

The Distribution of 2^n -Periodic Binary Sequences with Fixed k -Error Linear Complexity

Wenlun Pan^{1,2(✉)}, Zhenzhen Bao^{1,2}, Dongdai Lin¹, 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, baozhenzhen10@gmail.com, {ddlin,liufeng}@iie.ac.cn
² University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. The linear complexity and k -error linear complexity of sequences are important measures of the strength of key-streams generated by stream ciphers. Fu et al. studied the distribution of 2^n -periodic binary sequences with 1-error linear complexity in their SETA 2006 paper. Recently, people have strenuously promoted the solving of this problem from $k = 2$ to $k = 4$ step by step. Unfortunately, it still remains difficult to obtain the solutions for larger k . In this paper, we propose a new sieve method to solve this problem. We first define an equivalence relationship on error sequences and build a relation between the number of sequences with given k -error linear complexity and the number of pairwise non-equivalent error sequences. We introduce the concept of cube fragment and build specific equivalence relation based on the concept of the cube classes to figure out the number of pairwise non-equivalent error sequences. By establishing counting functions for several base cases and building recurrence relations for different cases of k and L , it is easy to manually get the complete counting function when k is not too large. And an efficient algorithm can be derived from this method to solve the problem using a computer when k is large.

Keywords: Sequence · Linear complexity · k -Error linear complexity · Counting function · Cube theory

1 Introduction

The linear complexity of sequence $S = (s_0 s_1 s_2 \dots)$, denoted by $LC(S)$, is defined as the length of the shortest linear feedback shift register (LFSR) that can generate S . Using Berlekamp-Massey algorithm [6], the LFSR that generates a given sequence can be determined by using only the first $2L$ elements of the sequence, where L is the linear complexity of the sequence.

For a positive integer N , the sequence S is called N -periodic if $s_{i+N} = s_i$ for all $i \geq 0$. Denote the set of all N -periodic binary sequence by S^N . For any sequence $S \in S^N$, define the polynomial corresponding to S as

$$S(x) = s_0 + s_1x + s_2x^2 + \dots + s_{N-1}x^{N-1}.$$

Lemma 1 [1]. *The linear complexity of the N -periodic binary sequence S denoted by $LC(S)$ is given by*

$$LC(S) = N - \deg(\gcd(x^N + 1, S(x))).$$

where $S(x) = s_0 + s_1x + s_2x^2 + \dots + s_{N-1}x^{N-1}$ is the corresponding polynomial.

Given a sequence $S \in S^N$ and a number m , where $0 \leq m < N$, we denote the Hamming weight of S and that of m as $w_H(S)$ and $w_H(m)$ which means the number of nonzero elements in S and the number of 1 in the binary representation of m . For any two sequences $S, S' \in S_N$, where $S = (s_0s_1\dots s_{N-1})$, $S' = (s'_0s'_1\dots s'_{N-1})$, we define the summation of the two sequences as $S + S' = (u_0u_1\dots u_{N-1})$, where $u_i = s_i + s'_i$.

For a cryptographically strong sequence, the linear complexity should not decrease drastically if a few symbols are changed. That means the linear complexity should be stable when we change some bits of the stream. This observation gives rise to the concept of k -error linear complexity of sequences which is introduced in [1, 10].

Definition 1 [1, 10]. For any sequence $S \in S^N$, denote the k -error linear complexity of S by $LC_k(S)$ which is given by

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

where $0 \leq k \leq N$ and the sequence E is called the error sequence.

The counting function of a sequence complexity measure gives the number of sequences with a given complexity measure value. 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 [9] determined the counting function of linear complexity for 2^n -periodic binary sequences as follow:

Lemma 2 [9]. *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*

$$\mathcal{N}(0) = 1, \quad \mathcal{A}(0) = \{(00 \cdots 0)\}, \text{ and}$$

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

In this paper, we study the counting function for the number of 2^n -periodic binary sequences with given k -error linear complexity. By using algebraic and combinatorial methods, Fu et al. [2] derived the counting function for the 1-error linear complexity in their SETA 2006 paper. Kavuluru [3, 4] characterized 2^n -periodic binary sequences with given 2-error or 3-error linear complexity and obtained the counting functions. Unfortunately, those results in [3, 4] on the counting function of 3-error linear complexity are not completely correct

[11]. After that, Zhou et al. use sieve method of combinations to sieve sequences $S + E$ with $LC_k(S + E) = L$ in $\mathbf{S} + \mathbf{E}$ where $\mathbf{S} = \{S \in S^N : LC(S) = L\}$, $\mathbf{E} = \{E \in S^N : w_H(E) \leq k\}$ and $\mathbf{S} + \mathbf{E} = \{S + E : S \in \mathbf{S} \text{ and } E \in \mathbf{E}\}$. And they obtained the complete counting functions for $k = 2, 3$ [13]. In the informal publication paper [12], Zhou et al. also study the counting functions for $k = 4, 5$. In the paper [8], Ming Su proposes a novel decomposing approach to study the complete set of error sequences and get the counting function for $k \leq 4$. However, those methods will become very complex when k becomes larger.

In this paper we propose a new sieve method to study this problem. Firstly, we define an equivalence relationship on error sequences and build a relation between the number of sequences with given k -error linear complexity and the number of pairwise non-equivalent error sequences. We propose a sieve process to figure out the number of counted pairwise non-equivalent error sequences. During the sieve process, a concept of cube fragment are used to characterize error sequences and to determine whether an error sequence should be sieved. By using the cube fragment and building specific equivalence relation based on cube classes, and by combinational theory we get the number of pairwise non-equivalent error sequences. By establishing counting functions for several base cases and building recurrence relations for different cases of k and L , it is easy to manually get the complete counting function when k is not too large. And an efficient algorithm can be derived from this method to solve the problem using a computer when k is large. Experiment results got by the implementation of the algorithm are shown in Table 2, which is unfeasible to get by other methods and by native exhaustive method.

Notice that, we analyze error sequences, instead of analyzing the resulted modified sequences which is did in [13]. That contributes to the simplicity of the method. The original cube concepts are introduced to compute the stable k -error linear complexity of periodic sequences in [14]. In this paper, we extend the concept of cubes to cube fragment and cube class to get counting functions.

2 Preliminaries

This section sets up notations and summarizes preliminary facts used in subsequent sections.

Lemma 3 [7]. *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.*

By Lemma 3, modifying only one bit in a binary sequence with periodic 2^n will result in the change of the linear complexity of this sequence. Consequently, we can resolve the problem of characterization of 2^n -periodic binary sequences with given k -error linear complexity into two sub-problems which will be introduced in detail at the end of this section.

Lemma 4 [7]. *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.*

Lemma 4 shows that to decrease the linear complexity of a given 2^n -periodic binary sequence by adding an error sequence, the error sequence must have the same linear complexity with the given sequence.

For a given sequence $S \in S^N$, denote $merr(S) = \min\{k : LC_k(S) < LC(S)\}$ which indicates the minimum value k such that $LC_k < LC(S)$, and which is called the **first descend point** of linear complexity of S . Kurosawa et al. in [5] derived a formula for the exact value of $merr(S)$.

Lemma 5 [5]. *Let S be a nonzero 2^n -periodic binary sequence, then $merr(S) = 2^{w_H(2^n - LC(S))}$.*

Lemma 5 shows a relation between linear complexity and k -error linear complexity of a sequence, that is, we must modify at least $2^{w_H(2^n - LC(S))}$ bits in sequence S to decrease the linear complexity of S .

For a given sequence $S \in S^N$, denote the support set of S by $supp(S)$, which is the set of positions of the nonzero elements in S , that is, $supp(S) = \{i : s_i \neq 0, 0 \leq i < N\}$. And we also call the elements in $supp(S)$ as points. Let $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ and denote $\mathbf{P}(\mathbb{Z}_m)$ the power set of \mathbb{Z}_m which is the set of all subsets of \mathbb{Z}_m , that is $\mathbf{P}(\mathbb{Z}_m) = \{U : U \subseteq \mathbb{Z}_m\}$. Notice that the set $\mathbf{P}(\mathbb{Z}_N)$ is one to one corresponding to S^N . Especially, the empty set in $\mathbf{P}(\mathbb{Z}_N)$ corresponds to the all-zero sequence in S^N . Hence, we define the linear complexity of a set $U \in \mathbf{P}(\mathbb{Z}_N)$ as the linear complexity of the sequence which it is corresponding to.

In [14], the authors use cube theorem to study the stable k -error linear complexity of periodic sequences. In this paper we use support set to define a cube which will be convenient for us to propose the concept of cube fragment and to study the counting functions.

Definition 2. Let u, v be two different none-negative integers, we define the distance between u and v as 2^t and denote $d(u, v) = 2^t$ if $|u - v| = 2^t b$ and $2 \nmid b$.

According to the definition of distance, it can easily be verified that for any different none-negative integers u_1, u_2, u_3 , if $d(u_1, u_2) = d(u_1, u_3)$, then $d(u_2, u_3) > d(u_1, u_2)$, otherwise $d(u_2, u_3) = \min\{d(u_1, u_2), d(u_1, u_3)\}$.

Definition 3. Let U, V be two nonempty subsets of \mathbb{Z}_N , define the distance between U and V as:

$$d(U, V) = \begin{cases} \min\{d(u, v) : u \in U, v \in V\}, & U \cap V = \emptyset \\ 0 & \text{otherwise} \end{cases}.$$

Lemma 6. *Let U, V be two nonempty subsets of \mathbb{Z}_N . If $0 < d(U, V) < \min\{d(U), d(V)\}$, then $U \cap V = \emptyset$ and $d(u, v) = d(U, V)$ for any $u \in U, v \in V$.*

Proof. Because $d(U, V) > 0$, then $U \cap V = \emptyset$. Suppose $d(U, V) = d(u_0, v_0)$ where $u_0 \in U, v_0 \in V$. Then for any $u \in U, v \in V$, according to Definitions 2 and 3, we have $d(u, v_0) = \min\{d(u, u_0), d(u_0, v_0)\} = d(u_0, v_0)$. Then $d(u, v) = \min\{d(u, v_0), d(v_0, v)\} = d(u_0, v_0) = d(U, V)$. \square

Definition 4 (Cube). Let $U = \{u_1, u_2, \dots, u_{2^T}\}$ be a subset of \mathbb{Z}_N .

- In the case of $T = 0$, there is only one point in U and we call U as a 0-cube with sides of length $+\infty$. Denote the set of all 0-cubes by $Cube_{+\infty}$.
- In the case of $T = 1$, there are two points in U and we call U as a 1-cube. If the distance between the two points in U is 2^{i_1} , then we say U is a 1-cube with sides of length $\{2^{i_1}\}$. We denote the set of all 1-cubes with sides of length 2^{i_1} by $Cube_{2^{i_1}}$.
- In the case of $T = 2$, there are four points in U . If U can be decomposed into two disjoint 1-cubes U' and U'' , such that $U', U'' \in Cube_{2^{i_1}}$ and $d(U', U'') = 2^{i_2}$ ($i_1 > i_2$), then we call U as a 2-cube with sides of length $\{2^{i_1}, 2^{i_2}\}$. We denote the set of all 2-cubes with sides of length $\{2^{i_1}, 2^{i_2}\}$ by $Cube_{2^{i_1}, 2^{i_2}}$.
- Generally, in the case of $T > 2$, U has 2^T points. Recursively, if U can be decomposed into two disjoint $(T-1)$ -cubes U' and U'' , such that $U', U'' \in Cube_{2^{i_1}, 2^{i_2}, \dots, 2^{i_{T-1}}}$ and $d(U', U'') = 2^{i_T}$ ($i_1 > i_2 > \dots > i_T$), then we call U as a T -cube. We denote the set of all T -cubes with sides length of $\{2^{i_1}, 2^{i_2}, \dots, 2^{i_T}\}$ by $Cube_{2^{i_1}, 2^{i_2}, \dots, 2^{i_T}}$.

We remark that a cube represents a subset of \mathbb{Z}_N with a special structure and “Cube” represents a class of subsets of \mathbb{Z}_N with the same structure. According to Lemma 1, we can easily know that the linear complexity of a cube with sides of length $\{2^{i_1}, 2^{i_2}, \dots, 2^{i_T}\}$ is $2^n - (2^{i_1} + 2^{i_2} + \dots + 2^{i_T})$.

Example 1. Let set $U = \{1, 2, 5, 6, 18, 22, 49, 53\}$.

As $U = \{1, 5, 49, 53\} \cup \{2, 6, 18, 22\}$ and $\{1, 5, 49, 53\} = \{1, 49\} \cup \{5, 53\}$, $\{2, 6, 18, 22\} = \{2, 18\} \cup \{6, 22\}$, then U is a cube with sides of length $\{16, 4, 1\}$.

Following the notation in [2, 3, 13], we denote by $\mathcal{A}_k(L)$ and $\mathcal{N}_k(L)$ the set of and the number of the sequences in S^{2^n} of which the k -error linear complexity being L , that is

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

When $k = 0$, $\mathcal{A}_k(L)$ and $\mathcal{N}_k(L)$ degenerated to $\mathcal{A}(L)$ and $\mathcal{N}(L)$.

Let us first consider the following trivial cases when $L = 2^n$, $L = 0$ and $k \geq 2^{n-1}$ before a full investigation on $\mathcal{A}_k(L)$ and $\mathcal{N}_k(L)$. When $L = 2^n$, from Lemma 3, we have that for any $k \geq 1$,

$$\mathcal{A}_k(2^n) = \emptyset, \quad \mathcal{N}_k(2^n) = 0.$$

Because only all-zero sequence has 0 linear complexity and only all-one sequence has 1 linear complexity, we always have

$$\mathcal{A}_k(0) = \{S \in S^{2^n} : w_H(S) \leq k\}, \quad \mathcal{N}_k(0) = \sum_{j=0}^k \binom{2^n}{j},$$

and for $k < 2^{n-1}$ we have

$$\mathcal{A}_k(1) = \{S \in S^{2^n} : w_H(S) \geq 2^n - k\}, \quad \mathcal{N}_k(1) = \sum_{j=2^n-k}^{2^n} \binom{2^n}{j} = \sum_{j=0}^k \binom{2^n}{j}.$$

Because a sequence can always be modified to be all-zero or all-one by changing no more than k bits when $k \geq 2^{n-1}$, thus when $k \geq 2^{n-1}$ we have

$$\mathcal{A}_k(1) = \{S \in S^{2^n} : w_H(S) > k\}, \quad \mathcal{N}_k(1) = \sum_{j=k+1}^{2^n} \binom{2^n}{j},$$

$$\mathcal{A}_k(L) = \emptyset, \quad \mathcal{N}_k(L) = 0 \quad \text{for } L \neq 0 \text{ and } 1.$$

Henceforth, we need only consider the cases when $1 < L < 2^n$ and $k < 2^{n-1}$. Thus we suppose $1 < L < 2^n$ and $0 < k < 2^{n-1}$ for the rest of this paper.

For two given sequences $S, S' \in S^{2^n}$, we denote the Hamming distance between the two sequences by $d_H(S, S')$ which represents the number of different bits between the two sequences, that is, $d_H(S, S') = w_H(S + S')$. Then for any sequences $S \in \mathcal{A}_k(L)$, there exists $S' \in \mathcal{A}(L)$ such that $d_H(S, S') \leq k$. Therefore we have

$$\mathcal{A}_k(L) \subseteq \bigcup_{j=0}^k (\mathcal{A}(L) + \mathbf{E}_j)$$

where $\mathbf{E}_j = \{S \in S^{2^n} : w_H(S) = j\}$ and $\mathcal{A}(L) + \mathbf{E}_j = \{S + E : S \in \mathcal{A}(L), E \in \mathbf{E}_j\}$. We denote $\mathbf{E} = \bigcup_{j=0}^k \mathbf{E}_j$.

Similar to [13], we decompose the set $\mathcal{A}_k(L)$ into two subsets based on whether the linear complexity of the sequences equal to its period or not. Let $\mathcal{A}'_k(L)$ and $\mathcal{N}'_k(L)$ respectively denote the set of and the number of 2^n -periodic binary sequences with given k -error linear complexity L ($0 < L < 2^n$) and with linear complexity less than 2^n , that is

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

and let $\mathcal{A}''_k(L)$ and $\mathcal{N}''_k(L)$ respectively denote the set of and the number of 2^n -periodic binary sequences with given k -error linear complexity L ($0 < L < 2^n$) and with linear complexity equal to 2^n , that is

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

Applying Lemma 3, we get

$$\mathcal{A}'_k(L) \subseteq \bigcup_{m=0}^{\lfloor \frac{k}{2} \rfloor} (\mathcal{A}(L) + \mathbf{E}_{2m}), \quad \mathcal{A}''_k(L) \subseteq \bigcup_{m=0}^{\lfloor \frac{k-1}{2} \rfloor} (\mathcal{A}(L) + \mathbf{E}_{2m+1}).$$

In the following, we first study the set $\mathcal{A}'_k(L)$ when k is even and then we will reduce other cases into this case.

3 Characterization of $\mathcal{A}'_k(L)$ When k is even

We first define an equivalence relationship on the error sequences set \mathbf{E} .

Lemma 7 [3]. *Let E and E' be two error sequences in \mathbf{E} . Then*

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

Corollary 1. *Let E and E' be two error sequences in \mathbf{E} . We have that $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$ if and only if there exists $S, S' \in \mathcal{A}(L)$ such that $S + E = S' + E'$.*

Proof. Assume there exists $S, S' \in \mathcal{A}(L)$ such that $S + E = S' + E'$. And suppose the corresponding polynomials of S and S' are $S(x) = (1+x)^{2^n-L}a(x)$, $S'(x) = (1+x)^{2^n-L}b(x)$ respectively where $a(1) = b(1) = 1$ and $\deg(a(x)), \deg(b(x)) < L$. For any sequence S'' in $\mathcal{A}(L)$, suppose the corresponding polynomial of S'' is $S''(x) = (1+x)^{2^n-L}c(x)$ where $c(1) = 1$ and $\deg(c(x)) < L$, we have $S'' + E = S'' + S + S' + E'$. Because $(S'' + S + S')(x) = (1+x)^{2^n-L}(a(x) + b(x) + c(x))$, denote $d(x) = a(x) + b(x) + c(x)$, and $d(1) = 1$, $\deg(d(x)) < L$, we have $S'' + S + S' \in \mathcal{A}(L)$. Therefore we have $S'' + E \in \mathcal{A}(L) + E'$. Similarly, we have $S + E' \in \mathcal{A}(L) + E$ for any S in $\mathcal{A}(L)$. Thus we have $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$. The backward direction is obvious. \square

Definition 5. Let E and E' be two error sequences in \mathbf{E} . We call E and E' equivalent if $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$. And we denote this by $E \sim E'$.

we remark that this equivalence relation is defined under a given linear complexity L . According to Lemma 3, the Hamming weight of equivalent error sequences have the same odd or even parity.

Theorem 1. *Let E and E' be two error sequences in \mathbf{E} . We have $E \sim E'$ if and only if $LC(E + E') < L$.*

Proof. Assume $E \sim E'$, then there exist two sequences $S, S' \in \mathcal{A}(L)$ such that $S + E = S' + E'$. Then we have $LC(E + E') = LC(S + S') < L$.

Assume $LC(E + E') < L$, suppose $E(x) + E'(x) = (E + E')(x) = (1+x)^{2^n-l}b(x)$, where $l < L$ and $b(1) = 1$. For any sequence $S \in \mathcal{A}(L)$, suppose $S(x) = (1+x)^{2^n-L}a(x)$, where $a(1) = 1$. We have $E(x) + S(x) = E'(x) + (1+x)^{2^n-l}a(x) + S(x) = E'(x) + (1+x)^{2^n-L}(a(x) + (1+x)^{L-l}b(x))$. Because $a(x) + (1+x)^{L-l}b(x) = 1$ when $x = 1$, we have $S' \in \mathcal{A}(L)$ where $S'(x) = (1+x)^{2^n-L}(a(x) + (1+x)^{L-l}b(x))$. According to Corollary 1, we have $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$, thus we get $E \sim E'$. \square

Theorem 2. *Let E be an error sequence in \mathbf{E} , then we have*

$$\mathcal{A}(L) + E \subseteq \mathcal{A}_k(L) \text{ or } (\mathcal{A}(L) + E) \cap \mathcal{A}_k(L) = \emptyset.$$

Proof. Assume there exists $S \in \mathcal{A}(L)$ such that $LC_k(S + E) = L$. On account of $LC_k(S + E) = \min_{E' \in \mathbf{E}} LC(S + E + E')$, it follows that $LC(E + E') \neq L$ for any $E' \in \mathbf{E}$, otherwise $LC_k(S + E) < L$. Thus for any $S' \in \mathcal{A}(L)$, we have $LC_k(S' + E) = \min_{E' \in \mathbf{E}} LC(S' + E + E') = \min_{E' \in \mathbf{E}} \max\{LC(S'), LC(E + E')\} \geq L$. Considering that $LC_k(S' + E) \leq LC(S' + E + E) = LC(S') = L$, so $LC_k(S' + E) = L$, that is $\mathcal{A}(L) + E \subseteq \mathcal{A}_k(L)$. So for any $E \in \mathbf{E}$, we have either $\mathcal{A}(L) + E \subseteq \mathcal{A}_k(L)$ or $(\mathcal{A}(L) + E) \cap \mathcal{A}_k(L) = \emptyset$. \square

From the above, we can know that for a given error sequence E , either all of the sequences in $\mathcal{A}(L) + E$ are in $\mathcal{A}_k(L)$ or none of them is in $\mathcal{A}_k(L)$. It follows that to get the value of $\mathcal{N}_k(L)$, we can figure out how many equivalence classes the set \mathbf{E} is split into, and in how many of them an element E leads all of the sequences in $\mathcal{A}(L) + E$ to be in $\mathcal{A}_k(L)$.

For a given $L = 2^n - (2^{n-r_1} + 2^{n-r_2} + \dots + 2^{n-r_T})$, where $0 < r_1 < r_2 < \dots < r_T \leq n$, $T = w_H(2^n - L)$ and $1 \leq T < n$, we define the following cube classes:

$$\begin{aligned} \mathbb{C}_2 &:= \bigcup_{t=1}^{r_1-1} \text{Cube}_{2^{n-t}}, & \mathbf{C}_2 &:= \text{Cube}_{2^{n-r_1}}, \\ \mathbb{C}_4 &:= \bigcup_{t=r_1+1}^{r_2-1} \text{Cube}_{2^{n-r_1}, 2^{n-t}}, & \mathbf{C}_4 &:= \text{Cube}_{2^{n-r_1}, 2^{n-r_2}}, \\ &\vdots & &\vdots \\ \mathbb{C}_{2^T} &:= \bigcup_{t=r_{T-1}+1}^{r_T-1} \text{Cube}_{2^{n-r_1}, 2^{n-r_2}, \dots, 2^{n-r_{T-1}}, 2^{n-t}}, & \mathbf{C}_{2^T} &:= \text{Cube}_{2^{n-r_1}, 2^{n-r_2}, \dots, 2^{n-r_T}}, \end{aligned}$$

and

$$\mathbb{C} := \bigcup_{i=1}^T \mathbb{C}_{2^i}, \quad \mathbf{C} := \mathbf{C}_{2^T}.$$

Furthermore, we denote:

$$\begin{aligned} \mathbf{C}(p) &:= \{U \subseteq \mathbb{Z}_{2^n} : |U| = p, \exists V \in \mathbf{C}, s.t. U \subseteq V\}, \text{ for } 1 \leq p \leq 2^T, \\ \mathbf{C}_{2^i}(p) &:= \{U \subseteq \mathbb{Z}_{2^n} : |U| = p, \exists V \in \mathbf{C}_{2^i}, s.t. U \subseteq V\}, \text{ for } 1 \leq p \leq 2^i \text{ and } 1 \leq i \leq T, \\ \mathbb{C}_{2^i}(p) &:= \{U \subseteq \mathbb{Z}_{2^n} : |U| = p, \exists V \in \mathbb{C}_{2^i}, s.t. U \subseteq V\}, \text{ for } 1 \leq p \leq 2^i \text{ and } 1 \leq i \leq T. \end{aligned}$$

We define $\mathbf{C}_1 := \text{Cube}_{+\infty}$ which represents the set of all sets with only one point. The concepts \mathbf{C}_{2^i} and \mathbb{C}_{2^i} represent classes of cubes with specific sides of length. And the concepts $\mathbf{C}_{2^i}(p)$ and $\mathbb{C}_{2^i}(p)$ represent the sets of all specific fragments of cubes in the cube classes \mathbf{C}_{2^i} and \mathbb{C}_{2^i} , where those cube fragments are all of size p . And we define $\mathbf{C}_{2^i}(p) = \emptyset$, $\mathbb{C}_{2^i}(p) = \emptyset$ if $p > 2^i$.

From the definition of cube fragment, we can easily get the property as follow which means we can splice small cube fragments into larger cube fragments in cube class \mathbf{C} or cube class \mathbb{C} .

Theorem 3. For any $U \in \mathbf{C}(i)$ and $V \in \mathbf{C}(j)$, if $d(U, V) = 2^{n-r_s} < \min\{d(U), d(V)\}$, then $U \cup V \in \mathbf{C}(i+j)$, where $i+j \leq 2^T$ and $1 < s \leq T$.

Proof. According to Lemma 6, it is clear that $U \cap V = \emptyset$. Thus we need only to prove that there exists $W \in \mathbf{C}$ such that $U \cup V \subseteq W$. Observe that $d(U) > 2^{n-r_s}$, we can add $(2^{s-1} - i)$ points to U to construct an $(s-1)$ -cube W_1 with sides of length $\{2^{n-r_1}, 2^{n-r_2}, \dots, 2^{n-r_{s-1}}\}$. Similarly, we can also add $(2^{s-1} - j)$ points to construct an $(s-1)$ -cube W_2 with sides of the same length with that of cube W_1 . If $W_1 \cap W_2 \neq \emptyset$, suppose $w \in W_1 \cap W_2$, $u \in U$, $v \in V$, then we have $d(u, v) \geq \min\{d(w, u), d(w, v)\} \geq 2^{n-r_{s-1}}$ which is contrary to $d(U, V) = 2^{n-r_s}$. Thus $W_1 \cap W_2 = \emptyset$. Then the distance of the two cubes W_1 and W_2 is 2^{n-r_s} and the two cubes can be combined into an s -cube with sides of length $\{2^{n-r_1}, 2^{n-r_2}, \dots, 2^{n-r_s}\}$ and we denote this cube by W . Since $U \cup V \subseteq W$, it follows $U \cup V \in \mathbf{C}(i+j)$. \square

Note that $(2^{s-1} - i)$ and $(2^{s-1} - j)$ are both larger than or equal to 0, otherwise it will contradict the fact that $d(U, V) = 2^{n-r_s} < \min\{d(U), d(V)\}$.

Theorem 3 shows that we can splice small cube fragments into larger cube fragments in cube class \mathbf{C} .

Example 2. Let $L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3})$ where $n = 6$, $r_1 = 1$, $r_2 = 3$ and $r_3 = 6$.

Let set $U_1 = \{1, 33\} \in \mathbf{C}(2)$, $U_2 = \{25, 57\} \in \mathbf{C}(2)$. On account of $d(U_1, U_2) = 8$, therefore $U_1 \cup U_2 \in \mathbf{C}(4)$.

Using the similar argument as in the proof of Theorem 3, we can easily carry out the following corollary. Thus, similarly, we can splice small fragments of cubes into larger fragments of cube in cube class \mathbf{C} .

Corollary 2. Let $U \in \mathbf{C}(i)$ and $V \in \mathbf{C}(j)$, if $d(U, V) = 2^{n-t} < \min\{d(U), d(V)\}$, then $U \cup V \in \mathbf{C}_{2^{s+1}}(i+j)$, where $r_s < t < r_{s+1}$, $1 \leq s < T$, and $i+j \leq 2^{s+1}$.

Example 3. Let $L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3})$ where $n = 6$, $r_1 = 1$, $r_2 = 3$ and $r_3 = 6$.

Let set $U_1 = \{1, 33\} \in \mathbf{C}(2)$, $U_2 = \{17, 49\} \in \mathbf{C}(2)$. On account of $d(U_1, U_2) = 16$, therefore $U_1 \cup U_2 \in \mathbf{C}(4)$.

Having introduced the concepts of cube classes and theorem on the equivalence of two error sequences (Theorem 1), now we give some relations between cubes and sequences.

Lemma 8 [14]. Let S be a binary sequence with period 2^n , and with linear complexity $LC(S) = L = 2^n - (2^{n-r_1} + 2^{n-r_2} + \dots + 2^{n-r_T})$, where $0 < r_1 < r_2 < \dots < r_T \leq n$. Then the support set of sequence S can be decomposed into several disjoint cubes, and only one cube has linear complexity L , other cubes possess distinct linear complexity which are all less than L .

Because any cube in \mathbf{C} has linear complexity L , according to Lemma 4, we have

Corollary 3. *Let V_1, V_2, \dots, V_t be pairwise disjoint cubes in class \mathbf{C} and $V = \bigcup_{j=1}^t V_j$. Then $LC(V) = L$ if t is odd; $LC(V) < L$ for otherwise.*

Theorem 4. *Let E and E' be two error sequences. We have $E \sim E'$ if and only if there exist pairwise disjoint cubes U_1, U_2, \dots, U_d and $V_1, V_2, \dots, V_{d'}$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j'=1}^{d'} V_{j'})$, where $U_j \in \mathbf{C}$, $V_{j'} \in \mathbf{C}$ for $1 \leq j \leq d$, $1 \leq j' \leq d'$ and d' is even.*

Proof. Assume $E \sim E'$, according to Theorem 1, we have $LC(E + E') < L$. Now, we use a sequential construction procedure to prove the forward direction. Suppose $V = \text{supp}(E + E') = \{e_1, e_2, \dots, e_t\}$ where $t = w_H(E + E')$.

1. Sequentially take pair $U_1 = \{e_i, e_j\}$ out from V and put them into a set \mathbb{U}_1 , where $d(e_i, e_j) > 2^{n-r_1}$. Denote the set of the remaining elements by V'_1 . Note that pairs are chosen step by step without replacement.

(a) We know that all those pairs $U_1 = \{e_i, e_j\}$ in \mathbb{U}_1 are cubes in \mathbf{C}_2 and $LC(\mathbb{U}_1) < L$, thus $LC(V'_1) < L$.

(b) We can prove that V'_1 can be expressed in a form that $V'_1 = \bigcup_{j=1}^{d_1} W_{1,j}$ where $d_1 = |V'_1|/2$ and $W_{1,j} \in \mathbf{C}_2$.

Proof.

(i) For any $v, v' \in V'_1$, we have $d(v, v') \leq 2^{n-r_1}$.

(ii) Sequentially take pair $U'_1 = \{e_i, e_j\}$ out from V'_1 and put them into a set \mathbb{U}'_1 , where $d(e_i, e_j) = 2^{n-r_1}$. Denote the set of the remaining elements by V''_1 .

(iii) We know that for all U'_1 in \mathbb{U}'_1 , $LC(U'_1) = 2^n - 2^{n-r_1}$, thus $U'_1 \in \mathbf{C}_2$ and $LC(\mathbb{U}'_1) \leq 2^n - 2^{n-r_1}$.

(iv) We can prove that $V''_1 = \emptyset$. If $V''_1 \neq \emptyset$, as $d(v, v') < 2^{n-r_1}$ for any $v, v' \in V''_1$ then $LC(V''_1) > 2^n - 2^{n-r_1}$ which leads to $LC(V'_1) = LC(\mathbb{U}'_1 + V''_1) = \max\{LC(\mathbb{U}'_1 + V''_1)\} > 2^n - 2^{n-r_1} > L$ which contradict with $LC(V'_1) < L$.

(v) Thus we have derived (b).

2. Sequentially take pair $U_2 = \{W_{1,i}, W_{1,j}\}$ out from V_1 and put them into a set \mathbb{U}_2 , where $d(W_{1,i}, W_{1,j}) > 2^{n-r_2}$. Denote the set of the remaining elements by V'_2 .

(a) We know that all $U_2 = \{W_{1,i}, W_{1,j}\}$ in \mathbb{U}_2 are union set of some disjoint cubes in \mathbf{C}_4 and $LC(\mathbb{U}_2) < L$, thus $LC(V'_2) < L$.

(b) We can prove that V'_2 can be expressed in a form that $V'_2 = \bigcup_{j=1}^{d_2} W_{2,j}$ where $d_2 = |V'_2|/2$ and $W_{2,j} \in \mathbf{C}_4$.

Proof.

(i) For any $1 \leq i < j \leq d_2$, $d(W_{2,i}, W_{2,j}) \leq 2^{n-r_2}$

(ii) Sequentially take pair $U'_2 = \{W_{2,i}, W_{2,j}\}$ out from V'_2 and put them into a set \mathbb{U}'_2 , where $d(W_{2,i}, W_{2,j}) = 2^{n-r_2}$. Denote the set of remaining elements by V''_2 .

- (iii) Similar to the reason why $V_1'' = \emptyset$, we can know V_2'' is also an empty set.
 - (iv) Thus we have derived (b).
3. Recursively, if we sequentially take elements out from V to form $\mathbb{U}_1, \mathbb{U}_2, \dots, \mathbb{U}_T$ step by step like above, where \mathbb{U}_i is union set of some pairwise disjoint cubes in \mathbb{C} and $\mathbb{U}_i \cap \mathbb{U}_j = \emptyset$ for $i \neq j$, and denote the set of remaining elements as V_T' , then V_T' is an empty set or a union set of some pairwise disjoint cubes in \mathbf{C}_{2^T} and $LC(V_T') < L$. Assume $V_T' = \bigcup_{j=1}^{d'} V_j$ where $V_1, V_2, \dots, V_{d'}$ are pairwise disjoint cubes in \mathbf{C} . According to Corollary 3, we have that d' is even. Consequently, we arrive at the conclusion that $\text{supp}(E + E')$ can be expressed as a union of pairwise disjoint cubes of which some are in cube class \mathbb{C} and some are in cube class \mathbf{C} . Besides, the number of cubes in cube class \mathbf{C} is even.

The backward direction of the theorem can easily be proven as following: Assume there exists pairwise disjoint cubes $U_1, U_2, \dots, U_d \in \mathbb{C}$ and $V_1, V_2, \dots, V_{d'}$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j=1}^{d'} V_j)$ where d' is even. Considering $LC(U_j) < L$ for any $1 \leq j \leq d$ and $LC(\bigcup_{j=1}^{d'} V_j) < L$, we have $LC(E + E') < L$, therefore $E \sim E'$. \square

If $E \sim E'$ and $\text{supp}(E + E') = \bigcup_{j=1}^d U_j$ where all U_j are cubes in \mathbb{C}_{2^i} , then we say that E is \mathbb{C}_{2^i} -equivalent to E' and denote this by $E \overset{\mathbb{C}_{2^i}}{\sim} E'$, and for ease of notations we denote this by $E \overset{i}{\sim} E'$.

Theorem 5. *Let $S \in \mathcal{A}(L)$ be a 2^n -periodic binary sequence with linear complexity L , and $E \in \mathbf{E}$ be an error sequence. We have $LC(S + E) < L$ if and only if there exist pairwise disjoint cubes U_1, U_2, \dots, U_d and $V_1, V_2, \dots, V_{d'}$ such that $\text{supp}(E) = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j'=1}^{d'} V_{j'})$, where $U_j \in \mathbb{C}$, $V_{j'} \in \mathbf{C}$ for $1 \leq j \leq d$, $1 \leq j' \leq d'$ and d' is odd.*

Proof. We shall adopt the same procedure as the proof of Theorem 4 to proof this theorem. If $LC(S + E) < L$, then $LC(E) = L$. Suppose $V = \text{supp}(E)$, then we can sequentially take $\mathbb{U}_1, \mathbb{U}_2, \dots, \mathbb{U}_T$ out from V step by step and denote the set of remaining elements in V by V_T' where \mathbb{U}_i are pairwise disjoint cubes in \mathbb{C}_{2^i} and V_T' is a union set of some pairwise disjoint cubes in \mathbf{C}_{2^T} . Suppose $V_T' = \bigcup_{j=1}^{d'} V_j$ where V_j are pairwise disjoint cubes in \mathbf{C} . Because $LC(\bigcup_{j=1}^T \mathbb{U}_j) < L$, then $LC(V_T') = L$. According to Lemma 3, we have that d' is odd.

In the backward direction, $\text{supp}(E) = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j=1}^{d'} V_j)$. Because $LC(\bigcup_{j=1}^d U_j) < L$ and $LC(\bigcup_{j=1}^{d'} V_j) = L$, we have $LC(E) = L$, thus $LC(S + E) < L$. Note that set in $\{\mathbb{U}_1, \mathbb{U}_2, \dots, \mathbb{U}_T\}$ maybe empty set. \square

The above two theorems show that we can decompose the support set of the sequences into some disjoint cubes. Because the characteristic of cubes is simple and clear, now we use it to get the characteristics of sequences.

Let $k = 2M$ ($M \geq 1$) be an positive even number. Throughout this section, if without specially pointing out, we always assume $k = 2M$, $M \geq 1$ and $0 \leq m \leq M$. Recall that $\mathcal{A}'_k \subseteq \bigcup_{m=0}^M (\mathcal{A}(L) + \mathbf{E}_{2m})$, to analysis the size of $\mathcal{A}'_k(L)$, we shall investigate the following sets:

$$\mathcal{A}(L), \mathcal{A}(L) + \mathbf{E}_2, \mathcal{A}(L) + \mathbf{E}_4, \dots, \mathcal{A}(L) + \mathbf{E}_{2M}.$$

Similar to the idea of using the Eratosthenes sieve method to find prime numbers, we use a sieve method to determine the size of the largest set of sequences in $\mathbf{E}' = \bigcup_{m=0}^M \mathbf{E}_{2m}$, in which sequences are pairwise non-equivalent, and in which sequences do not decrease the k -error linear complexity of the resulted sequences when adding them to those sequences in $\mathcal{A}(L)$. In other words, we use a sieve method to count different sequences in $\bigcup_{m=0}^M \mathbf{E}_{2m}$, subjects to the equivalence relationship defined in Definition 5 and are required to preserve the linear complexity of sequences in $\mathcal{A}(L)$. We build the iterative sieve process, which inducts on m for $0 \leq m \leq M$, on the following three steps:

1. Sequentially eliminate the sequences E from \mathbf{E}_{2m} , which satisfy that there exists sequence $E' \in \mathbf{E}_{2m'}$ such that $E' \sim E$, where $0 \leq m' < m$,
2. Sequentially eliminate the sequences E from \mathbf{E}_{2m} , which satisfy that there exists sequence $E' \in \mathbf{E}_{2m}$ such that $E' \sim E$, where $E' \neq E$,
3. Sequentially eliminate the sequences E from \mathbf{E}_{2m} , which satisfy that $LC_k(S + E) < L$ for $S \in \mathcal{A}(L)$.

Note that, $\mathbf{E}_0 = \{(00 \cdots 0)\}$ and $\mathcal{A}(L) + \mathbf{E}_0 = \mathcal{A}(L)$. Thus $\mathcal{A}(L) \cap \mathcal{A}_k(L) = \emptyset$ if $merr(S) = 2^{w_H(N-L)} \leq k$ and $\mathcal{A}(L) \subseteq \mathcal{A}_k(L)$ otherwise.

Step 1 eliminates those sequences from \mathbf{E}_{2m} which equivalent to a sequence with smaller Hamming weight. By this step, the remaining elements in different \mathbf{E}_{2m} , for $0 \leq m \leq M$, will be pairwise non-equivalent. Step 2 eliminates the duplicate sequences within \mathbf{E}_{2m} and Step 3 eliminates those error sequences which satisfy that when adding them to sequences in $\mathcal{A}(L)$, the resulted sequences have k -error linear complexity less than L . When the iterative procedure inducted on m terminates, the remaining sequences in \mathbf{E}' will be pairwise non-equivalent. And all remaining element E in \mathbf{E}' satisfy that $\mathcal{A}(L) + E \subseteq \mathcal{A}_k(L)$.

Next we determine whether or not the sequences in \mathbf{E}_{2m} should be eliminated.

Lemma 9. *Let E be an error sequence in \mathbf{E}_{2m} . If there exists a cube fragment in $\mathbf{C}(\text{Impvalue})$ being subset to $\text{supp}(E)$, then $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$. Where $\text{Impvalue} = m - k/2 + 2^{T-1}$ and $1 \leq \text{Impvalue} \leq 2m$.*

Proof. Assume there exists a set $U \in \mathbf{C}(\text{Impvalue})$, such that $U \subseteq \text{supp}(E)$. Suppose $\text{supp}(E) = U_0 \cup U$ where $U_0 \cap U = \emptyset$. We choose a set \bar{U} from $\{V \subseteq \mathbb{Z}_{2^n} : |V| = 2^t - \text{Impvalue}, V \cup U \in \mathbf{C}\}$. And then construct a sequence E' based on U_0 and \bar{U} , such that $\text{supp}(E') = U_0 \cup \bar{U}$. Because $w_H(E') \leq |U_0| + |\bar{U}| = (2m - \text{Impvalue}) + (2^t - \text{Impvalue}) = k$ and $LC(E + E') = LC(U + \bar{U}) = L$, thus for any $S \in \mathcal{A}(L)$ we have $LC(S + E + E') < L$. It follows that $LC_k(S + E) \leq LC(S + E + E') < L$, thus $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$. \square

Remark that the value of $Impvalue = m - k/2 + 2^{T-1}$ indicates the upper bound of the size of cube fragments in \mathbf{C} contained in an error sequence that counts. In other words, if an error sequence contains a cube fragment in class \mathbf{C} with size equal or larger than $Impvalue$, then we eliminate it.

Theorem 6. *Let $E \in \mathbf{E}_{2m}$ do not contain a cube fragment in $\mathbf{C}(Impvalue)$. There exists $E' \in \mathbf{E}_{2m'}$, such that $E' \sim E$, if and only if there exists a cube fragment in $\mathbb{C}_{2^t}(2^{t-1}+1)$ being subset to $supp(E)$, where $m' < m$ and $1 \leq t \leq T$.*

Proof. Assume there exists a set $U \in \mathbb{C}_{2^t}(2^{t-1}+1)$, such that $U \subseteq supp(E)$, where $1 \leq t \leq T$. Suppose $supp(E) = U_0 \cup U$ where $U_0 \cap U = \emptyset$. We choose a set \bar{U} from $\{V \subseteq \mathbb{Z}_{2^n} : |V| = 2^{t-1} - 1, V \cup U \in \mathbb{C}_{2^t}\}$. And then construct a sequence E' based on U_0 and \bar{U} , such that $U_0 \cup \bar{U} = supp(E')$. As $w_H(E') = |U_0 \cup \bar{U}| \leq |U_0| + |\bar{U}| < |U_0| + |U| = w_H(E)$ and $LC(E + E') = LC(U + \bar{U}) < L$. By Theorem 1, $E \sim E'$. Therefore, we conclude that there exists $E' \in \mathbf{E}_{2m'}$ where $m' < m$, such that $E \sim E'$.

Next, assume $E' \sim E$. From Theorem 4, there exists pairwise disjoint cubes $U_1, U_2, \dots, U_d \in \mathbf{C}$ and $V_1, V_2, \dots, V_{d'} \in \mathbf{C}$ such that $supp(E + E') = \bigcup_{j=1}^d U_j$, where d' is even. If $|supp(E) \cap W| \leq 2^{t-1}$ for all $W \in \mathbb{C}_{2^t}$, where $1 \leq t \leq T$, then the number of elements of any set U_j which comes from $supp(E)$ will be at most half of $|U_j|$. Because $Impvalue = m - k/2 + 2^{T-1} \leq 2^{T-1}$, the number of elements of each cube V_j which comes from E is also at most half of $|V_j|$. Thus $|supp(E)| \leq |supp(E')|$, which is contrary to the fact that $m' < m$. Therefore, there exists a set $U \in \mathbb{C}_{2^t}(2^{t-1}+1)$ such that $U \subseteq supp(E)$. \square

By Theorem 6, for a sequence in \mathbf{E}_{2m} we can determine whether or not there exists a sequence with lower Hamming weight being equivalent to it, and then we eliminate it from \mathbf{E}_{2m} if there exists such equivalent sequence. We denote the set of remaining sequences in \mathbf{E}_{2m} by $\mathbf{E}_{2m}^r = \{E \in \mathbf{E}_{2m} : \nexists E' \in \mathbf{E}_{2m'}, m' < m, \text{ s.t. } E' \sim E \text{ and } \nexists U \in \mathbf{C}(Impvalue) \text{ s.t. } U \subseteq supp(E)\}$. As a result, we have $\mathcal{A}'_k(L) \subseteq \bigcup_{m=0}^M (\mathcal{A}(L) + \mathbf{E}_{2m}^r)$ and $(\mathcal{A}(L) + \mathbf{E}_{2m}^r) \cap (\mathcal{A}(L) + \mathbf{E}_{2m'}^r) = \emptyset$, for $0 \leq m < m' \leq M$.

Similarly, for a given error sequence we can determine whether or not there exists an error sequence with same Hamming weight equivalent to it.

Theorem 7. *Let E be an error sequence in \mathbf{E}_{2m}^r . Then there exists $E' \in \mathbf{E}_{2m}$, $E' \neq E$, such that $E' \sim E$, if and only if there exists a cube fragment in $\mathbb{C}_{2^t}(2^{t-1})$ being subset to $supp(E)$, where $1 \leq t \leq T$.*

Proof. The proof is similar to that of Theorem 6. Assume there exists a set $U \in \mathbb{C}_{2^t}(2^{t-1})$ such that $U \subseteq supp(E)$, and suppose $supp(E) = U_0 \cup U$ where $U_0 \cap U = \emptyset$. We choose a set \bar{U} from $\{V \subseteq \mathbb{Z}_{2^n} : |V| = 2^{t-1}, U \cup V \in \mathbb{C}_{2^t}\}$. And then construct a sequence E' based on U_0 and \bar{U} , such that $supp(E') = U_0 \cup \bar{U}$. We have $w_H(E') = 2m$. Otherwise we have $U_0 \cap \bar{U} \neq \emptyset$, which follows that $(U_0 \cap \bar{U}) \cup U \subseteq supp(E)$ which is contrary to $E \in \mathbf{E}_{2m}^r$. Therefore, $LC(E + E') = LC(U + \bar{U}) < L$. Thus, we conclude that there exists $E' \in \mathbf{E}_{2m}$ such that $E' \sim E$.

Next, assume $E \sim E'$, according to Theorem 4, there exist pairwise disjoint cubes $U_1, U_2, \dots, U_d \in \mathbb{C}$ and $V_1, V_2, \dots, V_{d'} \in \mathbb{C}$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j=1}^{d'} V_j)$. If $|\text{supp}(E) \cap W| < 2^{t-1}$ for any $W \in \mathbb{C}_{2^t}$, where $1 \leq t \leq T$, then the number of elements of any cube U_j coming from $\text{supp}(E)$ is smaller than half of $|U_j|$. The number of elements of any cube V_j coming from $\text{supp}(E)$ is at most half of $|V_j|$, which leads to $w_H(E') > w_H(E)$. So there exists $U \in \mathbb{C}_{2^t}(2^{t-1})$ such that $U \subseteq \text{supp}(E)$. \square

We note that, given $E \in \mathbf{E}_{2m}^r$, and $E' \in \mathbf{E}_{2m}$, if $E' \sim E$, then it is easy to know that $E' \in \mathbf{E}_{2m}^r$.

By Theorem 7, we can determine whether the sequences in \mathbf{E}_{2m}^r have equivalent sequences with the same Hamming weight and then we can eliminate those redundant sequences and only keep those which are pairwise non-equivalent.

According to Lemma 9, for any error sequence E in \mathbf{E}_{2m} , if there exists a set $U \in \mathbf{C}(\text{Impvalue})$ such that $U \subseteq \text{supp}(E)$, then $(\mathcal{A}(L) + E) \cap \mathcal{A}_k(L) = \emptyset$. In fact, for error sequences being in \mathbf{E}_{2m}^r , it is a necessary and sufficient condition.

Theorem 8. *Let E be an error sequence in \mathbf{E}_{2m}^r . Then $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$, if and only if there exists a cube fragment in $\mathbf{C}(\text{Impvalue})$ being subset to $\text{supp}(E)$, where $\text{Impvalue} = m - k/2 + 2^{T-1}$ and $1 < \text{Impvalue} \leq 2m$.*

Proof. The proof of the sufficiency is same as that of Lemma 9. Here, we only prove the necessity. Assume $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$, then there exist $E' \in \mathbf{E}$ such that $LC(E + E') = L$. From Theorem 5, there exist pairwise disjoint cubes $U, U_1, U_2, \dots, U_d \in \mathbb{C}$ and $V_1, V_2, \dots, V_{d'} \in \mathbb{C}$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^d U_j) \cup (\bigcup_{j=1}^{d'} V_j)$, where d' is odd. Let $W = \text{supp}(E) \cap \text{supp}(E')$ and $W_1 = (\text{supp}(E) - W) \cap (\bigcup_{j=1}^{d'} V_j)$, $W_2 = (\text{supp}(E) - W) \cap (\bigcup_{j=1}^d U_j)$, $W'_1 = (\text{supp}(E') - W) \cap (\bigcup_{j=1}^{d'} V_j)$, $W'_2 = (\text{supp}(E') - W) \cap (\bigcup_{j=1}^d U_j)$. Then $W_1 \cup W'_1 = \bigcup_{j=1}^{d'} V_j$, $W_2 \cup W'_2 = \bigcup_{j=1}^d U_j$. According to the proof of Theorem 6, the number of elements of any cube U_j , which come from E , is at most half of $|U_j|$, thus $|W_2| \leq |W'_2|$. Therefore $2m - |W_1| - |W| \leq |\text{supp}(E')| - |W'_1| - |W|$, it follows that $2m - |W_1| \leq |\text{supp}(E')| - (d' \cdot 2^T - |W_1|)$ and $|W_1| \geq m - |\text{supp}(E')|/2 + d' \cdot 2^{T-1} \geq d' \cdot (m - k/2 + 2^{T-1})$. This implies that there exists $U' \subseteq V_1$ and $U' \in \mathbf{C}(\text{Impvalue})$ such that $U' \subseteq \text{supp}(E)$. \square

We remark that if $\text{Impvalue} = m - k/2 + 2^{T-1} \leq 1$, then for any $E \in \mathbf{E}_{2m}^r$, there exists a $U \in \mathbf{C}(1)$ such that $\text{supp}(E) \cap U = U$, which follows $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$, that is, $(\mathcal{A}(L) + \mathbf{E}_{2m}^r) \cap \mathcal{A}'_k(L) = \emptyset$. If $\text{Impvalue} > 2m$, then for any $E \in \mathbf{E}_{2m}^r$, there does not exist $U \in \mathbf{C}(\text{Impvalue})$ such that $\text{supp}(E) \cap U = U$, which follows $(\mathcal{A}(L) + E) \subseteq \mathcal{A}'_k(L)$, that is, $(\mathcal{A}(L) + \mathbf{E}_{2m}^r) \subseteq \mathcal{A}'_k(L)$.

For a given error sequence E , based on Theorem 3 and Corollary 2, we can easily identify the support set of E whether contains a specific cube fragment in cube class \mathbf{C} or \mathbb{C}_{2^i} where $1 \leq i \leq T$ by spicing small fragments of cubes to larger one.

Theorems 6, 7 and 8 characterize the sequences in \mathbf{E}_{2m} which we should eliminate. After eliminating those error sequences using the above sieve process, we denote the set of remaining sequences in \mathbf{E}_{2m} by

$$\mathbf{E}_{2m}^R := \{E \in \mathbf{E}_{2m}^r : \mathcal{A}(L) + E \subseteq \mathcal{A}'_k(L) \text{ and } \nexists E' \in \mathbf{E}_{2m}, \text{ s.t. } E' \sim E \text{ where } E' \neq E\}.$$

Consequently, we have

$$\mathcal{A}'_k(L) = \bigcup_{m=0}^M (\mathcal{A}(L) + \mathbf{E}_{2m}^R) \text{ and } (\mathcal{A}(L) + \mathbf{E}_{2m}^R) \cap (\mathcal{A}(L) + \mathbf{E}_{2m'}^R) = \emptyset, \text{ for } 0 \leq m < m' \leq M.$$

Denote by $NE_{2m}(k, T)$ the size of \mathbf{E}_{2m}^R where k is the number of errors and $T = w_H(2^n - L)$. Then we have that the number of sequences with k -error linear complexity L and linear complexity less than 2^n is

$$\mathcal{N}'_k(L) = \left(\sum_{m=0}^{k/2} NE_{2m}(k, T) \right) \cdot 2^{L-1}.$$

In the following we discuss the value of $NE_{2m}(k, T)$ in different cases.

Theorem 9. *Let $NE_{2m}(k, T)$ be the size of \mathbf{E}_{2m}^R as defined above, we have $NE_{2m}(k, T) = NE_{2m}(k+2, T)$ for $2m \leq k < 2^T - 2m - 2$ and $NE_{2m}(k, T) = NE_{2m}(k, T+1)$ for $2m \leq k < 2^T - 2m$.*

Proof. If $2m \leq k < 2^T - 2m - 2$, then $m - \frac{k+2}{2} + 2^{T-1} > 2m$. According to Theorem 8, we have that $\mathbf{E}_{2m} + \mathcal{A}(L) \subseteq \mathcal{A}'_k(L)$. Because $2m < 2^T - 2m - 2$, we have $2m < 2^{T-1} - 1$. Thus there does not exist error sequences in \mathbf{E}_{2m} being \mathbb{C}_{2^T} -equivalent to E . Therefore, we have $NE_{2m}(k, T) = NE_{2m}(k+2, T)$. Similarly, we have $NE_{2m}(k, T) = NE_{2m}(k, T+1)$ for $2m \leq k < 2^T - 2m$. \square

Note that, the equal between $NE_{2m}(k, T)$ and $NE_{2m}(k', T')$ means they have the same form. For example, let $L_1 = 2^n - (2^{n-r_1} + 2^{n-r_2} + \dots + 2^{n-r_T})$ and $L_2 = 2^n - (2^{n-r'_1} + 2^{n-r'_2} + \dots + 2^{n-r'_t} + 2^{n-r'_{t+1}})$, if $2m < k < 2^T - 2m$, then $NE_{2m}(k, T) = NE_{2m}(k, T+1)$ means $NE_{2m}(k, T)$ is a function of $m, k, r_1, r_2, \dots, r_t$ and $NE_{2m}(k, T+1)$ is a function of $m, k, r'_1, r'_2, \dots, r'_t$ where $t \leq T$, and the two functions have the same form on different parameters.

Considering $Impvalue = m - k/2 + 2^{T-1}$, according to Theorem 8, when $m = 0$ or $m > 0$ and $T = 1$, we have the following theorem:

Theorem 10. *Let $NE_{2m}(k, T)$ be the size of \mathbf{E}_{2m}^R as defined above, when $m = 0$, we have*

$$NE_0(k, T) = \begin{cases} 1 & \text{if } k < 2^T, \\ 0 & \text{otherwise} \end{cases} \quad \text{and } NE_{2m}(k, 1) = 0.$$

Theorem 11. *Let $NE_{2m}(k, T)$ be the size of \mathbf{E}_{2m}^R as defined above, when $T = 2$, we have*

$$NE_{2m}(k, 2) = \begin{cases} 2^{2m} \sum_{y=1}^{2m} 2^y \binom{2^{n-r_2}}{y} f_1(2m, y) & \text{if } k=2m, \\ 0 & \text{otherwise,} \end{cases}$$

where $f_1(x, y) := \sum_{\{m_1^{t_1}, \dots, m_s^{t_s}\} \in P(x, y)} \binom{x}{t_1, \dots, t_s} \cdot \prod_{i=0}^s \left(\binom{2^{r_2-r_1-1}}{m_i} / 2^{m_i-1} \right)^{t_i}$, and $P(x, y) = \{\{m_1^{t_1}, \dots, m_s^{t_s}\} : \sum_{i=1}^s t_i m_i = x, \sum_{i=1}^s t_i = y, t_i > 0, m_1 < m_2 < \dots < m_s\}$. We define $f_1(0, 0) = 1$, $f_1(x, 0) = 0$ and $f_1(0, y) = 0$ for $x, y > 0$.

Note that, $P(x, y)$ is the set of all possible partition of x into y parts. The set $\{m_1^{t_1}, \dots, m_s^{t_s}\}$ represent the multiset $\{m_1, \dots, m_1, m_2, \dots, m_2, \dots, m_s, \dots, m_s\}$ where the multiplicity of m_i is t_i for $1 \leq i \leq s$.

Proof. Firstly, we calculate the number of error sequences in \mathbf{E}_{2m} with specific structure by combinational theory. Then we figure out the number of error sequences which equivalent to those which have specific structures. And at last, we can get the size of \mathbf{E}_{2m}^R .

Let E be an error sequence in \mathbf{E}_{2m}^R . The support set of E can be regard as a union set of $2m$ cubes U_1, U_2, \dots, U_{2m} where $U_j \in \mathbf{C}_2(1)$ for $1 \leq j \leq 2m$. We can know that $d(U_i, U_j) \leq 2^{n-r_1}$, otherwise there exists a cube fragment in $\mathbf{C}_2(2)$ being subset to the support set of E which leading to $E \notin \mathbf{E}_{2m}^R$ according to Theorem 8. When $k = 2m$, we have $Impvalue = 2$, that is, the support set of E must not contain a cube fragment in $\mathbf{C}_{2r}(2)$. Thus, $d(U_i, U_j) < 2^{n-r_1}$ for $1 \leq i < j \leq 2m$. We classify those cubes U_1, U_2, \dots, U_{2m} as follow:

$$W(U_j) = \{U_j\} \cup \{U_s : d(U_s, U_j) > 2^{n-r_2}, 1 \leq s \leq 2m\}.$$

Suppose $\{W(U_j) : 1 \leq j \leq 2m\} = \{W_j : 1 \leq j \leq y\}$, that is, there are y different classes. And suppose the multiset $\{|W_j| : 1 \leq j \leq y\}$ equal to $\{m_1, \dots, m_1, m_2, \dots, m_2, \dots, m_s, \dots, m_s\}$ where the multiplicity of m_j is t_j for $1 \leq j \leq s$ and for simplify we denote it by $p = \{m_1^{t_1}, \dots, m_s^{t_s}\}$. Because $Impvalue = 2$, we have $d(W_i, W_j) < 2^{n-r_2}$. By combinational theory, we can get the number of error sequences in \mathbf{E}_{2m} which have the same structure as E is

$$\alpha = (2^{r_1-1})^{2m} \cdot 2^{2m} \cdot \prod_{j=1}^s \binom{2^{r_2-r_1-1}}{m_j}^{t_j} \cdot \binom{y}{t_1, t_2, \dots, t_s} \cdot 2^y \cdot \binom{2^{n-r_2}}{y}.$$

We say an error sequence E' have the same structure as E if E' could also be decomposed into $2m$ cube fragments $U'_1, U'_2, \dots, U'_{2m}$ where $U'_j \in \mathbf{C}_2(1)$ for $1 \leq j \leq 2m$, and those cube fragments can be also classified into y categories $W'_j, 1 \leq j \leq y$, and the set of the size of those categories is also p , that is, $\{|W'_j| : 1 \leq j \leq y\} = p$. Note that, if E' have the same structure as E then $\mathcal{A}(L) + E' \subseteq \mathcal{A}'_k(L)$.

Next we consider the number of error sequences that equivalent to E . For each U_j , suppose $U_j = \{u\}$, we can construct 2^{r_1-1} error sequence \mathbf{C}_2 -equivalent to E by replacing the point u by u' where $u' \equiv u \pmod{2^{n-r_1+1}}$. Thus we can find $(2^{r_1-1})^{2m}$ error sequences \mathbf{C}_2 -equivalent to E . For each W_j , suppose $|W_j| = m_0$

and $W_j = \{u_1, u_2, \dots, u_{m_0}\}$, we can construct an error sequence \mathbb{C}_4 -equivalent to E by replacing any two point u_{i_1}, u_{i_2} in W_j by u'_{i_1}, u'_{i_2} where $d(u'_{i_t}, u_{i_t}) = 2^{n-r_1}$ for $t = 1, 2$. And we can know that the constructed two error sequences which based on modifying the same two points will be \mathbb{C}_2 -equivalent. Thus we can construct $\binom{m_0}{0} + \binom{m_0}{2} + \dots + \binom{m_0}{2\lfloor m_0/2 \rfloor} = 2^{m_0-1}$ error sequences \mathbb{C}_4 -equivalent to E based on U_j and the total number of error sequences in \mathbf{E}_{2m} which \mathbb{C}_4 -equivalent to E is $\prod_{j=1}^s (2^{m_j-1})^{t_j}$.

Notice that, all of the constructed error sequences have the same structure as E and it is easy to verify that if an error sequence in \mathbf{E}_{2m} equivalent to E then it must be having the same structure. Therefore, the number of error sequences in \mathbf{E}_{2m}^R that have the same structure as E is

$$\alpha / (2^{r_1-1})^{2m} / \prod_{j=1}^s (2^{m_j-1})^{t_j} = 2^{2m+y} \binom{2^{n-r_2}}{y} \binom{y}{t_1, t_2, \dots, t_s} \prod_{j=1}^s \left(\binom{2^{r_2-r_1-1}}{m_j} / 2^{m_j-1} \right)^{t_j}.$$

So we sum the number of error sequences with different structures and get the total number of error sequences in \mathbf{E}_{2m}^R when $T = 2$ and $k = 2m$ is

$$NE_{2m}(2m, 2) = 2^{2m} \sum_{y=1}^{2m} 2^y \binom{2^{n-r_2}}{y} f_1(2m, y)$$

where $f_1(x, y)$ is as above defined.

When $k > 2m$, we have $Impvalue = m - k/2 + 2^{T-1} \leq 1$, thus $NE_{2m}(k, 2) = 0$. \square

Note that, when k is not very large, the form of function $f_1(x, y)$ can be very simple. For example, $f_1(5, 4) = 2^{4r_2-4r_1-4}(2^{r_2-r_1-1} - 1)$. From the proof of Theorem 11, we can know that it is easy to get the total number of error sequences with the same structure and determine the number of error sequences which equivalent to it for a given error sequence with specific structure. Using a similar method, we can get:

Theorem 12. Let $NE_{2m}(k, T)$ be the size of \mathbf{E}_{2m}^R as defined above, when $T = 3$, we have

$$NE_{2m}(k, 3) = \begin{cases} 0 & \text{if } k > 2m + 4, \\ 2^{2m} \sum_{y_1=1}^{2m} \sum_{y_2=1}^{y_1} 2^{y_1+y_2} \binom{2^{n-r_3}}{y_2} f_1(2m, y_1) f_2(y_1, y_2) & \text{if } k = 2m + 4, \\ NE_{2m}(2m + 4, 3) + \Delta_1(2m) & \text{if } k = 2m + 2, \\ NE_{2m}(2m + 2, 3) + \Delta_2(2m) & \text{if } k = 2m, \end{cases}$$

where

$$\begin{aligned} \Delta_1(2m) = & \sum_{x, y, x_i, y_i \geq 0} 2^{2m-x_1+x_2+y+y_2-2y_3} \binom{x}{x_1} \binom{x_2 \cdot 2^{r_3-r_2-1} - x}{y-y_1} \binom{2^{n-r_3}}{x_2, y_3, y_2-2y_3} g(x, x_2) \cdot \\ & f_1(2m - 2x_1, 2x - 2x_1 + y) f_2(y_1, y_2) \\ & + \sum_{y=2}^{2m} \sum_{y_2=2}^y \sum_{y_3=1}^{\lfloor \frac{y_2}{2} \rfloor} 2^{2m+y+y_2-2y_3} \binom{2^{n-r_3}}{y_3, y_2-2y_3} f_1(2m, y) f_2(y, y_2), \end{aligned}$$

$$\begin{aligned}
\Delta_2(2m) = & \sum_{x, y, z, x_i, y_i, z_i \geq 0} 2^{2m-y_1+y_2-y_3+z+z_3-2z_4} \binom{y}{y_1} \binom{y_2 \cdot 2^{r_3-r_2-1} - y}{z_2} \\
& \binom{2^{n-r_3}}{x, y_3, y_2 - y_3, z_4, z_3 - y_3 - 2z_4} \\
& f_1(2m - 2x - 2y_1, x + 2y - 2y_1 + z) f_2(z - z_1 - z_2, z_3) g(y, y_2) h(x, z_1) + \\
& \sum_{y, z, y_i, z_i \geq 0} 2^{2m-y_1+y_2-y_3+z+z_3-2z_4} \binom{y}{y_1} \binom{y_2 \cdot 2^{r_3-r_2-1} - y}{z_2} \\
& \binom{2^{n-r_3}}{y_3, y_2 - y_3, z_4, z_3 - y_3 - 2z_4} \\
& f_1(2m - 2y_1, 2y - 2y_1 + z) f_2(z - z_2, z_3) g(y, y_2).
\end{aligned}$$

$$\begin{aligned}
f_2(x, y) &:= \sum_{\{m_1^{t_1}, \dots, m_s^{t_s}\} \in P(x, y)} \binom{x}{t_1, \dots, t_s} \cdot \prod_{i=0}^s \binom{2^{r_3-r_2-1}}{m_i}^{t_i} \\
g(x, y) &:= \sum_{\{m_1^{t_1}, \dots, m_s^{t_s}\} \in P(x, y)} \binom{x}{t_1, \dots, t_s} \cdot \prod_{i=0}^s \left(\binom{2^{r_3-r_2-1}}{m_i} / 2^{m_i-1} \right)^{t_i} \\
h(x, y) &:= \sum_{\{m_1^{t_1}, \dots, m_s^{t_s}\} \in P(x, y)} \binom{x}{t_1, \dots, t_s} \cdot \prod_{i=0}^s \binom{2^{r_3-r_2-1}}{m_i + 1}^{t_i}
\end{aligned}$$

Note, $\Delta_1(2m)$ represents the number of error sequences in \mathbf{E}_{2m}^R of which the support set contains a cube fragment in $\mathbf{C}_{2^T}(2)$ but not contains a cube fragment in $\mathbf{C}_{2^T}(3)$. And $\Delta_2(2m)$ represents the number of error sequences in \mathbf{E}_{2m}^R of which the support set contains a cube fragment in $\mathbf{C}_{2^T}(3)$ but not contains a cube fragment in $\mathbf{C}_{2^T}(4)$. And the upper bounds of those parameters x, y, z, x_i, y_i, z_i in the summation are determined in the expressions. For example, in $\Delta_1(2m)$, we can get $0 \leq x_1 \leq m$ to make $f_1(2m - 2x_1, 2x - 2x_1 + y) \neq 0$.

According to Theorem 10–12, we can get the counting function $\mathcal{N}'_k(L)$ for any k when $T = w_H(2^n - L) \leq 3$.

Corollary 4. *Let $\mathcal{N}'_k(L)$ be the number of sequences with k -error linear complexity L and linear complexity less than 2^n . Then we have*

$$\mathcal{N}'_k(L) = \begin{cases} 0 & \text{if } L = 2^n - 2^{n-r_1}, \\ (2^k \sum_{y=1}^k 2^y \binom{2^{n-r_2}}{y} f_1(k, y)) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2}), \\ (\sum_{i=0}^2 NE_{k-4+2i}(k+2i, 3) \\ + \Delta_1(k-2) + \Delta_1(k) + \Delta_2(k)) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3}) \end{cases}$$

where $NE_{k-4+2i}(k+2i, 3)$, $\Delta_1(k)$, $\Delta_2(k)$ are given in Theorem 12.

For $k \in \{2, 4, 6\}$, according to Theorem 9–12, we can get Table 1 directly except for the value of b_4 and c_3 .

In Table 1: $a_1 = 2^{n-r_1}(2^{n-r_1+1} - 3 \cdot 2^{r_2-r_1-1} - 1)$, $a_2 = a_1 - 2^{n+r_3-2r_1}$, $a_3 = a_1 + 2^{n-r_2+1} + 2^{n+r_2-2r_1}$, $b_1 = \sum_{y=1}^4 2^{y+4} \binom{2^{n-r_2}}{y} f_1(4, y)$, $b_2 =$

Table 1. NE_{2m} for $k \in \{2, 4, 6\}$

NE_{2m}	NE_0			NE_2			NE_4		NE_6
$T \backslash k$	2	4	6	2	4	6	4	6	6
1	0	0	0	0	0	0	0	0	0
2	1	0	0	a_1	0	0	b_1	0	c_1
3	1	1	1	a_3	a_3	a_2	b_3	b_2	c_2
4	1	1	1	a_3	a_3	a_3	b_4	b_4	c_3
...
n	1	1	1	a_3	a_3	a_3	b_4	b_4	c_3

$$\begin{aligned}
& 2^4 \sum_{y_1=1}^4 \sum_{y_2=1}^{y_1} 2^{y_1+y_2} \binom{2^{n-r_3}}{y_2} f_1(4, y_1) f_2(y_1, y_2) + \Delta_1(4), \quad b_3 = b_2 + \Delta_2(4), \\
& b_4 = b_3 + 2^{n-r_3+1} + 2^{n+r_3-2r_2} (1 + 5 \cdot 2^{2r_2-2r_1-1} + 2^{4r_2-4r_1-2}), \\
& c_1 = 2^6 \sum_{y_1=1}^6 \sum_{y_2=1}^{y_1} 2^{y_1+y_2} \binom{2^{n-r_3}}{y_2} f_1(6, y_1) f_2(y_1, y_2), \quad c_2 = c_1 + \Delta_1(6) + \Delta_2(6), \\
& c_3 = c_2 + \delta_1 + \delta_2, \\
& \delta_1 = 2^{n-r_3+1} (2^{n-r_2} - 2^{r_3-r_2-1}) (2^{n+r_2-2r_1+1} - 2^{r_2-r_1} - 2^{2r_2-2r_1-1} - 2^{r_3+r_2-2r_1} \\
& \quad + 2), \\
& \delta_2 = 2^{n+r_3-r_2-r_1} (2^{n+2r_2-3r_1+1} + 2^{n-r_1+2} - 2^{r_3+2r_2-3r_1-1} - 2^{r_3-r_1} - 9 \cdot 2^{3r_2-3r_1-2} - \\
& \quad 3 \cdot 2^{2r_2-2r_1-1} - 9 \cdot 2^{r_2-r_1-1} - 1).
\end{aligned}$$

Next we explain how to calculate b_4 and c_3 . Because $b_4 = NE_4(4, 4)$ and $Impvalue = 8 > 4$, we have $\mathcal{A}(L) + \mathbf{E}_4 \subset \mathcal{A}'_4(L)$. Compared with b_3 which $Impvalue = 4$, we only need to add those error sequences whose support set contain a cube fragment in $\mathbf{C}_{2^r}(4)$. By combinational theory, the number of error sequences in \mathbf{E}_4 whose support set contain a cube fragment in $\mathbf{C}_4(4)$ is $\alpha = (2^{r_1-1})^4 \cdot (2^{r_2-r_1-1})^2 \cdot 2^{n-r_2}$ and it is easy to know there are $\beta = (2^{r_1-1})^4 \cdot (2^{r_2-r_1-1})^2 \cdot 2^{r_3-r_2-1}$ error sequences in \mathbf{E}_4 equivalent to it, where $(2^{r_1-1})^4$, $(2^{r_2-r_1-1})^2$, $2^{r_3-r_2-1}$ are respectively the numbers of error sequences which \mathbf{C}_2 , \mathbf{C}_4 , \mathbf{C}_8 -equivalent to it. Thus the number of error sequences in \mathbf{E}_4^R which contain a cube fragment in $\mathbf{C}_4(4)$ is $\alpha/\beta = 2^{n-r_3+1}$. Similarly, we can get the number of error sequences whose support set do not contain a cube fragment in $\mathbf{C}_4(4)$ but contain a cube fragment in $\mathbf{C}_4(3)$ and $\mathbf{C}_8(4)$ is $(2^{r_1-1})^4 \cdot 2^2 \cdot (2^{r_2-r_1-1})^3 \cdot 2^2 \cdot (2^{r_3-r_2-1})^2 \cdot 2 \cdot 2^{n-r_3}$ and there are $(2^{r_1-1})^4 \cdot 2^{r_2-r_1-1}$ error sequences equivalent to it. Thus the number of this kind of error sequences in \mathbf{E}_4^R is $2^{n+r_3-2r_1+1}$. If the support set of error sequences do not contain a cube fragment in $\mathbf{C}_4(3)$, then it must contain two cube fragments in $\mathbf{C}_4(2)$ and the distance of the two cube fragments is 2^{n-r_3} . The number of this kind of error sequences in \mathbf{E}_4^R is $2^{n+r_3-2r_2} (1 + 2^{2r_2-2r_1-1} + 2^{4r_2-4r_1-2})$. Thus we have $b_4 = b_3 + 2^{n-r_3+1} + 2^{n+r_3-2r_2} (1 + 5 \cdot 2^{2r_2-2r_1-1} + 2^{4r_2-4r_1-2})$.

Because $c_3 = NE_6(6, 4)$ and $Impvalue = 8$, comparing with c_2 which $Impvalue = 4$, we need to add the error sequences in \mathbf{E}_6 which contains cube fragment in $\mathbf{C}_8(4)$, $\mathbf{C}_8(5)$ and $\mathbf{C}_8(6)$ based on c_2 . Using the similar method

in calculating b_4 , we can get the number of error sequences in \mathbf{E}_6^R of which the support set contains a cube fragment in $\mathbf{C}_4(4)$ is δ_1 . And the number of error sequences in \mathbf{E}_6^R which contain a cube fragment in $\mathbf{C}_8(5)$ or $\mathbf{C}_8(6)$ but not contain a cube fragment in $\mathbf{C}_4(4)$ is δ_2 . Where δ_1 and δ_2 are given above.

According to Table 1, we can get the following theorem directly:

Theorem 13. *Let $\mathcal{N}'_k(L)$ be the number of binary 2^n -periodic sequences with k -error linear complexity L and linear complexity less than 2^n , then we have*

$$\begin{aligned} \mathcal{N}'_2(L) &= \begin{cases} 0 & \text{if } L = 2^n - 2^{n-r_1} \\ (1 + a_1) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2}) \\ (1 + a_3) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3} + x), 0 \leq x < 2^{n-r_3}, \end{cases} \\ \mathcal{N}'_4(L) &= \begin{cases} 0 & \text{if } L = 2^n - 2^{n-r_1} \\ b_1 \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2}) \\ (1 + a_3 + b_3) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3}) \\ (1 + a_3 + b_4) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3} + x), 0 \leq x < 2^{n-r_3}, \end{cases} \\ \mathcal{N}'_6(L) &= \begin{cases} 0 & \text{if } L = 2^n - 2^{n-r_1} \\ c_1 \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2}) \\ (1 + a_2 + b_2 + c_2) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3}) \\ (1 + a_3 + b_4 + c_3) \cdot 2^{L-1} & \text{if } L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3} + x), 0 \leq x < 2^{n-r_3}. \end{cases} \end{aligned}$$

Note that, $\mathcal{N}'_2(L)$, $\mathcal{N}'_4(L)$ can be compared with [8, 12, 13] and $\mathcal{N}'_6(L)$ is examined by a computer.

When k become large, the analytical expression of $\mathcal{N}'_k(L)$ will become too complexity. Based on our method, it is easy to construct an efficient algorithm to calculate the value $\mathcal{N}'_k(L)$. Table 2 lists part of the results by running a computer program on $\text{Num}_k(L)$, which represents the the size of $\mathbf{E}'^R = \sum_{m=0}^{k/2} \mathbf{E}_{2m}^R$, for $0 \leq k < 2^{n-1}$ and $0 < L < 2^n$, where $n = 6$. And it can be verified that $\sum_{L=0}^{64} \mathcal{N}'_k(L) = 2^{63}$ for $k = 2, 4, 6, \dots, 32$ which implies the correctness of this method.

4 Characterization for Other Cases

In this section, we firstly consider $\mathcal{A}''_k(L)$, where k is even. Let $k = 2M$, then $\mathcal{A}''_k(L) \subseteq \bigcup_{m=1}^M (\mathcal{A}(L) + \mathbf{E}_{2m-1})$. Similar to the analysis on $\mathcal{A}'_k(L)$, we sequentially eliminate the sequences E from \mathbf{E}_{2m-1} which satisfy that there exists sequence $E' \in \mathbf{E}_{2m'-1}$, where $0 \leq m' < m$, such that $E' \sim E$. And we denote the set of remaining error sequences by \mathbf{E}_{2m-1}^r . Then we sequentially eliminate those sequences E from \mathbf{E}_{2m-1} which satisfy that there exists sequence $E' \in \mathbf{E}_{2m-1}$, such that $E' \sim E$. And finally, we sequentially eliminate the sequences E from \mathbf{E}_{2m-1} which satisfy that $LC_k(S + E) < L$ for $S \in \mathcal{A}(L)$. Similar to Theorems 6, 7 and 8, we can get the following theorems.

Lemma 10. *Let E be an error sequence in \mathbf{E}_{2m-1} . If there exists a cube fragment in $\mathbf{C}(\text{Impvalue})$ being subset to $\text{supp}(E)$, then $(\mathcal{A}(L) + E) \cap \mathcal{A}'_k(L) = \emptyset$. Where $\text{Impvalue} = m - \frac{k}{2} + 2^{T-1}$ and $1 \leq \text{Impvalue} \leq 2m - 1$.*

Table 2. Part of the results on $\mathcal{N}'_k(L)$ for $n = 6$

L	w_H	$k = 6$	$k = 8$	\dots	$k = 26$	$k = 28$	$k = 30$
\dots	≤ 1	0	0		0	0	0
16	2	32800768	843448320		0	0	0
24	2	12361216	105334272		0	0	0
28	2	1364608	2915424		0	0	0
30	2	127456	205896		0	0	0
31	2	32032	51480		0	0	0
40	2	114688	65536		0	0	0
44	2	6400	256		0	0	0
46	2	448	16		0	0	0
47	2	112	4		0	0	0
52	2	0	0		0	0	0
54	2	0	0		0	0	0
55	2	0	0		0	0	0
58	2	0	0		0	0	0
59	2	0	0		0	0	0
61	2	0	0		0	0	0
8	3	74698177	4269895680		0	0	0
12	3	73495057	4000596704		0	0	0
14	3	71447441	3611187752		0	0	0
15	3	68356625	3111545144		0	0	0
20	3	49468513	1797161728		0	0	0
22	3	46577129	1420375632		0	0	0
23	3	41906633	993236724		0	0	0
26	3	22363121	292078272		0	0	0
27	3	15385637	133105152		0	0	0
29	3	3774849	22800792		0	0	0
36	3	854113	7480320		0	0	0
38	3	753929	4554704		0	0	0
39	3	618185	2459764	\dots	0	0	0
42	3	274577	361600		0	0	0
43	3	154997	122304		0	0	0
45	3	29265	16448		0	0	0
50	3	3985	0		0	0	0
51	3	901	0		0	0	0
53	3	65	0		0	0	0
57	3	1	0		0	0	0

Table 2. (*continued*)

L	w_H	$k = 6$	$k = 8$	\dots	$k = 26$	$k = 28$	$k = 30$
4	4	75611761	4501725649		80627405461098496	17127899176960000	0
6	4	75611761	4501648441		7325469431074816	236126248960000	0
7	4	75611761	4501494025		2073916240700416	59031562240000	0
10	4	75154969	4385391113		19048518337536	139314069504	0
11	4	75154969	4384858301		4936272171264	34828517376	0
13	4	74325013	4190250125		609858701856	4353564672	0
18	4	51711097	2174133193		399572992	1048576	0
19	4	51711097	2172898813		101072896	262144	0
21	4	50589805	1979144701		12535808	32768	0
25	4	28803133	693096413		388864	1024	0
34	4	942649	11435209		0	0	0
35	4	942649	11396605		0	0	0
37	4	898381	9273725		0	0	0
41	4	418429	1975901		0	0	0
49	4	9949	9949		0	0	0
2	5	75611761	4501777129		765884877961138529	1149125482916201841	735663252850019217
3	5	75611761	4501777129		549379354729134933	488415562254909925	83465513150235525
5	5	75611761	4501751389		127414035703583729	39208852967342625	1678693908850625
9	5	75154969	4385746325		1928380228863833	175169988640833	2240855430049
17	5	51711097	2174956117		296601473321	9419426161	42981185
33	5	942649	11460949		36457	497	1
1	6	75611761	4501777129		956315644440505325	2075085937425745213	3695373947956092637

In the 2nd column, w_H indicates the value of $T = w_H(2^n - L)$.

Note that $\mathcal{N}'_k(L) = \text{Num}_k(L) \cdot 2^{L-1}$, and for each column, it can be verified that $\mathcal{N}'_k(0) + \sum_{L=1}^{63} \text{Num}_k(L) \cdot 2^{L-1} = 2^{63}$.

Theorem 14. *Let $E \in \mathbf{E}_{2m-1}$ do not contain a cube fragment in $\mathbf{C}(\text{Impvalue})$. There exists $E' \in \mathbf{E}_{2m'-1}$, such that $E' \sim E$, if and only if there exists a cube fragment in $\mathbb{C}_{2^t}(2^{t-1}+1)$ being subset to $\text{supp}(E)$, where $m' < m$ and $1 \leq t \leq T$.*

Theorem 15. *Let E be an error sequence in \mathbf{E}_{2m-1}^r , then there exists $E' \in \mathbf{E}_{2m-1}$, $E' \neq E$, such that $E' \sim E$, if and only if there exists a cube fragment in $\mathbb{C}_{2^t}(2^{t-1})$ being subset to $\text{supp}(E)$, where $1 \leq t \leq T$.*

Theorem 16. *Let E be an error sequence in \mathbf{E}_{2m-1}^r , then $(\mathcal{A}(L)+E) \cap \mathcal{A}'_k(L) = \emptyset$, if and only if there exists a cube fragment in $\mathbf{C}(\text{Impvalue})$ being subset to $\text{supp}(E)$, where $\text{Impvalue} = m - k/2 + 2^{T-1}$ and $1 < \text{Impvalue} \leq 2m - 1$.*

Similarly, we can get the counting function $\mathcal{N}''_k(L)$, which is almost identical with $\mathcal{N}'_k(L)$.

In addition, for the cases in which k is odd, according to Lemma 3, we can know that

$$\mathcal{A}'_{2M+1}(L) = \mathcal{A}'_{2M}(L), \quad \mathcal{A}''_{2M-1}(L) = \mathcal{A}''_{2M}(L) \text{ for } 0 < L < 2^n.$$

As a result, for any k we can get the complete counting function $\mathcal{N}_k(L)$. For small k we can give the analytical expression directly and when k become large we can give the numbers of sequences with given k -error linear complexity by computer.

5 Conclusions

In this paper, we study the distribution of 2^n -periodic binary sequences with given k -error linear complexity. Firstly, we build an equivalence relationship on set of error sequences to reduce the problem of counting the number of 2^n -periodic binary sequences with fixed k -error linear complexity to the problem of figuring out how many equivalence classes the set of error sequences can be split into. We use the cube fragment and cube class, which are concept tools extended from the concept of a cube, to characterize error sequences. Based on a new sieve process, we eliminate the overlap among and within different sets of error sequences. We conclude that if the error sequences contain specific cube fragments, then it should be eliminated. Through compressing the support set of error sequences, we determine whether or not error sequences contain those specific cube fragments and we can easily get the number of error sequences in specific equivalence classes. As a result, we can manually get the recurrence expression of counting function for $k \in \{2, 4, 6\}$. For other even k , we claim that an automatic computer program can be build according to this method and efficiently solve the problem for any even k . After that, we explain that this method can be applied to other cases. Thus we can get the complete counting function for any k . Compared with that in [8, 12, 13], it can be seen that new and more concise expressions than that got by previous methods can be obtained following this method. We believe this method can be used to settle the problem for some other special periodic sequences.

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. Lecture Notes in Computer Science, vol. 561. Springer, Heidelberg (1991)
2. Fu, F.-W., Niederreiter, H., Su, M.: The characterization of 2^k -periodic binary sequences with fixed 1-error linear complexity. In: Gong, G., Helleseht, T., Song, H.-Y., Yang, K. (eds.) SETA 2006. LNCS, vol. 4086, pp. 88–103. Springer, Heidelberg (2006). doi:[10.1007/11863854_8](https://doi.org/10.1007/11863854_8)

3. 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](https://doi.org/10.1007/978-3-540-85912-3_23)
4. Kavuluru, R.: Characterization of 2^n -periodic binary sequences with fixed 2-error or 3-error linear complexity. *Des. Codes Crypt.* **53**(2), 75–97 (2009)
5. 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)
6. Massey, J.L.: Shift-register synthesis and bch decoding. *IEEE Trans. Inf. Theory* **15**(1), 122–127 (1969)
7. Meidl, W.: On the stability of 2^n -periodic binary sequences. *IEEE Trans. Inf. Theory* **51**(3), 1151–1155 (2005)
8. Ming, S.: Decomposing approach for error vectors of k -error linear complexity of certain periodic sequences. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E97–A**(7), 1542–1555 (2014)
9. Rueppel, A.R.: *Analysis and Design of Stream Ciphers*. Communications and Control Engineering Series. Springer, Heidelberg (1986)
10. 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)
11. Zhou, J.: A counterexample concerning the 3-error linear complexity of 2^n -periodic binary sequences. *Des. Codes Crypt.* **64**(3), 285–286 (2012)
12. Zhou, J., Liu, J., Liu, W.: The 4-error linear complexity distribution for 2^n -periodic binary sequences. *CoRR* abs/1310.0132 (2013)
13. Zhou, J., Liu, W.: The k -error linear complexity distribution for 2^n -periodic binary sequences. *Des. Codes Crypt.* **73**(1), 55–75 (2014)
14. Zhou, J., Liu, W., Zhou, G.: Cube theory and stable k -error linear complexity for periodic sequences. In: Lin, D., Xu, S., Yung, M. (eds.) *Inscrypt 2013*. LNCS, vol. 8567, pp. 70–85. Springer, Heidelberg (2014). doi:[10.1007/978-3-319-12087-4_5](https://doi.org/10.1007/978-3-319-12087-4_5)

Information Security Practice and Experience

12th International Conference, ISPEC 2016, Zhangjiajie,

China, November 16-18, 2016, Proceedings

Bao, F.; Chen, L.; Deng, R.H.; Wang, G. (Eds.)

2016, XII, 380 p. 82 illus., Softcover

ISBN: 978-3-319-49150-9