An Algorithm for Counting the Number of $2^n$-Periodic Binary Sequences with Fixed $k$-Error Linear Complexity

Wenlun Pan$^{1,2}$, Zhenzhen Bao$^3$, Dongdai Lin$^1$, and Feng Liu$^{1,2}$

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

Abstract. The linear complexity and $k$-error linear complexity of sequences are important measures of the strength of key-streams generated by stream ciphers. The counting function of a sequence complexity measure gives the number of sequences with given complexity measure value and it is useful to determine the expected value and variance of a given complexity measure of a family of sequences. Fu et al. studied the distribution of $2^n$-periodic binary sequences with 1-error linear complexity in their SETA 2006 paper and people has 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 $k$ and the counting functions become extremely complex when $k$ become large. In this paper, we define an equivalent relation on error sequences. We use a concept of *cube fragment* as basic modules to construct classes of error sequences with specific structures. Error sequences with the same specific structures can be represented by a single *symbolic representation*. We introduce concepts of *trace*, *weight trace* and *orbit* of sets to build quantitative relations between different classes. Based on these quantitative relations, we propose an algorithm to automatically generate symbolic representations of classes of error sequences, calculate *coefficients* from one class to another and compute *multiplicity* of classes defined based on specific equivalence on error sequences. This algorithm can efficiently get the number of sequences with given $k$-error linear complexity. The time complexity of this algorithm is $O(2^{k\log k})$ in the worst case which does not depend on the period $2^n$.

Keywords: Sequence; Linear Complexity; $k$-Error Linear Complexity; Counting Function; Cube Theory

1 Introduction

The linear complexity and $k$-error linear complexity of sequences are important measures of the strength of key-streams generated by stream ciphers. Let $S = (s_0s_1 \cdots s_{N-1})^\infty$ be an $N$-periodic sequence with the terms in finite field $F_2$. And we denote $S^N$ the set of all $N$-periodic binary sequences. The linear complexity of $S$, denoted by $LC(S)$, is defined as the length of the shortest linear feedback shift register (LFSR) that can generate $S$ which is given by [1]

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

where $S(x) = s_0 + s_1x + s_2x^2 + \cdots + s_{N-1}x^{N-1}$ and is called the corresponding polynomial to $S$. According to this formula, it can easily get the following two lemmas:

**Lemma 1 ([6]).** Let $S$ be a $2^n$-periodic binary sequence. Then $LC(S) = 2^n$ if and only if the Hamming weight of the sequence $S$ is odd.

**Lemma 2 ([6]).** 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.

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 [1,9].

**Definition 1 ([1,9]).** For any sequence $S \in S^N$, where $0 \leq k < N$, 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 $w_H(E)$ denote the Hamming weight of the sequence $E$ in one period and $E$ is called the error 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 3 ([5]). Let \( S \) be a nonzero \( 2^n \)-periodic binary sequence, then \( \text{merr}(S) = 2^n - \text{LC}(S) \).

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 [8] determined the counting function of linear complexity for \( 2^n \)-periodic binary sequences as follow:

Lemma 4 ([8]). 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

\[
\mathcal{N}(0) = 1, \quad \mathcal{A}(0) = \{ (00\ldots0) \}, \text{ and } \\
\mathcal{N}(L) = 2^{L-1}, \quad \mathcal{A}(L) = \{ S \in S^{2^n} : S(x) = (1-x)^{2^n-L}a(x), a(1) \neq 0 \} \text{ for } 1 \leq L \leq 2^n.
\]

In this paper, we study the counting function for the number of \( 2^n \)-binary sequences with given \( k \)-error linear complexity. Following the notation in [2,3,12], 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

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

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

According to the definition of \( k \)-error linear complexity of sequence, we can get the following trivial cases:

\[
\begin{align*}
\mathcal{A}_k(2^n) &= \emptyset, & \mathcal{N}_k(2^n) &= 0 \quad \text{for } k \geq 1, \\
\mathcal{A}_k(0) &= \{ S \in S^{2^n} : \text{HC}(S) \leq k \}, & \mathcal{N}_k(0) &= \sum_{j=0}^{k} \binom{2^n}{j}, \quad \text{for } k \geq 1, \\
\mathcal{A}_k(1) &= \{ S \in S^{2^n} : \text{HC}(S) > 2^n - k \}, & \mathcal{N}_k(1) &= \sum_{j=2^n-k}^{2^n} \binom{2^n}{j} = \sum_{j=0}^{k} \binom{2^n}{j}, \quad \text{for } k < 2^{n-1}, \\
\mathcal{A}_k(2) &= \{ S \in S^{2^n} : \text{HC}(S) > 2^n - 2k \}, & \mathcal{N}_k(2) &= \sum_{j=2^n-2k}^{2^n} \binom{2^n}{j} = \sum_{j=k+1}^{2^n} \binom{2^n}{j}, \quad \text{for } k \geq 2^{n-1}, \\
\mathcal{A}_k(L) &= \emptyset, & \mathcal{N}_k(L) &= 0 \quad \text{for } k \geq 2^{n-1}, \ L \neq 0 \text{ and } 1.
\end{align*}
\]

Henceforth, we need only consider the cases when \( 1 < L < 2^n \) and \( k < 2^{n-1} \). 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 [10]. After that, Jianqin Zhou et al. use sieve method of combinations to sieve sequences \( S + E \) with \( \text{LC}_k(S + E) = L \) in \( S + E \) where \( S = \{ S \in S^{2^n} : \text{LC}(S) = L \} \), \( E = \{ E \in S^{2^n} : \text{HC}(E) \leq k \} \) \( \text{and } S + E = \{ S + E : S \in S \text{ and } E \in E \} \). And they obtained the complete counting functions for \( k = 2, 3 \) [12]. In the informal publication paper [11], Jianqin Zhou et al. also study the counting functions for \( k = 4, 5 \). In the paper [7], 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 define an equivalence relationship on the error sequences set \( E \) based on the observation as the follows:

Lemma 5 ([3]). Let \( E \) and \( E' \) be two error sequences in \( E \). Then

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

Corollary 1. Let \( E \) be an error sequence in \( E \), 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 \( \text{LC}_k(S + E) = L \). On account of \( \text{LC}_k(S + E) = \min_{E' \in E} \text{LC}(S + E + E') \), it follows that \( \text{LC}(E + E') \neq L \) for any \( E' \in E \), otherwise \( \text{LC}_k(S + E) < L \). Thus for any \( S' \in \mathcal{A}(L) \), we have \( \text{LC}_k(S' + E) = \min_{E' \in E} \text{LC}(S' + E + E') = \min_{E' \in E} \max \{ \text{LC}(S'), \text{LC}(E + E') \} \geq L \). Considering that \( \text{LC}_k(S' + E) \leq \text{LC}(S' + E + E) = \text{LC}(S') = L \), so \( \text{LC}_k(S' + E) = L \), that is \( \mathcal{A}(L) + E \subseteq \mathcal{A}_k(L) \). So for any \( E \in E \), we have either \( \mathcal{A}(L) + E \subseteq \mathcal{A}_k(L) \) or \( (\mathcal{A}(L) + E) \cap \mathcal{A}_k(L) = \emptyset \). \( \square \)

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

From the above, we can know that for a given error sequence $E$, either all of the sequences in $A(L) + E$ are in $A_k(L)$ or none of them is in $A_k(L)$. It follows that to get the value of $N_k(L)$, we can figure out how many equivalence classes the set $E$ is split into, and in how many of them an element $E$ leads all of the sequences in $A(L) + E$ to be in $A_k(L)$. Thus, we define an equivalent relation as follow.

**Definition 2.** Let $E$ and $E'$ be two error sequences in $E$. We call $E$ and $E'$ equivalent if $A(L) + E = A(L) + E'$. And we denote this by $E \sim E'$.

Remark, this equivalence relation is defined under a given linear complexity $L$. According to Lemma 1, 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 $E$. We have $E \sim E'$ if and only if $LC(E + E') < L$.

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

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

Different from the sieve method in [12] or decomposing approach in [7], in this paper we only sieve the error sequences in set $E = \bigcup_{j=0}^{t} E_j$ where $E_j = \{ E \in S' : w_H(E) = j \}$ to get the maximum subset of $E$ in which elements are non-equivalent with each other and satisfy that $LC(E) = L$ when plus the error sequence $E$ to any sequence $S \in A(L)$. And different from [13] in which the cube concepts are introduced to compute the stable $k$-error linear complexity of periodic sequences, in this paper to get counting functions we first use a concept of cube fragment as basic modules to construct classes of error sequences with specific structures. Error sequences with the same specific structures can be represented by a single symbolic representation. We then introduce concepts of trace, weight trace and orbit of sets to build quantitative relations between different classes. Based on these quantitative relations, we propose an algorithm to automatically generate symbolic representations of classes of error sequences, calculate coefficients from one class to another and compute multiplicity of classes defined based on specific equivalence on error sequences. This algorithm can efficiently get the number of sequences with given $k$-error linear complexity at last. The time complexity of this algorithm is $O(2^k \log_2 L)$ in the worst case which does not depend on the period $2^k$. Experiment results got by the implementation of the algorithm are shown in Table 1. To get this table, it only cost a few minutes in a personal computer and notice that it is unfeasible to get these results by other methods or by native exhaustive method.

### 2 Cube Class, Cube Fragment and Classes of Error Sequences with Special Structures

In this section we extend the concept of Cubes[13] to cube classes and cube fragments and decompose sequences to specific cubes and cube fragments.

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, $supp(S) = \{ i : s_i \neq 0, 0 \leq i \leq N \}$. Let $\mathbb{Z}_m = \{ 0, 1, 2, \ldots, m - 1 \}$ and denote $P(\mathbb{Z}_m)$ the power set of $\mathbb{Z}_m$ which is the set of all subsets of $\mathbb{Z}_m$, that is $P(\mathbb{Z}_m) = \{ U : U \subseteq \mathbb{Z}_m \}$. Notice that the set $P(\mathbb{Z}_N)$ is one to one corresponding to $S^N$. Especially, the empty set in $P(\mathbb{Z}_N)$ corresponds to the all-zero sequence in $S^N$. In [13], 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 3.** Let $U = \{ u_1, u_2, \ldots, u_n \}$ be a subset of $\mathbb{Z}_N$, we call the elements in $U$ as points. For two points $u_i, u_j \in U$, define the distance between the two points as $\delta$, if $|u_i - u_j| = 2^\delta b$ and $2 \nmid b$. And denote it by $d(u_i, u_j) = \delta$.

According to the definition of distance, it can easily be verified that for any $u_1, u_2, u_3 \in U$, if $d(u_1, u_2) = d(u_1, u_3)$, then $d(u_2, u_3) > d(u_1, u_2)$, otherwise $d(u_2, u_3) = min\{d(u_1, u_2), d(u_1, u_3)\}$.
Furthermore, we denote:

For any $U$ cube fragments into larger cube fragments in cube class $i$, define $C$ represent classes of cubes with specific sides of length. And the concepts

Lemma 6. Let $U$ and $V$ be two 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 Definition 5 and 4, we have $d(u, v) = \min\{d(u, u_0), d(u_0, v_0)\} = d(u_0, v_0)$. Then $d(u, v) = \min\{d(u, v_0), d(v_0, v)\} = d(u_0, v_0) = d(U, V)$.

Definition 5 (Cube). Let $U = \{u_1, u_2, \ldots, u_{2^r}\}$ 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 $Cube_+$. 
- 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 $2^1$, then we say $U$ is a 1-cube with sides of length $\{2^1\}$. We denote the set of all 1-cubes with sides of length $2^1$ by $Cube_{2^1}$. 
- 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 $U', U'' \in Cube_{2^1}$ and $d(U', U'') = 2^2 (i_1 \geq i_2)$, then we call $U$ as a 2-cube with sides of length $\{2^1, 2^2\}$. We denote the set of all 2-cubes with sides of length $\{2^1, 2^2\}$ by $Cube_{2^1, 2^2}$. 
- 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 $U', U'' \in Cube_{2^{r_1}, 2^{r_2}, \ldots, 2^{r_{T-1}}}$ and $d(U', U'') = 2^T (i_1 > i_2 > \cdots > i_T)$, then we call $U$ as a $T$-cube. We denote the set of all $T$-cubes with sides length of $\{2^1, 2^2, \ldots, 2^T\}$ by $Cube_{2^1, 2^2, \ldots, 2^T}$.

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. Because the linear complexity can be get by $LC(S) = 2^n - \deg(\gcd(1 - x^{2^i}, S(x)))$, we can easily know that the linear complexity of a cube with sides of length $\{2^i, 2^j, \ldots, 2^T\}$ is $2^n - (2^i + 2^j + \cdots + 2^T)$.

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

$$
C_2 := \bigcup_{r=1}^{T-1} Cube_{2^{r-1}}, \\
C_4 := \bigcup_{r=1}^{T-1} Cube_{2^{r-1}, 2^{r-2}}, \\
\vdots \\
C_{2^T} := \bigcup_{r=1}^{T-1} Cube_{2^{r-1}, 2^{r-2}, \ldots, 2^{r-T+1}, 2^{r-T}}, \\
C := \bigcup_{i=1}^{T} C_{2^i},
$$

and

Remark, we define $C_1 := Cube_{+\infty}$ which represents the set of all sets with only one point. The concepts $C_{2^i}$ and $C_{2^j}$ represent classes of cubes with specific sides of length. And the concepts $C_{2^i}(p)$ and $C_{2^j}(p)$ represent the sets of all specific fragments of cubes in the cube classes $C_{2^i}$ and $C_{2^j}$, where those cube fragments are all of size $p$. And we define $C_{2^i}(p) = \emptyset$, $C_{2^j}(p) = \emptyset$ 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 $C$ or cube class $C_1$.

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


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

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

Using the similar argument as in the proof of Theorem 2, we can easily carry out the following corollary. Thus, similarly, we can split small fragments of cubes into larger fragments of cube in class \( C \).

**Corollary 3.** Let \( U \in \mathcal{C}(i) \) and \( V \in \mathcal{C}(j) \), if \( d(U, V) = 2^{n-t} < \min\{d(U), d(V)\} \), then \( U \cup V \in \mathcal{C}_{2^t+i+j} \), where \( r_t < t < r_{t+1} \), \( 1 \leq s < T \), and \( i + j \leq 2^{n-1} \).

In the paper [13], the authors decompose a sequences to some cubes as follows:

**Lemma 7** ([13]). Let \( S \) be a binary sequence with period \( 2^n \), and with linear complexity \( LC(S) = L = 2^n -(2^{n-t_1} + 2^{n-t_2} + \cdots + 2^{n-t_r}) \), where \( 0 < r_1 < r_2 < \cdots < r_r < n \). 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 \( L \).

We extend this decomposition as follows which are proved in Appendix A:

**Corollary 4.** Let \( E \) and \( E' \) be two error sequences. We have \( E \sim E' \) if and only if there exist pairwise disjoint cubes \( U_1, U_2, \ldots, U_q \) and \( V_1, V_2, \ldots, V_r \) such that \( supp(E+ E') = (\cup_{j=1}^d U_j) \cup (\cup_{j=1}^d V_j) \), where \( U_j \in \mathcal{C}, V_j \in \mathcal{C}, d' \geq 0 \) and \( d' \) is even.

If \( E \sim E' \) and \( supp(E + E') = \{j\}_{j=1}^d U_j \) where all \( U_j \) are cubes in \( \mathcal{C}_2 \), then we say that \( E \) is \( \mathcal{C}_2 \)-equivalent to \( E' \) and denote this by \( E \sim_1 E' \), and for ease of notations we denote this by \( E \sim_1 \).

**Corollary 5.** Let \( S \in \mathcal{A}(L) \) be a \( 2^t \)-periodic binary sequence with linear complexity \( L \), and \( E \in \mathcal{E} \) be an error sequence. We have \( LC(S + E) < L \) if and only if there exist pairwise disjoint cubes \( U_1, U_2, \ldots, U_q \) and \( V_1, V_2, \ldots, V_r \) such that \( supp(E) = (\cup_{j=1}^d U_j) \cup (\cup_{j=1}^d V_j) \), where \( U_j \in \mathcal{C}, V_j \in \mathcal{C} \) for \( 1 \leq j \leq d \) and \( 1 \leq j' \leq d' \).

We regard the cube fragment \( \mathcal{C}_2(p) \) as the basic modules and use it to construct classes of error sequences with special structures as follows and then we introduce the concept of “trace” and “weight trace” of a set which will be used to count the number of sequences with special structures.
where the notation \( p^{[d]} \) is symbolic representation of the multiset \( \{p, p, \ldots, p\} \). And \( p^{[d]}_j = p^{[d]}_{j-1} \cdots p^{[d]}_1 \) in \( r_i B^{[d]}_p \) and \( r_i B \{p^{[d]}_{j-1}, \ldots, p^{[d]}_1\} \) is symbolic representation of the union multisets \( \bigcup_{j=1}^d p^{[d]}_j \). We denote the set of all those multisets by \( Q = \{p^{[d]}_{j-1}, \ldots, p^{[d]}_1\} : p_j > p_{j-1} > \cdots > p_1 \geq 1, d_j \geq 1, 1 \leq j \leq \ell \}. \) And in the above definitions, \( Q, Q_1, Q_2, \ldots, Q_{\ell} \) are multisets in \( Q \), and \( Q_{j'} \neq Q_{j''} \) for \( 1 \leq j' < j'' \leq \ell \). The notation \( \bigcup \) denotes the union of multisets, for example \( \{1, 1, 2, 3\} \bigcup \{1, 2\} = \{1, 1, 1, 2, 2, 3\} \). The symbol \( \mathbb{Q} \) appeared in the rest of the paper always takes the meaning defined here.

For a given \( r_i \), where \( 1 \leq i \leq T \), we divide \( \mathbb{Z}_{2^n} \) to the subsets as follows:

\[
r_i U_j := \{j, j + 2^n - r_i, \ldots, j + 2^n - r_i + 1, \ldots, j + (2^n - 1) \cdot 2^n - r_i + 1\}, \quad \text{for } 0 \leq j < 2^n - r_i + 1.
\]

For any set \( U \subseteq \mathbb{Z}_{2^n} \), we define the trace of \( U \) in subsets \( \mathbb{Z}_{2^n - r_i + 1} \) as

\[
r_i Tr(U) := \{j : U \cap r_i U_j \neq \emptyset\}.
\]

Further more, if \( U \subseteq C_{2^n - 1}(p) \), we have \( d(u, v) > 2^n - r_i \) for any \( u, v \in U \), then there exists \( j \) such that \( U \subseteq r_i U_j \), where \( 0 \leq j < 2^n - r_i + 1 \). We define the weight trace of \( U \) which belongs to \( C_{2^n - 1}(p) \) in subsets \( \mathbb{Z}_{2^n - r_i + 1} \) as the following:

\[
r_i wTr(U) := \{(j)p\}.
\]

As the elements in set \( r_i B^{[d]}_p \), set \( r_i B^{[d]}_p B^{[d]-1}_{p_1-1} \cdots B^{[d]}_{p_1} \), in set \( r_i B^{[d]}_p \), and in set \( r_i B^{[d]}_p \), \( B^{[d]}_{Q-1} \cdots B^{[d]}_{Q_1} \) can all be decomposed into union set of some cube fragments subset to \( C_{2^n-1} \), therefore we can define the weight trace in \( \mathbb{Z}_{2^n - r_i + 1} \) of those elements as follows:

\[
r_i wTr(U) := \bigcup_{j=1}^d r_i wTr(U_j), \quad \text{for } U = \bigcup_{j=1}^d U_j \subseteq r_i B^{[d]}_p, \quad \text{and } U_j \subseteq r_i B^{[d]}_p;
\]

\[
r_i wTr(U) := \bigcup_{j=1}^l r_i wTr(U_j), \quad \text{for } U = \bigcup_{j=1}^l U_j \subseteq r_i B^{[d]}_p B^{[d]-1}_{p_1-1} \cdots B^{[d]}_{p_1}, \quad \text{and } U_j \subseteq r_i B^{[d]}_p;
\]

\[
r_i wTr(U) := \bigcup_{j=1}^l r_i wTr(U_j), \quad \text{for } U = \bigcup_{j=1}^l U_j \subseteq r_i B^{[d]}_p, \quad \text{and } U_j \subseteq r_i B^{[d]}_p;
\]

\[
r_i wTr(U) := \bigcup_{j=1}^l r_i wTr(U_j), \quad \text{for } U = \bigcup_{j=1}^l U_j \subseteq r_i B^{[d]}_p B^{[d]-1}_{p_1-1} \cdots B^{[d]}_{p_1}, \quad \text{and } U_j \subseteq r_i B^{[d]}_p;
\]

\[
r_i wTr(U) := \bigcup_{j=1}^l r_i wTr(U_j), \quad \text{for } U = \bigcup_{j=1}^l U_j \subseteq r_i B^{[d]}_p, \quad \text{and } U_j \subseteq r_i B^{[d]}_p.
\]

Remark 1, from the above definitions of traces and weight traces, \( r_i B^{[d]}_p \) is actually a class of union sets of \( d \) cube fragments in \( C_{2^n - 1}(p) \) with disjoint traces and weight traces in \( \mathbb{Z}_{2^n - r_i + 1} \). And \( r_i B^{[d]}_p \) is a class of union sets of \( d \) cube fragments in \( C_{2^n - 1}(p) \) with same traces in \( \mathbb{Z}_{2^n - r_i + 1} \). According to Corollary 3, for any \( U = \bigcup_{j=1}^d U_j \subseteq r_i B^{[d]}_p, \quad U_j \cup U_{j'} \subseteq C_{2^n}(p) \) for \( 1 \leq j' < j' \leq d \). Especially, \( r_i B_p := r_i B^{[1]}_p = r_i B^{[d]}_p \) is \( C_{2^n - 1}(p) \).

Remark 2, it can also be checked that \( r_i B^{[d]}_p B^{[d]-1}_{p_1-1} \cdots B^{[d]}_{p_1} \) is actually a class of union set of \( l \) elements with different traces in \( \mathbb{Z}_{2^n - r_i + 1} \), which respectively comes from \( r_i B^{[d]}_p, r_i B^{[d]-1}_{p_1-1}, \ldots, r_i B^{[d]}_p \). And \( r_i B^{[d]}_p, r_i B^{[d]-1}_{p_1-1}, \ldots, r_i B^{[d]}_p \) is a class of union set of \( l \) elements with same trace in \( \mathbb{Z}_{2^n - r_i + 1} \), which respectively comes from \( r_i B^{[d]}_p, r_i B^{[d]}_p, \ldots, r_i B^{[d]}_p \).

Remark 3, similarly, \( r_i B^{[d]}_p \) is a class of union of \( h \) elements in \( r_i B_p \) with pairwise disjoint traces. And \( r_i B^{[d]}_p B^{[d]-1}_{Q_1-1} B^{[d]}_{Q_1} \) is a class of union set of \( t \) elements with pairwise disjoint weight traces in \( \mathbb{Z}_{2^n - r_i + 1} \), which respectively comes from \( r_i B^{[d]}_p, r_i B^{[d]}_p, \ldots, r_i B^{[d]}_p \).

Example 1. Let \( L = 2^n - (2^n - r_1 + 2^n - r_2) \) where \( n = 6, r_1 = 1 \) and \( r_2 = 4 \).

1. Let \( U = \{1, 1, 11, 18, 33, 43, 50\} \), which is a union of the following sets: \( U_1 = \{1, 33\}, U_2 = \{18, 50\}, U_3 = \{11, 43\} \) and \( U_1, U_2, U_3 \subseteq C_2(2) \). Then \( r_2 wTr(U_1) = \{(1)\}, r_2 wTr(U_2) = \{(2)\}, r_2 wTr(U_3) = \{(3)\}, \) therefore \( U \subseteq r_2 B^2_2 \).
2. Let $U = \{1, 11, 18, 33, 50, 60\}$, which is a union of the following sets: $U_1 = \{1, 18, 33, 50\} \in r_2B_2^i$, $U_2 = \{11, 60\} \in r_2B_2^i$. Then $wTr(U_1) = \{(1, 2), (2, 1)\}$, $wTr(U_2) = \{(3), (4)\}$, therefore $U \in r_2B_2^i$.

3. Let $V = \{1, 9, 17, 33, 41, 49\}$, which is a union of the following sets: $V_1 = \{1, 33\}$, $V_2 = \{17, 49\}$, $V_3 = \{9, 41\}$ and $V_1, V_2, V_3 \in r_2B_2$. Then $wTr(V_1) = r_2wTr(V_2) = r_2wTr(V_3) = \{(1, 2)\}$, therefore $V \in r_2B_2[2]$.

4. Let $V = \{1, 9, 17, 33, 49, 57\}$, which is a union of the following sets: $V_1 = \{1, 17, 33, 49\}$, $V_2 = \{9, 57\}$, and $r_2wTr(V_1) = \{(1, 2), (1, 1)\}$, $r_2wTr(V_2) = \{(1, 1), (1, 1)\}$, therefore $V \in r_2B_2^2[2]$.

5. Let $W = \{1, 10, 17, 33, 50, 58\}$, which is a union of the following sets: $W_1 = \{1, 17, 33\}$, $W_2 = \{10, 50, 58\}$ and $W_1, W_2 \in r_2B_2[2][3]$, then $r_2wTr(W_1) = \{(1, 2), (1, 1)\}$, $r_2wTr(W_2) = \{(2, 2), (2, 1)\}$, therefore $W \in r_2B_2^2[2][3]$.

6. Let $W = \{1, 2, 17, 18, 33, 35, 49, 59\}$, which is a union of the following sets: $W_1 = \{1, 17, 33\} \in r_2B_2^2[2]$, $W_2 = \{2, 18, 35, 49, 59\} \in r_2B_2[2]$, then $r_2wTr(W_1) = \{(1), (2)\}, r_2wTr(W_2) = \{(2), (2), (1), (3), (3)\}$, thus $W \in r_2B_2^2B_2^2[2]$.

We denote $r'_i = r_i + 1$. For a given $r'_i$, where $1 \leq i \leq T$, we divide $Z_{2^n}$ to the subsets as follows:

$$r'_i U_j = \{j, j + 2^{n-r_i}, j + 2 \cdot 2^{n-r_i}, \cdots, j + (2^{r_i} - 1) \cdot 2^{n-r_i}\},$$

for $0 \leq j < 2^{n-r_i}$.

Similarly, we define the trace of $U \subseteq Z_{2^n}$ in subsets $Z_{2^{n-r_i}}$ as

$$r'_i Tr(U) := \{j : U \cap r'_i U_j \neq \emptyset\}.$$

And for any $U \in C_{2^n}(p)$, there exists $j$ such that $U \subseteq r'_i U_j$, where $0 \leq j < 2^{n-r_i}$. We define the weight trace of $U \in C_{2^n}(p)$ in subsets $Z_{2^{n-r_i}}$ as

$$r'_i wTr(U) := \{(j)\}_p.$$

Considering that the elements in sets $r'_i B_p^d$ and $r'_i B_p^{d-1} \cdots B_p^1$ can all be decomposed into union of some fragments of cubes in $C_{2^n}$, we define the weight trace of those elements in $Z_{2^{n-r_i}}$ as follows:

$$r'_i wTr(U) := \bigcup_{j=1}^d r'_i wTr(U_j)$$

and

$$r'_i wTr(U) := \bigcup_{j=1}^l r'_i wTr(U_j)$$

where $U = \bigcup_{j=1}^d U_j \in r'_i B_p^d$, $U_j \in r'_i B_p$ and $U = \bigcup_{j=1}^l U_j \in r'_i B_p^{d-1} \cdots B_p^1$, $U_j \in r'_i B_p^1$.

Particularly, we denote the trivial class $r'_i B_p^0 := \{U \subseteq Z_{2^n} : |U| = m\}$, which is the set of all support sets of the sequences in $E_{m}$. Note that, $r_0$ is defined for the sake of achieving a unified form with notations through the paper.

For convenience of description, we use notations $r'_i B$, $r'_i B'$ and $r'_i B'$ to denote sets of all classes as follows:

$$r'_i B := \{r'_i B_p^d \cdots B_p^1 : Q_j \in Q, Q_p \neq Q_p' \text{ and } h_j \geq 1 \text{ for } 1 \leq j \leq t\},$$

$$r'_i B' := \{r'_i B_p^{d-1} \cdots B_p^1 : p_1 > p_1 > \cdots > p_1 \geq 1 \text{ and } d_j \geq 1 \text{ for } 1 \leq j \leq l\},$$

$$r'_i B' := \{r'_i B_p^{d-1} \cdots B_p^1 : p_1 > p_1 > \cdots > p_1 \geq 1 \text{ and } d_j \geq 1 \text{ for } 1 \leq j \leq l\}.$$

Remark that $r'_i B'$ is a special subset $r'_i B$.

And for a class $B \in r'_i B \cup r'_i B' \cup r'_i B$, we define the trace and weight trace of the class in subsets $Z_{2^{n-r_i+1}}$ or $Z_{2^{n-r_i}}$ as:

$$r'_i Tr(B) := \{r'_i Tr(U) : U \in B\}$$

and

$$r'_i wTr(B) := \{r'_i wTr(U) : U \in B\}$$

for $r \in \{r'_i, r'_i\}$.

Based on the notations defined above, we can get many relationships between different classes. For example, let $U \in r_3B_Q$ where $Q = q_{s_1}^{e_1} \cdots q_{s_t}^{e_t}$, and suppose $r_3 Tr(U) = \{u\}$. Then $r_3 wTr(U) = \{(u)|_{q_1}, (u)|_{q_2}, \cdots, (u)|_{q_t}\}$ in which the number of $(u)|_{q_i}$ is $e_i$. And the weight trace of $U$ in subset $Z_{2^{n-r_i-1}}$ can be express as $r'_i wTr(U) = \{(u)|_{q_1}, (u)|_{q_2}, \cdots, (u)|_{q_t}\}$ in which $u_{j_k} \in \{u \cdot 2^{n-r_i-1} : 0 \leq l < 2^{n-r_i-1}\}$ and $u_{j_k} \neq u_{j_k}'$ for any $(k, j) \neq (k', j')$, where $1 \leq k \leq k' \leq s$ and $1 \leq j \leq e_j$, $1 \leq j' \leq e_{j'}$. In the next subsection we will focus on those relationships between different classes and after that we can get the algorithm for counting the number of sequences with given $k$-error linear complexity which can also get the counting function for small $k$.

3 Quantitative Relations Between Different Classes of Error Sequences

We first consider the relations between classes in $r_i B$ and $r_i B$ where $1 \leq i \leq T$. 
Definition 6. Let $U$ be a set in class $B$, where $B \in \mathcal{B}$. We define the orbit of $U$ in $Z_{2n-r+1}$ as

$$r_i O_U := \{U' \in B : r_i \text{ wTr}(U') = r_i \text{ wTr}(U)\}.$$ 

And we denote

$$r'_i \text{ wTr}(r_i O_U) := \{r'_i \text{ wTr}(U') : U' \in r_i O_U\}.$$ 

Given a multiset $Q = \{q_1^{r_1}, q_2^{r_2}, \ldots, q_l^{r_l}\} \in \mathcal{Q}$, we define $\text{Index}(Q) = \{e_r, e_{r-1}, \ldots, e_1\}$ which is also a multiset. And given a positive integer $N$ and a multiset $U = \{u_1, u_2, \ldots, u_m\} \in \mathcal{Q}$, we define $(N)_U = \prod_{u_j \in U} (N - \sum_{u_j \in U} 1).$

Lemma 8. Let $U$ be a set in class $B$, where $B \in \mathcal{B}_r$. If $U$ is also in class $B_1$, where $B_1 = r B_0$, then the size of the weight trace set of the orbit of $U$ is

$$|r_i \text{ wTr}(r_i O_U)| = \left(\frac{2^{r_i - r - 1}}{\text{Index}(Q)}\right)^j.$$ 

where the multiset $Q \in \mathcal{Q}$.

Proof. Suppose $Q = \{q_1^{r_1}, q_2^{r_2}, \ldots, q_l^{r_l}\}$ and $r_i \text{ wTr}(U) = \{q_j\}$, then $r'_i \text{ wTr}(U') = \{q_j\}$ in which the number of $r_i q_j$ is $e_j$. Then, $r'_i \text{ wTr}(U') = \{r'_i wTr(Q)\}$ in which $u_{j+k} \in \{u_{j+k}, 2^{r_i - r - 1}, 2^{r_i - r - 1} \cdots, 2^{r_i - r - 1} \cdot 2^{n-r-1}\}$, where $0 \leq u_{j+k} < 2^{n-r-1}$, and there are $(\frac{2^{r_i - r - 1}}{\text{Index}(Q)})$ possibilities. As a result, we have $|r'_i \text{ wTr}(r_i O_U)| = \prod_{j=1}^l \left(\frac{2^{r_i - r - 1}}{\text{Index}(Q)}\right)^b_j$. 

According to Theorem 3, the size of the weight trace of the orbit of $U$ only relate to $B$ and $B_1$, i.e. for any $U, V \in B$, if $U, V \in B_1$, then $|r'_i \text{ wTr}(r_i O_U)| = |r'_i \text{ wTr}(r_i O_V)|$. Therefore, we define a coefficient from class $B$ to $B_1$ as:

$$\text{Coef}(B_1 | B) := |r'_i \text{ wTr}(r_i O_U)|,$$ 

where $U \in B$ and $U \in B_1$.

Theorem 4. Let class $B \in \mathcal{B}_r$. We denote $r_i \text{ Gen}(B) = \{B' \in r_i B : \exists U \in B \text{ s.t. } U \in B'\}$. Then we have

$$|r'_i \text{ wTr}(B)| = \sum_{B' \in r_i \text{ Gen}(B)} \text{ Coef}(B' | B) \cdot |r_i \text{ wTr}(B')|.$$ 

Proof. By Theorem 3, we have that for a given $B' \in r_i \text{ Gen}(B)$, for all elements in $r_i \text{ wTr}(B')$, there are $\text{Coef}(B' | B)$ elements in $r'_i \text{ wTr}(B')$ corresponding to it. As $B = \bigcup_{r_i \in \mathcal{B}_r} B'$ and it is easy to know that $r_i \text{ wTr}(B') \bigcap r_i \text{ wTr}(B'') = \emptyset$ for any $B', B'' \in r_i \text{ Gen}(B)$ and $B' \neq B''$, then we have derived the theorem.

Example 2. Let $L = 2^n - (2^{r_i - r} + 2^{r_i - r} + 2^{n-r})$ where $n = 6$, $r_1 = 1$, $r_2 = 3$ and $r_3 = 6$. Let $U = \{1, 5, 9\} \in r_3 B_2 B_1$. Then $r_3 \text{ wTr}(U) = \{(1, 2), (1, 1)\}$, so $U \in r_3 B_2^{1 \oplus 1}$. And $r_3 \text{ wTr}(r_3 O_U) = \{(1, 2), (3, 2)\} \cdot \{(3, 5)\}$.

Let $V = \{1, 5, 8\} \in r_3 B_2 B_1$. Then $r_3 \text{ wTr}(V) = \{(0, 1), (2)\}$, so $V \in r_3 B_2 B_1$. And $r_3 \text{ wTr}(r_3 O_V) = \{(1, 2), (3, 2)\} \cdot \{(3, 2), (4)\}$.

$r_3 \text{ Gen}(r_3 B_2 B_1) = \{r_3 B_2^{1 \oplus 1} B_1, B_1\}. \text{ Coef}(r_3 B_2^{1 \oplus 1} | r_3 B_2 B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$. $r_3 \text{ wTr}(r_3 B_2^{1 \oplus 1} B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$. $r_3 \text{ wTr}(r_3 B_2 B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$. $r_3 \text{ wTr}(r_3 B_2^{1 \oplus 1} | r_3 B_2 B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3}) = 16$. $|r'_i \text{ wTr}(r_3 B_2 B_1)| = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, $r_3 \text{ wTr}(r_3 B_2^{1 \oplus 1} B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3}) = 2$ and $r_3 \text{ wTr}(r_3 B_2 B_1) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3}) = 2$. It is easy to check that $12 \cdot 2 + 16 \cdot 2 = 56$. 

For a given set \( U \) in class \( B \), where \( B \in \mathcal{B}_r \), we denote the set of all \( U' \in B \) which \( \mathcal{C}_2 \)-equivalent to \( U \) by

\[
\tau_r CE(U) := \{ U' : U' \sim_r U \}.
\]

and we denote

\[
\tau_{r-1} wTr(\tau_r CE(U)) = \{ \tau_{r-1} wTr(U') : U' \in \tau_r CE(U) \}.
\]

We define the multiplicity of \( U \) in \( B \) under \( \mathcal{C}_2 \)-equivalent as

\[
\tau_r Mult(U) := \begin{cases} 
1/|\tau_{r-1} wTr(\tau_r CE(U))|, & \text{if } \exists V \in \mathcal{C}_2(2^{r-1} + 1), \text{s.t. } V \subseteq U, \\
0, & \text{otherwise}.
\end{cases}
\]

Remark. \( \tau_r CE(U) \) includes \( U \) itself.

**Lemma 9.** Let \( U \) be a set in class \( B \), if \( U \) is also in \( B' \), where \( B \in \mathcal{B}_r \), \( B' = \tau_r B_Q \in \mathcal{B} \) and \( Q = q_i^{[r]} q_{i-1}^{[r]} \cdots q_1^{[r]} \in \mathbb{Q} \), \( q_i > q_{i-1} > \cdots > q_1 \), then we have:

\[
\tau_r Mult(U) = \begin{cases} 
0, & \text{if } e_i \geq 2 \text{ and } q_i > 2^{i-2} \text{ or } e_i = 1 \text{ and } q_i + q_{i-1} > 2^{i-1}, \\
1/2^{i-1}, & \text{if } e_i \geq 2 \text{ and } q_i = 2^{i-2}, \\
1/(e_i - 1 + 1), & \text{if } e_i = 1 \text{ and } q_i + q_{i-1} = 2^{i-1}, \\
1/(2^{i-1} - n - 1), & \text{if } e_i = 1, e_i = 1 \text{ and } q_i = 2^{i-1}, \\
1, & \text{otherwise}.
\end{cases}
\]

Proof. Suppose \( \tau_r U \sim_r U \) then

- \( \forall \tau_r wTr(U) = \{(u_{q_i}, \cdots, u_{q_1}, \cdots, u_{q_1}, \cdots, u_{q_i}) \} \) where the number of \( (u_{q_i}) \) is \( e_i \).
- \( \forall \tau_{r-1} wTr(U) = \{(u_{q_i}, \cdots, u_{q_i}, \cdots, u_{q_i}, \cdots) \} \) where \( u_{q_j} \in \{ u_{q_i + 1, 2^{i-1} - n} : 0 \leq i < 2^{i-1} - n - 1 \} \), \( u_{q_j} \neq u_{q_i}' \) for any \( (j, k) \neq (j', k') \) and \( 1 \leq j, j' \leq t, 1 \leq k < k' \).
- Let \( U_{j,k} \) denote the subset of \( U \), which satisfy that \( \tau_r U_{j,k} = \{(u_{q_i})\} \), for \( 1 \leq j \leq t \) and \( 1 \leq k < e_j \).

Case 1 (If \( e_i \geq 2 \) and \( q_i > 2^{i-2} \) or \( e_i = 1 \) and \( q_i + q_{i-1} > 2^{i-1} \)). As \( d(U_{j,k}, U_{j',k}) > 2^{r-1} \) for any \( (j, k) \neq (j', k') \), by Corollary 3, it follows that \( U_{j,k} + U_{j',k} \in \mathcal{C}_2(p) \) or \( U_{j,k} + U_{j'-1,k} \in \mathcal{C}_2(p') \). \( p, p' > 2^{r-1}, 1 \leq k < k' \leq e_i \) and \( 1 \leq k'' \leq e_{i-1} \). Therefore, \( Mult(U) = 0 \).

Now let us consider the others. Suppose \( U' \sim_r U \) where \( U' \in B \).

- \( \forall \tau_{r-1} wTr(U') = \{(u_{q_i}', \cdots, u_{q_i}', \cdots, u_{q_i}', \cdots) \} \) where \( u_{q_j} \neq u_{q_j}' \) for any \( (j, k) \neq (j', k') \) and \( 1 \leq j, j' \leq t, 1 \leq k < e_j \).
- Let \( U_{j,k} \) denote the subset of \( U' \), which satisfy that \( \tau_{r-1} wTr(U_{j,k}) = \{(u_{q_i}')\} \), for \( 1 \leq j \leq t \) and \( 1 \leq k \leq e_j \).

For any \( V \in \mathcal{C}_2 \), it can be decomposed into two cubes \( W_1 \) and \( W_2 \) which are both in \( \mathcal{C}_{2-1} \). Since \( U' \sim_r U \), then there exists \( V_1 V_2, \ldots, V_d \in \mathcal{C}_2 \) such that \( U + U' = \sum_{j=1}^{d} \sum_{k=1}^{e_j} U_{j,k} + \sum_{j=1}^{d} \sum_{k=1}^{e_j} U_{j,k}' = \sum_{j=1}^{d} V_j \). So for any \( U_{j,k} \), there must exist \( U_{j,k}' \) such that \( U_{j,k} + U_{j,k}' \in C_{2-1} \) or \( U_{j,k} + U_{j,k}' = \emptyset \). Based on this observation, we analysis the value of \( \tau_r Mult(U) \) for other cases as follows.

Case 2 (If \( e_i \geq 2 \) and \( q_i + q_{i-1} = 2^{i-2} \)). In this case, \( U_{j,k} = U_{j,k} ' \) for any \( 1 \leq j < t \) and \( 1 \leq k < e_j \). Now let us consider \( U_{1,1}, U_{1,2}, \ldots, U_{1,e_1} \). According to the above analysis, we can choose two sets \( U_{1,j} ' \) and \( U_{1,j}' \) to make \( U_{1,j} + U_{1,j} ' + U_{1,j}' \) be a cube in \( \mathcal{C}_{2-1} \) and eliminate all other \( U_{i,k} \), i.e., let \( U_{i,j}' = U_{1,j} ' \) for others. Similarly, we can choose four sets \( U_{j,i}' U_{j,i}', U_{j,i}' U_{j,i}', U_{j,i}', U_{j,i}' \) to make \( U_{j-i} + U_{j-i}' + U_{j-i}' + U_{j-i}' + U_{j-i}' + U_{j-i}' \) be the union of two disjoint cubes in \( \mathcal{C}_2 \) and eliminate all other \( U_{i,k} \). Without loss of generality, we can choose \( 6, 8, \ldots, 2 \cdot [e_j/2] \) sets added to the corresponding sets \( U_{i,j} \) and make the resulted sets be unions of \( 3, 4, \ldots, [e_i/2] \) disjoint cubes in \( \mathcal{C}_2 \). So, the number of the weight trace in \( \mathcal{C}_{2e_i-1} \) of all those \( U' \) is \( \binom{e_i}{0} + \binom{e_i}{1} + \cdots + \binom{e_i}{e_i/2} = 2^{e_i-1} \). Thus \( Mult(U) = 1/2^{e_i-1} \).

Case 3 (If \( e_i = 1 \) and \( q_i + q_{i-1} = 2^{e_i-2} \)). In this case, \( U_{i,j} ' = U_{j,k} ' \) for any \( 1 \leq j < t-1 \) and \( 1 \leq k < e_j \). We need only to consider \( U_{1,1}, U_{1,2}, \ldots, U_{1,e_1-1} \), and the corresponding \( U_{1,1}' U_{1,2}' U_{1,2}' U_{1,2}' \) make the resulted two sets become a cube and eliminate all other \( U_{i,j} \). It is easy to know that the number of the weight trace in \( \mathcal{C}_{2e_i-1} \) of all those \( U' \) is \( e_i + 1 \). So \( Mult(U) = 1/(e_i-1 + 1) \).
Case 4 (If \( t = 1, e_t = 1 \) and \( q_t = 2^{t-1} \)). Due to \( U' + U \in \mathbb{C}_2 \), it follows that \( d(U, U') > 2^{n-r} \), i.e. \( u'_t, 1 \in \{ u + l \cdot 2^{n-r+1} : 0 \leq l < 2^{n-r-1} \} \). Therefore, the number of the weight trace in \( \mathbb{Z}^{2^{n-r}} \) of all those \( U' \) is \( 2^{n-r-1} \) and \( \mathcal{r}_{Mult}(U) = 1/(2^{n-r-1}) \).

Case 5 (Else). According to the above mentioned analysis, there does not exist a set \( U' \in \mathcal{B} \) except \( U \) itself such that \( U' \not\sim U \). Therefore, \( \mathcal{r}_{Mult}(U) = 1 \).

From Lemma 9, it can easily be seen that, for two sets \( U, V \in \mathcal{B} \), where \( \mathcal{B} \in _r \mathcal{B} \), if \( U, V \in \mathcal{r}_{B_Q} \), we have \( \mathcal{r}_{Mult}(U) = \mathcal{r}_{Mult}(V) \). This value depends only on \( \mathcal{r}_{B_Q} \) because it does not require the knowledge of exact values of the elements in the individual set. Therefore, we define \( \mathcal{Mult}(\mathcal{r}_{B_Q}) = \mathcal{r}_{Mult}(U) \) where \( U \in \mathcal{r}_{B_Q} \). Generally, we have

**Theorem 5.** Let \( U \) and \( V \) be two sets in \( \mathcal{B} \). If \( U, V \in \mathcal{B}' \), where \( \mathcal{B} \in _r \mathcal{B} \), \( \mathcal{B}' \in \mathcal{r}_{B_Q} \), then \( \mathcal{r}_{Mult}(U) = \mathcal{r}_{Mult}(V) \). And we define \( \mathcal{Mult}(\mathcal{B}') = \mathcal{r}_{Mult}(U) \), where \( U \in \mathcal{B}' \). Further more, if \( \mathcal{B}' = \mathcal{r}_{B_Q} \mathcal{B}_{Q_{r-1}} \cdots \mathcal{B}_Q \in \mathcal{r}_{B} \), we have

\[
\mathcal{Mult}(\mathcal{B}') = \prod_{j=1}^n \mathcal{Mult}(\mathcal{r}_{B_Q})^{h_j}.
\]

**Proof.** Suppose \( U \in \mathcal{B}' \) and \( \mathcal{r}_{Tr}(U) = \{ u_{1,1}, u_{2,1}, \ldots, u_{h_1,1}, u_{1,2}, \ldots, u_{h_2,1} \} \). Let \( U_{i,j} \) denotes the subset of \( U \), which satisfy that \( U_{i,j} \in \mathcal{r}_{B_Q} \) and \( \mathcal{r}_{Tr}(U_{i,j}) = \{ u_{i,j} \} \). Applying Lemma 9, we get \( \mathcal{Mult}(\mathcal{r}_{B_Q}) = \mathcal{r}_{Mult}(U_{i,j}) \) for each \( U_{i,j} \). Considering that each set of weight traces \( \mathcal{r}_{Tr}(U_{i,j}) \) only correlate with \( \{ u_{i,j} + l \cdot 2^{n-r+1} : 0 \leq l < 2^{n-r-1} \} \), the multiplicity of \( U \) is \( \mathcal{r}_{Mult}(U) = \prod_{j=1}^n \mathcal{Mult}(\mathcal{r}_{B_Q})^{h_j} \). And this value has nothing to do with the set \( U \) that we chose, so \( \mathcal{Mult}(\mathcal{B}') = \prod_{j=1}^n \mathcal{Mult}(\mathcal{r}_{B_Q})^{h_j} \).

**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 \( U_1 = \{ 1, 9, 17, 25 \} \), then \( U_1 \in \mathcal{r}_{B_4} \) and \( \mathcal{r}_{Tr}(U_1) = \{ (1,4) \} \). Let \( U_2 = \{ 1, 3, 9, 17 \} \), then \( U_2 \in \mathcal{r}_{B_4} \) and \( \mathcal{r}_{Tr}(U_2) = \{ (1,3), (1,1) \} \). Let \( \mathcal{r}_{Tr}(U_2) = \{ (1,3), (1,1) \} \). And \( \mathcal{Mult}(\mathcal{r}_{B_4}) = \mathcal{Mult}(\mathcal{r}_{B_2}) = \frac{1}{2} \).

Remark. The multiplicity of a class \( r \in \mathcal{B} \) in \( \mathcal{B} \) measures the multiplicity of the class in the sense of equivalence. In other words, if \( \mathcal{Mult}(\mathcal{B}) \neq 0 \) then there are \( \mathcal{B} \cdot \mathcal{Mult}(\mathcal{B}) \) sequences which pairwise non-\( C_2 \)-equivalent, where \( \mathcal{B} \) denote the number of sequences in class \( \mathcal{B} \). In the next section, we will explain that if \( \mathcal{Mult}(\mathcal{B}) = 0 \) if and only if for any sequence in class \( \mathcal{B} \) there exists sequences with smaller Hamming weight equivalent to it. Here, we highlight that, according to the proof of Lemma 9 and Theorem 5, it is evident that if \( U \in \mathcal{B} \) and \( \mathcal{r}_{Mult}(U) \neq 0 \) then \( U' \in \mathcal{B} \) for any \( U' \not\sim U \) and \( \mathcal{r}_U^[u'] = |U| \).

For a given multiset \( Q = q_i^{e_i} \cdots q_i^{e_i} \subseteq Q \), where \( q_i > q_{i-1} > \cdots > q_1 \), we define \( \mathcal{Exr}(Q) = q_i \), and for a given \( \mathcal{B} = \mathcal{r}_{B_Q} \in \mathcal{r}_{B}, \) we define \( \mathcal{Exr}(\mathcal{B}) = \mathcal{r}_{B_Q} \mathcal{Exr}(Q) = \mathcal{r}_{B_Q} \).

In addition, for a given \( \mathcal{B} = \mathcal{r}_{B_Q} \mathcal{B}_{Q_{r-1}} \cdots \mathcal{B}_Q \in \mathcal{r}_{B} \), we define \( \mathcal{Exr}(\mathcal{B}) = \mathcal{r}_{B_Q} \mathcal{B}_{Q_{r-1}} \cdots \mathcal{B}_Q \mathcal{Exr}(Q_1) \).

Note that if \( \mathcal{Exr}(Q_1) = \mathcal{Exr}(Q_j) \), then the two terms \( \mathcal{B}_{Q_{r-1}} \mathcal{Exr}(Q_1) \) and \( \mathcal{B}_{Q_{r-1}} \mathcal{Exr}(Q_j) \) are merge to be a single term \( \mathcal{B}_{Q_{r-1}}^{h_{Q_{r-1}} + h_{Q_j}} \) for \( j \neq j \). If \( \mathcal{Exr}(Q_1) = \mathcal{Exr}(Q_{1,2}) = \cdots = \mathcal{Exr}(Q_{n,1}), \mathcal{Exr}(Q_{1,2}) = \mathcal{Exr}(Q_{1,2}) = \cdots = \mathcal{Exr}(Q_{1,2}), \cdots, \mathcal{Exr}(Q_{1,1}) = \mathcal{Exr}(Q_{1,2}) = \cdots = \mathcal{Exr}(Q_{1,1}), \) where \( \bigcup_{i=1}^{n} \mathcal{Exr}(Q_{i,1}) = \{ t, t-1, \cdots, 1 \} \), we define

\[
\mathcal{Coe}_{Exr}(\mathcal{B}) = \prod_{u=1}^t \left( \sum_{i=1}^{n} h_{u,v} \right).
\]

Based on the definition of \( \mathcal{Coe}_{Exr}(\mathcal{B}) \), it is clear that for any element in \( \mathcal{Exr}(\mathcal{B}) \), there are \( \mathcal{Coe}_{Exr}(\mathcal{B}) \) elements in \( \mathcal{B} \) which correspond to it. Thus, we get that:
Theorem 6. Let $B$ be a class in $\mathcal{B}$. If $B' = \text{Extr}(B)$, then $r_i wTr(B) = |r_i wTr(B')| \cdot \text{CoeffExtr}(B)$.

For the specific sets $U \subseteq r_i B_0$ and $V = \bigcup_{j=1}^t V_j \subseteq r_i B_0 B_0^{i-1} \cdots B_0^{i-Q}$, where $V_j \subseteq r_i B_0^{j}$, we define

$$r_i \text{Extr}(U) := U', \text{ where } U' \subseteq U \text{ and } U' \subseteq r_i B_0^{j},$$

$$r_i \text{Extr}(V) := \bigcup_{j=1}^t r_i \text{Extr}(V_j).$$

Remark. $r_i \text{Extr}(U)$ is a one to many mapping but all elements in the codomain have the same weight trace in $\mathbb{Z}_{2^\alpha - 1.1}$. Now we consider the relations between classes of error sequences in $r_i \mathcal{B}'$ and $r_i \mathcal{B}$. Similar to Definition 6, we define the orbit of a set in $\mathbb{Z}_{2^\alpha - 1}$ as follow:

Definition 7. Let $B$ be a class in $\mathcal{B}$, where $B \subseteq r_i B_0^{j}$. We define the orbit of $B$ in $\mathbb{Z}_{2^\alpha - 1}$ as

$$r_i \text{O}_U := \{U' \in B : r_i wTr(U') = r_i wTr(U)\}.$$ 

And we define

$$r_i wTr(r_i \text{O}_U) := \{r_i wTr(U') : U' \in r_i \text{O}_U\}.$$ 

Lemma 10. Let $B$ be a class in $\mathcal{B}$, where $B = r_i B_0^{j} \cdots B_0^{i} \subseteq r_i B'$. Suppose $U$ is also in class $B'$ where $B' = r_i B_0^{j} \in r_i B'$. And suppose $r_i \text{Tr}(U) = (u_1, u_2, \cdots, u_i)$ and $r_i wTr(U) = \{(u_1)_p, (u_2)_p, \cdots, (u_i)_p\}$, where $0 \leq u_j < 2^{\alpha - i + 1}$ and $d = \sum_{j=1}^i d_j$. We have that, for all $1 \leq k \leq d$, if there exists $w^k$ such that $(d(u_k), u_k') = 2^{\alpha - i}$ then $p_{u_k} + p_{u_k'} = q$, and if there does not exist $w^k$ such that $(d(u_k), u_k') = 2^{\alpha - i}$ then $p_{u_k} = q$, where $1 \leq k' \leq d$ and $k \neq k'$. Then recursively decompose $r_i \text{Tr}(U)$ into the following sets:

1. Let $V_0 = \{(u_k, u_k') : d(u_k, u_k') = 2^{\alpha - i} \text{ and } p_{u_k} + p_{u_k'} = q\}$.
2. Let $V_1 = \{(u_j, u_j') : p_{u_j} = q\}$. Let $W_1 = \{(u_j)_p : (u_j)_p \in r_i wTr(U), \exists w \in (V_0 \cup V_1), s.t. u \in w\}$.
3. Suppose we have get $W_{t-1}$, then $W_t = W_{t-1} - \bigcup_{j=1}^t r_i \text{Extr}(V_j)$.
4. We then recursively generate all $V_s$ until $s = t$, such that $W_t = \emptyset$ by applying the following procedure: choose an element $(u_j)_p$ from $W_{t-1}$, then construct $V_s = \{(u_j, u_j') : d(u_j, u_j') = 2^{\alpha - i}, p_{u_j} = q\}$, $W_s = \{(u'_j)_p : (u'_j)_p \in W_{t-1}, \exists w \in V_s, s.t. u' \in w\}$.

Then the size of the trace set of the orbit of $U$ is

$$|r_i wTr(r_i \text{O}_U)| = 2^{\alpha - s_{t-1} m_s} \cdot \binom{e}{m_0, m_1, \cdots, m_t}$$

where $m_s = |V_s|$ for $0 \leq s \leq t$.

Proof. It is easy to see that $e = \sum_{s=0}^t m_s$. For each $\{u_k\} \subseteq V_s$, we can construct $\{u_k'\}$ such that $d(u_k, u_k') = 2^{\alpha - i}$. Thus, we can construct an $U'$ by substituting $(u_k)_{p_{u_k}}$ with $(u_k')_{p_{u_k}}$ in $r_i wTr(U)$. That is $r_i wTr(U') = \{(u_1)_{p_{u_1}}, (u_2)_{p_{u_2}}, \cdots, (u_i)_{p_{u_i}}\}$. It is easy to check that $U' \in r_i \text{O}_U$. For each element $\{u_k, u_k'\} \in V_s$, we can also construct an $U'$ by exchanging the index of $\{u_k, u_k'\}$ in $r_i wTr(U)$. That is $r_i wTr(U') = \{(u_1)_{p_{u_1}}, \cdots, (u_s)_{p_{u_s}}, \cdots, (u_i)_{p_{u_i}}\}$. It is also easy to check that $U' \in r_i \text{O}_U$. Hence, using the above method, for a given $B_0$, we can construct $2^{\alpha - s_{t-1} m_s}$ elements in $r_i wTr(B)$ which have the same weight trace in $\mathbb{Z}_{2^\alpha - 1}$ as $U$. Besides, suppose $|V_0| \geq 1, |V_1| \geq 1$, with regard to elements $\{u_k, u_k'\} \in V_0$ and $\{u_k\} \in V_1$, we can construct $U'$, such that $r_i wTr(U') = r_i wTr(U) - \{(u_k)_0, (u_k')_0\} \cup \{(u_k)_0, (u_k)_0, (u_k')_0\}$. Where $d(u_k, u_k') = 2^{\alpha - i}$. It is easy to see that $U' \in r_i \text{O}_U$. Generally, with regard to any two elements in $V = \bigcup_{s=0}^t V_s$, we can construct a set $U' \in r_i \text{O}_U$ in a similar way. While, applying the above constructing process on two elements within a single set $V_s$ will lead an $U'$ with identity weight trace in $\mathbb{Z}_{2^\alpha - 1,i}$. Thus by combination method, for a given set $U$, we can construct $\binom{m_0, m_1, \cdots, m_t}{e}$ elements in $r_i wTr(B)$ which have the same weight trace in $\mathbb{Z}_{2^\alpha - 1}$ as $U$. Therefore the size of the weight trace set of the orbit of $U$ is $|r_i wTr(r_i \text{O}_U)| = 2^{\alpha - s_{t-1} m_s} \cdot \binom{e}{m_0, m_1, \cdots, m_t}$. \qed

Example 4. Let $L = 2^n - (2^{\alpha - i} + 2^{\alpha - i} + 2^{\alpha - i})$ where $n = 8, r_1 = 1, r_2 = 2, r_3 = 3$ and $r_4 = 4$. Let set $U$ such that $r_i \text{Tr}(U) = \{(1, 2, 3, 4, 5, 18, 19, 20, 21), r_i wTr(U) = \{(1)_6, (2)_5, (3)_4, (4)_4, (5)_3, (18)_1, (19)_1, (20)_2, (21)_1\}$. Then $B = B_0 B_0^{1} B_0^{2} B_0^{3} B_0^{4}$ and $U \subseteq B'$.

Then $r_i \text{O}_U = \{U \in B : r_i wTr = \{(1)_6, (2)_5, (3)_4, (4)_4, (5)_3\}\}$. Applying Lemma 10, we get $V_0 = \{(5, 21), V_1 = \{13\}, V_2 = \{(2), 18\}, V_3 = \{(3, 19\), \{4, 20\}\}.$

With regard to element $\{1\} \in V_1$, we can construct $U'$, s.t. $r_i wTr(U') = r_i wTr(U) - \{(1)_6\}$ with regard to element $\{2, 18\} \in V_2$, we can construct $U'$, s.t. $r_i wTr(U') = r_i wTr(U) - \{(2)_5\} \cup \{(18)_1\}$. With regard to element $\{1\} \in V_1$ and element $\{3, 19\} \in V_3$, we can construct $U'$, s.t. $r_i wTr(U') = r_i wTr(U) - \{(1)_6, (3)_4, (19)_2\} \cup \{(1)_4, (17)_2, (3)_6\}.$
For any $U' \in \mathcal{B}$, if $U' \in \mathcal{B}'$ then we can also get the sets $V'_0, V'_1, \ldots, V'_s$ which satisfy that $|V'_s| = |V_s| = m_s$ for $0 \leq s \leq t$. So we have $|_{r_i} wTr(\mathcal{O}_{U'}) = |_{r_i} wTr(\mathcal{O}_U)|$. We define Coef($\mathcal{B}' \mid \mathcal{B}$) = $|_{r_i} wTr(\mathcal{O}_{U'})$.

**Corollary 6.** Let $U$ be a set in class $\mathcal{B}$ where $\mathcal{B} \in \mathcal{B}'$. And suppose $U$ is also in class $\mathcal{B}' = r_iB'_0 \cdot B'_0 \cdot \cdots \cdot B'_m$. Suppose $U = \bigcup_{j=1}^t U_j \in \mathcal{B}'$ where $U_j \in r_iB'_j$, then we have

$$|_{r_i} wTr(\mathcal{O}_{U})| = \prod_{j=1}^t |_{r_i} wTr(\mathcal{O}_{U_j})|.$$ 

Similarly, for any $U' \in \mathcal{B}$, if $U' \in \mathcal{B}'$ then we can also get $|_{r_i} wTr(\mathcal{O}_{U'}) = |_{r_i} wTr(\mathcal{O}_U)|$. Denote $U_j \in \mathcal{B}_j$ where $\mathcal{B}_j$ is a class in $\mathcal{B}'$. We define Coef($\mathcal{B}' \mid \mathcal{B}$) = $\prod_{j=1}^t$ Coef($\mathcal{B}'_j \mid \mathcal{B}_j$). Then we have

**Theorem 7.** Let $\mathcal{B}$ be a class in $\mathcal{B}'$, we denote $\mathcal{B}' = \mathcal{B}'_0 \cdot \mathcal{B}'_1 \cdot \cdots \cdot \mathcal{B}'_t \in \mathcal{B}_0$. Then the size of the weight trace in $\mathbb{Z}_{2^{m-t}}$ of all elements in $\mathcal{B}$ is

$$|_{r_i} wTr(\mathcal{B})| = \sum_{\mathcal{B}' \in \mathcal{B}_0} \text{Coef}(\mathcal{B}' \mid \mathcal{B}) \cdot |_{r_i} wTr(\mathcal{B}')|.$$ 

Remark that, given $\mathcal{B} = r_iB'_0 \cdot r_iB'_1 \cdot \cdots \cdot r_iB'_t$ and $\mathcal{B}' = r_iB'_0 \cdot \cdots \cdot r_iB'_t \in \mathcal{B}$, we have that each $q_j$ is equal to the sum of $p_j$ and $p_j$ or to $p_j$ where $p_j, p_j \in \{p_1, p_1, \ldots, p_t\}$ and $j' \leq j'$. If we know all the decompose of each $q_j$, then we can directly compute the value of $\text{Coef}(\mathcal{B}' \mid \mathcal{B})$. For instance, for two given classes $\mathcal{B} = r_iB'_0 \cdot r_iB'_1 \cdot \cdots \cdot r_iB'_t$ and $\mathcal{B}' = r_iB'_0 \cdot \cdots \cdot r_iB'_t$, the decomposition of those $q_j$ are $7 = 4 + 3$, $6 = 3 + 3$, $5 = 4 + 1$, $4 = 2 + 2$, then we have $\text{Coef}(\mathcal{B}' \mid \mathcal{B}) = 2^2 \cdot 2^1 = 4$.

**Example 5.** Let $L = 2^n - (2^{n-1} + 2^{n-2} + 2^{n-3})$ where $n = 6, r_1 = 1, r_2 = 3$ and $r_3 = 6$.

Let set $U = \{1, 9, 19, 33, 51\} \in r_iB'_0$. Then $wTr(U) = \{(1), (3), (9), 1\}$ and $wTr(U) = \{(1), (3), (2), 1\} \subseteq \mathcal{A}'(L)$, so $U \in r_iB'_0 \cdot r_iB'_1 \cdot wTr(\mathcal{O}_{U'}) = \{(1), (3), (9), 1\}$, $(1), (3), (2), 1 \subseteq \mathcal{A}'(L)$. Coef($\mathcal{B}' \mid \mathcal{B}_2$) = 4.

To compute $\text{Coef}(\mathcal{B}' \mid \mathcal{B}_2)$ = 2, $\text{Coef}(\mathcal{B}' \mid \mathcal{B}_2)$ = 2, $\text{Coef}(\mathcal{B}' \mid \mathcal{B}_2)$ = 4, $\text{Coef}(\mathcal{B}' \mid \mathcal{B}_2)$ = 8. It is evident to check that $1680 = 56 \cdot 2^1 + 56 \cdot 2^1 + 168 = 8^3$.

In the next section, we will use the quantitative relations above to get the number of sequences with given $k$-error linear complexity.

**4 The Algorithm for Computing $\mathcal{N}_k(L)$**

For each error sequences set $\mathcal{E}_m$, we denote $E^R_m$ the maximum subset of $\mathcal{E}_m$ in which the error sequences are pairwise non-equivalent and there does not exist error sequence with Hamming weight not larger than $m$ equivalent with it and $\mathcal{A}(L) + E \subseteq A_k(L)$ for any $E \in E^R_m$, that is,

$E^R_m := \{E \in \mathcal{E}_m : \mathcal{A}(L) + E \subseteq A_k(L) \}$ and $\#E' \in E_m$, $m \leq m'$, s.t. $E' \sim E$ where $E' \neq E \}, 0 < m \leq k$.

Consequently, we have

$$A_k(L) = \bigcup_{m=0}^k \mathcal{A}(L) + E^R_m$$

Denote by $\mathcal{N}_e(k, L)$ the size of $E^R_m$ when the errors is $k$ and $L = wH(2^n)$. Then we have that the number of sequences with $k$-error linear complexity $L$ is

$$\mathcal{N}_k(L) = \left( \sum_{m=0}^k \mathcal{N}_e(k, L) \right) \cdot 2^{L-1}.$$ 

In the following we will use those quantitative relations in the last section to construct an algorithm for computing the value of $\mathcal{N}_e(k, L)$ for given $k$ and $L$.

For a given set $U \subseteq r_iB'_m$, we define a mapping

$$F(U) := (U_0', U_1, U'_1, \ldots, U_T, U'_T)$$
where $U_0^n = U$, and $U_i = U_{i-1}^{m-i}$, for $1 \leq i \leq T$. And we define:

$$\text{Gen}(\varphi B_0^{n}) = \{ (B_0^n, B_1, B_1', \ldots, B_T, B_T', B_T'') : \exists \mathcal{B} \in \varphi B_0^{n}, \text{s.t.} F(U) \in \{ B_0^n, B_1, B_1', \ldots, B_T, B_T', B_T'' \} \}.$$ 

Where $B_0^n = \varphi B_0^{n}$, $B_1 \in \mathcal{R} \mathcal{B} \subseteq B'$, and $B_T' \subseteq B$. Note that $F(U) \in \{ B_0^n, B_1, B_1', \ldots, B_T, B_T', B_T'' \}$ means that $U_0^n \in B_0^n$ and $U_i \in B_i$, $U' \in B'$, and $U'' \in B''$ for $1 \leq i \leq T$.

**Theorem 8.** For giving errors $k$ and $k$-error linear complexity $L$, then the size of $E_m^k$ ($1 \leq m \leq k$) is

$$\text{Num}(E_m^k) = \sum_{\mathcal{B} \in \text{Gen}(\varphi B_0^{2^n})} \left| \varphi wTr(B_T'') \right| \cdot \prod_{j=1}^{T} \text{Imp}(B_j') \cdot \text{Coeff}(B_j') \cdot \text{Coeff}_{\text{Ext}}(B_j) \cdot \text{Coeff}(B_j | B_{j-1}').$$

Note that $\mathcal{B} = (B_0^n, B_1, B_1', \ldots, B_T, B_T', B_T'') \in \text{Gen}(\varphi B_0^{2^n})$. And for a given $\mathcal{B}$ in $\varphi \mathcal{B}$, where $\mathcal{B} = \varphi B_0^{n}, \varphi B_1, \ldots, \varphi B_T$. $\text{Imp}(\mathcal{B})$ is defined as follow:

$$\text{Imp}(\mathcal{B}) := \begin{cases} 1, & \text{if } q \leq \text{Imvalue} \\ 0, & \text{otherwise} \end{cases}, \text{ where } \text{Imvalue} = \left\lceil \frac{2T + m - k}{2} \right\rceil.$$ 

Especially, $\text{Num}(E_m^k) = 1$ if $\text{Imvalue} > 0$ and $\text{Num}(E_m^k) = 0$ for else.

We need to provide some lemmas before proceeding the proof of Theorem 8.

**Lemma 11.** All of the elements in $\varphi B_0^{n}$ can be decomposed into pairwise disjoint subsets $U_j$, such that for any $U \in \mathcal{U}_j$, $F(U)$ belong to the same $\mathcal{B}$, where $\mathcal{B} \in \text{Gen}(\varphi B_0^{n})$. And we have that the number of sets in $\varphi B_0^{n}$ is

$$|\varphi B_0^{n}| = \left( \frac{2^n}{m} \right) = \sum_{\mathcal{B} \in \text{Gen}(\varphi B_0^{n})} \left| \varphi wTr(B_T'') \right| \cdot \prod_{j=1}^{T} \text{Coeff}(B_j') \cdot \text{Coeff}_{\text{Ext}}(B_j) \cdot \text{Coeff}(B_j | B_{j-1}').$$

**Proof.** For a given $\mathcal{B} \in \text{Gen}(\varphi B_0^{n})$, combing Theorem 4, 6 and 7, we obtain that the number of $U \in \varphi B_0^{n}$ which satisfy $F(U) \in \mathcal{B}$ is $|\varphi wTr(B_T'')| \cdot \prod_{j=1}^{T} \text{Coeff}(B_j') \cdot \text{Coeff}_{\text{Ext}}(B_j) \cdot \text{Coeff}(B_j | B_{j-1}')$. Then the lemma will be proved by showing that for any $U \in \varphi B_0^{n}$ there only exists one $\mathcal{B} \in \text{Gen}(\varphi B_0^{n})$ such that $F(\mathcal{B}) \in \mathcal{B}$. Suppose $F(U) = (U_0^n, U_1, U_1^n \ldots, U_l, U_l^n, U_l'^n)$ (Recall that $U_l = U_{l-1}'^n, U_l'' = \text{Ext}(U_l)$, and $U_l'^n = U_l''$ for $1 \leq i \leq T$). According to the definition of $\text{Ext}(U)$, no matter which $U_l'$ we choose, they are all in the same $B_i$. Thus the choice of $U_l'$ has nothing with $B_i$. Then, it is evident to see that the lemma holds.

**Lemma 12.** Let $\mathcal{B} = (B_0^n, B_1, B_1', \ldots, B_T, B_T', B_T'') \in \text{Gen}(\varphi B_0^{n})$, for any set $U \in \varphi B_0^{n}$, $F(U) \in \mathcal{B}$, there exists $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$, and only if there exists $j$ such that $\text{Mult}(B_j) = 0$. Where $0 \leq t < T$ and $1 \leq j \leq T$.

**Proof.** Suppose there exists $j$ such that $\text{Mult}(B_j) = 0$, where $1 \leq j \leq T$. Suppose $B_j = B_0^n B_1 B_1'' \ldots B_j$. From Theorem 5, we have that there exists $t$ such that $\text{Mult}(B_j) = 0$, where $1 \leq t \leq s$. It follows that, there exists $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$, where $1 \leq l \leq T$.

Assume there exists $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$ where $0 \leq t < T$. Denote the smallest $t$ by $t_0$. Then we have $\text{Mult}(B_j) \neq 0$ for $1 \leq j < t_0$. Therefore, there exists $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$ where $t' < t_0$ which contradict with $t_0$ is the smallest number. Suppose $B_0 = B_0^n B_1 B_1'' \ldots B_{j-1}'$, if $\text{Mult}(B_0) \neq 0$, then we have $\text{Mult}(B_0) \neq 0$ for $1 \leq j \leq s$. So there does not exist $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$. As $\text{Ext}(U_{t_0-1}') = U_{t_0-1}' = U_{t_0-1} = U_{t_0}$, so there does not exist $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U_{t_0-1}$ as well. By that analogy, we have that there does not exist $V \in \mathcal{C}_2 (2^n - 1)$ such that $V \subseteq U$ which contradict the condition. Thus $\text{Mult}(B_0) = 0$.

**Lemma 13.** Let $E$ be an error sequence in set $E_m$. Then there exists $E' \in E_m'$, such that $E' \sim E$, if and only if there exists a set $U \in \mathcal{C}_2 (2^n - 1)$, such that $\text{Mult}(B_j) = 0$, where $m' < m$ and $1 \leq t \leq T$.

**Proof.** Assume there exists $U \in \mathcal{C}_2 (2^n - 1)$, such that $U \subseteq \text{supp}(E)$, where $1 \leq t \leq T$. Suppose $\text{supp}(E) = U_0 U$, where $U_0 \cap U = \emptyset$. We choose a set $U$ from $\{ V \subseteq \mathcal{C}_2 : |V| = 2^n - 1 \}$, $|V \subseteq \mathcal{C}_2 |$. And then construct a sequence $E'$ based on $U_0$ and $\mathcal{U}$, such that $E'(V) = U_0 U_0$. As $\text{Mult}(E') = |U_0| + |U| < |U_0| + |U| = w_t(E)$ and $\text{LC}(E + E') = \text{LC}(U + U) < L$. According to Theorem 1, we have $E' \sim E$. Therefore, we conclude that there exists $E' \in E_m'$, such that $m' < m$, such that $E' \sim E$.

Next, assume $E \sim E$. From Theorem 4, there exists a pair of disjoint subsets $U_1, U_2, \ldots, U_q \subseteq \mathcal{C}$ and $V_1, V_2, \ldots, V_d \subseteq \mathcal{C}$ such that $\text{supp}(E + E') = U_0 U_0 \cup U_1$, where $d'$ is even. If $|\text{supp}(E) \cap W| \leq 2^{d'-1}$ for all $W \in \mathcal{C}_2$, where $1 \leq t \leq T$, then the number of elements of any set $U_i$ which comes from $\text{supp}(E)$ will be at most half of $|U_i|$. Because $\text{Imvalue} = m - k/2 + 2^{T-1} - 2^{T-1}$, the number of elements of each cube $V_j$ which comes from $E$ is also at most half of $|V_j|$. Thus $|\text{supp}(E)| \leq (|\text{supp}(E')|)$, which is contrary to the fact that $m' < m$. Therefore, there exists a set $U \in \mathcal{C}_2 (2^n - 1)$ such that $U \subseteq \text{supp}(E)$. $\square$
Lemma 14. Let $\mathcal{B} = (B_0, B_1, B_1', B_1'', \cdots, B_T, B_T') \in Gen(\mathcal{E})$. For any set $U \in \mathcal{E}$, which satisfies that $F(U) \in \mathcal{B}$, there exists set $V \in C(\text{Impvalue})$ such that $V \subseteq U$, if and only if there exists $j$ such that $\text{Imp}(B'_j) = 0$, where $1 \leq j \leq T$.

For the proof of this lemma please refer to Appendix A.

Lemma 15. Let $E$ be an error sequence in the set of remaining sequences in $E_{\mathcal{B}}$, and there does not exist error sequence $E'$ with lower Hamming weight equivalent to it. We have that $(\mathcal{A}(L) + E) \cap A'_2(L) = \emptyset$, if and only if there exists a set $U \in C(\text{Impvalue})$ such that $U \subseteq \text{supp}(E)$, where $\text{Impvalue} = m - k/2 + 2T - 1$ and $1 \leq \text{Impvalue} \leq m$.

Proof. The proof is similar as Lemma 14. Here, we only prove the necessity. Assume $(\mathcal{A}(L) + E) \cap A'_2(L) = \emptyset$, then there exist $E' \in \mathcal{E}$ such that $\mathcal{L}(E' + E) = \mathcal{L}(E)$. From Theorem 5, there exist pairwise disjoint cubes $U_1, U_2, \ldots, U_T \in \mathcal{C}$ and $V_1, V_2, \cdots, V_d \in \mathcal{C}$ such that $\text{Imp}(E' + E) = \sum_{p = 1}^{T}\sum_{d = 1}^{T} V_d$, where $d'$ is odd. Let $W = \text{supp}(E) \cap \text{supp}(E')$. Then, $W_1 = (\text{supp}(E) - W) \cup (\bigcup_{d = 1}^{T} V_d)$. Let $W_1 = (\text{supp}(E) - W) \cup (\bigcup_{d = 1}^{T} V_d)$. Then, $W_1 \cup W_2 = (\text{supp}(E) - W) \cup (\bigcup_{d = 1}^{T} V_d)$. According to the proof of Theorem 13, the number of elements of any cube $U_p$, which come from $E$, is at most half of $|U_p|$, thus $|W_2| \leq |W_1|$. Therefore $2m - |W_1| - |W| \leq |\text{supp}(E')| - |W|$, it follows that $2m - |W_1| \leq |\text{supp}(E')| - |W|$. This implies that there exists $U' \subseteq V_1$ and $U' \in C(\text{Impvalue})$ such that $U' \subseteq \text{supp}(E)$.

Combining Lemma 11, 12 and 14, we can get the value $\text{Num}(E_{\mathcal{B}}^m)$ when $m$ and $k$ are both even. The other cases of the proof value $\text{Num}(E_{\mathcal{B}}^m)$ are all similar with this case and we omit the proof. In Appendix ?, we use a simple example to illustrate the process of computing $\text{Num}(E_{\mathcal{B}}^m)$.

Therefore, the main difficult of computing the value $\text{Num}(E_{\mathcal{B}}^m)$ lies in how to generate all elements in $\text{Gen}(\mathcal{E})$, which lead to nonzero terms in the function of $\text{Num}(E_{\mathcal{B}}^m)$, i.e. those $\mathcal{B} \in \text{Gen}(\mathcal{E})$ which lead $\text{Imp}(B'_j) \neq 0$ and $\text{Mult}(\mathcal{B}) \neq 0$ (for $1 \leq i \leq T$). According to the analysis in Section 7, the problem of generating $\mathcal{B}$ can be reduced into the following two problems:

1. For a given $\mathcal{B} \in \mathcal{E}$, how to generate set $\mathcal{E}(\mathcal{B})$.
2. For a given $\mathcal{B} \in \mathcal{B}$, how to generate set $\mathcal{B}$. for $\mathcal{B}$.

In the first problem, considering that for any $\mathcal{B} \in \mathcal{E}$, the class $\mathcal{E}(\mathcal{B})$ is uniquely determined, thus it is natural to begin with generating $\mathcal{E}(\mathcal{B})$ from $\mathcal{B}$. For a given $\mathcal{B} = (B_0, B_1, B_1', B_1'', \cdots, B_T, B_T') \in \mathcal{E}$, we denote $\mathcal{E}(\mathcal{B}) = \{n, \mathcal{E}(\mathcal{B}) : \mathcal{B} = \mathcal{B}(n, \mathcal{E}(\mathcal{B}))\}$, which can be generated by the following enumeration description:

$$
\mathcal{E}(\mathcal{B}) = \{n, B_{p_1}', B_{p_2}', \cdots, B_{p_l}' \} : \begin{cases}
  e_j = d_j, & \text{if } p_j > 2^{i-2} \\
  0 \leq e_j \leq d_j, & \text{if } \exists j > j, \text{ s.t. } p_j + p_i \leq 2^{i-1}, \text{ for all } 1 \leq j \leq l \\
  1 \leq e_j \leq d_j, & \text{otherwise}
\end{cases}
$$

Note that if $e_j = 0$, then the corresponding term $B_{p_j}'$ is moved out.

For any $\mathcal{B}' = (B_{p_1}', B_{p_2}', \cdots, B_{p_l}') \in \mathcal{E}(\mathcal{B})$, denote $\mathcal{E}(\mathcal{B}) = \{n, B'' : n \in \mathcal{B}, \text{ and } \mathcal{B} = \mathcal{B}(n, \mathcal{B})\}$. We define

$$
\text{Coeff}(\mathcal{B}' | \mathcal{B}) = \sum_{\mathcal{B}'' \in \mathcal{E}(\mathcal{B})} \text{Coeff}(\mathcal{B}' | \mathcal{B}) \cdot \text{Coeff}(\mathcal{B}'' | \mathcal{B}) \cdot \text{Mult}(\mathcal{B}'').
$$

Then problem 1 turns into how to fast compute the value of $\text{Coeff}(\mathcal{B}' | \mathcal{B})$. For a $\mathcal{B'} = (B_{p_1}', B_{p_2}', \cdots, B_{p_l}') \in \mathcal{E}(\mathcal{B})$, we denote $\Delta = (B_{p_1}', B_{p_2}', \cdots, B_{p_l}')$ where $f_j = d_j - e_j$ for $1 \leq j \leq l$. Then, each $\mathcal{B}' \in \mathcal{E}(\mathcal{B})$ can be regarded as a kind of assignment which assigns a cube fragment of $\mathcal{B}$ in $\Delta$ to $\mathcal{B}'$. And the set $\mathcal{E}(\mathcal{B})$ can be regarded as all possible assignment. For instance, let $\mathcal{B} = (B_{p_1}', B_{p_2}', B_{p_3}', B_{p_4}')$, then $\Delta = (B_{p_1}', B_{p_2}', B_{p_3}', B_{p_4}')$. We inverse the operation ‘Extr’ by assigning cube fragments $r_{B_3}, r_{B_4}, r_{B_1}$ and $r_{B_1}$ in $\Delta$ to $\mathcal{B}'$, that is, $\mathcal{E}(\mathcal{B}) = \{n, B_{p_1}', B_{p_2}', B_{p_3}', B_{p_4}' \}$. The specific procedure of assigning $\Delta$ to $\mathcal{B}'$ to generate $\mathcal{E}(\mathcal{B})$ and then return the value of $\text{Coeff}(\mathcal{B}' | \mathcal{B})$ is shown as Algorithm 2 in Appendix B.

As for problem 2, for a given class $\mathcal{B} = (B_0, B_0', B_1, B_1', B_1'', \cdots, B_T, B_T')$, we need to generate all elements in $\mathcal{E}(\mathcal{B})$. This problem can be regard as generating all sets $V$ from a given multiset $U$, where $U = (r_{B_0}, r_{B_1}, r_{B_2}, \cdots, r_{B_p}, \cdots, r_{B_T}, r_{B_T}')$, in which the number of $r_{B_0}$ is $d_1$ for $1 \leq j \leq l$. And where the set $V$ satisfy that the element in it equals to one in $U$ or equal to the “sum” of two elements in $U$. For example, let $\mathcal{B} = (B_0, B_0')$, then $U = (r_{B_0}, r_{B_0'})$. From $U$, we can generate $(r_{B_3}, r_{B_3}, r_{B_2}, r_{B_0}, r_{B_0}), (r_{B_5}, r_{B_3}, r_{B_5})$ in which $r_{B_0}$ and $r_{B_3}$ are respectively regarded as the “sum” of $r_{B_0}$ and $r_{B_3}$ and the “sum” of $r_{B_0}$ and $r_{B_3}$. Algorithm 3 in Appendix B shows the specific procedure to generate $\mathcal{E}(\mathcal{B})$ for a given class $\mathcal{B} \in \mathcal{B}$.
Considering that different $B$ in $Gen(J_{0}B^{2m}_{k})$ can have same prefix and start to be different from a particular class $B$, we actually organize those $B$ in $Gen(J_{0}B^{2m}_{k})$ by a prefix tree structure to automatically compute the value of $Num(E^{B}_{2m})$. Fig. 1 depicts how the elements in $Gen(J_{0}B^{1}_{k})$ and $Gen(J_{0}B^{2}_{k})$ under various Impvalue are organized by trees.

For a given class $B$ in $r_{i-1}B$, similar to the definition of $Gen(J_{0}B^{2m}_{k})$, we define

$$Gen(B) := \{ (B'_{i-1}, B_{i}, B'_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) : \exists U \in B \ s.t. \ F_{i-1}(U) \in (B''_{i-1}, B_{i}, B'_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \}$$

where $F_{i-1}(U) = (U''_{i-1}, U_{i}, U'_{i}, \cdots, U_{T}, U'_{T}, U''_{T})$ and $U''_{i-1} = U, U_{i} = U''_{i-1}, U'_{i} = r_{i-1}Extr(U_{i})$ and $U''_{i} = U'_{i}$ for $i \leq j \leq T$. And $F_{i-1}(U) \in (B''_{i-1}, B_{i}, B'_{i}, \cdots, B_{T}, B'_{T}, B''_{T})$ means $U''_{i-1} \in B''_{i-1}$ and $U_{j} \in B_{j}, U'_{j} \in B'_{j}, U''_{j} \in B''_{j}$ for $i \leq j \leq T$.

And similar to the definition of $Num(J_{0}B^{2m}_{k})$, we define

$$r_{i-1}Num(B) := \sum_{B \in Gen(B)} |_{r_{i-1}Tr(B''_{T})} \cdot \prod^{T}_{j=i}Imp(B''_{j}) \cdot Coef(B''_{j} | B'_{j}) \cdot Coef_{Extr}(B_{j}) \cdot Mult(B_{j}) \cdot Coef(B_{j} | B''_{j-1}),$$

where $\mathbb{B} = (B''_{i-1}, B_{i}, B'_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \in Gen(B)$.

For a given class $B$ in $r_{i}B'$, similarly, we define

$$Gen(B) := \{ (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) : \exists U \in B \ s.t. \ F_{i}(U) \in (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \}$$

where $F_{i}(U) = (U_{i}, U'_{i}, U''_{i}, \cdots, U_{T}, U'_{T}, U''_{T})$ and $U_{i} = U, U'_{i} = r_{i}Extr(U_{i}), U''_{i} = U'_{i}$ and $U_{j+1} = U''_{i}$ for $i \leq j < T$. And $F_{i}(U) \in (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T})$ means $U_{j} \in B_{j}, U'_{j} \in B'_{j}$ and $U''_{j} \in B''_{j}$ for $i \leq j \leq T$.

And for a given class $B$ in $r_{i}B'$, we define

$$r_{i}Num(B) := \sum_{B \in Gen(B)} Coef(B''_{i} | B_{i}) \cdot |_{r_{i}Tr(B''_{T})} \cdot \prod^{T}_{j=i+1}Imp(B''_{j}) \cdot Coef(B''_{j} | B'_{j}) \cdot Coef_{Extr}(B_{j}) \cdot Mult(B_{j}) \cdot Coef(B_{j} | B''_{j-1}),$$

where $\mathbb{B} = (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \in Gen(B)$.

**Theorem 9.** The recursive Algorithm 1 can compute the value of $r_{i-1}Num(B)$ for any class $B$ in $r_{i-1}B$ and the value of $r_{i}Num(B)$ for any class $B$ in $r_{i}B'$.

**Proof.** According to Theorem 5 and Lemma 9, for a given class $B$ in $r_{i-1}B$, if Max2 < $2^{i-1}$, then for any $B = (B''_{i-1}, B_{i}, B'_{i}, \cdots, B_{T}, B'_{T}, B''_{T})$ in $Gen(B)$, we have that $Mult(B_{j}) = 1$ for $i \leq j \leq T$.

For a given class $B$ in $r_{i}B'$, if Max4 < $2^{i}$, then $Max2 < 2^{i}$ for any $B$ in $r_{i}Gen(B)$. Therefore for a given class $B$ in $r_{i}B'$, if Max4 < $2^{i}$, then for any $B = (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \in Gen(B)$, we have that $Mult(B_{j}) = 1$ for $i < j \leq T$.

If $Max2 < Impvalue$ for a given class $B$ in $r_{i}B'$, then for any $B = (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \in Gen(B)$, we have that $Imp(B''_{j}) = 1$ for $i \leq j \leq T$.

If $Max2 < Impvalue$ for a given class $B$ in $r_{i}B'$, then for any $B = (B_{i}, B'_{i}, B''_{i}, \cdots, B_{T}, B'_{T}, B''_{T}) \in Gen(B)$, we have that $Imp(B''_{j}) = 1$ for $i < j \leq T$.

Thus, for a given class $B$ in $r_{i}B'$, if $r_{i}IsEND = 1$, then we have $r_{i}Num(B) = \binom{2^{n-r_{i}}}{{r_{i}}}$. Similarly, for a given class $B$ in $r_{i}B'$ if $r_{i}IsEND = 1$, then we have $r_{i}Num(B) = \binom{2^{n-r_{i}}}{r_{i}}$.

Therefore, according to the definition of $r_{i-1}Num(B)$ for class $B$ in $r_{i-1}B$ and $r_{i}Num(B)$ for class $B$ in $r_{i}B'$, Algorithm 1 can compute the value of $r_{i-1}Num(B)$ and the value of $r_{i}Num(B)$.

According to Theorem 9, once input $J_{0}B^{2m}$ to procedure $J_{0}Num(B)$ in Algorithm 1, i.e. call procedure $J_{0}Num(J_{0}B^{2m}_{k})$, we will get the value of $Num(E^{B}_{2m})$. Since in many cases, values of $Coef(B''_{j} | B_{j})$ are zero and $J_{0}IsEND(B')$ are 1 for given $B$ in $r_{i-1}B$ and $B'$ in $Extr(J_{0}Gen(B))$, the execution of procedure $J_{0}Num(J_{0}B^{2m}_{k})$ is very fast, and thus it is very efficient to get the value of $Num(E^{B}_{2m}_{k})$. In Appendix D, we present the experiment results on $N^{k}_{k}(L)$ when $k$ is even and the periodic $2^{k}$ is 64 using algorithms in this paper. The entire experiment costs only a few minutes.
of classes defined based on the specific equivalence we build on error sequences. To calculate coefficients of error sequences. Based on these quantitative relations, we propose an algorithm to automatically generate those sequences.

We introduce concepts of other special periodic sequences. Thus we can use those cube fragment as basic modules to construct classes of error sequences with specific structures. Error sequences with the same specific structures can be represented by a single symbolic representation, instead of the sequences plus error sequences, that leads to the simplicity of the resulted procedure. We use the weight trace and orbit as basic modules to construct classes of error sequences with specific orbit numbers.

Algorithm 1 Compute $n_{r}^\prime \cdot \text{Num}(B)$ for $B \in \epsilon_{n}^\prime B$ and $n_{r}\cdot \text{Num}(B)$ for $B \in \epsilon_{n} B$.

```
1: procedure $n_{r}^\prime \cdot \text{Num}(B)$
2: Input: $B \in \epsilon_{n}^\prime B$
3: Output: $n_{r}^\prime \cdot \text{Num}(B)$
4: num ← 0
5: while $\exists B' \in \text{Ext}(_{n} \text{Gen}(B))$ and $\text{Coeff}(B' \mid B) \neq 0$ do
6: if $\epsilon_{r} \text{ISEND}(B') = 1$ then
7: num ← num + Coef($B' \mid B$) \cdot $2^{r-1}$
8: else
9: num ← num + Coef($B' \mid B$) \cdot $r_{n} \cdot \text{Num}(B')$
10: end if
11: end while
12: return num
13: end procedure

14: function $\epsilon_{r} \text{ISEND}(B)$
15: Input: $B \in \epsilon_{r} B$
16: Output: 0 or 1
17: if Max$_{2^r-1} < \text{Impvalue}$ and Max$_{4} < 2^l$ then
18: return 1
19: else
20: return 0
21: end if
22: end function

⇒ Here, Max$_j$ is the sum of the maximal $j$ elements in the multiset $p_l \cdot p_{l-1} \cdot \ldots \cdot p_1$ where $p_1 \geq p_2 \geq \ldots \geq p_{l-1} \geq 1$ in $B = i_{r} B_{p_l}^1 B_{p_{l-1}}^1 \cdots B_{p_1}^1$. Note that, there may be duplicate among the maximal $j$ elements, for example Max$_4$ is $4 \cdot p_1$ when $l \geq 4$.

⇒ Index($B$) denote the set $\{d_1, d_1-1, \ldots, d_1\}$ for $B = i_{r} B_{p_l}^1 B_{p_{l-1}}^1 \cdots B_{p_1}^1 \in \epsilon_{r} B$, or $B = i_{r} B_{p_l}^1 B_{p_{l-1}}^1 \cdots B_{p_1}^1 \in \epsilon_{n} B$.

5 Conclusions

In this paper, we propose an algorithm to automatically get the number of $2^n$-periodic binary sequences with given $k$-error linear complexity. The time complexity of this algorithm is $O(2^{k \log k})$ in the worst case which does not depend on the period $2^n$.

We build an equivalence relationship on set of error sequences. Thus, only error sequences are need to be considered, instead of the sequences plus error sequences, that leads to the simplicity of the resulted procedure. We use the cube fragment and cube classes, which are concept tools extended from the concept of a cube, to characterize error sequences. Thus we can use those cube fragment as basic modules to construct classes of error sequences with specific structures. Error sequences with the same specific structures can be represented by a single symbolic representation. We introduce concepts of trace, weight trace and orbit of sets to build quantitative relations between different classes of error sequences. Based on these quantitative relations, we propose an algorithm to automatically generate those symbolic representations of classes of error sequences, calculate coefficients from one class to another and compute multiplicity of classes defined based on the specific equivalence we build on error sequences.

This algorithm can efficiently get the number of sequences with given $k$-error linear complexity. Experiment results got by the implementation of the algorithm are shown in Table 1. To get this table, it only cost a few minutes in a personal computer and notice that it is unfeasible to get these results by other methods or by native exhaustive method. Compared with [11,12,7], it can be seen that new results can be automatically and efficiently obtained using the proposed algorithm. Actually if manually performs the algorithm and doing symbolic computation on $n$, we can easily get the analytical expression of the counting function for small $k$. We would like to make our source codes available in public web site such as GitHub later. We believe this method can be used to settle the problem for some other special periodic sequences.

References

Corollary 4. Let $E$ and $E'$ be two error sequences. We have $E \sim E'$ if and only if there exist pairwise disjoint cubes $U_1, U_2, \cdots, U_d$ and $V_1, V_2, \cdots, V_d$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^{d} U_j) \bigcup (\bigcup_{j=1}^{d} V_j)$, where $U_j \in \mathcal{C}$, $V_j \in \mathcal{C}$, $d' \geq 0$ and $d' = \text{supp}(E + E')$.

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

1. Sequentially take pair $U_1 = \{e_1, e_t\}$ out from $V$ and put them into a set $U_1$, where $d(e_1, e_t) > 2^{n - r_1}$. 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 $U_1 = \{e_1, e_t\}$ in $U_1$ are cubes in $\mathcal{C}_2$ and $\text{LC}(U_1) \leq L$, thus $\text{LC}(V_1') \leq L$.

(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 $W_{1,j} \in \mathcal{C}_2$.

Proof. i. For any $v, v' \in V_1'$, we have $d(v, v') \leq 2^{n - r_1}$.

ii. Sequentially take pair $U_1' = \{e_1, e_t\}$ out from $V_1'$ and put them into a set $U_1'$, where $d(e_1, e_t) = 2^{n - r_1}$.

Denote the set of the remaining elements by $V_1''$.

iii. We know that for all $U_1' \in \mathcal{U}_2$, $\text{LC}(U_1') = 2^n - 2^{n - r_1}$, thus $U_1' \in \mathcal{C}_2$ and $\text{LC}(U_1') \leq 2^n - 2^{n - r_1}$.

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 $\text{LC}(V_1'') > 2^n - 2^{n - r_1}$ which leads to $\text{LC}(V_1') = \text{LC}(U_1' + V_1'') = \max\{\text{LC}(U_1') + \text{LC}(V_1'')\} > 2^n - 2^{n - r_1} > L$ which contradict with $\text{LC}(V_1') \leq L$.

v. Thus we have derived 1b.

2. Sequentially take pair $U_2 = \{W_{1,i}, W_{1,j}\}$ out from $V_1$ and put them into a set $U_2$, 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 $U_2$ are union set of some disjoint cubes in $\mathcal{C}_4$ and $\text{LC}(U_2) < L$, thus $\text{LC}(V_2') < L$.

(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 $W_{2,j} \in \mathcal{C}_4$.

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 $U_2'$, where $d(W_{2,i}, W_{2,j}) = 2^{n - r_2}$.

Denote the set of the 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 2b.

3. Recursively, if we sequentially take elements out from $V$ to form $U_1, U_2, \cdots, U_T$ step by step like above, where $U_i$ is union set of some pairwise disjoint cubes in $\mathcal{C}$ and $U_i \cap U_j = \emptyset$ for $i \neq j$, and denote the set of the remaining elements as $V_T$, then $V_T'$ is an empty set or a union set of some pairwise disjoint cubes in $\mathcal{C}_T$ and $\text{LC}(V_T') < L$.

Assume $V_T' = \bigcup_{j=1}^{d_T} V_T$ where $V_1, V_2, \cdots, V_T$ are pairwise disjoint cubes in $\mathcal{C}$. According to Corollary 4, we have that $d_T$ 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 $\mathcal{C}$ and some are in cube class $\mathcal{C}_2$. Besides, the number of cubes in cube class $\mathcal{C}$ is even.
The backward direction of the theorem can easily be proven as following: Assume there exists pairwise disjoint cubes $U_1, U_2, \ldots, U_d \in \mathbb{C}$ and $V_1, V_2, \ldots, V_{d'}$ such that $\text{supp}(E + E') = (\bigcup_{j=1}^{d'} U_j) \cup (\bigcup_{i=1}^{d} V_i)$ where $d'$ is even. Considering $\text{LC}(U_j) < L$ for any $1 \leq j \leq d$ and $\text{LC}(\bigcup_{j=1}^{d'} V_j) < L$, we have $\text{LC}(E + E') < L$, therefore $E \sim E'$.

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

**Proof.** We shall adopt the same procedure as the proof of Corollary 4 to prove this corollary. If $\text{LC}(S + E) < L$, then $\text{LC}(E) = L$. Suppose $V = \text{supp}(E)$, then we can sequentially take $U_1, U_2, \ldots, U_d$ out from $V$ step by step and denote the set of remaining elements in $V$ by $V'_T$ where $U_t$ are pairwise disjoint cubes in $\mathbb{C}_L$ and $V'_T$ is a union set of some pairwise disjoint cubes in $\mathbb{C}_L$. Suppose $V'_T = (\bigcup_{j=1}^{d'} U_j)$ where $V_j$ are pairwise disjoint cubes in $\mathbb{C}$. Because $\text{LC}(\bigcup_{j=1}^{d'} U_j) < L$ and $\text{LC}(\bigcup_{j=1}^{d'} V_j) = L$, we have $\text{LC}(E) = L$, thus $\text{LC}(S + E) < L$. Note that in $\{U_1, U_2, \ldots, U_d\}$ maybe empty set.

**Lemma 14.** Let $\mathbb{B} = (B_0^m, B_1^m, B_1^m, \ldots, B_T^m, B_T^m)$ $\in \text{Gen}(U_1^m)$. For any set $U \in \mathbb{B}$, there exists set $V \in \mathbb{C}(\text{Impvalue})$ such that $V \subseteq U$, if and only if there exists $j$ such that $\text{Imp}(B_j^m) = 0$, where $1 \leq j \leq T$.

**Proof.** For the backward direction, suppose $B_j^m = r_j B_j^m B_{j+1}^{m-1} \cdots B_0^m$ where $q_j > q_{j-1} > \cdots > q_1$. According to the definition of the function Imp, if $\text{Imp}(B_j^m) = 0$ then $q_j \geq \text{Impvalue}$. Recall that $U \in \mathbb{B}^m = r_j B_j^m B_{j+1}^{m-1} \cdots B_0^m$, thus there exists $U' \subseteq U$ such that $U' \in r_j B_q$, therefore $U' \subseteq \mathbb{C}_j(q_j)$. By the remark after the the definition of the function Imp, there exists $V \in \text{Impvalue}(U)$ such that $V \subseteq U' \subseteq U$.

For the forward direction, the proof is as follows:

**Assume:** There exist a set $V \in \mathbb{C}(\text{Impvalue})$, such that $V \subseteq U$.

**Prove:** There exists $j$ such that $\text{Imp}(B_j^m) = 0$, where $1 \leq j \leq T$.

**Proof.** Let $d(V) = 2^{-m}$, $F(U) = (U_0^m, U_1, U_1', \ldots, U_T, U_T')$. We prove $\text{Imp}(B_j^m) = 0$ by constructing a set $V'$ from the set $V$, which satisfy $\text{Imp}(V') = 0$ and $V' \in \mathbb{C}_j(\text{Impvalue})$.

1. Because $V \in \mathbb{C}_j(\text{Impvalue})$, we have $d(v, v') = 2^{-j}$ for any $v, v' \in V$, where $1 \leq j \leq l$

(a) For any $r_j$ or $r_i$, we have
   i. $V \cap r_j U_j \in \mathbb{C}_2 \setminus (|V \cap r_j U_j|)$
   ii. $V \cap r_i U_i \in \mathbb{C}_2 \setminus (|V \cap r_i U_i|)$ where $1 \leq i \leq l$.

(b) Thus we can suppose
   i. $r_j \text{Tr}(V) = \{|v, i, j : 1 \leq j \leq d_l, \text{ and } 1 \leq i \leq l\}$.
   ii. $d(v, v, v') = 2^{m-n_j}$, $d(v, v', v') = 2^{m-n_j}$ for $1 \leq j < j' \leq d_l$ and $1 \leq j < j' \leq d_l$, where $1 \leq j \leq l, i \leq 1, j_1, j_2 > i$.

2. Suppose:
   (a) $B_j^m = r_j B_j^m B_j^m - 1 \cdots B_0^m$
   (b) $r_j \text{Tr}(U_j) = \{|u, j : 1 \leq j \leq t, \text{ and } 1 \leq k \leq h_j\}$.
   (c) $U_{j, k} \subseteq U_j$, where $U_{j, k} \in r_j B_q$ and $r_j \text{Tr}(U_{j, k}) = \{|u, k, j : 1 \leq j \leq t, 1 \leq k \leq h_j\}$.
   (d) $\forall p, q \leq T$
   (a) $B_p = r_p B_p B_p' - 1 \cdots B_0^m$
   (b) $r_p \text{Tr}(U_p)= \{|u, j : 1 \leq j \leq t', \text{ and } 1 \leq k \leq h_j'\}$.
   (c) $U_{j, k} \subseteq U_p$, where $U_{j, k} \in r_p B_q$ and $r_p \text{Tr}(U_{j, k}) = \{|u, k, j : 1 \leq j \leq t', 1 \leq k \leq h_j'\}$.

3. Construction:
   (a) Initially, let $V_0^m = V$.
   (b) Firstly, let $V_1 = V_0^m$. Since $V_1 = V \subseteq U = U_1$, we have $r_1 \text{Tr}(V_1) = r_1 \text{Tr}(U_1)$. For all $U_{j, k}$, if $r_1 \text{Tr}(U_{j, k}) \in r_1 \text{Tr}(V_1)$, then we replace the points in $V_1 \cap U_{j, k}$ by $(U_1 \cap U_{j, k})$ in $V_1$. We denote the resulted set by $V_1'$ after the replacing process on $V_1$. Considering that $U_1 \cap U_{j, k} \in \mathbb{C}_1(0)$ and $V_1 \subseteq U_1 \in \mathbb{C}_1(1)$, we have $r_1 \text{Tr}(V_1') \subseteq r_1 \text{Tr}(V_1)$ and $|V_1'| \geq |V_1|$, $V_1' \subseteq U_1'$ and $V_1' \subseteq \mathbb{C}_1(\text{Impvalue})$. Let $V_0^m = V_1'$.
   (c) Now, for $1 < p \leq l$, suppose we have got $V_{p-1}^m$ which satisfy that $V_{p-1}^m \subseteq U_{p-1}^m$ and $V_{p-1}^m \subseteq \mathbb{C}(\text{Impvalue})$ and $|V_{p-1}^m| = |V|$. Similar to the construction of $(V_1, V_1')$, we construct $(V_p, V_p', V_p'' \cdots)$ inductively.

Let $V_p = V_{p-1}^m$. Since $V_p = V_{p-1}^m \subseteq U_{p-1}^m = U_p$, we have $r_p \text{Tr}(V_p) \subseteq r_p \text{Tr}(U_p)$. For all $U_{j, k}$, if $r_p \text{Tr}(U_{j, k}) \in r_p \text{Tr}(V_p)$, then we replace the points in $V_p \cap U_{j, k}$ by $(U_p \cap U_{j, k})$ in $V_p$. We denote the resulted set by $V_p''$. 

after the replacing process on $V_p$. Considering that $U_p' \cap U_j' \in C_{2^n-1}(I_1)$ and $V_p' \cap U_j' \in C_{2^n-1}(I_2)$, in addition, $r_p Tr(U_p' \cap U_j') = r_p Tr(V_p \cap U_j')$, where $I_1 = |U_p' \cap U_j'|$ and $I_2 = |V_p \cap U_j'|$, and obviously $I_1 \geq I_2$, we get that $r_p Tr(V_p) = r_p Tr(V_p')$ and $|V_p'| \geq |V_p|$. Let $V''_p = V_p$.

(d) When $p = l$, the construction process terminate. According to the construction process, we have $V''_l \subseteq U'''_l$ and $V''_l \in C_{2^l}(I)$, where $I = |V''_l| \geq |V| = Impvalue$.

4. By the remark after the definition of the function $Imp$, we have $Imp(B''_l) = 0$. 

\[\square\]
B Algorithms

Algorithm 2 Preliminary and Algorithm to Compute Coef(B | B) for B ∈ \( E_{1,...,n} \) and B’ ∈ Extr(\( E_{1,...,n} \)Gen(B))

1: procedure \( \text{Ass} \)Free
2: \( n \) \( \text{Define} \) class \( B = r_1B_{p_1}^e \cdots B_{p_t}^e \) by a mixed-radix matrix: \( B = \begin{bmatrix} \alpha & \cdots & \beta \\ \gamma \cdots \delta \end{bmatrix} \), where \( \alpha > \gamma > \beta > \delta > p_1 \).
3: \( \text{Denote} \) a single term in \( B \) by \( B \left[ \frac{d_j}{p_j} \right] \), where \( 1 \leq j \leq m \). \( \text{We say} \) that the maximal term in \( B \) is \( B \left[ \frac{d_m}{p_m} \right] \), and denote it by \( B \left[ \frac{d_{\text{max}}}{p_{\text{max}}} \right] \). \( \text{The minimal term} \) in \( B \) is \( B \left[ \frac{d_1}{p_1} \right] \), and we denote it by \( B \left[ \frac{d_{\text{min}}}{p_{\text{min}}} \right] \). \( \text{We denote} \) the number of terms in \( B \) by \( \left| B \right| \).

4: \( \text{For} \) \( B_1 = r_1B_{p_1}^e \cdots B_{p_t}^e \) and \( B_2 = r_1B_{p_1}^e \cdots B_{p_t}^e \), \( \text{we say} \) that \( B_2 \subseteq B_1 \) if \( 0 \leq e_j \leq d_j \) for all \( j \), where \( 1 \leq j \leq l \). \( \text{In other} \) words, \( B_0 \subseteq B_1 \) if for any \( U_2 \subset B_2 \) there exists \( U_1 \subset B_1 \) such that \( U_2 \subseteq U_1 \).

5: \( \text{Define a} \) cube fragments set for \( B_1 = r_1B_{p_1}^e \cdots B_{p_t}^e \) and \( B_2 = r_1B_{p_1}^e \cdots B_{p_t}^e \), which represents the set of all possibilities to assign cube fragments in \( B_1 \) to \( B_2 \), as follows:
6: \( \text{Assign} \) \( \{ B_1 \rightarrow B_2 \} = \{ r_1B_{p_1}^e \cdots B_{p_t}^e \} : \sum_{i=1}^{\delta} e_i = \epsilon \), \( \{ B_1 \rightarrow B_2 \} = \{ \alpha_iB_{u_1}^e \cdots B_{u_t}^e \} : \sum_{i=1}^{\delta} e_i = \epsilon \).

7: \( \text{Define a} \) “+” operator between \( B_1 \) and \( B_2 \) as \( B_1 + B_2 = [v_1 \cdots v_1] \), where \( \{ u_1 \cdots u_1 \} = \{ p_m \cdots p_1 \} \).
8: \( \text{Define a} \) “−” operator between \( B_1 \) and \( B_2 \) where \( B_3 \subseteq B_1 \) as \( B_1 - B_2 = \left[ \frac{e_m \cdots e_1}{p_m \cdots p_1} \right] \), where \( B_1 = \left[ \frac{e_m \cdots e_1}{p_m \cdots p_1} \right] \).

9: \( \text{Input:} \) \( B = r_1B_{p_1}^e \cdots B_{p_t}^e \) \( \text{and} \) \( B' = r_1B_{p_1}^e \cdots B_{p_t}^e \) \( \text{in} \) \( B \) and \( B' \) \( \text{in} \) \( B \) \( \text{in} \) \( E_{1,...,n} \).
10: \( \text{Output:} \) \( \text{coef}(B' | B) \) \( \text{computed} \) recursively call itself. \( \text{When it} \) terminates, \( \text{variable} \) \( \zeta \) \( \text{turns to} \) the value of \( \text{coef}(B' | B) \).

11: \( \text{end procedure} \)

12: \( \text{end procedure} \)

13: \( \text{end for} \)

14: \( \text{end procedure} \)

15: \( \text{end procedure} \)

16: \( \text{end procedure} \)
Algorithm 3 Algorithm to Generate set $\mathcal{G}(B)$ for class $B \in B^r$

1: procedure $\mathcal{G}(B)$
2: Input: $B = B_{pp_1}^l \cdots B_{pp_l}^l \in r, B^r$
3: Output: $\mathcal{G}(B)$
4: $B' \leftarrow \emptyset$, $GenSet \leftarrow \emptyset$
5: $MainGen$
6: Output $GenSet$
7: $\triangleright MainGen$ is the main generation procedure which handle the maximal terms $\frac{dmax}{pmax}$ in $B$ and determine whether class $B' \in r$, $Gen(B)$ has been generated. It recursively call itself and the subroutine $SubGen$. When it terminate, $GenSet$ turns to be $\mathcal{G}(B)$.
8: end procedure

9: procedure $MainGen$
10: if $|B| = 0$ then $\triangleright$ a class $B'$ has been generated
11: $GenSet \leftarrow add B'$
12: else
13: $\frac{\alpha}{\beta} \leftarrow B \frac{d_{max}}{p_{max}}$
14: if $\alpha \geq 2$ then
15: if $2 \times \beta < \text{Impvalue}$ then
16: for $t \leftarrow \left\lfloor \frac{\alpha}{2} \right\rfloor$ to 1 do
17: $B' \leftarrow B' + \left\lfloor \frac{t}{2 \times \beta} \right\rfloor$, $B \leftarrow B - \left\lfloor \frac{2 \times t}{\beta} \right\rfloor$
18: if $\alpha - 2 \times t = 0$ then
19: $MainGen$
20: else
21: if $|B| = 1$ then
22: $\gamma \leftarrow \left\lfloor \frac{\alpha - 2 \times t}{\beta} \right\rfloor$
23: $B' \leftarrow B' + \left\lfloor \frac{\gamma}{\delta} \right\rfloor$, $B \leftarrow B - \left\lfloor \frac{\gamma}{\delta} \right\rfloor$
24: $MainGen$
25: $B' \leftarrow B' - \left\lfloor \frac{\gamma}{\delta} \right\rfloor$, $B \leftarrow B + \left\lfloor \frac{\gamma}{\delta} \right\rfloor$
26: else
27: $SubGen(|B| - 1)$
28: end if
29: end if
30: $B' \leftarrow B' - \left\lfloor \frac{t}{2 \times \beta} \right\rfloor$, $B \leftarrow B + \left\lfloor \frac{2 \times t}{\beta} \right\rfloor$
31: end for
32: else if $SubGen(|B| - 1)$
33: $\triangleright$ if $\alpha = 1$
34: else if $\alpha = 1$
35: $B' \leftarrow B' + \left\lfloor \frac{\alpha}{\beta} \right\rfloor$, $B \leftarrow B - \left\lfloor \frac{\alpha}{\beta} \right\rfloor$
36: $MainGen$
37: $B' \leftarrow B' - \left\lfloor \frac{\alpha}{\beta} \right\rfloor$, $B \leftarrow B + \left\lfloor \frac{\alpha}{\beta} \right\rfloor$
38: $SubGen(|B| - 1)$
39: end if
40: end if
41: end procedure

42: procedure $SubGen(m')$
43: if $m' = 0$ then
44: $B' \leftarrow B' + \left\lfloor \frac{\alpha}{\beta} \right\rfloor$, $B \leftarrow B - \left\lfloor \frac{\alpha}{\beta} \right\rfloor$
45: $MainGen$
46: $B' \leftarrow B' - \left\lfloor \frac{\alpha}{\beta} \right\rfloor$, $B \leftarrow B + \left\lfloor \frac{\alpha}{\beta} \right\rfloor$
47: else
48: for $j \leftarrow m'$ to 1 do
49: $\frac{\gamma}{\delta} \leftarrow \left\lfloor \frac{\alpha - s}{\beta} \right\rfloor$
50: $B' \leftarrow B' + \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
51: $B \leftarrow B - \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
52: if $\alpha - s = 0$ then
53: $MainGen$
54: else
55: if $|B| = 1$ then
56: $\left\lfloor \frac{\gamma}{\delta} \right\rfloor \left\lfloor \frac{\alpha - s}{\beta} \right\rfloor$
57: $B' \leftarrow B' + \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
58: $B \leftarrow B - \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
59: end if
60: end if
61: end if
62: $B' \leftarrow B' - \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
63: $B \leftarrow B + \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
64: end if
65: $SubGen(j - 1)$
66: end if
67: end if
68: $B' \leftarrow B' - \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
69: $B \leftarrow B + \left\lfloor \frac{s}{\beta + \mu} \right\rfloor$
70: end if
71: end for
72: end if
73: end for
74: end if
75: end procedure
C Trees to Organize Symbolic Representations of Class of Error Sequences

(a) Tree of $\text{Gen}(\mathcal{G}_0 B^1_i)$ when $\text{Impvalue} > 2$

(b) Tree of $\text{Gen}(\mathcal{G}_0 B^1_i)$ when $\text{Impvalue} = 2$

(c) Tree of $\text{Gen}(\mathcal{G}_0 B^1_i)$ when $\text{Impvalue} = 2$

Note. A path from root node to leaf node represents an element $\mathcal{B}$ in $\text{Gen}(\mathcal{G}_0 B^1_i)$ or in $\text{Gen}(\mathcal{G}_0 B^1_i)$. Red leaf node with a stop character \( \perp \) indicates that $\text{Mult}(B_k) = 1$ and $\text{Impvalue}(B^i_k) = 1$, for all $B_k$ and $B^i_k$ after this element in $\mathcal{B}$. And the meaning of black leaf node is that there exists another node being the same as it and thus we omit its descendant nodes. The numbers on edge between two nodes represent $\text{Coeff}(B_{k\mid B_1})$, $\text{Coeff}(B_{k\mid B_2}) \cdot \text{Mult}(B_3)$ or $\text{Coeff}_{\text{Ext}}(B_3)$ where $B_1 \in \mathcal{B}$, $B_2 \in \mathcal{G}_j$ and $B_3 \in n_i \mathcal{B}$.

Fig. 1: Trees of $\text{Gen}(\mathcal{G}_0 B^1_i)$ and $\text{Gen}(\mathcal{G}_0 B^1_i)$ under various $\text{Impvalue}$

D Experiment Results
Table 1: Part of the results on $\mathcal{N}_k^n(L)$ for $n = 6$

<table>
<thead>
<tr>
<th>$L$</th>
<th>$w_H$</th>
<th>$k = 6$</th>
<th>$k = 8$</th>
<th>$\ldots$</th>
<th>$k = 26$</th>
<th>$k = 28$</th>
<th>$k = 30$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\leq 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>32800768</td>
<td>843448320</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>12361216</td>
<td>105342727</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>164608</td>
<td>2915424</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>127456</td>
<td>205896</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>32032</td>
<td>51480</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40</td>
<td>2</td>
<td>114688</td>
<td>65536</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>44</td>
<td>2</td>
<td>6400</td>
<td>256</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>46</td>
<td>2</td>
<td>448</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>47</td>
<td>2</td>
<td>112</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>52</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>54</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>55</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>58</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>59</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>61</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>74698177</td>
<td>4269895680</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>73495057</td>
<td>4000596704</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>71447441</td>
<td>3611187752</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>68356625</td>
<td>3111545144</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>49468513</td>
<td>1797161728</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>46577129</td>
<td>1420375632</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>41906633</td>
<td>993236728</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>3</td>
<td>22363121</td>
<td>292078272</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>15385637</td>
<td>133101512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>3</td>
<td>3774849</td>
<td>22800792</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>36</td>
<td>3</td>
<td>854113</td>
<td>7480320</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>38</td>
<td>3</td>
<td>753929</td>
<td>4554704</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>39</td>
<td>3</td>
<td>618185</td>
<td>2459764</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>42</td>
<td>3</td>
<td>274577</td>
<td>361600</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>43</td>
<td>3</td>
<td>154997</td>
<td>122304</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>45</td>
<td>3</td>
<td>29265</td>
<td>16448</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>3</td>
<td>3985</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>51</td>
<td>3</td>
<td>901</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>53</td>
<td>3</td>
<td>65</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>57</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>75611761</td>
<td>4501725649</td>
<td>80627405461098496</td>
<td>1712789176960000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>75611761</td>
<td>4501648441</td>
<td>7325469431074816</td>
<td>236126248960000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>75611761</td>
<td>4501494025</td>
<td>2073916240700416</td>
<td>590315622400000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>75154969</td>
<td>4385391113</td>
<td>1904851837536</td>
<td>139314069504</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>75154969</td>
<td>4384585301</td>
<td>4936272171264</td>
<td>34828517376</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>74325013</td>
<td>4190250125</td>
<td>609858701856</td>
<td>4353564672</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>51710997</td>
<td>2174331913</td>
<td>399572992</td>
<td>1048576</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>4</td>
<td>51710997</td>
<td>2172889183</td>
<td>101072896</td>
<td>262144</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
<td>50589805</td>
<td>1979144701</td>
<td>12535808</td>
<td>32768</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>28803133</td>
<td>693096413</td>
<td>38864</td>
<td>1024</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>34</td>
<td>4</td>
<td>942649</td>
<td>1135209</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>35</td>
<td>4</td>
<td>942649</td>
<td>11396605</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>37</td>
<td>4</td>
<td>898381</td>
<td>9273725</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>41</td>
<td>4</td>
<td>418429</td>
<td>1975901</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>49</td>
<td>4</td>
<td>9949</td>
<td>9949</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>75611761</td>
<td>4501777129</td>
<td>765884877961138529</td>
<td>149125458291620814</td>
<td>735663252850019217</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>75611761</td>
<td>4501777129</td>
<td>549379354729134933</td>
<td>488415562254909925</td>
<td>83465531502355525</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>75611761</td>
<td>4501751389</td>
<td>1274140570353583729</td>
<td>39208852967342625</td>
<td>167869308850825</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>75154969</td>
<td>4385476325</td>
<td>192838022868363833</td>
<td>175169988640833</td>
<td>2240855430049</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>5</td>
<td>51710997</td>
<td>2174956117</td>
<td>296601473321</td>
<td>9419426161</td>
<td>42981185</td>
<td>0</td>
</tr>
<tr>
<td>33</td>
<td>5</td>
<td>942649</td>
<td>11460949</td>
<td>36457</td>
<td>497</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>75611761</td>
<td>4501777129</td>
<td>956315644440505325</td>
<td>2075085937425745213</td>
<td>3695373947956092637</td>
<td>0</td>
</tr>
</tbody>
</table>

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

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