{A}(L)$ that deal with changing two symbols per period at fixed positions in sequences in $\mathcal{A}(L)$ and used them to obtain the characterization. For $0 \le L \le 2^n$ and $1 \le k \le 2^n$, denote by $\mathcal{A}_k(L)$ the set of 2^n-periodic binary sequences with given k-error linear complexity L and let $\mathcal{N}_k(L) = |\mathcal{A}_k(L)|$, the cardinality of $\mathcal{A}_k(L)$. With this notation the characterization of $\mathcal{A}_1(L)$ by Fu et al. can be summarized as follows.

Theorem 1.3 ([3]). *Let $\mathbf{E}_i$, $0 \le i \le 2^n - 1$, be the 2^n-periodic binary sequence with a 1 at position i and 0 elsewhere in each period and $\mathbf{0}$ be the zero sequence. We have $\mathcal{A}(0) = \{\mathbf{0}, \mathbf{E}_0, \cdots, \mathbf{E}_{2^n-1}\}$ and $\mathcal{N}_1(0) = 2^n + 1$.*

1. *If $2^n - 2^{n-r} < L < 2^n - 2^{n-r-1}$ for some $0 \le r \le n - 2$, then*

$$\mathcal{A}_1(L) = \mathcal{A}(L) \bigcup \left(\bigcup_{i=0}^{2^{n-r}-1} (\mathcal{A}(L) + \mathbf{E}_i) \right)$$

   and $\mathcal{N}_1(L) = (2^{n-r} + 1)2^{L-1}$.

2. *If $L = 2^n - 2^{n-r}$, $r = 1, 2, \cdots, n$, then $\mathcal{A}_1(L) = \mathcal{A}(L)$ and $\mathcal{N}_1(L) = 2^{L-1}$.*

For a 2^n-periodic sequence $\mathbf{S}$ and t integers $i_1, \cdots, i_t$ such that $0 \le i_j \le 2^n - 1$, $j = 1, \cdots, t$, denote by $\mathbf{S}_{i_1,\cdots,i_t}$ the 2^n-periodic binary sequence with the corresponding polynomial

$$\mathbf{S}_{i_1,\cdots,i_t}(x) = \mathbf{S}(x) + x^{i_1} + \cdots + x^{i_t}.$$

The sequence $\mathbf{S}_{i_1,\cdots,i_t}$ is said to be a formed by a t symbol change in $\mathbf{S}$.

In this paper we first study the effect of t symbol changes in 2^n-periodic binary sequences for small t. Specifically, for various special cases of L we determine some t symbol changes of sequences in $\mathcal{A}(L)$ that result in sequences in $\mathcal{A}(L)$ for $t = 2$, 4, and 6. We also characterize

specific 2, 4, and 6 symbol changes of sequences in $\mathcal{A}(L)$ that result in 2^n-periodic binary sequences with linear complexity strictly less than L. We use these characterizations to construct disjoint decompositions of the sets $\mathcal{A}_2(L)$ and $\mathcal{A}_3(L)$ of sequences with fixed 2-error or 3-error linear complexity L. Each set in the decompositions arises by changing all sequences in $\mathcal{A}(L)$ in a fixed set of positions. Using the characterizations of $\mathcal{A}_2(L)$ and $\mathcal{A}_3(L)$ we determine the expressions for $\mathcal{N}_2(L)$ and $\mathcal{N}_3(L)$. The rest of this section discusses some basics and is organized to present a summary of the main results of the paper.

By Lemma 1.1 the linear complexity of any 2^n-periodic sequence $\mathbf{S}$ with $0 < L(\mathbf{S}) < 2^n$ and $merr(\mathbf{S}) = 2^{m+1}$, $m \in \{1, \cdots, n-1\}$, can be uniquely expressed as

$$L(\mathbf{S}) = 2^n - \sum_{i=1}^{m+1} 2^{n-r_i}, \tag{4}$$

where $1 \le r_1 < \cdots < r_{m+1} \le n$. From equation (4), the linear complexity of any 2^n-periodic binary sequence $\mathbf{S}$ with $0 < L(\mathbf{S}) < 2^n$ and $merr(\mathbf{S}) \ge 2^{m+1}$, $m \in \{1, \cdots, n-1\}$, can be bounded as

$$2^n - \left(\sum_{i=1}^{m-1} 2^{n-r_i} + 2^{n-r_m+1} \right) < L(\mathbf{S}) < 2^n - \sum_{i=1}^{m} 2^{n-r_i}, \tag{5}$$

for some $r_i \in \{1, \cdots, n\}$, $i = 1, \cdots, m$, satisfying $1 \le r_1 < \cdots < r_m$. Note that for any sequence $\mathbf{S}$ satisfying the inequality (5), we have $merr(\mathbf{S}) \ge 2^{m+1}$. We also note that the bounds in (5) are unique in the sense that the linear complexity of any 2^n-periodic sequence $\mathbf{S}$ with $merr(\mathbf{S}) \ge 2^{m+1}$ satisfies exactly one inequality of the particular form given in equation (5). Note that by equation (5) any L such that $w_H(2^n - L) \ge 3$ can be bounded as $2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1})$ for some $1 \le r_1 \le r_2 < n$. With this,

L	$2^n - (2^{n-r_1} + 2^{n-r_2}), \quad 1 \le r_1 \le r_2 < n$
$\mathcal{N}_2(L)$	$\left(\binom{2^{n-r_1+1}}{2} - 3 \cdot 2^{n+r_2-2r_1-1} + 2^{n-r_1+1} + 1 \right) 2^{L-1}$
$\mathcal{N}_3(L)$	$\left(\binom{2^{n-r_1+1}}{3} + \binom{2^{n-r_1+1}}{2} - 7 \cdot 2^{n+r_2-2r_1-1} + 2^{n-r_1+1} + 1 \right) 2^{L-1}$

Table 1: $\mathcal{N}_2(L)$ and $\mathcal{N}_3(L)$ when $w_H(2^n - L) = 2$

we give the expressions for $\mathcal{N}_2(L)$ and $\mathcal{N}_3(L)$ derived in this paper. When $w_H(2^n - L) = 0$ or 1 and $k = 2$, 3 we have

$$\mathcal{N}_k(0) = \sum_{i=0}^{k} \binom{2^n}{i}, \quad \mathcal{N}_k(2^n) = 0, \quad \text{and} \quad \mathcal{N}_k(2^n - 2^t) = 0, \quad 0 \le t < 2^n.$$

The results when $w_H(2^n - L) = 2$ are shown in Table 1. The results when $w_H(2^n - L) \ge 3$ are shown in Table 2. The characterizations of $\mathcal{A}_2(L)$ and $\mathcal{A}_3(L)$ are complicated to describe without resorting to much additional notation. Hence these details are directly handled in Sections 4 and 5.

L	$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}), \quad 1 \le r_1 \le r_2 < n$
$\mathcal{N}_2(L)$	$\left(\binom{2^{n-r_1+1}}{2} - 2^{n-r_2}(2^{2r_2-2r_1} - 1) + 2^{n-r_1+1} + 1\right) 2^{L-1}$
$\mathcal{N}_3(L)$	$\mathcal{N}_2(L) + \left(\binom{2^{n-r_1+1}}{3} - 4 \cdot 2^{n-r_2}\binom{2^{r_2-r_1}}{2}\right) 2^{L-1}$

Table 2: $\mathcal{N}_2(L)$ and $\mathcal{N}_3(L)$ when $w_H(2^n - L) \ge 3$

2 Effect of Small Changes On the Linear Complexity

We recall that $\mathcal{A}(L)$ is the set of 2^n-periodic sequences with fixed linear complexity L, $0 \le L \le 2^n$. For any two 2^n-periodic sequences $\mathbf{S}_1$ and $\mathbf{S}_2$, let $d_H(\mathbf{S}_1, \mathbf{S}_2)$ denote the Hamming distance between the tuples $\mathbf{S}_1^{(2^n)}$ and $\mathbf{S}_2^{(2^n)}$.

In this section we study the effect of small changes on the linear complexity of sequences in $\mathcal{A}(L)$ and derive some properties of $\mathcal{A}(L)$ which extend those in Fu et al.'s paper [3]. First we state a well known result on 2^n-periodic binary sequences.

Lemma 2.1 ([3]). *For any 2^n-periodic sequence $\mathbf{S}$, $L(\mathbf{S}) = 2^n$ if and only if $w_H(\mathbf{S})$ is odd.*

We give a generalization of [3, Theorem 1] using a more straightforward approach.

Theorem 2.2. *For a given $r \in \{1, \cdots, n-1\}$, let $1 \le L < 2^{n-r}$. Then for any two distinct sequences $\mathbf{S}, \mathbf{S}' \in \mathcal{A}(L)$ we have*

$$d_H(\mathbf{S}, \mathbf{S}') = t \cdot 2^{r+1} \text{ for some } t \in \{1, 2, 3, \cdots, 2^{n-r-1}\},$$

which implies $d_H(\mathbf{S}, \mathbf{S}') \ge 2^{r+1}$.

Proof. For any sequence $\mathbf{S} \in \mathcal{A}(L)$, consider the corresponding polynomial $\mathbf{S}(x) = (1+x)^{2^n - L}a(x)$, where $a(x) \in \mathbb{F}_2[x]$ such that $\deg(a(x)) \le L-1$ and $a(1) \ne 0$. Since $1 \le L < 2^{n-r}$, we have $2^n - L > 2^n - 2^{n-r}$. The generating function for $\mathbf{S}$ is given by

$$\frac{\mathbf{S}(x)}{1-x^{2^n}} = \frac{(1+x)^{(2^n - 2^{n-r}) + (2^{n-r} - L)}a(x)}{(1+x)^{2^n}} = \frac{(1+x)^{2^{n-r} - L}a(x)}{1 - x^{2^{n-r}}},$$

which implies 2^{n-r} is a period of $\mathbf{S}$. Corresponding to any sequence $\mathbf{M} \in \mathcal{A}(L)$, let $\mathbf{M}_{(r)}$ denote the 2^{n-r}-periodic sequence $(m_0, m_1, \cdots, m_{2^{n-r}-1})^\infty$. Since $1 \le L < 2^{n-r}$, from Lemma 2.1 we know that $w_H(\mathbf{S}_{(r)})$ and $w_H(\mathbf{S}'_{(r)})$ are even. Hence the Hamming distance between $\mathbf{S}_{(r)}$ and $\mathbf{S}'_{(r)}$ is even. That is $d_H(\mathbf{S}_{(r)}, \mathbf{S}'_{(r)}) = 2t$ for some $t \in \{1, 2, 3, \cdots, 2^{n-r-1}\}$. Since 2^{n-r} is a period of $\mathbf{S}$ and $\mathbf{S}'$, we have $d_H(\mathbf{S}, \mathbf{S}') = 2^r \cdot d_H(\mathbf{S}_{(r)}, \mathbf{S}'_{(r)}) = t \cdot 2^{r+1}$. This completes the proof of the theorem. □

We use the following result by Fu et al. [3] for the main results of this section. For the rest of the paper we use $\oplus$ for the operation of addition modulo 2^n.

```
CG (S, n)
    begin
    if n = 0 then
        return (S_0)
    fi
    if S_L^(2^(n-1)) = S_R^(2^(n-1)) then
        return CG (S_L, n − 1)
    else
        return 2^(n-1)+ CG (S_L + S_R, n − 1)
    fi
    end
```

Figure 1: The Games-Chan Algorithm

Lemma 2.3. *For any sequence* $\mathbf{S} \in \mathcal{A}(L)$*, where* $2^n - 2^{n-r} < L < 2^n - 2^{n-r-1}$ *for some* $1 \le r \le n-2$*, and for any integer* $0 \le i \le 2^n - 1$*, the number of sequences* $\mathbf{S}_{i,j} \in \mathcal{A}(L)$*, where* $0 \le j \le 2^n - 1$ *and* $j \ne i$*, is exactly* $2^r - 1$ *corresponding to all* $j \in \{i \oplus t2^{n-r} : 1 \le t \le 2^r - 1\}$.

The first main result of this section deals with extending Lemma 2.3 to the case when four symbols per period are changed.

The Games-Chan algorithm [4] is a fast algorithm to compute the linear complexity of a 2^n-periodic binary sequence, which we use for the rest of this section.

For any $\mathbf{S} \in \mathcal{A}(L)$ with period $\mathbf{S}^{(2^n)} = (s_0, \cdots, s_{2^n-1})$, denote the left and right halves of $\mathbf{S}^{(2^n)}$ by

$$\mathbf{S}_L^{(2^{n-1})} = (s_0, \cdots, s_{2^{n-1}-1}) \quad \text{and} \quad \mathbf{S}_R^{(2^{n-1})} = (s_{2^{n-1}}, \cdots, s_{2^n-1}).$$

Let $\mathbf{S}_L$ and $\mathbf{S}_R$ denote the 2^{n-1} periodic sequences

$$\mathbf{S}_L = (s_0, \cdots, s_{2^{n-1}-1})^\infty \quad \text{and} \quad \mathbf{S}_R = (s_{2^{n-1}}, \cdots, s_{2^n-1})^\infty.$$

The Games-Chan algorithm can be recursively described as in Figure 1. We make some observations and establish notation we use for the rest of the section. Note that the recursive procedure of the Games-Chan algorithm in Figure 1 is called a total of $n+1$ times to compute the linear complexity of any $\mathbf{S} \in \mathcal{A}(L)$. In the ith step, $i = 0, \cdots, n$, the algorithm computes the linear complexity of a 2^{n-i}-periodic binary sequence. Let $\psi^i(\mathbf{S})$, $i = 0, \cdots, n$, denote the first period of the 2^{n-i}-periodic binary sequence considered in the ith step of the algorithm when run with input sequence $\mathbf{S}$. For $i = 0, \cdots, n-1$, let $\psi_L^i(\mathbf{S})$ and $\psi_R^i(\mathbf{S})$ denote, respectively, the left and right halves of $\psi^i(\mathbf{S})$. Let $m^i(\mathbf{S})$ denote the total value contributed to $L(\mathbf{S})$ in the algorithm during the execution from the 0-th step to the i-th step of the algorithm. For any two finite binary sequences of the same length, $\mathbf{S}$ and $\mathbf{S}'$, let $d_H(\mathbf{S}, \mathbf{S}')$ denote the Hamming distance between $\mathbf{S}$ and $\mathbf{S}'$. We slightly abuse the notation because we also use $d_H(\mathbf{S}, \mathbf{S}')$ to denote the Hamming distance between the first periods of $\mathbf{S}$, $\mathbf{S}' \in A(L)$. The next lemma follows from the Games-Chan algorithm.

Lemma 2.4. *Let* $\mathbf{S}$ *be a* 2^n*-periodic binary sequence. For any* t *integers* $r_1, \cdots, r_t$ *such that* $0 < r_1 < r_2 < \cdots < r_t \leq n$*, we have*

$$L(\mathbf{S}) = 2^n - (2^{n-r_1} + 2^{n-r_2} + \cdots + 2^{n-r_t}) \tag{6}$$

if and only if

$$\psi_L^{u-1}(\mathbf{S}) = \psi_R^{u-1}(\mathbf{S}) \quad \textit{exactly when} \quad u \in \{r_1, \cdots, r_t\}. \tag{7}$$

We describe four symbol changes for sequences in $\mathcal{A}(L)$ such that the linear complexity of the modified sequences remains L. We assume that the four positions where the changes are made are distinct since the cases of four symbol changes when more than two positions are identical are covered by Lemma 2.3.

Theorem 2.5. *Let* $\mathbf{S} \in \mathcal{A}(L)$ *where*

$$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}), \tag{8}$$

for some r_1 *and* r_2 *satisfying* $1 \leq r_1 \leq r_2 < n$*.*

1. *Consider any four integers* i*,* j*,* k*, and* l *such that* $0 \leq i < j < k < l \leq 2^{n-r_1+1} - 1$*. Then* $L(\mathbf{S}_{i,j,k,l}) = L(\mathbf{S})$ *if and only if* i*,* j*,* k*, and* l *are in the form*

$$i = u + g_1 2^{n-r_2}, \quad j = u + g_2 2^{n-r_2}, \quad k = i + 2^{n-r_1}, \quad \textit{and} \quad l = j + 2^{n-r_1}, \tag{9}$$

   where $0 \leq u \leq 2^{n-r_2} - 1$ *and* $0 \leq g_1 < g_2 \leq 2^{r_2-r_1} - 1$*.*

2. *There do not exist integers* $i_1, \cdots, i_6$ *such that* $0 \leq i_1 < \cdots < i_6 \leq 2^{n-r_1+1} - 1$ *and* $L(\mathbf{S}_{i_1,\cdots,i_6}) = L(\mathbf{S})$*.*

Proof. We only prove the forward direction of part 1 of the theorem. The other direction is straightforward and can be proved by reversing the argument used for the forward case.

Consider any sequence

$$\mathbf{S}_{i,j,k,l} \in \mathcal{A}(L), \quad \text{where} \quad 0 \leq i < j < k < l \leq 2^{n-r_1+1} - 1. \tag{10}$$

From equation (8) we have

$$w_H(2^n - L) \geq 3 \quad \text{and} \quad L = 2^n - (2^{n-r_1} + 2^{n-r_2-1} + c), \tag{11}$$

for some $0 < c < 2^{n-r_2-1}$. From equations (6), (7), and (11), we have

$$\forall\ \mathbf{S} \in \mathcal{A}(L), \quad \psi_L^{r_1-1}(\mathbf{S}) = \psi_R^{r_1-1}(\mathbf{S}) \quad \text{and} \quad \psi_L^{r_2}(\mathbf{S}) = \psi_R^{r_2}(\mathbf{S}). \tag{12}$$

By Lemma 2.4 and equation (11) the left and right halves are not equal during the first $r_1 - 2$ steps of the Games-Chan procedure for any $\mathbf{S} \in \mathcal{A}(L)$. Thus, since $0 \leq i, j, k, l \leq 2^{n-r_1+1} - 1$, by the procedure of the Games-Chan algorithm we get

$$d_H(\psi^{r_1-1}(\mathbf{S}), \psi^{r_1-1}(\mathbf{S}_{i,j,k,l})) = 4. \tag{13}$$

By equations (12) and (13), the four positions where the vectors $\psi^{r_1-1}(\mathbf{S})$, $\psi^{r_1-1}(\mathbf{S}_{i,j,k,l})$ differ are of the form

$$c_1, \quad c_2, \quad c_1 + 2^{n-r_1}, \quad \text{and} \quad c_2 + 2^{n-r_1}, \quad \text{for some} \quad 0 \le c_1 < c_2 \le 2^{n-r_1} - 1. \tag{14}$$

From equations (12) and (13), we have $d_H(\psi_L^{r_1-1}(\mathbf{S}), \psi_L^{r_1-1}(\mathbf{S}_{i,j,k,l})) = 2$. This implies

$$d_H(\psi^{r_1}(\mathbf{S}), \psi^{r_1}(\mathbf{S}_{i,j,k,l})) = 2. \tag{15}$$

Now we treat $\psi^{r_1}(\mathbf{S})$ and $\psi^{r_1}(\mathbf{S}_{i,j,k,l})$ as the first periods of 2^{n-r_1}-periodic binary sequences $\mathbf{S}'$ and $\mathbf{S}'_{i,j,k,l}$, respectively, that differ at 2 positions. With this notation, from equations (14) and (15) we have $\mathbf{S}' = (\psi^{r_1}(\mathbf{S}))^\infty$, $\mathbf{S}'_{i,j,k,l} = (\psi^{r_1}(\mathbf{S}_{i,j,k,l}))^\infty$, and

$$\mathbf{S}'_{i,j,k,l}(x) = \mathbf{S}'(x) + x^{c_1} + x^{c_2}. \tag{16}$$

As a consequence of the procedure of the Games-Chan algorithm, since the left and right halves are different in the first $r_1 - 2$ steps for both $\mathbf{S}$ and $\mathbf{S}_{i,j,k,l}$, we have

$$m^{r_1-1}(\mathbf{S}) = m^{r_1-1}(\mathbf{S}_{i,j,k,l}) = 2^{n-1} + \cdots + 2^{n-r_1+1} = 2^n - 2^{n-r_1+1}. \tag{17}$$

Using Lemma 2.4 and by equations (10), (16), and (17) we have

$$\mathbf{S}', \mathbf{S}'_{i,j,k,l} \in \mathcal{A}(L') \quad \text{where} \quad L' = L - (2^n - 2^{n-r_1+1}). \tag{18}$$

Equations (8) and (18) imply that L' satisfies

$$2^{n-r_1} - 2^{n-r_2} < L' < 2^{n-r_1} - 2^{n-r_2-1}. \tag{19}$$

By Lemma 2.3 and equation (19), the positions c_1 and c_2 in equations (14) and (16) must be in the form

$$c_i = u + g_i 2^{n-r_2}, \quad i = 1, 2, \quad \text{where} \quad 0 \le u \le 2^{n-r_2} - 1, \quad 0 \le g_1 < g_2 \le 2^{r_2-r_1} - 1. \tag{20}$$

From equations (14) and (20), the four positions, denoted f_1, f_2, f_3, and f_4, where $\psi^{r_1-1}(\mathbf{S})$ and $\psi^{r_1-1}(\mathbf{S}_{i,j,k,l})$ differ are of the form

$$f_1 = c_1, \quad f_2 = c_2, \quad f_3 = c_1 + 2^{n-r_1}, \quad \text{and} \quad f_4 = c_2 + 2^{n-r_1}, \tag{21}$$

where c_1 and c_2 are as in equation (20).

From the procedure of Games-Chan algorithm observe that a symbol change at any position c in $\psi^{r_1-1}(\mathbf{S})$, $0 \le c \le 2^{n-r_1+1} - 1$, can be effected by changing the symbol at one of the corresponding positions $\{(c + b2^{n-r_1+1}) \bmod 2^n : b = 0, \cdots, 2^{r_1-1} - 1\}$ in each period of $\mathbf{S}$. Thus from equations (20) and (21), i, j, k, and l must be in the form given in equation (9).

To prove part 2 assume that there exist integers $i_1, \cdots, i_6$ such that $0 \le i_1 < \cdots < i_6 \le 2^{n-r_1+1} - 1$ and

$$L(\mathbf{S}_{i_1,\cdots,i_6}) = L(\mathbf{S}). \tag{22}$$

From the procedure of the Games-Chan algorithm, using an argument similar to that used to arrive at equation (15) we have

$$d_H(\psi^{r_1}(\mathbf{S}), \psi^{r_1}(\mathbf{S}_{i_1,\cdots,i_6})) = 3. \tag{23}$$

By equation (11) and Lemma 2.4 we know $w_H(\psi^{r_1}(\mathbf{S}))$ is even since otherwise $L(\mathbf{S}) = 2^n - 2^{n-r_1}$. Using this, equation (23) implies that $w_H(\psi^{r_1}(\mathbf{S}_{i_1,\cdots,i_6}))$ is odd, which contradicts equation (22). Thus part 2 of the theorem is proved. □

Remark 1. Note that in Theorem 2.5(1) when $r_1 = r_2 = 1$ there are no possible distinct values for g_1 and g_2 in equation (9). Thus when $0 < L < 2^{n-2}$ there do not exist distinct four symbol changes to any sequence in $\mathcal{A}(L)$ that result in sequences with linear complexity L. This is an alternative proof of Theorem 2.2 when $r = 2$.

Also, for some values of L in equation (8), in order to write L in the form as in equation (5), we must allow $r_1 = r_2$.

Next we extend Lemma 2.3 to the case when the linear complexity is of the form $L = 2^n - 2^{n-r}$, $1 \le r \le n$.

Lemma 2.6. *For any sequence $\mathbf{S} \in \mathcal{A}(L)$, where $L = 2^n - 2^{n-r}$ for some $1 \le r \le n$, and for any integer $0 \le i \le 2^n - 1$, the number of sequences $\mathbf{S}_{i,j} \in \mathcal{A}(L)$, where $0 \le j \le 2^n - 1$ and $j \ne i$, is exactly $2^{r-1} - 1$ corresponding to all $j \in \{i \oplus t2^{n-r+1} : 1 \le t \le 2^{r-1} - 1\}$.*

Proof. First we prove the reverse direction of the lemma. Say $j = i \oplus t2^{n-r+1}$ for some $1 \le t \le 2^{r-1} - 1$. Let the polynomial corresponding to $\mathbf{S}$ be

$$\mathbf{S}(x) = (1 + x)^{2^{n-r}} a(x), \tag{24}$$

for some $a(x) \in \mathbb{F}_2[x]$ such that $\deg(a(x)) \le 2^n - 2^{n-r} - 1$ and $a(1) = 1$. Consider the polynomial

$$x^i + x^{i+t2^{n-r+1}} = x^i(1 + x^t)^{2^{n-r+1}} = x^i(1 + x)^{2^{n-r+1}}(1 + \cdots + x^{t-1})^{2^{n-r+1}}. \tag{25}$$

By equations (24), (25) and the definition of linear complexity we have

$$\begin{aligned}
L(\mathbf{S}_{i,j}) &= 2^n - \deg(\gcd(1 + x^{2^n}, \mathbf{S}_{i,j}(x))) \\
&= 2^n - \deg(\gcd(1 + x^{2^n}, \mathbf{S}(x) + x^i + x^{i \oplus t2^{n-r+1}})) \\
&= 2^n - \deg(\gcd(1 + x^{2^n}, \mathbf{S}(x) + x^i + x^{i + t2^{n-r+1}})) \\
&= 2^n - \deg(\gcd((1 + x)^{2^n}, (1 + x)^{2^{n-r}} a(x) + x^i(1 + x)^{2^{n-r+1}}(1 + \cdots + x^{t-1})^{2^{n-r+1}})) \\
&= 2^n - 2^{n-r} = L.
\end{aligned}$$

Now we prove the forward direction. We have $\mathbf{S}_{i,j} \in \mathcal{A}(L)$. From Lemma 2.4 we have

$$\psi_L^{r-1}(\mathbf{S}) = \psi_R^{r-1}(\mathbf{S}) \quad \text{and} \quad \psi_L^{r-1}(\mathbf{S}_{i,j}) = \psi_R^{r-1}(\mathbf{S}_{i,j}). \tag{26}$$

Assume $j \notin \{i \oplus t2^{n-r+1} : 1 \le t \le 2^{r-1} - 1\}$. That is i and j are not congruent modulo 2^{n-r+1}. By the procedure of the Games-Chan algorithm, since the left and right halves are not equal during the first $(r - 2)$ steps of the algorithm for both $\mathbf{S}$ and $\mathbf{S}_{i,j}$ we have

$$d_H(\psi^{r-1}(\mathbf{S}), \psi^{r-1}(\mathbf{S}_{i,j})) = 2. \tag{27}$$

By equations (26) and (27) we have $d_H(\psi^r(\mathbf{S}), \psi^r(\mathbf{S}_{i,j})) = 1$. This implies that $w_H(\psi^r(\mathbf{S}))$ and $w_H(\psi^r(\mathbf{S}_{i,j}))$ can not both be odd, which contradicts the fact that $L(\mathbf{S}) = L(\mathbf{S}_{i,j}) = 2^n - 2^{n-r}$. Thus it must be the case that $j \in \{i \oplus t2^{n-r+1} : 1 \le t \le 2^{r-1} - 1\}$. □

The following result can be proved using Lemma 2.6 and the approach used in Theorem 2.5.

Theorem 2.7. *Let $\mathbf{S} \in \mathcal{A}(L)$ where $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$ for some r_1, r_2 such that $1 \le r_1 < r_2 \le n$.*

1. *Consider any four integers i, j, k, and l such that $0 \le i < j < k < l \le 2^{n-r_1+1} - 1$. Then $L(\mathbf{S}_{i,j,k,l}) = L(\mathbf{S})$ if and only if i, j, k, and l are in the form*

$$i = u + g_1 2^{n-r_2+1}, \quad j = u + g_2 2^{n-r_2+1}, \quad k = i + 2^{n-r_1}, \quad \text{and} \quad l = j + 2^{n-r_1}, \tag{28}$$

where

$$0 \le u \le 2^{n-r_2+1} - 1 \quad \text{and} \quad 1 \le g_1 < g_2 \le 2^{r_2-r_1-1} - 1. \tag{29}$$

2. *There do not exist integers $i_1, \cdots, i_6$ such that $0 \le i_1 < \cdots < i_6 \le 2^{n-r_1+1} - 1$ and $L(\mathbf{S}_{i_1,\cdots,i_6}) = L(\mathbf{S})$.*

For any polynomial $a(x) \in \mathbb{F}_2[x]$ given by $a(x) = 1 + x^{a_1} + \cdots + x^{a_{q-1}}$, define the weight $W(a(x)) = q$.

We also need to handle two symbol changes that decrease the linear complexity of 2^n-periodic binary sequences.

Lemma 2.8. *For any sequence $\mathbf{S} \in \mathcal{A}(L)$, where $L = 2^n - 2^{n-r}$ for some $1 \le r \le n$, and for any integer $0 \le i \le 2^n - 1$, the number of sequences $\mathbf{S}_{i,j}$ such that $L(\mathbf{S}_{i,j}) < L$, where $0 \le j \le 2^n - 1$ and $j \ne i$, is exactly 2^{r-1} corresponding to all $j \in \{i \oplus (2t+1)2^{n-r} : 0 \le t \le 2^{r-1} - 1\}$.*

Proof. First we prove the forward direction of the result. Let $\mathbf{S}(x) = (1+x)^{2^{n-r}} a(x)$ for some $a(x) \in \mathbb{F}_2[x]$ such that $\deg(a(x)) \le 2^n - 2^{n-r} - 1$ and $a(1) = 1$. The corresponding polynomial for $\mathbf{S}_{i,j}$ is

$$\mathbf{S}_{i,j}(x) = (1+x)^{2^{n-r}} a(x) + x^i + x^j.$$

So $L(\mathbf{S}_{i,j}) = 2^n - \deg(\gcd((1+x)^{2^n}, (1+x)^{2^{n-r}} a(x) + x^i + x^j))$ and hence we have

$$L(\mathbf{S}_{i,j}) < L \quad \text{if and only if} \quad \gcd((1+x)^{2^n}, x^i + x^j) = (1+x)^{2^{n-r}}. \tag{30}$$

Without loss of generality we may assume $i < j$. It is a well known fact that $\gcd(1+x^a, 1+x^b) = 1 + x^{\gcd(a,b)}$. Hence we get

$$\gcd((1+x)^{2^n}, x^i + x^j) = \gcd(1 + x^{2^n}, 1 + x^{j-i}) = 1 + x^{\gcd(2^n, j-i)} = 1 + x^{2^{n-r}}$$

if and only if 2^{n-r} divides $j - i$ and no higher power of 2 divides $j - i$. Thus equation (30) implies that $L(\mathbf{S}_{i,j}) < L$ if and only if $j = i + d2^{n-r}$ for some odd integer d which proves the forward direction. The reverse direction can be proved using an argument similar to that used in proving the reverse direction of Lemma 2.6. □

Corollary 2.9. *For any sequence* $\mathbf{S} \in \mathcal{A}(L)$*, where* $L = 2^n - 2^{n-r}$ *for some* $1 \le r \le n$*, there are* 2^{n+r-2} *distinct pairs* i*,* j*,* $0 \le i < j \le 2^n - 1$*, such that* $L(\mathbf{S}_{i,j}) < L$*. All such* i*,* j *are described as*

$$i \quad \text{and} \quad j = i + (2t+1)2^{n-r}, \tag{31}$$

where

$$0 \le i \le 2^n - 2^{n-r} - 1 \quad \text{and} \quad 0 \le t \le 2^{r-1} - 1 - \lceil (\lfloor i/2^{n-r} \rfloor)/2 \rceil. \tag{32}$$

Also, the distinct pairs i*,* j*,* $0 \le i < j \le 2^n - 1$*, such that*

$$1 + x^{j-i} = (1+x)^{2^{n-r}} b(x), \tag{33}$$

for some $b(x) \in \mathbb{F}_2[x]$*,* $b(1) = 1$*,* $\deg(b(x)) \le 2^n - 2^{n-r} - 1$*, are exactly those described in equations* (31) *and* (32)*.*

Proof. By Lemma 2.8 for each $i \ge 2^n - 2^{n-r}$ there are no js such that $i < j \le 2^n - 1$ and $L(\mathbf{S}_{i,j}) < L$. Also, for each $0 \le i \le 2^n - 2^{n-r} - 1$ there are exactly $2^{r-1} - \lceil (\lfloor i/2^{n-r} \rfloor)/2 \rceil$ odd multiples of 2^{n-r} corresponding to $0 \le t \le 2^{r-1} - 1 - \lceil (\lfloor i/2^{n-r} \rfloor)/2 \rceil$ such that $L(\mathbf{S}_{i,i+(2t+1)2^{n-r}}) < L$. Thus all i, j, $0 \le i < j \le 2^n - 1$, such that $L(\mathbf{S}_{i,j}) < L$ are as described in equations (31) and (32).

The number of distinct pairs i, j obtained from equations (31) and (32) is

$$\begin{aligned} \sum_{i=0}^{2^n-1} \left(2^{r-1} - \lceil (\lfloor i/2^{n-r} \rfloor)/2 \rceil\right) &= \sum_{i=0}^{2^{n-r}-1} 2^{r-1} + \sum_{l=1}^{2^{r-1}-1} \left(\sum_{i=(2l-1)2^{n-r}}^{(2l+1)2^{n-r}-1} (2^{r-1} - l) \right) \\ &= 2^{n-r} 2^{r-1} + 2^{n-r+1} \left(\sum_{l=1}^{2^{r-1}-1} (2^{r-1} - l) \right) \\ &= 2^{n+r-2}. \end{aligned} \tag{34}$$

By the definition of linear complexity it is straightforward to see that the integers i, j in equations (31) and (32) are exactly those that satisfy equation (33). □

Our next result deals with four symbol changes that decrease the linear complexity of 2^n-periodic binary sequences.

Theorem 2.10. *Let* $\mathbf{S} \in \mathcal{A}(L)$ *where* $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$ *for some* r_1*,* r_2 *such that* $1 \le r_1 < r_2 \le n$*.*

1. *Consider any four integers* i*,* j*,* k*, and* l *such that* $0 \le i < j < k < l \le 2^{n-r_1+1} - 1$*. Then* $L(\mathbf{S}_{i,j,k,l}) < L$ *if and only if* i*,* j*,* k*, and* l *are in the form*

$$i, \quad j = i + (2t+1)2^{n-r_2}, \quad k = i + 2^{n-r_1}, \quad \text{and} \quad l = j + 2^{n-r_1}, \tag{35}$$

where

$$0 \le i \le 2^{n-r_1} - 2^{n-r_2} - 1 \quad \text{and} \quad 0 \le t \le 2^{r_2-r_1-1} - 1 - \lceil (\lfloor i/2^{n-r_2} \rfloor)/2 \rceil. \tag{36}$$

Furthermore, if $\mathcal{K}(L)$ *is the set of four symbol changes to* $\mathbf{S}$ *described in equations* (35) *and* (36) *that decrease its linear complexity, then*

$$\begin{aligned} |\mathcal{K}(L)| &= |\{\{i,j,k,l\} : 0 \le i < j < k < l \le 2^{n-r_1+1} - 1 \quad \text{and} \quad L(\mathbf{S}_{i,j,k,l}) < L\}| \\ &= 2^{n+r_2-2r_1-2}. \end{aligned} \tag{37}$$

2. *For any four integers i_t, $t = 1, \cdots, 4$, such that $0 \le i_1 < i_2 < i_3 < i_4 \le 2^n - 1$, we have $L(\mathbf{S}_{i_1,i_2,i_3,i_4}) < L$ if and only if $\{i_t \bmod 2^{n-r_1+1} : t = 1, \cdots, 4\} \in \mathcal{K}(L)$.*

3. *There do not exist integers $i_1, \cdots, i_6$, $0 \le i_1 < \cdots < i_6 \le 2^n - 1$, such that $L(\mathbf{S}_{i_1,\cdots,i_6}) < L$.*

Proof. First we prove the forward direction of part 1. Let $\mathbf{S}(x) = (1+x)^{2^{n-r_1}+2^{n-r_2}} a(x)$ for some $a(x) \in \mathbb{F}_2[x]$ such that $\deg(a(x)) \le 2^n - 2^{n-r_1} - 2^{n-r_2} - 1$ and $a(1) = 1$. The corresponding polynomial for $\mathbf{S}_{i,j,k,l}$ is

$$\mathbf{S}_{i,j,k,l}(x) = (1+x)^{2^{n-r_1}+2^{n-r_2}} a(x) + x^i + x^j + x^k + x^l.$$

So $L(\mathbf{S}_{i,j,k,l}) = 2^n - \gcd((1+x)^{2^n}, (1+x)^{2^{n-r_1}+2^{n-r_2}} a(x) + x^i + x^j + x^k + x^l)$ and hence $L(\mathbf{S}_{i,j,k,l}) < L$ if and only if $\gcd((1+x)^{2^n}, x^i + x^j + x^k + x^l) = (1+x)^{2^{n-r_1}+2^{n-r_2}}$. This holds if and only if

$$\begin{aligned} 1 + x^{j-i} + x^{k-i} + x^{l-i} &= (1+x)^{2^{n-r_1}+2^{n-r_2}} b(x) \\ &= (1+x^{2^{n-r_2}}) b(x) + x^{2^{n-r_1}} (1+x^{2^{n-r_2}}) b(x) \end{aligned} \tag{38}$$

for some $b(x) \in \mathbb{F}_2[x]$ such that $b(1) = b(0) = 1$. Since $0 \le i < j < k < l \le 2^{n-r_1+1} - 1$ we have

$$\deg(b(x)) \le 2^{n-r_1} - 2^{n-r_2} - 1. \tag{39}$$

Since $W((1+x^{2^{n-r_2}})b(x)) \ge 2$, by equations (38) and (39) we see that

$$1 + x^{j-i} = (1+x^{2^{n-r_2}}) b(x). \tag{40}$$

By Corollary 2.9 and equations (38), (39), and (40) we see that i, j, k, and l should be as in equation (35). The proof of the reverse direction of part 1 is straightforward and is similar to the proof of the reverse direction of Lemma 2.6. Equation (37) follows from equations (35), (36), (39), (40), Lemma 2.8, and an argument similar to that used in Corollary 2.9 by substituting n by $n - r_1$ and r by $r_2 - r_1$ in equation (34).

To prove the forward direction of part 2, we first note that $L(\mathbf{S}_{i_1,i_2,i_3,i_4}) < L$ if and only if the polynomial

$$e(x) = x^{i_1} + x^{i_2} + x^{i_3} + x^{i_4} = (1+x)^{2^{n-r_1}+2^{n-r_2}} b'(x) \tag{41}$$

for some $b'(x) \in \mathbb{F}_2[x]$ such that $\deg(b'(x)) \le 2^n - 2^{n-r_1} - 2^{n-r_2} - 1$ and $b'(1) = 1$. Let u be the largest power of $(1+x)$ dividing

$$e'(x) = x^{i_1 \bmod 2^{n-r_1+1}} + x^{i_2 \bmod 2^{n-r_1+1}} + x^{i_3 \bmod 2^{n-r_1+1}} + x^{i_4 \bmod 2^{n-r_1+1}} \tag{42}$$

so that

$$e'(x) = (1+x)^u b''(x) \tag{43}$$

for some $b''(x) \in \mathbb{F}_2[x]$ such that $\deg(b(x)) \le 2^{n-r_1+1} - u$ and $b''(1) = 1$. For $t = 1, \cdots, 4$ denoting $q_t = \lfloor i_t / 2^{n-r_1+1} \rfloor$ we have

$$\begin{aligned} x^{i_t \bmod 2^{n-r_1+1}} + x^{i_t} &= x^{i_t \bmod 2^{n-r_1+1}} + x^{i_t \bmod 2^{n-r_1+1} + q_t 2^{n-r_1+1}} \\ &= x^{i_t \bmod 2^{n-r_1+1}} (1+x)^{2^{n-r_1+1}} (1 + \cdots + x^{q_t - 1})^{2^{n-r_1+1}}. \end{aligned}$$

By equations (41) and (43), this implies

$$(1+x)^{2^{n-r_1+1}} \mid e(x)+e'(x) = (1+x)^{2^{n-r_1}+2^{n-r_2}} b'(x) + (1+x)^u b''(x).$$

So

$$u = 2^{n-r_1} + 2^{n-r_2} \tag{44}$$

since $2^{n-r_1+1} > 2^{n-r_1} + 2^{n-r_2}$. Since $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$, by equations (42)-(44), and the definition of linear complexity we see that the four symbol changes at positions $i_t \mod 2^{n-r_1+1}$, $t = 1, \cdots, 4$, lower the linear complexity of any $\mathbf{S} \in \mathcal{A}(L)$. Thus $\{i_t \mod 2^{n-r_1+1} : t = 1, \cdots, 4\} \in \mathcal{K}(L)$, which concludes the proof of the forward direction of part 2. The reverse direction of part 2 can be proved similarly.

To prove part 3, let there be integers $i_1, \cdots, i_6$, $0 \le i_1 < \cdots < i_6 \le 2^{n-r_1+1} - 1$, such that $L(\mathbf{S}_{i_1,\cdots,i_6}) < L$. By the argument used to arrive at equation (38) we have

$$x^{i_1} + \cdots + x^{i_6} = (1 + x^{2^{n-r_2}})c(x) + x^{2^{n-r_1}}(1 + x^{2^{n-r_2}})c(x), \tag{45}$$

for some $c(x) \in \mathbb{F}_2[x]$ such that $c(1) = 1$ and $\deg(c(x)) \le 2^{n-r_1} - 2^{n-r_2} - 1$. By equation (45) and the upper bound on $\deg(c(x))$ it follows that $(1 + x^{2^{n-r_2}})c(x) = x^{i_1} + x^{i_2} + x^{i_3}$, which is not possible since $(1 + x^{2^{n-r_2}})c(x)$ has an even number of terms. So the result follows when $0 \le i_1 < \cdots < i_6 \le 2^{n-r_1+1} - 1$. The result holds even when $0 \le i_1 < \cdots < i_6 \le 2^n - 1$ due to an argument similar to that used to prove part 2. □

Remark 2. Theorem 2.5 can also be proved with the approach of Theorem 2.10 by using results on polynomial weights [5, Proposition 3.2].

3 Notation and Auxiliary Results

In this section we establish the notation used for the rest of the paper and derive some auxiliary results on the k-error linear complexity of 2^n-periodic binary sequences.

Recall that $\mathcal{A}_k(L)$ is the set of 2^n-periodic binary sequences with k-error linear complexity L and $\mathcal{N}_k(L) = |\mathcal{A}_k(L)|$. For any $1 \le t \le 2^n$, let $\mathbf{E}_{i_1,\cdots,i_t}$, $0 \le i_1 < \cdots < i_t \le 2^n - 1$, denote the 2^n-periodic binary sequence of weight t with a 1 at positions with subscripts $i_1, \cdots, i_t$ in the first period and 0 elsewhere. Further let $\mathbb{E}_t = \{\mathbf{E}_{i_1,\cdots,i_t} : 0 \le i_1 < i_2 < \cdots < i_t \le 2^n - 1\}$ for $t \ge 1$ and $\mathbb{E}_0 = \{\mathbf{0}\}$. We denote by $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}$ the set $\{\mathbf{S} + \mathbf{E}_{i_1,\cdots,i_t} : \mathbf{S} \in \mathcal{A}(L)\}$. For the rest of the paper, for any set $\mathcal{R}$ of 2^n-periodic binary sequences, by $\mathcal{A}(L)[\mathcal{R}]$ denote the set of sets $\{\mathcal{A}(L) + \mathbf{R} : \mathbf{R} \in \mathcal{R}\}$.

We have two simple results that will be used in the rest of the paper.

Lemma 3.1 ([3]). *For any 2^n-periodic sequence $\mathbf{S}$, if $w_H(\mathbf{S})$ is even then $L_1(\mathbf{S}) = L(\mathbf{S})$. If $w_H(\mathbf{S})$ is odd, then $L_2(\mathbf{S}) = L_1(\mathbf{S}) < L(\mathbf{S}) = 2^n$.*

Lemma 3.2 ([7]). *For any 2^n-periodic binary sequence $\mathbf{S}$ and for $k \ge 2$, $L_k(\mathbf{S})$ is different from $2^n - 2^t$ for every integer t with $0 \le t < n$.*

We derive two auxiliary results used for the rest of the paper.

Theorem 3.3. *Let* $\{i_1, \cdots, i_{t_1}\}$ *and* $\{j_1, \cdots, j_{t_2}\}$ *denote two sets of subscripts where* $0 \leq i_l, j_m \leq 2^n - 1$ *for* $l = 1, \cdots, t_1$ *and* $m = 1, \cdots, t_2$. *Then*

$$(\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_{t_1}}) \cap (\mathcal{A}(L) + \mathbf{E}_{j_1,\cdots,j_{t_2}}) = \emptyset$$

or

$$\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_{t_1}} = \mathcal{A}(L) + \mathbf{E}_{j_1,\cdots,j_{t_2}}.$$

Proof. We assume

$$0 < L \leq 2^n \tag{46}$$

since the result holds trivially for $L = 0$.

Suppose $(\mathcal{A}(L)+\mathbf{E}_{i_1,\cdots,i_{t_1}})\cap(\mathcal{A}(L)+\mathbf{E}_{j_1,\cdots,j_{t_2}}) \neq \emptyset$. So there exist sequences $\mathbf{S}$, $\mathbf{S}' \in \mathcal{A}(L)$ such that $\mathbf{S} + \mathbf{E}_{i_1,\cdots,i_{t_1}} = \mathbf{S}' + \mathbf{E}_{j_1,\cdots,j_{t_2}}$. This implies that

$$\mathbf{S} + \mathbf{E}_{i_1,\cdots,i_{t_1}} + \mathbf{E}_{j_1,\cdots,j_{t_2}} = \mathbf{S}'. \tag{47}$$

Consider the corresponding polynomials of $\mathbf{S}$ and $\mathbf{S}'$ given by

$$\mathbf{S}(x) = (1-x)^{2^n-L}a(x) \quad \text{and} \quad \mathbf{S}'(x) = (1-x)^{2^n-L}a'(x), \tag{48}$$

where $a(1) = a'(1) = 1$. From equations (46) and (48) we have

$$\deg(\gcd((1-x^{2^n}), \mathbf{S}(x) + \mathbf{S}'(x))) > 2^n - L. \tag{49}$$

From equations (47) and (49) we have

$$\deg(\gcd((1-x^{2^n}), x^{i_1} + \cdots + x^{i_{t_1}} + x^{j_1} + \cdots + x^{j_{t_2}})) > 2^n - L. \tag{50}$$

To prove the theorem we first show that every sequence in $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_{t_1}}$ is in $\mathcal{A}(L) + \mathbf{E}_{j_1,\cdots,j_{t_2}}$. Consider any $\mathbf{R} \in \mathcal{A}(L)$ with the corresponding polynomial

$$\mathbf{R}(x) = (1-x)^{2^n-L}b(x), \quad \text{where} \quad b(1) = 1. \tag{51}$$

Then let $\mathbf{R}' = \mathbf{R}+\mathbf{E}_{i_1,\cdots,i_{t_1}}+\mathbf{E}_{j_1,\cdots,j_{t_2}}$ with the corresponding polynomial $\mathbf{R}'(x)$. By equations (50) and (51) we have

$$\begin{aligned} &\deg(\gcd((1-x^{2^n}), \mathbf{R}'(x))) \\ &= \deg(\gcd((1-x)^{2^n}, \mathbf{R}(x) + x^{i_1} + \cdots + x^{i_{t_1}} + x^{j_1} + \cdots + x^{j_{t_2}})) \\ &= 2^n - L. \end{aligned} \tag{52}$$

From equation (52), using the definition of linear complexity we have $\mathbf{R}' \in \mathcal{A}(L)$, which implies $\mathcal{A}(L)+\mathbf{E}_{i_1,\cdots,i_{t_1}} \subseteq \mathcal{A}(L)+\mathbf{E}_{j_1,\cdots,j_{t_2}}$. By symmetry $\mathcal{A}(L)+\mathbf{E}_{j_1,\cdots,j_{t_2}} \subseteq \mathcal{A}(L)+\mathbf{E}_{i_1,\cdots,i_{t_1}}$, which proves the theorem. □

We need the following generalization of [3, Theorem 4] in the latter sections.

Lemma 3.4. *Let* $\mathbf{S}$ *be a* T*-periodic binary sequence. Consider any two positive integers* u, v *such that* $0 \leq v \leq u$ *and* $u + v < merr(\mathbf{S})$. *Then for any* T*-periodic binary sequence* $\mathbf{E}$ *such that* $w_H(\mathbf{E}) = v$ *we have*

$$L_u(\mathbf{S} + \mathbf{E}) = L(\mathbf{S}).$$

Proof. First we note that $L_i(\mathbf{S}) = L(\mathbf{S})$ for $i = 0, \cdots, merr(\mathbf{S}) - 1$. Since $u + v < merr(\mathbf{S})$, by definitions of $L_u(\mathbf{S})$ and $L_{u+v}(\mathbf{S})$ we get

$$L_u(\mathbf{S} + \mathbf{E}) \geq L_{u+v}(\mathbf{S}) = L(\mathbf{S}). \tag{53}$$

Also, from the observations that $(\mathbf{S} + \mathbf{E}) + \mathbf{E} = \mathbf{S}$ and $w_H(\mathbf{E}) = v \leq u$, we get

$$L_u(\mathbf{S} + \mathbf{E}) \leq L(\mathbf{S}). \tag{54}$$

The lemma follows from equations (53) and (54). □

Next we prove a generalized result on the characterization and counting function of $\mathcal{A}_k(L)$ for certain specific values of k and L.

Theorem 3.5. *Consider $L \geq 0$ such that $w_H(2^n - L) \geq r + 1$ for some $0 \leq r \leq n - 1$.*

1. *The set*

$$\mathcal{A}_k(L) = \bigcup_{t=0}^{k} \left(\bigcup_{\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t} (\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}) \right) \quad for \quad k = 1, \cdots, 2^r - 1. \tag{55}$$

2. *Furthermore, if $1 \leq L < 2^{n-r}$ then the sets $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}$, $\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t$ for $t = 0, \cdots, 2^r - 1$ are disjoint and*

$$\mathcal{N}_k(L) = \left(\sum_{i=0}^{k} \binom{2^n}{i} \right) 2^{L-1} \quad for \quad k = 1, \cdots, 2^r - 1. \tag{56}$$

Proof. First we make these two observations to show part 1.

1. Hypothesis $w_H(2^n - L) \geq r + 1$ implies that for any $\mathbf{S} \in \mathcal{A}(L)$ we have $merr(\mathbf{S}) \geq 2^{r+1}$.
2. For $k = 1, \cdots, 2^r - 1$, we have $2k \leq 2^{r+1} - 2$.

From these two observations and using Lemma 3.4 we have

$$\bigcup_{t=0}^{k} \left(\bigcup_{\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t} (\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}) \right) \subseteq \mathcal{A}_k(L).$$

Using this, equation (55) follows from the definition of k-error linear complexity.

To show part 2 assume that $1 \leq L < 2^{n-r}$. To show that the sets $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}$, $\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t$, $t = 0, \cdots, 2^r - 1$, are all disjoint, by Theorem 3.3, it is enough to show that no two of these sets are equal. We show this by contradiction. Any two sets $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_u}$ and $\mathcal{A}(L) + \mathbf{E}_{j_1,\cdots,j_v}$, $0 \leq u, v \leq 2^r - 1$, are equal if and only if

$$\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_u,j_1,\cdots,j_v} = \mathcal{A}(L) \quad \text{with} \quad u + v \leq 2^{r+1} - 2. \tag{57}$$

By Theorem 2.2 for any two sequences $\mathbf{S}$, $\mathbf{S}' \in \mathcal{A}(L)$ we have $d_H(\mathbf{S}, \mathbf{S}') \geq 2^{r+1}$. Thus the set equality in equation (57) does not hold and all the sets $\mathcal{A}(L) + \mathbf{E}_{i_1,\cdots,i_t}$, $\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t$, $t = 0, \cdots, 2^r - 1$, are disjoint. Using this, the counting function in equation (56) follows from equation (55). □

4 Characterization When $w_H(2^n - L) \neq 2$

In this section we characterize the 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity when the linear complexity is not of the form $2^n-(2^i+2^j)$, $1 \leq i < j \leq n-1$, by using the results from the previous section. First we obtain the results for 2-error linear complexity and then extend them to the 3-error case.

It is straightforward to see that

$$\mathcal{A}_2(0) = \mathbb{E}_1 \cup \mathbb{E}_2 \cup \{\mathbf{0}\} \quad \text{and} \quad \mathcal{N}_2(0) = \binom{2^n}{2} + 2^n + 1. \tag{58}$$

From Lemmas 2.1 and 3.1 we have

$$\mathcal{A}_2(2^n) = \emptyset \quad \text{and} \quad \mathcal{N}_2(2^n) = 0. \tag{59}$$

From Lemma 3.2 we get

$$\mathcal{A}_2(L) = \emptyset \quad \text{and} \quad \mathcal{N}_2(L) = 0 \quad \text{for} \quad L = 2^n - 2^t, \quad 0 \leq t < n. \tag{60}$$

A characterization of 2^n-periodic binary sequences with fixed 2-error linear complexity L such that $w_H(2^n - L) = 0$ or 1 is given in equations (58)-(60). Next we give the characterization when $w_H(2^n - L) \geq 3$.

For any $1 \leq L < 2^{n-1}$, from Theorem 2.2 we know that for any two sequences $\mathbf{S}, \mathbf{S}' \in \mathcal{A}(L)$, $d_H(\mathbf{S}, \mathbf{S}') \geq 4$. Hence we have

$$\mathcal{A}(L) \cap (\mathcal{A}(L) + \mathbf{E}_t) = \emptyset, \tag{61}$$
$$\mathcal{A}(L) \cap (\mathcal{A}(L) + \mathbf{E}_{i,j}) = \emptyset, \quad \text{and} \tag{62}$$
$$(\mathcal{A}(L) + \mathbf{E}_t) \cap (\mathcal{A}(L) + \mathbf{E}_{i,j}) = \emptyset, \tag{63}$$

for all $\mathbf{E}_t \in \mathbb{E}_1$ and $\mathbf{E}_{i,j} \in \mathbb{E}_2$.

Theorem 4.1. *Let $w_H(2^n - L) \geq 3$ where*

$$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}), \tag{64}$$

for some r_1 and r_2 satisfying $1 \leq r_1 \leq r_2 \leq n-1$. Then

$$\mathcal{A}_2(L) = \mathcal{A}(L) \bigcup \left(\bigcup_{\mathbf{E}_i \in \mathbb{E}_1} (\mathcal{A}(L) + \mathbf{E}_i) \right) \bigcup \left(\bigcup_{\mathbf{E}_{i,j} \in \mathbb{E}_2} (\mathcal{A}(L) + \mathbf{E}_{i,j}) \right). \tag{65}$$

Define the sets

$$\begin{aligned} \mathbb{D}_1(L) &= \{\mathbf{E}_i : 0 \leq i \leq 2^{n-r_1+1} - 1\} \quad \textit{and} \\ \mathbb{D}_2(L) &= \{\mathbf{E}_{i,j} : 0 \leq i < j \leq 2^{n-r_1+1} - 1\}, \end{aligned} \tag{66}$$

where the definitions implicitly depend on L. Define the sets $\mathcal{D}^1(L)$ and $\mathcal{D}^2(L)$ by

$$\mathcal{D}^1(L) = \{\mathbf{E}_{i,i+2^{n-r_1}} : i = u + t2^{n-r_2}, 1 \leq t \leq 2^{r_2-r_1} - 1, \quad \textit{and} \quad 0 \leq u \leq 2^{n-r_2} - 1\} \tag{67}$$

and

$$\begin{aligned}\mathcal{D}^2(L) =&\{\mathbf{E}_{i,j}, \mathbf{E}_{i,j+2^{n-r_1}} : i = u + t_1 2^{n-r_2}, j = u + t_2 2^{n-r_2}, 0 \le t_1 < t_2 \le 2^{r_2-r_1} - 1,\\ &\textit{and} \quad 0 \le u \le 2^{n-r_2} - 1\}.\end{aligned} \tag{68}$$

Consider the set $\overline{\mathcal{D}}(L)$ *formed from the sets in equations* (66), (67), *and* (68) *by*

$$\overline{\mathcal{D}}(L) = \mathbb{D}_2(L) - (\mathcal{D}^1(L) \cup \mathcal{D}^2(L)). \tag{69}$$

Then the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, *and* $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$, *are disjoint and constitute all of* $\mathcal{A}_2(L)$. *Furthermore,*

$$\mathcal{N}_2(L) = \left(\binom{2^{n-r_1+1}}{2} - 2^{n-r_2}(2^{2r_2-2r_1} - 1) + 2^{n-r_1+1} + 1 \right) 2^{L-1}. \tag{70}$$

Proof. Note that any L such that $w_H(2^n - L) \ge 3$ can be expressed as in equation (64). The characterization in equation (65) follows by using $r = 2$ in the hypothesis of Theorem 3.5 and $k = 2$ in equation (55). The rest of the proof deals with determining the disjoint set decomposition of $\mathcal{A}_2(L)$ in equation (65) there by obtaining the expression for $\mathcal{N}_2(L)$.

Case 1: $r_1 = r_2 = 1$
When $r_1 = r_2 = 1$ we have $1 \le L < 2^{n-2}$ and the characterization and counting function are already covered by part 2 of Theorem 3.5 with $r = 2$ and $k = 2$ in equation (56). Also, note that the expression for the counting function in equation (56) with $k = 2$ equals that in equation (70) with $r_1 = r_2 = 1$.

Case 2: $1 = r_1 < r_2$ or $1 < r_1 \le r_2$
First we determine the disjoint sets in $\mathcal{A}(L)[\mathbb{E}_1]$. By equation (64) we have

$$2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}. \tag{71}$$

Using Theorem 3.3 and Lemma 2.3, from equation (71) we have

$$(\mathcal{A}(L) + \mathbf{E}_u) \cap (\mathcal{A}(L) + \mathbf{E}_v) = \emptyset, \quad 0 \le u < v \le 2^{n-r_1+1} - 1, \tag{72}$$

and for $u = 0, \cdots, 2^{n-r_1+1} - 1$,

$$\mathcal{A}(L) + \mathbf{E}_u = \mathcal{A}(L) + \mathbf{E}_{u+t2^{n-r_1+1}}, \quad t = 0, \cdots, 2^{r_1-1} - 1. \tag{73}$$

Thus, from equation (72) there are 2^{n-r_1+1} disjoint sets $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, in $\mathcal{A}(L)[\mathbb{E}_1]$. To obtain the disjoint sets in $\mathcal{A}(L)[\mathbb{E}_2]$, we only have to characterize the disjoint sets in $\mathcal{A}(L)[\mathbb{D}_2(L)]$ because from equation (73) we have $\mathcal{A}(L) + \mathbf{E}_{i,j,i+v2^{n-r_1+1},j+w2^{n-r_1+1}} = \mathcal{A}(L)$, for $0 \le i < j \le 2^{n-r_1+1} - 1$ and $0 \le v, w \le 2^{r_1-1} - 1$.

From Theorem 3.3, we know that $\mathcal{A}(L) + \mathbf{E}_{i,j} = \mathcal{A}(L) + \mathbf{E}_{k,l}$ if and only if there exists a sequence $\mathbf{S} \in \mathcal{A}(L)$ such that $\mathbf{S} + \mathbf{E}_{i,j,k,l} \in \mathcal{A}(L)$. Hence we observe that redundantly counted sets in $\mathcal{A}(L)[\mathbb{D}_2(L)]$ arise if only if there exist integers i, j, k, and l, $0 \le i < j < k < l \le 2^{n-r_1+1} - 1$, that are in the form given in equation (9). So the sets of integers i, j,

k, and l, $0 \leq i < j < k < l \leq 2^{n-r_1+1} - 1$, such that $L(\mathbf{S}_{i,j,k,l}) = L(\mathbf{S})$ for any $\mathbf{S} \in \mathcal{A}(L)$ are thus the i, j, k, and l in the form

$$i = u + g_1 2^{n-r_2}, \quad j = u + g_2 2^{n-r_2}, \quad k = i + 2^{n-r_1}, \quad l = j + 2^{n-r_1}, \tag{74}$$

where

$$0 \leq u \leq 2^{n-r_2} - 1 \quad \text{and} \quad 0 \leq g_1 < g_2 \leq 2^{r_2-r_1} - 1. \tag{75}$$

So for all settings of i and j in equation (74) we have the set equalities

$$\mathcal{A}(L) + \mathbf{E}_{i,j} = \mathcal{A}(L) + \mathbf{E}_{i+2^{n-r_1},j+2^{n-r_1}} \tag{76}$$

and

$$\mathcal{A}(L) + \mathbf{E}_{i,j+2^{n-r_1}} = \mathcal{A}(L) + \mathbf{E}_{i+2^{n-r_1},j}. \tag{77}$$

Also, for each $u = 0, \cdots, 2^{n-r_2} - 1$, we have $2^{r_2-r_1} - 1$ set equalities

$$\mathcal{A}(L) + \mathbf{E}_{u,u+2^{n-r_1}} = \mathcal{A}(L) + \mathbf{E}_{i,i+2^{n-r_1}}, \quad \text{where} \quad i = u + t2^{n-r_2} \tag{78}$$

for $1 \leq t \leq 2^{r_2-r_1} - 1$.

Note that each error vector appearing on the left hand side or right hand side of equations (76) or (77) corresponding to all settings of i and j in equation (74) appears only in one of those equations and does not appear in the set equalities in equation (78). Also note that each error vector appearing on the left hand side or right hand side of set equalities in equation (78) does not appear in left hand side or right hand side of equations (76) and (77). Thus by equation (74), each of the set equalities in equations (76) and (77) results in a redundantly counted set in $\mathcal{A}(L)[\mathbb{D}_2(L)]$. These redundantly counted sets for all settings of i and j in equation (74) are listed as $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \mathcal{D}^2(L)$. Similarly, for each $u = 0, \cdots, 2^{n-r_2} - 1$, the set equalities in equation (78) result in $2^{r_2-r_1} - 1$ redundantly counted sets in $\mathcal{A}(L)[\mathbb{D}_2(L)]$. These redundantly counted sets are listed as $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \mathcal{D}^1(L)$.

Note that any L such that $2^{n-1} \leq L < 2^n$ and $w_H(2^n - L) \geq 3$, satisfies equations (61) and (63). From Lemma 2.3 and equation (71) we have

$$\mathcal{A}(L) \cap (\mathcal{A}(L) + \mathbf{E}_{i,j}) = \emptyset, \quad \mathbf{E}_{i,j} \in \mathbb{D}_2(L). \tag{79}$$

Thus, from equations (65), (61)-(63), (69), (74)-(78), and (79), the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$, are disjoint and constitute all of $\mathcal{A}_2(L)$.

From equations (67) and (68) we get

$$|\mathcal{D}^1(L)| = 2^{n-r_2}(2^{r_2-r_1} - 1) \quad \text{and} \quad |\mathcal{D}^2(L)| = 2^{n-r_2}\left(2\binom{2^{r_2-r_1}}{2}\right). \tag{80}$$

The number of disjoint sets in $\mathcal{A}(L)[\mathbb{E}_2]$ is equal to $|\overline{\mathcal{D}}(L)|$. From equations (69) and (80) we have

$$\begin{aligned} |\overline{\mathcal{D}}(L)| &= |\mathbb{D}_2(L)| - (|\mathcal{D}^1(L)| + |\mathcal{D}^2(L)|) \\ &= \binom{2^{n-r_1+1}}{2} - 2^{n-r_2}\left(2^{r_2-r_1} - 1 + 2\binom{2^{r_2-r_1}}{2}\right). \end{aligned} \tag{81}$$

From Lemma 1.2 we have $|\mathcal{A}(L)| = 2^{L-1}$, $1 \leq L \leq 2^n$. Hence the counting function in equation (70) follows from equations (65), (61)-(63), (72), (79), and (81). This completes the proof of the theorem. □

Next we give the characterization of 2^n-periodic binary sequences with fixed 3-error linear complexity L when $w_H(2^n - L) \neq 2$. Using the characterization we also obtain the corresponding counting function. For convenience we use the notation established in the statement of Theorem 4.1.

It is straightforward to see that

$$\mathcal{A}_3(0) = \mathbb{E}_1 \cup \mathbb{E}_2 \cup \mathbb{E}_3 \cup \{\mathbf{0}\} \quad \text{and} \quad \mathcal{N}_3(0) = \binom{2^n}{3} + \binom{2^n}{2} + 2^n + 1.$$

We also have $\mathcal{A}_3(2^n) = \emptyset$ and $\mathcal{N}_3(2^n) = 0$. From Lemma 3.2 we also get $\mathcal{A}_3(L) = \emptyset$ and $\mathcal{N}_3(L) = 0$ for $L = 2^n - 2^t$, $0 \leq t < n$.

Theorem 4.2. *Let $1 \leq L < 2^n$ be a positive integer such that $w_H(2^n - L) \geq 3$. Then*

$$\mathcal{A}_3(L) = \mathcal{A}_2(L) \bigcup \left(\bigcup_{\mathbf{E}_{i,j,k} \in \mathbb{E}_3} (\mathcal{A}(L) + \mathbf{E}_{i,j,k}) \right). \tag{82}$$

Furthermore, let L be uniquely bounded as

$$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}),$$

for some r_1 and r_2 satisfying $1 \leq r_1 \leq r_2 \leq n-1$. Let $\overline{\mathcal{D}}(L)$ be as in equation (69). Define the sets $\mathbb{D}_3(L)$, $\mathcal{D}^3(L)$, and $\mathcal{E}(L)$ by

$$\mathbb{D}_3(L) = \{\mathbf{E}_{i,j,k} : 0 \leq i < j < k \leq 2^{n-r_1+1} - 1\},$$

$$\begin{aligned} \mathcal{D}^3(L) = \{&\mathbf{E}_{i,j,k}, \mathbf{E}_{i,j,l}, \mathbf{E}_{j,k,l}, \mathbf{E}_{i,k,l} : i = u + g_1 2^{n-r_2}, \quad j = u + g_2 2^{n-r_2}, \\ &k = i + 2^{n-r_1}, \quad l = j + 2^{n-r_1}, \quad 0 \leq g_1 < g_2 < 2^{r_2-r_1}, \\ &\text{and} \quad 0 \leq u \leq 2^{n-r_2} - 1\}, \end{aligned} \tag{83}$$

and

$$\mathcal{E}(L) = \mathbb{D}_3(L) - \mathcal{D}^3(L). \tag{84}$$

Then the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \mathcal{E}(L)$ are disjoint and constitute all of $\mathcal{A}_3(L)$. Furthermore,

$$\mathcal{N}_3(L) = \mathcal{N}_2(L) + \left(\binom{2^{n-r_1+1}}{3} - 4 \cdot 2^{n-r_2} \binom{2^{r_2-r_1}}{2} \right) 2^{L-1}. \tag{85}$$

Proof. The characterization in equation (82) follows by using $r = 2$ in the hypothesis of Theorem 3.5 and $k = 3$ in equation (55). The rest of the proof deals with determining the disjoint set decomposition of $\mathcal{A}_3(L)$ in equation (82) there by obtaining the expression for $\mathcal{N}_3(L)$.

The case when $r_1 = r_2 = 1$, that is, when $1 \leq L < 2^{n-2}$, is covered by part 2 of Theorem 3.5 with $r = 2$ and $k = 3$ in equation (56). It is straightforward to verify that the results using Theorem 3.5 when $r_1 = r_2 = 1$ agree with those stated in this theorem statement.

The rest of the proof handles the case when $r_1 = 1 < r_2$ or $1 < r_1 \leq r_2$. We characterize the disjoint sets in the union given in equation (82). From Theorem 4.1 the disjoint sets in $\mathcal{A}_2(L)$ in equation (65) are $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$. Next we characterize the disjoint sets in $\mathcal{A}(L)[\mathbb{E}_3]$. For this, from equations (72) and (73) we only have to describe the disjoint sets in $\mathcal{A}(L)[\mathbb{D}_3(L)]$. From part 2 of Theorem 2.5 we can see that all sets in $\mathcal{A}(L)[\mathbb{D}_3(L)]$ are disjoint.

Finally, we show that the sets in $\mathcal{A}(L)[\mathbb{D}_3(L)]$ are disjoint from the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$. Since Hamming weights of all sequences in the sets in $\mathcal{A}(L)[\mathbb{D}_3(L)]$ are odd, these sets are disjoint from sets $\mathcal{A}(L)$ and $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$. From Theorem 3.3 a set $\mathcal{A}(L) + \mathbf{E}_i$, $0 \leq i \leq 2^{n-r_1+1} - 1$, is equal to some set $\mathcal{A}(L) + \mathbf{E}_{j,k,l}$, $0 \leq j, k, l \leq 2^{n-r_1+1} - 1$, if and only if there exists a sequence $\mathbf{S} \in \mathcal{A}(L)$ such that $\mathbf{S}_{i,j,k,l} \in \mathcal{A}(L)$. Exactly all such i, j, k, and l are described in equations (74) and (75). From equations (74) and (75), for each $u = 0, \cdots, 2^{n-r_2} - 1$ there are exactly $\binom{2^{r_2-r_1}}{2}$ distinct pairs i, j and hence distinct sets $\{i, j, k, l\}$ such that $0 \leq i < j < k < l \leq 2^{n-r_1+1} - 1$ and $\mathcal{A}(L) + \mathbf{E}_{i,j,k,l} = \mathcal{A}(L)$. For each such distinct set $\{i, j, k, l\}$ we have four set equalities

$$\begin{aligned} &\mathcal{A}(L) + \mathbf{E}_{i,j,k} = \mathcal{A}(L) + \mathbf{E}_l, \quad \mathcal{A}(L) + \mathbf{E}_{i,j,l} = \mathcal{A}(L) + \mathbf{E}_k, \\ &\mathcal{A}(L) + \mathbf{E}_{j,k,l} = \mathcal{A}(L) + \mathbf{E}_i, \quad \text{and} \quad \mathcal{A}(L) + \mathbf{E}_{i,k,l} = \mathcal{A}(L) + \mathbf{E}_j. \end{aligned} \tag{86}$$

Based on the settings of possible i, j, k, and l in equations we note that each error vector with Hamming weight 3 that appears in the set equalities in equation (86) appears in exactly one of them. This leads to four redundantly counted sets for each distinct setting of i, j, k, and l as described above. Thus all the redundantly counted sets in the intersection of $\mathcal{A}(L)[\mathbb{D}_3(L)]$ and $\mathcal{A}(L)[\mathbb{D}_1(L)]$ are $\mathcal{A}(L) + \mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \mathcal{D}^3(L)$. Hence the sets in $\mathcal{E}(L)$ in equation (84) are disjoint from the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$. Using the definition of k-error linear complexity the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{D}_1(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{D}}(L)$, and $\mathcal{A}(L) + \mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \mathcal{E}(L)$, are disjoint and thus constitute all of $\mathcal{A}_3(L)$. Using this, the counting function in equation (85) follows from the definition of $\mathcal{E}(L)$ in equation (84). □

5 Characterization When $w_H(2^n - L) = 2$

We use results in Section 2 and the notation established in Section 4 to obtain the characterization of sequences in $\mathcal{A}(L)$ with fixed 2-error or 3-error linear complexity when $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$, $1 \leq r_1 < r_2 \leq n$.

Theorem 5.1. *Let $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$ for some $1 \leq r_1 < r_2 \leq n$. Define the sets*

$$\begin{aligned} \mathbb{G}_1(L) &= \{\mathbf{E}_i : 0 \leq i \leq 2^{n-r_1+1} - 1\} \quad \textit{and} \\ \mathbb{G}_2(L) &= \{\mathbf{E}_{i,j} : 0 \leq i < j \leq 2^{n-r_1+1} - 1\}. \end{aligned} \tag{87}$$

Consider the sets

$$\mathcal{H}^1(L) = \{\mathbf{E}_{i,i+2^{n-r_1}} : 0 \leq i \leq 2^{n-r_1} - 1\}, \tag{88}$$

$$\begin{aligned} \mathcal{H}^2(L) = \{&\mathbf{E}_{i,j}, \mathbf{E}_{i+2^{n-r_1},j+2^{n-r_1}}, \mathbf{E}_{i,j+2^{n-r_1}}, \mathbf{E}_{j,i+2^{n-r_1}} : 0 \leq i \leq 2^{n-r_1} - 2^{n-r_2} - 1, \\ &j = i + (2t+1)2^{n-r_2}, \quad \textit{and} \quad 0 \leq t \leq 2^{r_2-r_1-1} - 1 - \lceil (\lfloor i/2^{n-r_2} \rfloor)/2 \rceil\}, \end{aligned} \tag{89}$$

and

$$\mathcal{H}^3(L) = \{\mathbf{E}_{i,j}, \mathbf{E}_{i,j+2^{n-r_1}} : i = u + g_1 2^{n-r_2+1}, \quad j = u + g_2 2^{n-r_2+1}, \\ 0 \le g_1 < g_2 \le 2^{r_2-r_1-1} - 1, \quad \textit{and} \quad 0 \le u \le 2^{n-r_2+1} - 1\}. \tag{90}$$

Finally, define the set

$$\overline{\mathcal{H}}(L) = \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L) \cup \mathcal{H}^3(L)). \tag{91}$$

Then the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{G}_1(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)$, *are disjoint and constitute all of* $\mathcal{A}_2(L)$. *That is*

$$\mathcal{A}_2(L) = \mathcal{A}(L) \bigcup \left(\bigcup_{\mathbf{E}_i \in \mathbb{G}_1(L)} (\mathcal{A}(L) + \mathbf{E}_i) \right) \bigcup \left(\bigcup_{\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)} (\mathcal{A}(L) + \mathbf{E}_{i,j}) \right). \tag{92}$$

Furthermore,

$$\mathcal{N}_2(L) = \left(\binom{2^{n-r_1+1}}{2} - 3 \cdot 2^{n+r_2-2r_1-1} + 2^{n-r_1+1} + 1 \right) 2^{L-1}. \tag{93}$$

Proof. By the definition of k-error linear complexity we have

$$\mathcal{A}_2(L) \subseteq \mathcal{A}(L) \bigcup \left(\bigcup_{\mathbf{E}_i \in \mathbb{E}_1} (\mathcal{A}(L) + \mathbf{E}_i) \right) \bigcup \left(\bigcup_{\mathbf{E}_{i,j} \in \mathbb{E}_2} (\mathcal{A}(L) + \mathbf{E}_{i,j}) \right). \tag{94}$$

For the rest of the proof let $\mathbf{S}$ be any sequence in $\mathcal{A}(L)$. By Lemma 1.1 we have $L_2(\mathbf{S}) = L$ and by Lemma 3.4 we get $L_2(\mathbf{S} + \mathbf{E}_i) = L$ for any $\mathbf{E}_i \in \mathbb{E}_1$. Thus

$$\mathcal{A}(L) \bigcup \left(\bigcup_{\mathbf{E}_i \in \mathbb{E}_1} (\mathcal{A}(L) + \mathbf{E}_i) \right) \subseteq \mathcal{A}_2(L). \tag{95}$$

Since $2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}$, equations (72) and (73) also hold in the current setting. Thus there are 2^{n-r_1+1} disjoint sets $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{G}_1(L)$, in $\mathcal{A}(L)[\mathbb{E}_1]$. So we have

$$\bigcup_{\mathbf{E}_i \in \mathbb{E}_1} (\mathcal{A}(L) + \mathbf{E}_i) = \bigcup_{\mathbf{E}_i \in \mathbb{G}_1(L)} (\mathcal{A}(L) + \mathbf{E}_i). \tag{96}$$

Equations (72) and (73) also imply that $\mathcal{A}(L)[\mathbb{E}_2] = \mathcal{A}(L)[\mathbb{G}_2(L)]$. Next we determine which of the sets in $\mathcal{A}(L)[\mathbb{G}_2(L)]$ have sequences that belong to $\mathcal{A}_2(L)$. Equations (35) and (36) describe all distinct four symbol changes i, j, k, and l, $0 \le i < j < k < l \le 2^{n-r_1+1} - 1$, such that $L(\mathbf{S}_{i,j,k,l}) < L$. By equations (35) and (36) it is evident that for each integer u, $0 \le u \le 2^{n-r_1} - 1$, there exist integers v_1 and v_2, $0 \le v_1, v_2 \le 2^{n-r_1+1} - 1$, such that $L(\mathbf{S} + \mathbf{E}_{u,u+2^{n-r_1}} + \mathbf{E}_{v_1,v_2}) < L$. Thus

$$\forall \quad \mathbf{S} \in \mathcal{A}(L) \quad \exists \quad i,j: \quad L_2(\mathbf{S} + \mathbf{E}_{i,j}) < L, \quad \mathbf{E}_{i,j} \in \mathcal{H}^1(L). \tag{97}$$

For each set of four symbol changes in equation (35) there are four distinct sequences $\mathbf{E}_{i,j}$, $\mathbf{E}_{i,j+2^{n-r_1}}$, $\mathbf{E}_{j,i+2^{n-r_1}}$, and $\mathbf{E}_{i+2^{n-r_1},j+2^{n-r_1}}$ in $\mathbb{G}_2(L)$ that when added to $\mathbf{S}$ result in sequences with 2-error linear complexity less than L. That is

$$\forall \quad \mathbf{S} \in \mathcal{A}(L) \quad \exists \quad i,j: \quad L_2(\mathbf{S}+\mathbf{E}_{i,j}) < L, \quad \mathbf{E}_{i,j} \in \mathcal{H}^2(L). \tag{98}$$

By equations (97), (98), and part 2 of Theorem 2.10 we have

$$\forall \quad \mathbf{S} \in \mathcal{A}(L) \quad \text{and} \quad \forall \quad i,j: \quad L_2(\mathbf{S}+\mathbf{E}_{i,j}) = L, \quad \mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L))$$

and thus

$$\begin{aligned} \bigcup_{\mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L))} (\mathcal{A}(L) + \mathbf{E}_{i,j}) \subseteq \mathcal{A}_2(L) \quad \text{and} \\ \bigcup_{\mathbf{E}_{i,j} \in \mathcal{H}^1(L) \cup \mathcal{H}^2(L)} (\mathcal{A}(L) + \mathbf{E}_{i,j}) \cap \mathcal{A}_2(L) = \emptyset. \end{aligned} \tag{99}$$

Next we describe the disjoint sets in $\{\mathcal{A}(L) + \mathbf{E}_{i,j} : \mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L))\}$. From Theorem 3.3, we know that $\mathcal{A}(L) + \mathbf{E}_{i,j} = \mathcal{A}(L) + \mathbf{E}_{k,l}$ if and only if there exists a sequence $\mathbf{R} \in \mathcal{A}(L)$ such that the new sequence $\mathbf{R} + \mathbf{E}_{i,j,k,l} \in \mathcal{A}(L)$. Exactly all such i, j, k, and l are in the form given in equations (28) and (29). From the definitions in equations (88)-(90) we see the following.

1. If $\mathbf{E}_{i,j} \in \mathcal{H}^1(L)$ then $j-i$ is 2^{n-r_1}.
2. If $\mathbf{E}_{i,j} \in \mathcal{H}^2(L)$ then $j-i$ is an odd multiple of 2^{n-r_2}.
3. If $\mathbf{E}_{i,j} \in \mathcal{H}^3(L)$ then $j-i$ is an even multiple of 2^{n-r_2} and $|j-i| < 2^{n-r_1}$.

From these observations we conclude

$$\mathcal{H}^3(L) \cap \mathcal{H}^1(L) \cap \mathcal{H}^2(L) = \emptyset. \tag{100}$$

For each of the $2^{n-r_2+1}\binom{2^{r_2-r_1-1}}{2}$ distinct settings of i and j in equations (28) and (29) the set equalities in equations (76) and (77) hold. By equation (100) and using an argument similar to that used in Theorem 4.1, this implies that there are $2 \cdot 2^{n-r_2+1}\binom{2^{r_2-r_1-1}}{2}$ redundantly counted sets in $\{\mathcal{A}(L) + \mathbf{E}_{i,j} : \mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L))\}$ enumerated as $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \mathcal{H}^3(L)$. So we have

$$\bigcup_{\mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L))} (\mathcal{A}(L) + \mathbf{E}_{i,j}) = \bigcup_{\mathbf{E}_{i,j} \in \mathbb{G}_2(L) - (\mathcal{H}^1(L) \cup \mathcal{H}^2(L) \cup \mathcal{H}^3(L))} (\mathcal{A}(L) + \mathbf{E}_{i,j}). \tag{101}$$

Since $2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}$, by Lemma 2.3 and Theorem 3.3 we can see that

$$\begin{aligned} \mathcal{A}(L) \cap (\mathcal{A}(L) + \mathbf{E}_u) &= \emptyset, \\ \mathcal{A}(L) \cap (\mathcal{A}(L) + \mathbf{E}_{i,j}) &= \emptyset, \quad \text{and} \\ (\mathcal{A}(L) + \mathbf{E}_u) \cap (\mathcal{A}(L) + \mathbf{E}_{i,j}) &= \emptyset, \end{aligned} \tag{102}$$

for all $\mathbf{E}_u \in \mathbb{G}_1(L)$ and $\mathbf{E}_{i,j} \in \mathbb{G}_2(L)$. Thus by equations (94)-(96) and (99)-(102) the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{G}_1(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)$, are disjoint and constitute all of $\mathcal{A}_2(L)$ and the characterization in equation (92) follows.

By equations (88) and (90) we have

$$|\mathcal{H}^1(L)| = 2^{n-r_1} \quad \text{and} \quad |\mathcal{H}^3(L)| = 2 \cdot 2^{n-r_2+1} \binom{2^{r_2-r_1-1}}{2} = 2^{n+r_2-2r_1-1} - 2^{n-r_1}. \tag{103}$$

Each set of four symbol changes in equation (28) contributes four elements to the cardinality of $\mathcal{H}^2(L)$ as specified in equation (89). So by equations (37) and (89) we have

$$|\mathcal{H}^2(L)| = 4 \cdot 2^{n+r_2-2r_1-2} = 2^{n+r_2-2r_1}. \tag{104}$$

Thus by equations (87), (91), (100), (103), and (104) we obtain

$$\begin{aligned} |\overline{\mathcal{H}}(L)| &= |\mathbb{G}_2(L)| - (|\mathcal{H}^1(L)| + |\mathcal{H}^2(L)| + |\mathcal{H}^3(L)|) \\ &= \binom{2^{n-r_1+1}}{2} - \left(2^{n-r_1} + 2^{n+r_2-2r_1} + 2^{n+r_2-2r_1-1} - 2^{n-r_1}\right) \\ &= \binom{2^{n-r_1+1}}{2} - 3 \cdot 2^{n+r_2-2r_1-1}. \end{aligned} \tag{105}$$

The counting function in equation (93) follows from equations (3), (87), (92), and (105). □

For convenience, we use the notation established in the statement of Theorem 5.1 in the next result.

Theorem 5.2. *Let $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$ for some $1 \le r_1 < r_2 \le n$. Define the sets $\mathbb{G}_3(L)$, $\mathcal{M}^1(L)$, and $\mathcal{M}^2(L)$ by*

$$\mathbb{G}_3(L) = \{\mathbf{E}_{i,j,k} : 0 \le i < j < k \le 2^{n-r_1+1}\},$$

$$\begin{aligned} \mathcal{M}^1(L) = \bigcup_{i=0}^{2^{n-r_1}-2^{n-r_2}-1} \{\mathbf{E}_{i,j,k}, \mathbf{E}_{i,j,l}, \mathbf{E}_{i,k,l}, \mathbf{E}_{j,k,l} : \quad & j = i + (2t+1)2^{n-r_2}, \\ & k = i + 2^{n-r_1}, \quad l = j + 2^{n-r_1}, \\ & \text{and} \quad 0 \le t \le 2^{r_2-r_1-1} - 1 - \lceil (\lfloor i/2^{n-r_2} \rfloor)/2 \rceil\}, \end{aligned} \tag{106}$$

and

$$\begin{aligned} \mathcal{M}^2(L) = \bigcup_{u=0}^{2^{n-r_2+1}-1} \{\mathbf{E}_{i,j,k}, \mathbf{E}_{i,j,l}, \mathbf{E}_{i,k,l}, \mathbf{E}_{j,k,l} : i = u + g_1 2^{n-r_2+1}, \quad & j = u + g_2 2^{n-r_2+1}, \\ k = i + 2^{n-r_1}, \quad l = j + 2^{n-r_1}, \quad & \text{and} \quad 0 \le g_1 < g_2 \le 2^{r_2-r_1-1} - 1\}. \end{aligned} \tag{107}$$

Finally, define the set

$$\overline{\mathcal{M}}(L) = \mathbb{G}_3(L) - (\mathcal{M}^1(L) \cup \mathcal{M}^2(L)). \tag{108}$$

Let $\overline{\mathcal{H}}(L)$ be as in equation (91) in Theorem 5.1. Then the sets $\mathcal{A}(L)$, $\mathcal{A}(L)+\mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)$, $\mathcal{A}(L)+\mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \overline{\mathcal{M}}(L)$, are disjoint and constitute all of $\mathcal{A}_3(L)$. That is

$$\mathcal{A}_3(L) = \mathcal{A}(L) \bigcup \left(\bigcup_{\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)} (\mathcal{A}(L)+\mathbf{E}_{i,j}) \right) \bigcup \left(\bigcup_{\mathbf{E}_{i,j,k} \in \overline{\mathcal{M}}(L)} (\mathcal{A}(L)+\mathbf{E}_{i,j,k}) \right). \tag{109}$$

Furthermore,

$$\mathcal{N}_3(L) = \left(\binom{2^{n-r_1+1}}{3} + \binom{2^{n-r_1+1}}{2} - 7 \cdot 2^{n+r_2-2r_1-1} + 2^{n-r_1+1} + 1 \right) 2^{L-1}. \tag{110}$$

Proof. By the definition of k-error linear complexity we have

$$\mathcal{A}_3(L) \subseteq \mathcal{A}(L) \bigcup_{t=1}^{3} \left(\bigcup_{\mathbf{E}_{i_1,\cdots,i_t} \in \mathbb{E}_t} (\mathcal{A}(L)+\mathbf{E}_{i_1,\cdots,i_t}) \right). \tag{111}$$

For the rest of the proof let $\mathbf{S}$ be any sequence in $\mathcal{A}(L)$. By Lemma 1.1 we have $L_3(\mathbf{S}) = L$ and so

$$\mathcal{A}(L) \subseteq \mathcal{A}_3(L). \tag{112}$$

Since $2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}$, equations (72) and (73) also hold in the current setting. Thus there are 2^{n-r_1+1} disjoint sets $\mathcal{A}(L)+\mathbf{E}_i$, $\mathbf{E}_i \in \mathbb{G}_1(L)$, in $\mathcal{A}(L)[\mathbb{E}_1]$ and thus equation (96) holds. By the format of four symbol changes that decrease the linear complexity of $\mathbf{S}$ given in equations (35) and (36), for each $i_1 = 0, \cdots, 2^{n-r_1+1}-1$, there exist three integers i_2, i_3, and i_4 such that $L(\mathbf{S}_{i_1,i_2,i_3,i_4}) < L$, which implies

$$\bigcup_{\mathbf{E}_i \in \mathbb{G}_1(L)} (\mathcal{A}(L)+\mathbf{E}_i) \cap \mathcal{A}_3(L) = \emptyset. \tag{113}$$

By the proof of Theorem 5.1 we know that sequences in sets $\mathcal{A}(L)+\mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \mathbb{E}_2$, with 3-error linear complexity L are given by the disjoint union

$$\bigcup_{\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)} (\mathcal{A}(L)+\mathbf{E}_{i,j}) \subseteq \mathcal{A}_3(L). \tag{114}$$

Equations (72) and (73) imply $\mathcal{A}(L)[\mathbb{E}_3] = \mathcal{A}(L)[\mathbb{G}_3(L)]$. So it is sufficient to determine the sequences in sets $\mathcal{A}(L)+\mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \mathbb{G}_3(L)$, that belong to $\mathcal{A}_3(L)$. For each set of four symbol changes in equation (35) there are four distinct sequences $\mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,l}$, $\mathbf{E}_{i,k,l}$, and $\mathbf{E}_{j,k,l}$ in $\mathbb{G}_3(L)$ that when added to $\mathbf{S}$ result in sequences with 3-error linear complexity less than L. That is

$$\bigcup_{\mathbf{E}_{i,j,k} \in \mathcal{M}^1(L)} (\mathcal{A}(L)+\mathbf{E}_{i,j,k}) \cap \mathcal{A}_3(L) = \emptyset. \tag{115}$$

Equations (28) and (29) describe all i, j, k, and l, $0 \le i < j < k < l \le 2^{n-r_1+1}-1$, such that $L(\mathbf{S}_{i,j,k,l}) = L$. For each set of these four symbol changes we have four set equalities

$\mathcal{A}(L) + \mathbf{E}_i = \mathcal{A}(L) + \mathbf{E}_{j,k,l}$, $\mathcal{A}(L) + \mathbf{E}_j = \mathcal{A}(L) + \mathbf{E}_{i,k,l}$, $\mathcal{A}(L) + \mathbf{E}_k = \mathcal{A}(L) + \mathbf{E}_{i,j,l}$, and $\mathcal{A}(L) + \mathbf{E}_l = \mathcal{A}(L) + \mathbf{E}_{i,j,k}$. By equation (113) this implies that

$$\bigcup_{\mathbf{E}_{i,j,k} \in \mathcal{M}^2(L)} (\mathcal{A}(L) + \mathbf{E}_{i,j,k}) \cap \mathcal{A}_3(L) = \emptyset. \tag{116}$$

By equation (106) for each $\mathbf{E}_{i,j,k} \in \mathcal{M}^1(L)$ we have either $i-j$, $j-k$, or $k-i$ is an odd multiple of 2^{n-r_2}. By equation (107) for each $\mathbf{E}_{i,j,k} \in \mathcal{M}^2(L)$ we have $i-j$, $j-k$, and $k-i$ are all even multiples of 2^{n-r_2}. From this we see that

$$\mathcal{M}^1(L) \cap \mathcal{M}^2(L) = \emptyset. \tag{117}$$

By equations (115), (116), and (117), part 2 of Theorem 2.5 and part 3 of Theorem 2.10, and using the fact that an odd number of changes to $\mathbf{S}$ results in an sequence with linear complexity 2^n, sequences in sets $\mathcal{A}(L) + \mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \mathbb{G}_3(L)$, with 3-error linear complexity L are given by the disjoint union

$$\bigcup_{\mathbf{E}_{i,j,k} \in \mathbb{G}_3(L) - (\mathcal{M}^1(L) \cup \mathcal{M}^2(L))} (\mathcal{A}(L) + \mathbf{E}_{i,j,k}) \subseteq \mathcal{A}_3(L). \tag{118}$$

By equations (111)-(114), (118), and using the fact that odd number of changes to $\mathbf{S}$ result in sequences with linear complexity 2^n, the sets $\mathcal{A}(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j}$, $\mathbf{E}_{i,j} \in \overline{\mathcal{H}}(L)$, $\mathcal{A}(L) + \mathbf{E}_{i,j,k}$, $\mathbf{E}_{i,j,k} \in \overline{\mathcal{M}}(L)$, are disjoint and constitute all of $\mathcal{A}_3(L)$ and the characterization in equation (109) follows.

From equations (28), (35), (37), and (106)-(108) we have

$$\begin{aligned} |\overline{\mathcal{M}}(L)| &= |\mathbb{G}_3(L)| - (|\mathcal{M}^1(L)| + |\mathcal{M}^2(L)|) \\ &= \binom{2^{n-r_1+1}}{3} - \left(4 \cdot 2^{n+r_2-2r_1-2} + 4 \cdot 2^{n-r_2+1} \binom{2^{r_2-r_1-1}}{2}\right) \\ &= \binom{2^{n-r_1+1}}{3} + 2^{n-r_1+1} - 4 \cdot 2^{n+r_2-2r_1-1}. \end{aligned} \tag{119}$$

The counting function in equation (110) follows from equations (3), (105), (109), and (119). □

6 Concluding Remarks

In this paper, we characterized 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity. First we derived some properties of 2^n-periodic binary sequences with fixed linear complexity. We used the Games-Chan algorithm to find the exact form of specific four symbol changes that can be made in a 2^n-periodic sequence so that the resulting sequence has the same linear complexity as the original sequence. Using straightforward algebraic methods we also described four symbol changes to a 2^n-periodic binary sequence so that the resulting sequence has smaller linear complexity than the original sequence. We used these properties to obtain the characterizations and the corresponding counting functions. Here we make some observations based on the counting functions derived in the paper.

Let $\mathcal{N}_{\geq}(L)$, $0 \leq L \leq 2^n$, be the number of 2^n-periodic binary sequences with linear complexity at least L. From Lemma 1.2 we have

$$\mathcal{N}_{\geq}(L) = \left(\frac{2^{2^n - L + 1} - 1}{2^{2^n - L + 1}} \right) 2^{2^n}. \tag{120}$$

Define $f_k(L)$, $1 \leq k \leq 2^n$, by

$$f_k(L) = \frac{\mathcal{N}_k(L)}{\mathcal{N}_{\geq}(L)}. \tag{121}$$

So $f_k(L)$ describes the proportion of sequences with k-error linear complexity L among sequences with linear complexity at least L. For cryptographic purposes we would like to have $f_k(L)$ as high as possible for large L and at least for small k.

By equations (70), (93), (120) and (121) after simplification we obtain

$$f_2(L) = \frac{2^{2n-2r_1+1} + 2^{n-r_1} + 2^{n-r_2} + 1 - 2^{n+r_2-2r_1}}{2^{2^n - L + 1} - 1} \tag{122}$$

when $2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1})$ with $1 \leq r_1 \leq r_2 \leq n-1$ and

$$f_2(L) = \frac{2^{2n-2r_1+1} + 2^{n-r_1} + 1 - 3 \cdot 2^{n+r_2-2r_1-1}}{2^{2^n - L + 1} - 1} \tag{123}$$

when $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$, $1 \leq r_1 < r_2 \leq n$. Using these formulae we find $f_2(L)$ for $L = 2^n - 3$, $2^n - 5$, $2^n - 6$, and $2^n - 7$. When $L = 2^n - 7$, we have $w_H(2^n - L) = 3$ and we can uniquely bound L as $2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1})$ with $r_1 = r_2 = n-2$. Using $L = 2^n - 7$ and $r_1 = r_2 = n-2$ in equation (122) we have $f_2(2^n - 7) = 37/255 \approx 1/7$. When $L = 2^n - 3$, we have $w_H(2^n - L) = 2$ and $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$ with $r_1 = n-1$ and $r_2 = n$. So we have $f_2(2^n - 3) = 5/15 = 1/3$ by equation (123). Similarly we obtain $f_2(2^n - 5) = 13/63 \approx 1/5$ and $f_2(2^n - 6) = 25/127 \approx 1/5$. Using equations (85), (110), (120), and (121) we also obtain corresponding values for $f_3(L)$. Using Theorem 1.3 we determine the corresponding values for $f_1(L)$. All these values are summarized in Table 3. Since the

L	$f_1(L)$	$f_2(L)$	$f_3(L)$
$2^n - 3$	$1/3$	$1/3$	$1/15$
$2^n - 5$	$1/7$	$13/63 \approx 1/5$	$37/63 \approx 1/2$
$2^n - 6$	$9/127 \approx 1/14$	$25/127 \approx 1/5$	$65/127 \approx 1/2$
$2^n - 7$	$9/255 \approx 1/28$	$37/255 \approx 1/7$	$93/255 \approx 1/3$

Table 3: $f_1(L)$, $f_2(L)$, and $f_3(L)$ for large L

number of sequences with high linear complexity is large for 2^n-periodic binary sequences, we see that considerable number of sequences have high linear complexity and high 2-error or 3-error linear complexity.

Using the counting functions derived in the paper statistical properties like expected value and variance can also be considered for the 2-error or 3-error linear complexity of 2^n-periodic binary sequences. The resulting expressions for the expected values are quite complicated and unlikely to yield a simple closed form. However, estimates may be possible. Extension to p^n-periodic sequences over $\mathbb{F}_p$ can also be considered. Similar results for periodic sequences with arbitrary period or periods of other forms are desirable.

Acknowledgements

Thanks to Dr. Andrew Klapper for several helpful suggestions during the preparation of this paper. Thanks to Dr. Zongming Fei for providing office space and resources while researching for this paper.

References

[1] T. W. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland, 1998.

[2] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*. Springer, 1991.

[3] F.-W. Fu, H. Niederreiter, and M. Su. The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity. In G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, editors, *SETA 2006*, volume 4086 of *LNCS*, pages 88–103. Springer.

[4] R. A. Games and A. H. Chan. A fast algorithm for determining the complexity of a pseudo-random sequence with period 2^n. *IEEE Trans. Inform. Theory*, 29(1):144–146, 1983.

[5] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto. A relationship between linear complexity and k-error linear complexity. *IEEE Trans. Inform. Theory*, 46(2):694–698, 2000.

[6] J. L. Massey. Shift register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, 15(1):122–127, 1969.

[7] W. Meidl. On the stability of 2^n-periodic binary sequences. *IEEE Trans. Inform. Theory*, 51(3):1151–1155, 2005.

[8] W. Meidl and H. Niederreiter. Counting functions and expected values for the k-error linear complexity. *Finite Fields and Applications*, 8:142–154, 2002.

[9] W. Meidl and H. Niederreiter. Linear complexity, k -error linear complexity, and the discrete fourier transform. *J. Complexity*, 18(1):87–103, 2002.

[10] W. Meidl and H. Niederreiter. On the expected value of linear complexity and the k-error linear complexity of periodic sequences. *IEEE Trans. Inform. Theory*, 48(11):2817–2825, 2002.

[11] W. Meidl and A. Venkateswarlu. Remarks on the k-error linear complexity of p^n-periodic sequences. *Design, Codes and Cryptography*, 42(2):181–193, 2007.

[12] R. A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer, 1986.

[13] M. Stamp and C. F. Martin. An algorithm for the k-error linear complexity of binary sequences with period 2^n. *IEEE Trans. Inform. Theory*, 39(4):1398–1401, 1993.