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 peoples have strenuously promoted the solving of this problem from $k = 2$ to $k = 4$ step by step. Unfortunately, it still remains difficult to obtain the solutions for larger k 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 $S = (s_0 s_1 \cdots s_{N-1})^\infty$ be an N-periodic sequence with the terms in finite field $\mathbb{F}_2$. And we denote S^N the set of all N-periodic binary sequences. 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 $S(x) = s_0 + s_1 x + s_2 x^2 + ... + s_{N-1} x^{N-1}$ 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 $0 \le k < N$, denote the k-error linear complexity of S by $LC_k(S)$ which is given by*

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

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 $merr(S) = 2^{w_H(2^n - LC(S))}$.*

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 $0 \le L \le 2^n$. Then*

$$\begin{aligned} &\mathcal{N}(0) = 1, \qquad \mathcal{A}(0) = \{(00\cdots 0)\}, \text{ and} \\ &\mathcal{N}(L) = 2^{L-1}, \quad \mathcal{A}(L) = \{S \in S^{2^n} : \ S(x) = (1-x)^{2^n - L} a(x),\ a(1) \neq 0\} \ for\ 1 \le L \le 2^n. \end{aligned}$$

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

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

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:

$$\begin{array}{lll} \mathcal{A}_k(2^n) = \emptyset, & \mathcal{N}_k(2^n) = 0 & \text{for } k \ge 1, \\ \mathcal{A}_k(0) = \{S \in S^{2^n} : \ w_H(S) \le k\} & \mathcal{N}_k(0) = \displaystyle\sum_{j=0}^{k} \binom{2^n}{j}, & \text{for } k \ge 1, \\ \mathcal{A}_k(1) = \{S \in S^{2^n} : \ w_H(S) > 2^n - k\}, & \mathcal{N}_k(1) = \displaystyle\sum_{j=2^n-k}^{2^n} \binom{2^n}{j} = \sum_{j=0}^{k} \binom{2^n}{j} & \text{for } k < 2^{n-1}, \\ \mathcal{A}_k(1) = \{S \in S^{2^n} : \ w_H(S) > k\}, & \mathcal{N}_k(1) = \displaystyle\sum_{j=k+1}^{2^n} \binom{2^n}{j} & \text{for } k \ge 2^{n-1}, \\ \mathcal{A}_k(L) = \emptyset, & \mathcal{N}_k(L) = 0 & \text{for } k \ge 2^{n-1}\ ,\ L \neq 0 \text{ and } 1. \end{array}$$

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 $LC_k(S+E) = L$ in $\mathbf{S}+\mathbf{E}$ where $\mathbf{S} = \{S \in S^N : \ LC(S) = L\}$, $\mathbf{E} = \{E \in S^N : \ w_H(E) \le k\}$ and $\mathbf{S}+\mathbf{E} = \{S+E : \ S \in \mathbf{S} \text{ and } E \in \mathbf{E}\}$. And they obtained the complete counting functions for $k = 2,\ 3$ [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 $k \le 4$. However, those methods will become very complex when k becomes larger.

In this paper, we define an equivalence relationship on the error sequences set $\mathbf{E}$ based on the observation as the follows.

Lemma 5 ([3]). *Let E and E' be two error sequences in $\mathbf{E}$. Then*

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

Corollary 1. *Let E be an error sequence in $\mathbf{E}$, then we have*

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

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

Corollary 2. *Let E and E' be two error sequences in $\mathbf{E}$. We have that $\mathcal{A}(L) + E = \mathcal{A}(L) + E'$ if and only if there exists $S,\ S' \in \mathcal{A}(L)$ such that $S + E = S' + E'$.*

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

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

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

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 $\mathbf{E}$. We have $E \sim E'$ if and only if $LC(E+E') < L$.*

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

Assume $LC(E+E') < L$, suppose $E(x)+E'(x) = (E+E')(x) = (1-x)^{2^n-l}b(x)$, where $l < L$ and $b(1) = 1$. For any sequence $S \in \mathcal{A}(L)$, suppose $S(x) = (1-x)^{2^n-L}a(x)$, where $a(1) = 1$. We have $E(x)+S(x) = E'(x)+(1-x)^{2^n-l}a(x)+S(x) = E'(x)+(1-x)^{2^n-L}(a(x)+(1-x)^{L-l}b(x))$. Because $a(x)+(1-x)^{L-l}b(x) = 1$ when $x = 1$, we have $S' \in \mathcal{A}(L)$ where $S'(x) = (1-x)^{2^n-L}(a(x)+(1-x)^{L-l}b(x))$. According to Corollary 2, we have $\mathcal{A}(L)+E = \mathcal{A}(L)+E'$, 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 $\mathbf{E} = \bigcup_{j=0}^{k} \mathbf{E}_j$ where $\mathbf{E}_j = \{E \in S^{2^n} : w_H(E) = j\}$ to get the maximum subset of $\mathbf{E}$ in which elements are non-equivalent with each other and satisfy that $LC_k(S+E) = L$ when plus the error sequence E to any sequence $S \in \mathcal{A}(L)$. 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 $O(2^{k\log k})$ in the worst case which does not depend on the period 2^n. 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, $supp(S) = \{i : s_i \neq 0,\ 0 \leq i < N\}$. Let $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$ and denote $\mathbf{P}(\mathbb{Z}_m)$ the power set of $\mathbb{Z}_m$ which is the set of all subsets of $\mathbb{Z}_m$, that is $\mathbf{P}(\mathbb{Z}_m) = \{U :\ U \subseteq \mathbb{Z}_m\}$. Notice that the set $\mathbf{P}(\mathbb{Z}_N)$ is one to one corresponding to S^N. Especially, the empty set in $\mathbf{P}(\mathbb{Z}_N)$ corresponds to the all-zero sequence in S^N. 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 $U = \{u_1, u_2, ..., u_m\}$ 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 2^t, if $|u_i - u_j| = 2^t b$ and $2 \nmid b$. And denote it by $d(u_i, u_j) = 2^t$.*

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 $d(u_2, u_3) = min\{d(u_1, u_2), d(u_1, u_3)\}$.

Definition 4. *Let U,V be two nonempty subsets of $\mathbb{Z}_N$, define the* ***distance of*** *U and the* ***distance between*** *U* ***and*** *V as:*

$$d(U)=\begin{cases}\min\{d(u,u'):\ u,u'\in U\}, & |U|>1\\ +\infty & \text{otherwise}\end{cases},\ d(U,V)=\begin{cases}\min\{d(u,v):\ u\in U,v\in V\}, & U\bigcap V=\emptyset\\ 0 & \text{otherwise}\end{cases}.$$

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

Proof. Because $d(U,V)>0$, then $U\bigcap V=\emptyset$. 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 3 and 4, we have $d(u,v_0)=\min\{d(u,u_0),d(u_0,v_0)\}=d(u_0,v_0)$. Then $d(u,v)=\min\{d(u,v_0),d(v_0,v)\}=d(u_0,v_0)=d(U,V)$. □

Definition 5 (Cube). *Let $U=\{u_1,u_2,...,u_{2^T}\}$ be a subset of $\mathbb{Z}_N$.*

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

We remark that, a cube represents a subset of $\mathbb{Z}_N$ with a special structure and "*Cube*" represents a class of subsets of $\mathbb{Z}_N$ with the same structure. Because the linear complexity can be get by $LC(S)=2^n-\deg(\gcd(1-x^{2^n},S(x)))$, we can easily know that the linear complexity of a cube with sides of length $\{2^{i_1},2^{i_2},\cdots,2^{i_T}\}$ is $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_T})$.

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

$$\mathbb{C}_2:=\bigcup_{t=1}^{r_1-1}Cube_{2^{n-t}},\qquad \mathbf{C}_2:=Cube_{2^{n-r_1}},$$

$$\mathbb{C}_4:=\bigcup_{t=r_1+1}^{r_2-1}Cube_{2^{n-r_1},2^{n-t}},\qquad \mathbf{C}_4:=Cube_{2^{n-r_1},2^{n-r_2}},$$

$$\vdots\qquad\qquad\vdots$$

$$\mathbb{C}_{2^T}:=\bigcup_{t=r_{T-1}+1}^{r_T-1}Cube_{2^{n-r_1},2^{n-r_2},...,2^{n-r_{T-1}},2^{n-t}}.\qquad \mathbf{C}_{2^T}:=Cube_{2^{n-r_1},2^{n-r_2},\cdots,2^{n-r_T}},$$

and

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

Furthermore, we denote:

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

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

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

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

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

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

Using the similar argument as in the proof of Theorem 2, we can easily carry out the following corollary. Thus, similarly, we can splice small fragments of cubes into larger fragments of cube in cube class $\mathbb{C}$.

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

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

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 $U_1,\ U_2,\ \cdots,\ U_d$ and $V_1,\ V_2,\ \cdots,\ V_{d'}$ such that $supp(E+E')=(\bigcup_{j=1}^{d}U_j)\bigcup(\bigcup_{j=1}^{d'}V_j)$, where $U_j\in\mathbb{C}$, $V_j\in\mathbf{C}$, $d'\geq 0$ and d' is even.*

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

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

We regard the cube fragment $\mathbf{C}_{2^i}(p)$ 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.

$$ {}_{r_i}B_p^d:=\{\bigcup_{j=1}^{d}U_j:\ U_j\in\mathbf{C}_{2^{i-1}}(p)\text{ and }0<d(U_{j'},U_{j''})\leq 2^{n-r_i}\text{ for }1\leq j'<j''\leq d\}, $$

$$ {}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}:=\{\bigcup_{j=1}^{l}\mathbf{U}_j:\ \mathbf{U}_j\in{}_{r_i}B_{p_j}^{d_j}\text{ and }0<d(\mathbf{U}_{j'},\mathbf{U}_{j''})\leq 2^{n-r_i}\text{ for }1\leq j'<j''\leq l\}, $$

$$ {}_{r_i}B_{p^{[d]}}:=\{\bigcup_{j=1}^{d}U_j:\ U_j\in\mathbf{C}_{2^{i-1}}(p)\text{ and }2^{n-r_i}<d(U_{j'},U_{j''})<2^{n-r_{i-1}}\text{ for }1\leq j'<j''\leq d\}, $$

$$ {}_{r_i}B_{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}}:=\{\bigcup_{j=1}^{l}\mathbf{U}_j:\ \mathbf{U}_j\in{}_{r_i}B_{p_j^{[d_j]}}\text{ and }2^{n-r_i}<d(\mathbf{U}_{j'},\mathbf{U}_{j''})<2^{n-r_{i-1}}\text{ for }1\leq j'<j''\leq l\}, $$

$$ {}_{r_i}B_Q^h:=\{\bigcup_{j=1}^{h}\mathbf{U}_j:\ \mathbf{U}_j\in{}_{r_i}B_Q\text{ and }0<d(\mathbf{U}_{j'},\mathbf{U}_{j''})\leq 2^{n-r_i}\text{ for }1\leq j'<j''\leq h\}, $$

$$ {}_{r_i}B_{Q_t}^{h_t}B_{Q_{t-1}}^{h_{t-1}}\cdots B_{Q_1}^{h_1}:=\{\bigcup_{j=1}^{t}\mathbf{U}_j:\ \mathbf{U}_j\in{}_{r_i}B_{Q_j}^{h_j}\text{ and }0<d(\mathbf{U}_{j'},\mathbf{U}_{j''})\leq 2^{n-r_i}\text{ for }1\leq j'<j''\leq t\}, $$

$$ {}_{r_i'}B_p^d:=\{\bigcup_{j=1}^{d}U_j:\ U_j\in\mathbf{C}_{2^i}(p)\text{ and }0<d(U_{j'},U_{j''})<2^{n-r_i}\text{ for }1\leq j'<j''\leq d\}, $$

$$ {}_{r_i'}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}:=\{\bigcup_{j=1}^{l}\mathbf{U}_j:\ \mathbf{U}_j\in{}_{r_i'}B_{p_j}^{d_j}\text{ and }0<d(\mathbf{U}_{j'},\mathbf{U}_{j''})<2^{n-r_i}\text{ for }1\leq j'<j''\leq l\}, $$

where the notation $p^{[d]}$ is symbolic representation of the multiset $\underbrace{\{p,p,\dots,p\}}_{d}$. And $p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}$ in ${}_{r_i}B_{p^{[d]}}$ and ${}_{r_i}B_{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}}$ is symbolic representation of the union multisets $\biguplus_{j=1}^{l} p_j^{[d_j]}$. We denote the set of all those multisets by $\mathcal{Q}=\{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}:\ p_l>p_{l-1}>\cdots>p_1\geq 1,\ d_j\geq 1,\ 1\leq j\leq l\}$. And in the above definitions, $Q,\ Q_1,\ Q_2,\ \cdots,\ Q_t$ are mulisets in $\mathcal{Q}$, and $Q_{j'}\neq Q_{j''}$ for $1\leq j'<j''\leq t$. The notation $\uplus$ denotes the union of multisets, for example $\{1,1,2,3\}\uplus\{1,2\}=\{1,1,1,2,2,3\}$. The symbol $\mathcal{Q}$ appeared in the rest of the paper always takes the meaning define here.

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

$$ {}_{r_i}U_j:=\{j,\ j+2^{n-r_i+1},\ j+2\cdot 2^{n-r_i+1},\ \cdots,\ j+(2^{r_i-1}-1)\cdot 2^{n-r_i+1}\},\ \text{for } 0\leq j<2^{n-r_i+1}. $$

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

$$ {}_{r_i}Tr(U):=\{j:\ U\bigcap{}_{r_i}U_j\neq\emptyset\}. $$

Further more, if $U\in\mathbf{C}_{2^{i-1}}(p)$, 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 $\mathbf{C}_{2^{i-1}}(p)$ in subsets $\mathbb{Z}_{2^{n-r_i+1}}$ as the following:

$$ {}_{r_i}wTr(U):=\{(j)_p\}. $$

As the elements in set ${}_{r_i}B_p^d$, in set ${}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}$, in set ${}_{r_i}B_{p^{[d]}}$, in set ${}_{r_i}B_{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}}$, in set ${}_{r_i}B_Q^h$ and in set ${}_{r_i}B_{Q_t}^{h_t}B_{Q_{t-1}}^{h_{t-1}}\cdots B_{Q_1}^{h_1}$ can all be decomposed into union set of some cube fragments subset to $\mathbf{C}_{2^{i-1}}$, therefore we can define the weight trace in $\mathbb{Z}_{2^{n-r_i+1}}$ of those elements as follows:

$$
\begin{aligned}
{}_{r_i}wTr(U)&:=\bigcup_{j=1}^{d}{}_{r_i}wTr(U_j),\ \text{ for } U=\bigcup_{j=1}^{d}U_j\in{}_{r_i}B_p^d\ \text{ and } U_j\in{}_{r_i}B_p;\\
{}_{r_i}wTr(\mathbf{U})&:=\bigcup_{j=1}^{l}{}_{r_i}wTr(\mathbf{U}_j),\ \text{ for } \mathbf{U}=\bigcup_{j=1}^{l}\mathbf{U}_j\in{}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}\ \text{ and } \mathbf{U}_j\in{}_{r_i}B_{p_j}^{d_j};\\
{}_{r_i}wTr(V)&:=\biguplus_{j=1}^{d}{}_{r_i}wTr(V_j),\ \text{ for } V=\bigcup_{j=1}^{d}V_j\in{}_{r_i}B_{p^{[d]}}\ \text{ and } V_j\in{}_{r_i}B_p;\\
{}_{r_i}wTr(\mathbf{V})&:=\biguplus_{j=1}^{l}{}_{r_i}wTr(\mathbf{V}_j),\ \text{ for } \mathbf{V}=\bigcup_{j=1}^{l}\mathbf{V}_j\in{}_{r_i}B_{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}}\ \text{ and } \mathbf{V}_j\in{}_{r_i}B_{p_j^{[d_j]}};\\
{}_{r_i}wTr(W)&:=\biguplus_{j=1}^{h}{}_{r_i}wTr(W_j),\ \text{ for } W=\bigcup_{j=1}^{h}W_j\in{}_{r_i}B_Q^h\ \text{ and } W_j\in{}_{r_i}B_Q;\\
{}_{r_i}wTr(\mathbf{W})&:=\biguplus_{j=1}^{t}{}_{r_i}wTr(\mathbf{W}_j),\ \text{ for } \mathbf{W}=\bigcup_{j=1}^{t}\mathbf{W}_j\in{}_{r_i}B_{Q_t}^{h_t}B_{Q_{t-1}}^{h_{t-1}}\cdots B_{Q_1}^{h_1}\ \text{ and } \mathbf{W}_j\in{}_{r_i}B_{Q_j}^{h_j}.
\end{aligned}
$$

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

Remark 2, it can also be checked that ${}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}$ 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 ${}_{r_i}B_{p_l}^{d_l},\ {}_{r_i}B_{p_{l-1}}^{d_{l-1}},\ \cdots,\ {}_{r_i}B_{p_1}^{d_1}$. And ${}_{r_i}B_{p_l^{[d_l]}p_{l-1}^{[d_{l-1}]}\cdots p_1^{[d_1]}}$ is a class of union set of l elements with same trace in $\mathbb{Z}_{2^{n-r_i+1}}$, which respectively comes from ${}_{r_i}B_{p_l{[d_l]}},\ {}_{r_i}B_{p_{l-1}{[d_{l-1}]}},\ \cdots,\ {}_{r_i}B_{p_1{[d_1]}}$.

Remark 3, similarly, ${}_{r_i}B_Q^h$ is a class of union of h elements in ${}_{r_i}B_Q$ with pairwise disjoint traces. And ${}_{r_i}B_{Q_t}^{h_t}B_{Q_{t-1}}^{h_{t-1}}\cdots B_{Q_1}^{h_1}$ 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 ${}_{r_i}B_{Q_t}^{h_t},\ {}_{r_i}B_{Q_{t-1}}^{h_{t-1}},\ \cdots,\ {}_{r_i}B_{Q_1}^{h_1}$.

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 $U=\{1,11,18,33,43,50\}$, which is a union of the following sets: $U_1=\{1,33\}$, $U_2=\{18,50\}$, $U_3=\{11,43\}$ and $U_1,U_2,U_3\in C_2(2)$. Then ${}_{r_2}wTr(U_1)=\{(1)_2\}$, ${}_{r_2}wTr(U_2)=\{(2)_2\}$, ${}_{r_2}wTr(U_3)=\{(3)_2\}$, therefore $U\in{}_{r_2}B_2^3$.

2. Let $\mathbf{U}=\{1,11,18,33,50,60\}$, which is a unoin of the following sets: $\mathbf{U}_1=\{1,18,33,50\}\in {}_{r_2}B_2^2$, $\mathbf{U}_2=\{11,60\}\in {}_{r_2}B_1^2$. Then ${}_{r_2}wTr(\mathbf{U}_1)=\{(1)_2,(2)_2\}$, ${}_{r_2}wTr(\mathbf{U}_2)=\{(3)_1,(4)_1\}$, therefore $\mathbf{U}\in {}_{r_2}B_2^2B_1^2$.
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 $V_1,V_2,V_3\in {}_{r_2}B_2$. Then ${}_{r_2}wTr(V_1)={}_{r_2}wTr(V_2)={}_{r_2}wTr(V_3)=\{(1)_2\}$, therefore $V\in {}_{r_2}B_{2^{[3]}}$.
4. Let $\mathbf{V}=\{1,9,17,33,49,57\}$, which is a union of the following sets: $\mathbf{V}_1=\{1,17,33,49\}$, $\mathbf{V}_2=\{9,57\}$, and ${}_{r_2}wTr(\mathbf{V}_1)=\{(1)_2,(1)_2\}$, ${}_{r_2}wTr(\mathbf{V}_2)=\{(1)_1,(1)_1\}$, therefore $\mathbf{V}\in {}_{r_2}B_{2^{[2]}1^{[2]}}$.
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 $W_1,W_2\in {}_{r_2}B_{2^{[1]}1^{[1]}}$, then ${}_{r_2}wTr(W_1)\{(1)_2,(1)_1\}$, ${}_{r_2}wTr(W_2)=\{(2)_2,(2)_1\}$, therefore $W\in {}_{r_2}B^2_{2^{[1]}1^{[1]}}$.
6. Let $\mathbf{W}=\{1,2,17,18,33,35,49,59\}$, which is a union of the following sets: $\mathbf{W}_1=\{1,17,33\}\in {}_{r_2}B_{2^{[2]}}$, $\mathbf{W}_2=\{2,18,35,59\}\in {}_{r_2}B^2_{1^{[2]}}$ then ${}_{r_2}wTr(\mathbf{W}_1)=\{(1)_2,(1)_1\}$, ${}_{r_2}wTr(\mathbf{W}_2)=\{(2)_1,(2)_1,(3)_1,(3)_1\}$, thus $\mathbf{W}\in {}_{r_2}B_{2^{[2]}}B^2_{1^{[2]}}$.

We denote $r_i'=r_i+1$. For a given r_i', where $1\le i\le T$, we divide $\mathbb{Z}_{2^n}$ to the subsets as follows:

$${}_{r_i'}U_j:=\{j,\ j+2^{n-r_i},\ j+2\cdot 2^{n-r_i},\ \cdots,\ j+(2^{r_i}-1)\cdot 2^{n-r_i}\},\ \text{for } 0\le j<2^{n-r_i}.$$

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

$${}_{r_i'}Tr(U):=\{j:\ U\bigcap {}_{r_i'}U_j\neq\emptyset\}.$$

And for any $U\in\mathbf{C}_{2^i}(p)$, there exists j such that $U\subseteq {}_{r_i'}U_j$, where $0\le j<2^{n-r_i}$. We define the weight trace of $U\in\mathbf{C}_{2^i}(p)$ in subsets $\mathbb{Z}_{2^{n-r_i}}$ as

$${}_{r_i'}wTr(U):=\{(j)_p\}.$$

Considering that the elements in sets ${}_{r_i'}B_p^d$ and ${}_{r_i'}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}$ can all be decomposed into union of some fragments of cubes in C_{2^i}, we define the weight trace of those elements in $\mathbb{Z}_{2^{n-r_i}}$ as follows:

$${}_{r_i'}wTr(U):=\bigcup_{j=1}^{d}{}_{r_i'}wTr(U_j)\quad\text{and}\quad {}_{r_i'}wTr(\mathbf{U}):=\bigcup_{j=1}^{l}{}_{r_i'}wTr(\mathbf{U}_j)$$

where $U=\bigcup_{j=1}^{d}U_j\in {}_{r_i'}B_p^d$, $U_j\in {}_{r_i'}B_p$ and, $\mathbf{U}=\bigcup_{j=1}^{l}\mathbf{U}_j\in {}_{r_i'}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}$, $\mathbf{U}_j\in {}_{r_i'}B_{p_j}^{d_j}$.

Particularly, we denote the trivial class ${}_{r_0'}B_1^m:=\{U\subseteq\mathbb{Z}_{2^n}:\ |U|=m\}$, 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 ${}_{r_i}\mathcal{B}$, ${}_{r_i}\mathcal{B}'$ and ${}_{r_i'}\mathcal{B}$ to denote sets of all classes as follows:

$$\begin{aligned}
{}_{r_i}\mathcal{B}&:=\{{}_{r_i}B_{Q_t}^{h_t}B_{Q_{t-1}}^{h_{t-1}}\cdots B_{Q_1}^{h_1}:\ Q_j\in\mathcal{Q},\ Q_{j'}\neq Q_{j''}\text{ and } h_j\ge 1\text{ for } 1\le j\le t\},\\
{}_{r_i}\mathcal{B}'&:=\{{}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}:\ p_l>p_{l-1}>\cdots>p_1\ge 1\text{ and } d_j\ge 1\text{ for } 1\le j\le l\},\\
{}_{r_i'}\mathcal{B}&:=\{{}_{r_i'}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1}:\ p_l>p_{l-1}>\cdots>p_1\ge 1\text{ and } d_j\ge 1\text{ for } 1\le j\le l\}.
\end{aligned}$$

Remark that ${}_{r_i}\mathcal{B}'$ is a special subset of ${}_{r_i}\mathcal{B}$.

And for a class $\mathbf{B}\in {}_{r_i}\mathcal{B}\bigcup {}_{r_i}\mathcal{B}'\bigcup {}_{r_i'}\mathcal{B}$, we define the trace and weight trace of the class in subsets $\mathbb{Z}_{2^{n-r_i+1}}$ or $\mathbb{Z}_{2^{n-r_i}}$ as:

$${}_rTr(\mathbf{B}):=\{{}_rTr(U):U\in\mathbf{B}\}\quad\text{and}\quad {}_rwTr(\mathbf{B}):=\{{}_rwTr(U):U\in\mathbf{B}\}\text{ for } r\in\{r_i,r_i'\}.$$

Based on the notations defined above, we can get many relationships between different classes. For example, let $U\in {}_{r_i}B_Q$ where $Q=q_s^{[e_s]}q_{s-1}^{[e_{s-1}]}\cdots q_1^{[e_1]}$, and suppose ${}_{r_i}Tr(U)=\{u\}$. Then ${}_{r_i}wTr(U)=\{(u)_{q_s},(u)_{q_s},\cdots,(u)_{q_1},\cdots,(u)_{q_1}\}$ in which the number of $(u)_{q_j}$ is e_j. And the weight trace of U in subset $\mathbb{Z}_{2^{n-r_{i-1}}}$ can be express as ${}_{r_{i-1}'}wTr(U)=\{(u_{s,1})_{q_s},\ (u_{s,2})_{q_s},\ \cdots,\ (u_{s,e_s})_{q_s},\ \cdots,(u_{1,1})_{q_1},\ \cdots,(u_{1,e_1})_{q_1}\}$ in which $u_{k,j}\in\{u+l\cdot 2^{n-r_i+1}:\ 0\le l<2^{r_i-r_{i-1}-1}\}$ and $u_{k,j}\neq u_{k',j'}$ for any $(k,j)\neq(k',j')$, where $1\le k\le k'\le s$ and $1\le j\le e_j$, $1\le j'\le e_{j'}$. 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 ${}_{r_{i-1}'}\mathcal{B}$ and ${}_{r_i}\mathcal{B}$ where $1\le i\le T$.

Definition 6. *Let U be a set in class $\mathbf{B}$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$. We define the orbit of U in $\mathbb{Z}_{2^{n-r_i+1}}$ as*

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

And we denote

$$_{r'_{i-1}}wTr({}_{r_i}O_U) := \{{}_{r'_{i-1}}wTr(U') : \ U' \in {}_{r_i}O_U\}.$$

Given a multiset $Q = q_s^{[e_s]} q_{s-1}^{[e_{s-1}]} \cdots q_1^{[e_1]} \in \mathcal{Q}$, we define $Index(Q) = \{e_s, e_{s-1}, \cdots, e_1\}$ which is also a multiset. And given a positive integer N and a multiset $U = \{u_1, u_2, \cdots, u_m\} \in \mathcal{Q}$, we define $\binom{N}{U} = \binom{N}{u_1} \cdot \prod_{j=1}^{m-1} \binom{N-\sum_{k=1}^{j} u_k}{u_{j+1}}$.

Lemma 8. *Let U be a set in class $\mathbf{B}$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$. If U is also in class $\mathbf{B}_1$, where $\mathbf{B}_1 = {}_{r_i}B_Q$, then the size of the weight trace set of the orbit of U is*

$$\left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right| = \binom{2^{r_i - r_{i-1} - 1}}{Index(Q)},$$

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

Proof. Suppose $Q = q_s^{[e_s]} q_{s-1}^{[e_{s-1}]} \cdots q_1^{[e_1]}$ and ${}_{r_i}Tr(U) = \{u\}$. We have ${}_{r_i}wTr(U) = \{(u)_{q_s}, \cdots, (u)_{q_s}, \cdots, (u)_{q_1}, \cdots, (u)_{q_1}\}$ in which the number of $(u)_{q_j}$ is e_j. Then ${}_{r'_{i-1}}wTr(U) = \{(u_{s,1})_{q_s}, (u_{s,2})_{q_s}, \cdots, (u_{s,e_s})_{q_s}, \cdots, (u_{1,1})_{q_1}, \cdots, (u_{1,e_1})_{q_1}\}$ in which $u_{j,k} \in \{u + l \cdot 2^{n-r_i+1} : 0 \le l < 2^{r_i - r_{i-1} - 1}\}$ and $u_{j,k} \neq u_{j',k'}$ for any $(j,k) \neq (j',k')$ where $1 \le j \le j' \le s$ and $1 \le k \le e_j$, $1 \le k' \le e_{j'}$. Then we get $\left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right| = \binom{2^{r_i - r_{i-1} - 1}}{Index(Q)}$ by combinations theorem. □

Generally, we have the following theorem:

Theorem 3. *Let U be a set in class $\mathbf{B}$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$. If U is also in class $\mathbf{B}_1$, where $\mathbf{B}_1 = {}_{r_i}B_{Q_t}^{h_t} B_{Q_{t-1}}^{h_{t-1}} \cdots B_{Q_1}^{h_1} \in {}_{r_i}\mathcal{B}$, then the size of the weight trace set of the orbit of U is*

$$\left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right| = \prod_{j=1}^{t} \binom{2^{r_i - r_{i-1} - 1}}{Index(Q_j)}^{h_j}.$$

Proof. Suppose $U = \bigcup_{j=1}^{t} \mathbf{U}_j$ where $\mathbf{U}_j = \bigcup_{k=1}^{h_j} U_{j,k} \in {}_{r_i}B_{Q_j}^{h_j}$ and $U_{j,k} \in {}_{r_i}B_{Q_j}$. Suppose ${}_{r_i}Tr(U_{j,k}) = \{u_{j,k}\}$, then ${}_{r_i}Tr(U) = \bigcup_{j=1}^{t} \bigcup_{k=1}^{h_j} {}_{r_i}Tr(U_{j,k}) = \{u_{j,k} : \ 1 \le j \le t, \ 1 \le k \le h_j\}$ and $u_{j,k} \neq u_{j',k'}$ for any $(j,k) \neq (j',k')$ where $1 \le j \le j' \le t$ and $1 \le k \le h_j$, $1 \le k' \le h_{j'}$. According to Lemma 8, each ${}_{r'_{i-1}}wTr(U_{j,k})$ corresponds to $|Q_j|$ elements in the set $\{u_{j,k}, \ u_{j,k} + 2^{n-r_i+1}, \ \cdots, \ u_{j,k} + (2^{r_i - r_{i-1} - 1} - 1) \cdot 2^{n-r_i+1}\}$, where $0 \le u_{j,k} < 2^{n-r_i+1}$, and there are $\binom{2^{r_i - r_{i-1} - 1}}{Index(Q_j)}$ possibilities. As a result, we have $\left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right| = \prod_{j=1}^{t} \binom{2^{r_i - r_{i-1} - 1}}{Index(Q_j)}^{h_j}$. □

According to Theorem 3, the size of the weight trace of the orbit of U only relate to $\mathbf{B}$ and $\mathbf{B}_1$, i.e. for any $U, V \in \mathbf{B}$, if $U, V \in \mathbf{B}_1$, then $\left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right| = \left|{}_{r'_{i-1}}wTr({}_{r_i}O_V)\right|$. Therefore, we define a coefficient from class $\mathbf{B}$ to $\mathbf{B}_1$ as :

$$Coef(\mathbf{B}_1 \mid \mathbf{B}) := \left|{}_{r'_{i-1}}wTr({}_{r_i}O_U)\right|, \text{ where } U \in \mathbf{B} \text{ and } U \in \mathbf{B}_1.$$

Theorem 4. *Let class $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$. We denote ${}_{r_i}Gen(\mathbf{B}) = \{\mathbf{B}' \in {}_{r_i}\mathcal{B} : \ \exists U \in \mathbf{B} \ s.t. \ U \in \mathbf{B}'\}$. Then we have*

$$\left|{}_{r'_{i-1}}wTr(\mathbf{B})\right| = \sum_{\mathbf{B}' \in {}_{r_i}Gen(\mathbf{B})} Coef(\mathbf{B}' \mid \mathbf{B}) \cdot \left|{}_{r_i}wTr(\mathbf{B}')\right|.$$

Proof. By Theorem 3, we have that for a given $\mathbf{B}' \in {}_{r_i}Gen(\mathbf{B})$, for all elements in ${}_{r_i}wTr(\mathbf{B}')$, there are $Coef(\mathbf{B}' \mid \mathbf{B})$ elements in ${}_{r'_{i-1}}wTr(\mathbf{B}')$ corresponding to it. As $\mathbf{B} = \bigcup_{\mathbf{B}' \in {}_{r_i}Gen(\mathbf{B})} \mathbf{B}'$ and it is easy to know that ${}_{r_i}wTr(\mathbf{B}') \bigcap {}_{r_i}wTr(\mathbf{B}'')$ $= \emptyset$ for any $\mathbf{B}', \mathbf{B}'' \in {}_{r_i}Gen(\mathbf{B})$ and $\mathbf{B}' \neq \mathbf{B}''$, then we have derived the theorem.

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

Let $U = \{1,5,9\} \in {}_{r'_2}B_2B_1$. Then ${}_{r_3}wTr(U) = \{(1)_2, (1)_1\}$, so $U \in {}_{r_3}B_{2^{[1]}1^{[1]}}$. And ${}_{r'_2}wTr({}_{r_3}O_U) = \{\{(1)_2, (3)_1\}$, $\{(1)_2, (5)_1\}$, $\{(1)_2, (7)_1\}$, $\{(3)_2, (1)_1\}$, $\{(3)_2, (5)_1\}$, $\{(3)_2, (7)_1\}$, $\{(5)_2, (1)_1\}$, $\{(5)_2, (3)_1\}$, $\{(5)_2, (7)_1\}$, $\{(7)_2, (1)_1\}$, $\{(7)_2, (3)_1\}$, $\{(7)_2, (5)_1\}\}$.

Let $V = \{1,5,8\} \in {}_{r'_2}B_2B_1$. Then ${}_{r_3}wTr(V) = \{(0)_1, (1)_2\}$, so $V \in {}_{r_3}B_2B_1$. And ${}_{r'_2}wTr({}_{r_3}O_V) = \{\{(1)_2, (0)_1\}$, $\{(1)_2, (2)_1\}$, $\{(1)_2, (4)_1\}$, $\{(1)_2, (6)_1\}$, $\{(3)_2, (0)_1\}$, $\{(3)_2, (2)_1\}$, $\{(3)_2, (4)_1\}$, $\{(3)_2, (6)_1\}$, $\{(5)_2, (0)_1\}$, $\{(5)_2, (2)_1\}$, $\{(5)_2, (4)_1\}$, $\{(5)_2, (6)_1\}$, $\{(7)_2, (0)_1\}$, $\{(7)_2, (2)_1\}$, $\{(7)_2, (4)_1\}$, $\{(7)_2, (6)_1\}\}$.

${}_{r_3}Gen({}_{r'_2}B_2B_1) = \{{}_{r_3}B_{2^{[1]}1^{[1]}}, {}_{r_3}B_2B_1\}$. $Coef({}_{r_3}B_{2^{[1]}1^{[1]}} \mid {}_{r'_2}B_2B_1) = \binom{4}{\{1,1\}} = 12$ and $Coef({}_{r_3}B_2B_1 \mid {}_{r'_2}B_2B_1) = \binom{4}{1}\binom{4}{1} = 16$. $\left|{}_{r'_2}wTr({}_{r'_2}B_2B_1)\right| = \binom{8}{2}\binom{2}{1} = 56$, ${}_{r_3}wTr({}_{r_3}B_{2^{[1]}1^{[1]}}) = \binom{2}{1} = 2$ and ${}_{r_3}wTr({}_{r_3}B_2B_1) = \binom{2}{1}\binom{1}{1} = 2$. It is easy to check that $12 \cdot 2 + 16 \cdot 2 = 56$.

For a given set U in class $\mathbf{B}$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$, we denote the set of all $U' \in \mathbf{B}$ which $\mathbb{C}_{2^i}$-equivalent to U by

$$_{r_i}CE(U) := \{U' \in \mathbf{B} : U' \overset{i}{\sim} U\}.$$

and we denote

$$_{r'_{i-1}}wTr(_{r_i}CE(U)) = \{_{r'_{i-1}}wTr(U') : U' \in {}_{r_i}CE(U)\}.$$

We define the multiplicity of U in $\mathbf{B}$ under $\mathbb{C}_{2^i}$-equivalent as

$$_{r_i}\mathit{Mult}(U) := \begin{cases} 1/\left|_{r'_{i-1}}wTr(_{r_i}CE(U))\right|, & \text{if } \nexists V \in \mathbb{C}_{2^i}(2^{i-1}+1), \text{s.t. } V \subseteq U, \\ 0 & \text{otherwise.} \end{cases}$$

Remark, $_{r_i}CE(U)$ includes U itself.

Lemma 9. *Let U be a set in class $\mathbf{B}$, if U is also in $\mathbf{B}'$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$, $\mathbf{B}' = {}_{r_i}B_Q \in {}_{r_i}\mathcal{B}$ and $Q = q_t^{[e_t]} q_{t-1}^{[e_{t-1}]} \cdots q_1^{[e_1]} \in \mathcal{Q}$, $q_t > q_{t-1} > \cdots > q_1$, then we have:*

$$_{r_i}\mathit{Mult}(U) = \begin{cases} 0, & \text{if } e_t \geq 2 \text{ and } q_t > 2^{i-2} \text{ or } e_t = 1 \text{ and } q_t + q_{t-1} > 2^{i-1}, \\ 1/2^{e_t-1}, & \text{if } e_t \geq 2 \text{ and } q_t = 2^{i-2}, \\ 1/(e_{t-1}+1), & \text{if } e_t = 1 \text{ and } q_t + q_{t-1} = 2^{i-1}, \\ 1/(2^{r_i - r_{i-1} - 1}), & \text{if } t = 1,\ e_t = 1 \text{ and } q_t = 2^{i-1}, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Suppose $_{r_i}Tr(U) = \{u\}$, then

- $_{r_i}wTr(U) = \{(u)_{q_t}, \cdots, (u)_{q_t}, \cdots, (u)_{q_1}, \cdots, (u)_{q_1}\}$ where the number of $(u)_{q_j}$ is e_j.
- $_{r'_{i-1}}wTr(U) = \{(u_{t,1})_{q_t}, \cdots, (u_{t,e_t})_{q_t}, \cdots, (u_{1,1})_{q_1}, \cdots, (u_{1,e_1})_{q_1}\}$ where $u_{j,k} \in \{u + l \cdot 2^{n-r_i+1} : 0 \leq l < 2^{r_i - r_{i-1} - 1}\}$, $u_{j,k} \neq u_{j',k'}$ for any $(j,k) \neq (j',k')$ and $1 \leq j, j' \leq t$, $1 \leq k \leq e_j$, $1 \leq k' \leq e_{j'}$.
- Let $U_{j,k}$ denote the subset of U, which satisfy that $_{r'_{i-1}}wTr(U_{j,k}) = \{(u_{j,k})_{q_j}\}$, for $1 \leq j \leq t$ and $1 \leq k \leq e_j$.

Case 1 (If $e_t \geq 2$ and $q_t > 2^{i-2}$ or $e_t = 1$ and $q_t + q_{t-1} > 2^{i-1}$). As $d(U_{j,k}, U_{j',k'}) > 2^{n-r_i}$ for any $(j,k) \neq (j',k')$, by Corollary 3, it follows that $U_{t,k} + U_{t,k'} \in \mathbb{C}_{2^i}(p)$ or $U_{t,1} + U_{t-1,k''} \in \mathbb{C}_{2^i}(p')$, where $p, p' > 2^{i-1}$, $1 \leq k < k' \leq e_t$ and $1 \leq k'' \leq e_{t-1}$. Therefore, $\mathit{Mult}(U) = 0$.

Now let us consider the other cases. Suppose $U' \overset{i}{\sim} U$ where $U' \in \mathbf{B}$.

- $_{r'_{i-1}}wTr(U') = \{(u'_{t,1})_{q_t}, \cdots, (u'_{t,e_t})_{q_t}, \cdots, (u'_{1,1})_{q_1}, \cdots, (u'_{1,e_1})_{q_1}\}$ where $u'_{j,k} \neq u'_{j',k'}$ for any $(j,k) \neq (j',k')$ and $1 \leq j, j' \leq t$, $1 \leq k \leq e_j$, $1 \leq k' \leq e_{j'}$.
- Let $U'_{j,k}$ denote the subset of U', which satisfy that $_{r'_{i-1}}wTr(U'_{j,k}) = \{(u'_{j,k})_{q_j}\}$, for $1 \leq j \leq t$ and $1 \leq k \leq e_j$.

For any $V \in \mathbb{C}_{2^i}$, it can be decomposed into two cubes W_1 and W_2 which are both in $C_{2^{i-1}}$. Since $U' \overset{i}{\sim} U$, then there exists $V_1, V_2, \cdots, V_d \in \mathbb{C}_{2^i}$ such that $U + U' = \sum_{j=1}^{t} \sum_{k=1}^{e_j} U_{j,k} + \sum_{j'=1}^{t} \sum_{k'=1}^{e_j} U'_{j',k'} = \sum_{j=1}^{d} V_j$. So for any $U_{j,k}$, there must exist $U'_{j',k'}$ such that $U_{j,k} + U'_{j',k'} \in C_{2^{i-1}}$ or $U_{j,k} + U'_{j',k'} = \emptyset$. Based on this observation, we analysis the value of $_{r_i}\mathit{Mult}(U)$ for other cases as follow.

Case 2 (If $e_t \geq 2$ and $q_t = 2^{i-2}$). In this case, $U'_{j,k} = U_{j,k}$ for any $1 \leq j < t$ and $1 \leq k \leq e_j$. Now let us consider $U_{t,1}, U_{t,2}, \cdots, U_{t,e_t}$. According to the above analysis, we can choose two sets $U'_{t,j}$ and $U'_{t,j'}$ to make $U_{t,j} + U'_{t,j} + U_{t,j'} + U'_{t,j'}$ be a cube in $\mathbb{C}_{2^i}$ and eliminate all other $U_{t,k}$, i.e. let $U'_{j,k} = U_{j,k}$ for others. Similarly, we can choose four sets $U'_{t,j_1}, U'_{t,j_2}, U'_{t,j_3}, U'_{t,j_4}$ to make $U_{t,j_1} + U'_{t,j_1} + U_{t,j_2} + U'_{t,j_2} + U_{t,j_3} + U'_{t,j_3} + U_{t,j_4} + U'_{t,j_4}$ be the union of two disjoint cubes in $\mathbb{C}_{2^i}$ and eliminate all other $U_{t,k}$. Without loss of generality, we can choose $6, 8, \cdots, 2 \cdot \lfloor e_t/2 \rfloor$ sets added to the corresponding sets $U_{t,j}$ and make the resulted sets be unions of $3, 4, \cdots, \lfloor e_t/2 \rfloor$ disjoint cubes in $\mathbb{C}_{2^i}$. So, the number of the weight trace in $\mathbb{Z}_{2^{n-r_{i-1}}}$ of all those U' is $\binom{e_t}{0} + \binom{e_t}{2} + \cdots + \binom{e_t}{2 \cdot \lfloor e_t/2 \rfloor} = 2^{e_t-1}$. Thus $_{r_i}\mathit{Mult}(U) = 1/2^{e_t-1}$.

Case 3 (If $e_t = 1$ and $q_t + q_{t-1} = 2^{i-1}$). In this case, $U'_{j,k} = U_{j,k}$ for any $1 \leq j < t-1$ and $1 \leq k \leq e_j$. We need only to consider $U_{t,1}, U_{t-1,1}, U_{t-1,2}, \cdots, U_{t-1,e_{t-1}}$ and the corresponding $U'_{t,1}, U'_{t-1,1}, U'_{t-1,2}, \cdots, U'_{t-1,e_{t-1}}$. According to the above analysis, we can only add points in $U'_{t-1,k}$ and $U'_{t,1}$ to $U_{t,1}$ and $U_{t-1,k'}$ and make the resulted two sets become a cube and eliminate all other $U_{t-1,k}$. It is easy to know that the number of the weight trace in $\mathbb{Z}_{2^{n-r_{i-1}}}$ of all those U' is $e_{t-1}+1$. So $_{r_i}\mathit{Mult}(U) = 1/(e_{t-1}+1)$.

Case 4 (If $t=1, e_t=1$ and $q_t=2^{i-1}$). Due to $U'+U \in \mathbb{C}_{2^i}$, it follows that $d(U,U') > 2^{n-r_i}$, i.e. $u'_{t,1} \in \{u + l \cdot 2^{n-r_i+1} : 0 \le l < 2^{r_i - r_{i-1} - 1}\}$. Therefore, the number of the weight trace in $\mathbb{Z}_{2^{n-r_{i-1}}}$ of all those U' is $2^{r_i-r_{i-1}-1}$ and ${}_{r_i}Mult(U) = 1/(2^{r_i-r_{i-1}-1})$.

Case 5 (Else). According to the above mentioned analysis, there does not exist a set $U' \in \mathbf{B}$ except U itself such that U' $\mathbb{C}_{2^i}$-equivalent to U. Therefore, ${}_{r_i}Mult(U) = 1$.

□

From Lemma 9, it can easily be seen that, for two sets $U, V \in \mathbf{B}$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$, if $U, V \in {}_{r_i}B_Q$, we have ${}_{r_i}Mult(U) = {}_{r_i}Mult(V)$. This value depends only on ${}_{r_i}B_Q$ because it does not require the knowledge of exact values of the elements in the individual set. Therefore, we define $Mult({}_{r_i}B_Q) = {}_{r_i}Mult(U)$ where $U \in {}_{r_i}B_Q$. Generally, we have

Theorem 5. *Let U and V be two sets in $\mathbf{B}$. If $U, V \in \mathbf{B}'$, where $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$, $\mathbf{B}' \in {}_{r_i}\mathcal{B}$, then ${}_{r_i}Mult(U) = {}_{r_i}Mult(V)$. And we define $Mult(\mathbf{B}') = {}_{r_i}Mult(U)$, where $U \in \mathbf{B}'$. Further more, if $\mathbf{B}' = {}_{r_i}B_{Q_t}^{h_t} B_{Q_{t-1}}^{h_{t-1}} \cdots B_{Q_1}^{h_1} \in {}_{r_i}\mathcal{B}$, we have*

$$Mult(\mathbf{B}') = \prod_{j=1}^{t} Mult({}_{r_i}B_{Q_j})^{h_j}.$$

Proof. Suppose $U \in \mathbf{B}'$ and ${}_{r_i}Tr(U) = \{u_{t,1}, u_{t,2}, \cdots, u_{t,h_t}, \cdots, u_{1,1}, u_{1,2}, \cdots, u_{1,h_1}\}$. Let $\mathbf{U}_{j,k}$ denotes the subset of U, which satisfy that $\mathbf{U}_{j,k} \in {}_{r_i}B_{Q_j}$ and ${}_{r_i}Tr(\mathbf{U}_{j,k}) = \{u_{j,k}\}$, for $1 \le j \le t$ and $1 \le k \le h_j$. Applying Lemma 9, we get $Mult({}_{r_i}B_{Q_j}) = {}_{r_i}Mult(\mathbf{U}_{j,k})$ for each $\mathbf{U}_{j,k}$. Considering that each set of weight traces ${}_{r'_{i-1}}wTr(\mathbf{U}_{j,k})$ only correlate with $\{u_{j,k} + l \cdot 2^{n-r_i+1} : 0 \le l < 2^{r_i-r_{i-1}-1}\}$, so the multiplicity of U is ${}_{r_i}Mult(U) = \prod_{j=1}^{t} Mult({}_{r_i}B_{Q_j})^{h_j}$. And this value has nothing to do with the set U that we chose, so $Mult(\mathbf{B}') = \prod_{j=1}^{t} Mult({}_{r_i}B_{Q_j})^{h_j}$. □

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 $U_1 \in {}_{r_3}B_4$ and ${}_{r_3}wTr(U_1) = \{(1)_4\}$. ${}_{r_2}wTr({}_{r_3}CE(U_1)) = \{(1)_4, (3)_4, (5)_4, (7)_4\}$ and $Mult({}_{r_3}B_4) = {}_{r_i}Mult(U) = \frac{1}{4}$.

Let set $U_2 = \{1, 3, 9, 17\}$, then $U_2 \in {}_{r_3}B_{3[1]\,1[1]}$ and ${}_{r_3}wTr(U_2) = \{(1)_3, (1)_1\}$. ${}_{r_2}wTr({}_{r_3}CE(U_2)) = \{\{(1)_3, (3)_1\}, \{(1)_1, (3)_3\}\}$, so $Mult({}_{r_3}B_{3[1]\,1[1]}) = {}_{r_i}Mult(U) = \frac{1}{2}$.

Remark, the multiplicity of a class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}$ measures the multiplicity of the class in the sense of equivalence. In other words, if $Mult(\mathbf{B}) \neq 0$ then there are $|\mathbf{B}| \cdot Mult(\mathbf{B})$ sequences which pairwise non- $\mathbb{C}_{2^i}$-equivalent, where $|\mathbf{B}|$ denote the number of sequences in class $\mathbf{B}$. In the next section, we will explain that if $Mult(\mathbf{B}) = 0$ if and only if for any sequence in class $\mathbf{B}$ there exists sequences with smaller Hamming weight which equivalent to it. Here, we highlight that, according the proof of Lemma 9 and Theorem 5, it is evident that if $U \in \mathbf{B}$ and ${}_{r_i}Mult(U) \neq 0$ then $U' \in \mathbf{B}$ for any $U' \overset{i}{\sim} U$ and $|U'| = |U|$.

For a given multiset $Q = q_t^{e_t} q_{t-1}^{e_{t-1}} \cdots q_1^{e_1} \in \mathcal{Q}$, where $q_t > q_{t-1} > \cdots > q_1$, we define

$$Extr(Q) = q_t,$$

and for a given $\mathbf{B} = {}_{r_i}B_Q \in {}_{r_i}\mathcal{B}$, we define

$$Extr(\mathbf{B}) = {}_{r_i}B_{Extr(Q)} = {}_{r_i}B_{q_t}.$$

In addition, for a given $\mathbf{B} = {}_{r_i}B_{Q_t}^{h_t} B_{Q_{t-1}}^{h_{t-1}} \cdots B_{Q_1}^{h_1} \in {}_{r_i}\mathcal{B}$, we define

$$Extr(\mathbf{B}) = {}_{r_i}B_{Extr(Q_t)}^{h_t} B_{Extr(Q_{t-1})}^{h_{t-1}} \cdots B_{Extr(Q_1)}^{h_1}.$$

Note that if $Extr(Q_j) = Extr(Q_{j'})$, then the two terms $B_{Extr(Q_j)}^{h_j}$ and $B_{Extr(Q_{j'})}^{h_{j'}}$ are merge to be a single term $B_{Extr(Q_j)}^{h_j + h_{j'}}$ for $j \neq j'$. If $Extr(Q_{i_{1,1}}) = Extr(Q_{i_{1,2}}) = \cdots = Extr(Q_{i_{1,j_1}})$, $Extr(Q_{i_{2,1}}) = Extr(Q_{i_{2,2}}) = \cdots = Extr(Q_{i_{2,j_2}})$, $\cdots$, $Extr(Q_{i_{t,1}}) = Extr(Q_{i_{t,2}}) = \cdots = Extr(Q_{i_{t,j_t}})$, where $\bigcup_{u=1}^{t} \bigcup_{v=1}^{j_u} \{i_{u,v}\} = \{t,\ t-1,\ \cdots,\ 1\}$, we define

$$Coef_{Extr}(\mathbf{B}) = \prod_{u=1}^{t} \binom{\sum_{v=1}^{j_u} h_{u,v}}{h_{u,1},\ h_{u,2},\ \cdots,\ h_{u,j_u}}.$$

Based on the definition of $Coef_{Extr}(\mathbf{B})$, it is clear that for any element in $Extr(\mathbf{B})$, there are $Coef_{Extr}(\mathbf{B})$ elements in $\mathbf{B}$ which correspond to it. Thus, we get that:

Theorem 6. *Let* $\mathbf{B}$ *be a class in* ${}_{r_i}\mathcal{B}$. *If* $\mathbf{B}' = Extr(\mathbf{B})$, *then* $\left|{}_{r_i}wTr(\mathbf{B})\right| = \left|{}_{r_i}wTr(\mathbf{B}')\right| \cdot Coef_{Extr}(\mathbf{B})$.

For the specific sets $U \in {}_{r_i}B_Q$ and $V = \bigcup_{j=1}^{t} V_j \in {}_{r_i}B_{Q_t}^{h_t} B_{Q_{t-1}}^{h_{t-1}} \cdots B_{Q_1}^{h_1}$, where $V_j \in {}_{r_i}B_{Q_j}^{h_j}$, we define

$$ {}_{r_i}Extr(U) := U', \text{ where } U' \subseteq U \text{ and } U' \in {}_{r_i}B_{q_t}, $$

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

Remark, ${}_{r_i}Extr(U)$ is a one to many mapping but all elements in the codomain have the same weight trace in $\mathbb{Z}_{2^{n-r_i+1}}$.

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 $\mathbb{Z}_{2^{n-r_i}}$ as follow:

Definition 7. *Let* U *be a set in class* $\mathbf{B}$, *where* $\mathbf{B} \in {}_{r_i}\mathcal{B}'$. *We define the orbit of* U *in* $\mathbb{Z}_{2^{n-r_i}}$ *as*

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

And we define

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

Lemma 10. *Let* U *be a set in class* $\mathbf{B}$, *where* $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l} B_{p_{l-1}}^{d_{l-1}} \cdots B_{p_1}^{d_1} \in {}_{r_i}\mathcal{B}'$. *Suppose* U *is also in class* $\mathbf{B}'$ *where* $\mathbf{B}' = {}_{r_i'}B_q^e \in {}_{r_i'}\mathcal{B}$. *And suppose* ${}_{r_i}Tr(U) = \{u_1,\ u_2,\ \cdots,\ u_d\}$ *and* ${}_{r_i}wTr(U) = \{(u_1)_{p_{j_1}},\ (u_2)_{p_{j_2}},\ \cdots,\ (u_d)_{p_{j_d}}\}$, *where* $0 \le u_j < 2^{n-r_i+1}$ *and* $d = \sum_{j=1}^{l} d_j$. *We have that, for all* $1 \le k \le d$, *if there exists* $u_{k'}$ *such that* $d(u_k, u_{k'}) = 2^{n-r_i}$ *then* $p_{j_k} + p_{j_{k'}} = q$, *and if there does not exist* $u_{k'}$ *such that* $d(u_k, u_{k'}) = 2^{n-r_i}$ *then* $p_{j_k} = q$, *where* $1 \le k' \le d$ *and* $k \neq k'$. *We then recursively decompose* ${}_{r_i}Tr(U)$ *into the following sets:*

1. *Let* $V_0 = \{\{u_k, u_{k'}\} : d(u_k, u_{k'}) = 2^{n-r_i}$ and $p_{j_k} = p_{j_{k'}} = \frac{q}{2}\}$.
2. *Let* $V_1 = \{\{u_k\} : p_{j_k} = q\}$. *Let* $W_1 = \{(u)_p : \ (u)_p \in {}_{r_i}wTr(U),\ \nexists w \in (V_0 \bigcup V_1),\ s.t. u \in w\}$.
3. *Suppose we have get* V_{s-1}, *and* W_{s-1}, $W_{s-1} \neq \emptyset$, $s > 1$.
4. *We then recursively generate all* V_s *until* $s = t$, *such that* $W_t = \emptyset$ *by applying the following procedure: choose an element* $(u)_p$ *from* W_{s-1}, *then construct* $V_s = \{\{u_k, u_{k'}\} : d(u_k, u_{k'}) = 2^{n-r_i},\ p_{j_k} = p\}$, $W_s = \{(u')_{p'} : (u')_{p'} \in W_{s-1}, \nexists w \in V_s \ s.t.\ u' \in w\}$.

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

$$ \left|{}_{r_i}wTr({}_{r_i'}O_U)\right| = 2^{\sum_{s=1}^{t} m_s} \cdot \binom{e}{m_0, m_1, \cdots, m_t} $$

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

Proof. It is easy to see that $e = \sum_{s=0}^{t} m_s$. For each $\{u_k\} \in V_1$, we can construct $\{u_k'\}$ such that $d(u_k, u_k') = 2^{n-r_i}$. Thus, we can construct an U' by substituting $(u_k)_{p_{j_k}}$ with $(u_k')_{p_{j_k}}$ in ${}_{r_i}wTr(U)$. That is ${}_{r_i}wTr(U') = \{(u_1)_{p_{j_1}}, (u_2)_{p_{j_2}}, \cdots, (u_k')_{p_{j_k}}, \cdots, (u_d)_{p_{j_d}}\}$. It is easy to check that $U' \in {}_{r_i'}O_U$. For each element $\{u_k, u_{k'}\} \in V_s$ $(2 \le s \le t)$, we can also construct an U' by exchanging the index of element $(u_k)_{p_{j_k}}$ and $(u_{k'})_{p_{j_{k'}}}$ in ${}_{r_i}wTr(U)$. That is ${}_{r_i}wTr(U') = \{(u_1)_{p_{j_1}}, \cdots, (u_k)_{p_{j_{k'}}}, \cdots, (u_{k'})_{p_{j_k}}, \cdots, (u_d)_{p_{j_d}}\}$. It is also easy to check that $U' \in {}_{r_i'}O_U$. Hence, using the above method, for a given U, we can construct $2^{\sum_{s=1}^{t} m_s}$ elements in ${}_{r_i}wTr(\mathbf{B})$ which have the same weight trace in $\mathbb{Z}_{2^{n-r_i}}$ as U. Besides, suppose $|V_0| \ge 1$, $|V_1| \ge 1$, with regard to elements $\{u_k, u_{k'}\} \in V_0$ and $\{u_{k_1}\} \in V_1$, we can construct U', such that ${}_{r_i}wTr(U') = {}_{r_i}wTr(U) - \{(u_k)_{q/2},\ (u_{k'})_{q/2},\ (u_{k_1})_q\} + \{(u_k)_q,\ (u_{k_1})_{q/2},\ (u_{k_1}')_{q/2}\}$, where $d(u_{k_1}, u_{k_1}') = 2^{n-r_i}$. It is easy to see that $U' \in {}_{r_i'}O_U$. Generally, with regard to any two elements in $V = \bigcup_{s=0}^{t} V_s$, we can construct a set $U' \in {}_{r_i'}O_U$ 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 $\mathbb{Z}_{2^{n-r_i+1}}$. Thus by combination theorems, for a given set U, we can construct $\binom{e}{m_0, m_1, \cdots, m_t}$ elements in ${}_{r_i}wTr(\mathbf{B})$ which have the same weight trace in $\mathbb{Z}_{2^{n-r_i}}$ as U. Therefore the size of the weight trace set of the orbit of U is $|{}_{r_i}wTr({}_{r_i'}O_U)| = 2^{\sum_{s=1}^{t} m_s} \cdot \binom{e}{m_0, m_1, \cdots, m_t}$. □

Example 4. Let $L = 2^n - (2^{n-r_1} + 2^{n-r_2} + 2^{n-r_3})$ where $n = 8$, $r_1 = 1$, $r_2 = 2$, $r_3 = 3$ and $r_4 = 4$. Let set U such that ${}_{r_4}Tr(U) = \{1, 2, 3, 4, 5, 18, 19, 20, 21\}$ and ${}_{r_4}wTr(U) = \{(1)_6, (2)_5, (3)_4, (4)_4, (5)_3, (18)_1, (19)_2, (20)_2, (21)_3\}$. Then $U \in \mathbf{B} = {}_{r_4}B_6 B_5 B_4^2 B_3^2 B_2^2 B_1$ and $U \in \mathbf{B}' = {}_{r_4'}B_6^5$.

Then ${}_{r_4}O_U = \{U \in \mathbf{B} : \ {}_{r_4'}wTr = \{(1)_6, (2)_6, (3)_6, (4)_6, (5)_6\}\}$. 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. ${}_{r_4}wTr(U') = {}_{r_4}wTr(U) - \{(1)_6\} + \{(17)_6\}$. With regard to element $\{2, 18\}$ in V_2, we can construct U', s.t. ${}_{r_4}wTr(U') = {}_{r_4}wTr(U) - \{(2)_5, (18)_1\} + \{(2)_1, (18)_5\}$. With regard to element $\{1\} \in V_1$ and element $\{3, 19\} \in V_3$, we can construct U', s.t. ${}_{r_4}wTr(U') = {}_{r_4}wTr(U) - \{(1)_6, (3)_4, (19)_2\} + \{(1)_4, (17)_2, (3)_6\}$.

For any $U' \in \mathbf{B}$, if $U' \in \mathbf{B}'$ then we can also get the sets V_0', V_1', $\cdots$, V_t' which satisfy that $|V_s'| = |V_s| = m_s$ for $0 \le s \le t$. So we have $\left|{}_{r_i}wTr({}_{r_i'}O_{U'})\right| = \left|{}_{r_i}wTr({}_{r_i'}O_U)\right|$. We define $Coef(\mathbf{B}' \mid \mathbf{B}) = \left|{}_{r_i}wTr({}_{r_i'}O_U)\right|$.

Corollary 6. *Let U be a set in class $\mathbf{B}$ where $\mathbf{B} \in {}_{r_i}\mathcal{B}'$. And suppose U is also in class $\mathbf{B}' = {}_{r_i'}B_{q_s}^{e_s}B_{q_{s-1}}^{e_{s-1}}\cdots B_{q_1}^{e_1}$. Suppose $U = \bigcup_{j=1}^{s} U_j \in \mathbf{B}'$ where $U_j \in {}_{r_i'}B_{q_j}^{e_j}$, then we have*

$$\left|{}_{r_i}wTr({}_{r_i'}O_U)\right| = \prod_{j=1}^{s}\left|{}_{r_i}wTr({}_{r_i'}O_{U_j})\right|.$$

Similarly, for any $U' \in \mathbf{B}$, if $U' \in \mathbf{B}'$ then we can also get $|{}_{r_i}wTr({}_{r_i'}O_{U'})| = |{}_{r_i}wTr({}_{r_i'}O_U)|$. Denote $U_j \in \mathbf{B}_j$ where $\mathbf{B}_j$ is a class in ${}_{r_i}\mathcal{B}'$, we define $Coef(\mathbf{B}' \mid \mathbf{B}) = \prod_{j=1}^{s} Coef({}_{r_i'}B_{q_j}^{e_j}|\mathbf{B}_j)$. Then we have

Theorem 7. *Let $\mathbf{B}$ be a class in ${}_{r_i}\mathcal{B}'$, we denote ${}_{r_i'}Gen(\mathbf{B}) = \{\mathbf{B}' \in {}_{r_i'}\mathcal{B} : \exists U \in \mathbf{B} \text{ s.t } U \in \mathbf{B}'\}$. Then the size of the weight trace in $\mathbb{Z}_{2^{n-r_i}}$ of all elements in $\mathbf{B}$ is*

$$\left|{}_{r_i}wTr(\mathbf{B})\right| = \sum_{\mathbf{B}' \in {}_{r_i'}Gen(\mathbf{B})} Coef(\mathbf{B}' \mid \mathbf{B}) \cdot \left|{}_{r_i'}wTr(\mathbf{B}')\right|.$$

Remark that, given $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1} \in {}_{r_i}\mathcal{B}'$ and $\mathbf{B}' = {}_{r_i'}B_{q_s}^{e_s}B_{q_{s-1}}^{e_{s-1}}\cdots B_{q_1}^{e_1} \in {}_{r_i'}Gen(\mathbf{B})$, we have that each q_j is equal to the sum of $p_{j'}$ and $p_{j''}$ or equal to $p_{j'}$ where $p_{j'}, p_{j''} \in \{p_l, p_{l-1}, \cdots, p_1\}$ and $j' \le j''$. If we know all the decompose of each q_j, then we can directly compute the value of $Coef(\mathbf{B}' \mid \mathbf{B})$. For instance, for two given classes $\mathbf{B} = {}_{r_i}B_4^2B_3^3B_2^2B_1$ and $\mathbf{B}' = {}_{r_i'}B_7B_6B_5B_4$, the decomposition of those q are $7 = 4+3,\ 6 = 3+3,\ 5 = 4+1,\ 4 = 2+2$, then we have $Coef(\mathbf{B}' \mid \mathbf{B}) = 2\cdot 1\cdot 2\cdot 1 = 4$.

Example 5. 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 $U = \{1,9,19,33,51\} \in {}_{r_2}B_2^2B_1$. Then ${}_{r_2}wTr(U) = \{(1)_2,(3)_2,(9)_1\}$ and ${}_{r_2'}wTr(U) = \{(1)_3,(3)_2\}$, so $U \in {}_{r_2'}B_3B_2$. ${}_{r_2}wTr({}_{r_2'}O_U) = \{\{(1)_2,(3)_2,(9)_1\},\{(1)_1,(3)_2,(9)_2\},\{(1)_2,(11)_2,(9)_1\},\{(1)_1,(11)_2,(9)_2\}\}$. $Coef({}_{r_2'}B_3B_2 \mid {}_{r_2}B_2^2B_1) = 4$.

${}_{r_2'}Gen({}_{r_2}B_2^2B_1) = \{{}_{r_2'}B_4B_1, {}_{r_2'}B_3B_2, {}_{r_2'}B_2^2B_1\}$. We have $\left|{}_{r_2}wTr({}_{r_2}B_2^2B_1)\right| = \binom{16}{2,1} = 1680$ and $\left|{}_{r_2'}wTr({}_{r_2'}B_4B_1)\right| = \binom{8}{1,1} = 56$, $\left|{}_{r_2'}wTr({}_{r_2'}B_3B_2)\right| = \binom{8}{1,1} = 56$, $\left|{}_{r_2'}wTr({}_{r_2'}B_2^2B_1)\right| = \binom{8}{2,1} = 168$.

$Coef({}_{r_2'}B_4B_1 \mid {}_{r_2}B_2^2B_1) = 2$, $Coef({}_{r_2'}B_3B_2 \mid {}_{r_2}B_2^2B_1) = 4$, $Coef({}_{r_2'}B_2^2B_1 \mid {}_{r_2}B_2^2B_1) = 8$. It is evident to check that $1680 = 56\cdot 2 + 56\cdot 4 + 168\cdot 8$.

In the next section, we will use the quantitative relations between different classes of error sequences 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 $\mathbf{E}_m$, we denote $\mathbf{E}_m^R$ the maximum subset of $\mathbf{E}_m$ 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 $\mathcal{A}(L) + E \subseteq \mathcal{A}_k(L)$ for any $E \in \mathbf{E}_m^R$, that is,

$$\mathbf{E}_m^R := \{E \in \mathbf{E}_m : \mathcal{A}(L) + E \subseteq \mathcal{A}_k'(L) \text{ and } \nexists E' \in \mathbf{E}_{m'},\ m' \le m, \text{ s.t. } E' \sim E \text{ where } E' \ne E\}, 0 < m \le k.$$

Consequently, we have

$$\mathcal{A}_k(L) = \bigcup_{m=0}^{k}(\mathcal{A}(L) + \mathbf{E}_m^R) \text{ and } (\mathcal{A}(L) + \mathbf{E}_m^R)\bigcap(\mathcal{A}(L) + \mathbf{E}_{m'}^R) = \emptyset, \text{ for } 0 \le m < m' \le k.$$

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

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

In the following we will use those quantitative relations in the last section to construct an algorithm for computing the value of $NE_{2m}(k,\ T)$ for giving k and L.

For a given set $U \in {}_{r_0'}B_1^m$, we define a mapping

$$F(U) := (U_0'',\ U_1,\ U_1',\ U_1'',\ \ldots,\ U_T,\ U_T',\ U_T'')$$

where $U_0''=U$, and $U_i=U_{i-1}''$, $U_i'={}_{r_i}Extr(U_i)$, $U_i''=U_i'$, for $1\le i\le T$. And we define:

$Gen({}_{r_0'}B_1^m)=\{(\mathbf{B}_0'',\ \mathbf{B}_1,\ \mathbf{B}_1',\ \mathbf{B}_1'',\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}_T',\ \mathbf{B}_T''):\ \exists U\in {}_{r_0'}B_1^m,\ \text{s.t. } F(U)\in(\mathbf{B}_0'',\ \mathbf{B}_1,\ \mathbf{B}_1',\ \mathbf{B}_1'',\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}_T',\ \mathbf{B}_T'')\}$.

Where $\mathbf{B}_0''={}_{r_0'}B_1^m$, $\mathbf{B}_i\in{}_{r_i}\mathcal{B}$, $\mathbf{B}_i'\in{}_{r_i}\mathcal{B}'$, and $\mathbf{B}_i''\in{}_{r_i'}\mathcal{B}$. Note that $F(U)\in(\mathbf{B}_0'',\ \mathbf{B}_1,\ \mathbf{B}_1',\ \mathbf{B}_1'',\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}_T',\ \mathbf{B}_T'')$ means that $U_0''\in\mathbf{B}_0''$ and $U_i\in\mathbf{B}_i$, $U_i'\in\mathbf{B}_i'$ and $U_i''\in\mathbf{B}_i''$ for $1\le i\le T$.

Theorem 8. *For giving errors k and k-error linear complexity L, then the size of* $\mathbf{E}_m^R$ $(1\le m\le k)$ *is*

$$Num(\mathbf{E}_m^R)=\sum_{\mathbb{B}\in Gen({}_{r_0'}B_1^m)}\left|{}_{r_T'}wTr(\mathbf{B}_T'')\right|\cdot\prod_{j=1}^{T}Imp(\mathbf{B}_j'')\cdot Coef(\mathbf{B}_j''\mid\mathbf{B}_j')\cdot Coef_{Extr}(\mathbf{B}_j)\cdot Mult(\mathbf{B}_j)\cdot Coef(\mathbf{B}_j\mid\mathbf{B}_{j-1}'').$$

Note that $\mathbb{B}=(\mathbf{B}_0'',\ \mathbf{B}_1,\ \mathbf{B}_1',\ \mathbf{B}_1'',\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}_T',\ \mathbf{B}_T'')\in Gen({}_{r_0'}B_1^m)$. *And for a given* $\mathbf{B}$ *in* ${}_{r_i'}\mathcal{B}$ *where* $\mathbf{B}={}_{r_i'}B_{q_s}^{e_s}B_{q_{s-1}}^{e_{s-1}}\cdots B_{q_1}^{e_1}$, $Imp(\mathbf{B})$ *is defined as follow:*

$$Imp(\mathbf{B}):=\begin{cases}1, & \text{if } q_s<Impvalue\\ 0, & \text{otherwise}\end{cases},\quad where\quad Impvalue=\left\lceil\frac{2^T+m-k}{2}\right\rceil.$$

Especially, $Num(\mathbf{E}_0^R)=1$ *if* $Impvalue>0$ *and* $Num(\mathbf{E}_0^R)=0$ *for else.*

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

Lemma 11. *All of the elements in* ${}_{r_0'}B_1^m$ *can be decomposed into pairwise disjoint subsets* $\mathbf{U}_j$*, such that for any* $U\in\mathbf{U}_j$*,* $F(U)$ *belong to the same* $\mathbb{B}$*, where* $\mathbb{B}\in Gen({}_{r_0'}B_1^m)$*. And we have that the number of sets in* ${}_{r_0'}B_1^m$ *is*

$$\left|{}_{r_0'}B_1^m\right|=\binom{2^n}{m}=\sum_{\mathbb{B}\in Gen({}_{r_0'}B_1^m)}\left|{}_{r_i'}wTr(\mathbf{B}_T'')\right|\cdot\prod_{j=1}^{T}Coef(\mathbf{B}_j''\mid\mathbf{B}_j')\cdot Coef_{Extr}(\mathbf{B}_j)\cdot Coef(\mathbf{B}_j\mid\mathbf{B}_{j-1}'').$$

Proof. For a given $\mathbb{B}\in Gen({}_{r_0'}B_1^m)$, combining Theorem 4, 6 and 7, we obtain that the number of $U\in{}_{r_0'}B_1^m$ which satisfy $F(U)\in\mathbb{B}$ is $\left|{}_{r_i'}wTr(\mathbf{B}_T'')\right|\cdot\prod_{j=1}^{T}Coef(\mathbf{B}_j''\mid\mathbf{B}_j')\cdot Coef_{Extr}(\mathbf{B}_j)\cdot Coef(\mathbf{B}_j\mid\mathbf{B}_{j-1}'')$. Then the lemma will be proved by showing that for any $U\in{}_{r_0'}B_1^m$, there only exists one $\mathbb{B}\in Gen({}_{r_0'}B_1^m)$ such that $F(U)\in\mathbb{B}$. Suppose $F(U)=(U_0'',\ U_1,\ U_1',\ U_1'',\ \cdots,\ U_T,\ U_T',\ U_T'')$. Recall that $U_i=\mathbf{U}_{i-1}''$, $U_i'={}_{r_i}Extr(\mathbf{U}_i)$, and $U_i''=\mathbf{U}_i'$, for $1\le i\le T$. According to the definition of ${}_{r_i}Extr(U)$, no matter which U_i' we choose, they are all in the same $\mathbf{B}_i'$. Thus the choice of U_i' has nothing with $\mathbf{B}_i'$. Then, it is evident to see that the lemma holds. □

Lemma 12. *Let* $\mathbb{B}=(\mathbf{B}_0'',\ \mathbf{B}_1,\ \mathbf{B}_1',\ \mathbf{B}_1'',\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}_T',\ \mathbf{B}_T'')\in Gen({}_{r_0'}B_1^m)$*, for any set* $U\in{}_{r_0'}B_1^m$*,* $F(U)\in\mathbb{B}$*, there exists* $V\in\mathbb{C}_{2^t}(2^{t-1}+1)$ *such that* $V\subseteq U$*, if and only if there exists* j *such that* $Mult(\mathbf{B}_j)=0$*. Where* $0\le t<T$ *and* $1\le j\le T$*.*

Proof. Assume there exists j such that $Mult(B_j)=0$, where $1\le j\le T$. Suppose $\mathbf{B}_j={}_{r_i}B_{Q_s}^{e_s}B_{Q_{s-1}}^{e_{s-1}}\cdots B_{Q_1}^{e_1}$. From Theorem 5, we have that there exists t such that $Mult({}_{r_i}B_{Q_t})=0$, where $1\le t\le s$. It follows that, there exists $V\in\mathbb{C}_{2^t}(2^{t-1}+1)$ such that $V\subseteq U$, where $1\le t\le T$.

Assume there exists $V\in\mathbb{C}_{2^t}(2^{t-1}+1)$ such that $V\subseteq U$ where $0\le t<T$. Denote the smallest t by t_0. Then we have $Mult(\mathbf{B}_j)\neq 0$ for $1\le j<t_0$ otherwise there exists $V'\in\mathbb{C}_{2^{t'}}(2^{t'-1}+1)$ such that $V'\subseteq U$ where $t'<t_0$ which contradict with t_0 is the smallest number. Suppose $\mathbf{B}_{t_0}={}_{r_{t_0}}B_{Q_s}^{e_s}B_{Q_{s-1}}^{e_{s-1}}\cdots B_{Q_1}^{e_1}$, if $Mult(\mathbf{B}_{t_0})\neq 0$, then we have $Mult({}_{r_{t_0}}B_{Q_j})\neq 0$ for $1\le j\le s$. So there does not exist $V\in\mathbb{C}_{2^{t_0}}(2^{t_0-1}+1)$ such that $V\subseteq U_{t_0}$. As $Extr(U_{t_0-1})=U_{t_0-1}'=U_{t_0-1}''=U_{t_0}$, so there does not exist $V\in\mathbb{C}_{2^{t_0}}(2^{t_0-1}+1)$ such that $V\subseteq U_{t_0-1}$ as well. By that analogy, we have that there does not exist $V\in\mathbb{C}_{2^{t_0}}(2^{t_0-1}+1)$ such that $V\subseteq U_1$ which contradict the condition. Thus $Mult(\mathbf{B}_{t_0})=0$. □

Lemma 13. *Let* E *be an error sequence in set* $\mathbf{E}_m$*. Then there exists* $E'\in\mathbf{E}_{m'}$*, such that* $E'\sim E$*, if and only if there exists a set* $U\in\mathbb{C}_{2^t}(2^{t-1}+1)$*, such that* $U\subseteq supp(E)$*, where* $m'<m$ *and* $1\le t\le T$*.*

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

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

Lemma 14. *Let $\mathbb{B} = (\mathbf{B}_0'', \mathbf{B}_1, \mathbf{B}_1', \mathbf{B}_1'', \cdots, \mathbf{B}_T, \mathbf{B}_T', \mathbf{B}_T'') \in Gen({}_{r_0'}B_1^{2m})$. For any set $U \in {}_{r_0'}B_1^{2m}$, which satisfy that $F(U) \in \mathbb{B}$, there exists set $V \in \mathbf{C}(Impvalue)$ such that $V \subseteq U$, if and only if there exists j such that $Imp(\mathbf{B}_j'') = 0$, where $1 \le j \le T$.*

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 $\mathbf{E}_m$ and there does not exist error sequence E' with lower Hamming weight equivalent to it. We have that $(\mathcal{A}(L)+E)\bigcap\mathcal{A}_k'(L) = \emptyset$, if and only if there exists a set $U \in C(Impvalue)$ such that $U \subseteq supp(E)$, where $Impvalue = m - k/2 + 2^{T-1}$ and $1 < Impvalue \le m$.*

Proof. The sufficiency is same as Lemma **??**. Here, we only prove the necessity. Assume $(\mathcal{A}(L)+E)\bigcap\mathcal{A}_k'(L) = \emptyset$, then there exist $E' \in \mathbf{E}$ such that $LC(E+E') = L$. From Theorem 5, there exist pairwise disjoint cubes $U, U_1, U_2, \cdots, U_d \in \mathbb{C}$ and $V_1, V_2, \cdots, V_{d'} \in C$ such that $supp(E+E') = (\bigcup_{j=1}^{d} U_j)\bigcup(\bigcup_{j=1}^{d'} V_j)$, where d' is odd. Let $W = supp(E)\bigcap supp(E')$ and $W_1 = (supp(E)-W)\bigcap(\bigcup_{j=1}^{d'} V_j)$, $W_2 = (supp(E)-W)\bigcap(\bigcup_{j=1}^{d} U_j)$, $W_1' = (supp(E')-W)\bigcap(\bigcup_{j=1}^{d'} V_j)$, $W_2 = (supp(E')-W)\bigcap(\bigcup_{j=1}^{d} U_j)$. Then $W_1\bigcup W_1' = \bigcup_{j=1}^{d'} V_j$, $W_2\bigcup W_2' = \bigcup_{j=1}^{d} U_j$. According to the proof of Theorem 13, the number of elements of any cube U_j, which come from E, is at most half of $|U_j|$, thus $|W_2| \le |W_2'|$. Therefore $2m - |W_1| - |W| \le |supp(E')| - |W_1'| - |W|$, it follows that $2m - |W_1| \le |supp(E')| - (d' \cdot 2^T - |W_1|)$ and $|W_1| \ge m - |supp(E')|/2 + d' \cdot 2^{T-1} \ge d' \cdot (m - k/2 + 2^{T-1})$. This implies that there exists $U' \subseteq V_1$ and $U' \in C(Impvalue)$ such that $U' \subseteq supp(E)$. □

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

Therefore, the main difficult of computing the value $Num(\mathbf{E}_{2m}^R)$ lies in how to generate all elements in $Gen({}_{r_0'}B_1^{2m})$ which lead to nonzero terms in the function of $Num(\mathbf{E}_{2m}^R)$, i.e. those $\mathbb{B} \in Gen({}_{r_0'}B_1^{2m})$ which lead $Imp(\mathbf{B}_i'') \ne 0$ and $Mult(\mathbf{B}_i) \ne 0$ (for $1 \le i \le T$). According to the analysis in Section **??**, the problem of generating $\mathbb{B}$ can be reduced into the following two problems:

1. For a given $\mathbf{B} \in {}_{r_{i-1}'}\mathcal{B}$, how to generate set ${}_{r_i}Gen(\mathbf{B})$,
2. For a given $\mathbf{B} \in {}_{r_i}\mathcal{B}$, how to generate set ${}_{r_i'}Gen(\mathbf{B})$.

In the first problem, considering that for any $\mathbf{B} \in {}_{r_{i-1}'}\mathcal{B}$, the class ${}_{r_i}Extr(\mathbf{B})$ is uniquely determined, thus it is natural to begin with generating ${}_{r_i}Extr(\mathbf{B})$ from $\mathbf{B}$. For a given $\mathbf{B} = {}_{r_{i-1}'}B_{p_l}^{d_l}\cdots B_{p_1}^{d_1} \in {}_{r_{i-1}'}\mathcal{B}$, we denote $Extr({}_{r_i}Gen(\mathbf{B})) = \{{}_{r_i}Extr(\mathbf{B}') : \mathbf{B}' \in {}_{r_i}Gen(\mathbf{B})\}$, which can be given by the following enumeration description:

$$Extr({}_{r_i}Gen(\mathbf{B})) = \{{}_{r_i}B_{p_l}^{e_l}\cdots B_{p_1}^{e_1} : \begin{cases} e_j = d_j, & \text{if } p_j > 2^{i-2} \\ 0 \le e_j \le d_j, & \text{if } \exists j' > j,\ s.t.\ p_{j'} + p_j \le 2^{i-1} \\ 1 \le e_j \le d_j, & \text{otherwise} \end{cases}, \text{ for all } 1 \le j \le l\}.$$

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

For any $\mathbf{B}' = {}_{r_i}B_{p_l}^{e_l}\cdots B_{p_1}^{e_1} \in Extr({}_{r_i}Gen(\mathbf{B}))$, denote $ExtrGen(\mathbf{B}',\mathbf{B}) = \{\mathbf{B}'' : \mathbf{B}'' \in {}_{r_i}Gen(\mathbf{B}), \text{ and } Extr(\mathbf{B}'') = \mathbf{B}'\}$. We define

$$Coef(\mathbf{B}' \mid \mathbf{B}) = \sum_{\mathbf{B}'' \in ExtrGen(\mathbf{B}',\mathbf{B})} Coef(\mathbf{B}'' \mid \mathbf{B}) \cdot Coef_{Extr}(\mathbf{B}'') \cdot Mult(\mathbf{B}'').$$

Then problem 1 turns into how to fast compute the value of $Coef(\mathbf{B}' \mid \mathbf{B})$. For a $\mathbf{B}' = {}_{r_i}B_{p_l}^{e_l}\cdots B_{p_1}^{e_1} \in Extr({}_{r_i}Gen(\mathbf{B}))$, we denote $\Delta = {}_{r_i}B_{p_l}^{f_l}\cdots B_{p_1}^{f_1}$ where $f_j = d_j - e_j$ for $1 \le j \le l$. Then, each $\mathbf{B}'' \in ExtrGen(\mathbf{B}'|\mathbf{B})$ can be regarded as a kind of assignment which assigns a cube fragment of ${}_{r_i}B_{p_j}$ in Δ to $\mathbf{B}'$. And the set $ExtrGen(\mathbf{B}',\mathbf{B})$ can be regarded as all possible assignment. For instance, let $\mathbf{B} = {}_{r_{i-1}'}B_3^2B_1^3$, $\mathbf{B}' = {}_{r_i}B_3B_1$, then $\Delta = {}_{r_i}B_3B_1^2$. We inverse the operation 'Extr' by assigning cubes fragments ${}_{r_i}B_3$, ${}_{r_i}B_1$, and ${}_{r_i}B_1$ in Δ to $\mathbf{B}'$, that is, $ExtrGen({}_{r_i}B_3B_1,\ {}_{r_{i-1}'}B_3^2B_1^3) = \{{}_{r_i}B_{3[2]1[2]}B_1,\ {}_{r_i}B_{3[2]1}B_{1[2]},\ {}_{r_i}B_{3[2]}B_{1[3]}\}$. The specific procedure of assigning Δ to $\mathbf{B}'$ to generate $ExtrGen(\mathbf{B}',\mathbf{B})$ and then return the value of $Coef(\mathbf{B}' \mid \mathbf{B})$ is shown as Algorithm 2 in Appendix B.

As for problem 2, for a given class $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l}B_{p_{l-1}}^{d_{l-1}}\cdots B_{p_1}^{d_1} \in {}_{r_i}\mathcal{B}'$, we need to generate all elements in ${}_{r_i'}Gen(\mathbf{B})$. This problem can be regard as generating all sets $\mathbf{V}$ from a given multiset $\mathbf{U}$, where $\mathbf{U} = \{{}_{r_i}B_{p_l}, \cdots, {}_{r_i}B_{p_l}, \cdots, {}_{r_i}B_{p_1}, \cdots, {}_{r_i}B_{p_1}\}$, in which the number of ${}_{r_i}B_{p_j}$ is d_j for $1 \le j \le l$. And where the set $\mathbf{V}$ satisfy that the element in it equals to one in $\mathbf{U}$ or equal to the "sum" of two elements in $\mathbf{U}$. For example, let $\mathbf{B} ={}_{r_i} B_3^2B_2$, then $\mathbf{U} = \{{}_{r_i}B_3,\ {}_{r_i}B_3,\ {}_{r_i}B_2\}$. From $\mathbf{U}$, we can generate $\{{}_{r_i}B_3,\ {}_{r_i}B_3,\ {}_{r_i}B_2\}$, $\{{}_{r_i}B_6,\ {}_{r_i}B_2\}$, $\{{}_{r_i}B_5,\ {}_{r_i}B_3\}$ in which ${}_{r_i}B_6$ and ${}_{r_i}B_5$ are respectively regarded as the "sum" of ${}_{r_i}B_3$ and ${}_{r_i}B_3$ and the "sum" of ${}_{r_i}B_3$ and ${}_{r_i}B_2$. Algorithm 3 in Appendix B shows the specific procedure to generate ${}_{r_i'}Gen(\mathbf{B})$ for a given class $\mathbf{B} \in_{r_i} \mathcal{B}'$.

Considering that different $\mathbb{B}$ in $Gen({}_{r'_0}B_1^{2m})$ can have same prefix and start to be different from a particular class $\mathbf{B}$, we actually organize those $\mathbb{B}$ in $Gen({}_{r'_0}B_1^{2m})$ by a prefix tree structure to automatically compute the value of $Num(\mathbf{E}_{2m}^R)$. Fig. 1 depicts how the elements in $Gen({}_{r'_0}B_1^{2})$ and $Gen({}_{r'_0}B_1^{4})$ under various *Impvalue* are organized by trees.

For a given class $\mathbf{B}$ in ${}_{r'_{i-1}}\mathcal{B}$, similar to the definition of $Gen({}_{r'_0}B_1^{2m})$, we define

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

where $F_{i-1}(U) = (U''_{i-1},\, U_i,\, U'_i,\, \cdots,\, U_T,\, U'_T,\, U''_T)$ and $U''_{i-1} = U$, $U_j = U''_{i-1}$, $U'_j =_{r_j} Extr(U_j)$ and $U''_j = U'_j$ for $i \le j \le T$. And $F_{i-1}(U) \in (\mathbf{B}''_{i-1},\, \mathbf{B}_i,\, \mathbf{B}'_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T)$ means $U''_{i-1} \in \mathbf{B}''_{i-1}$ and $U_j \in \mathbf{B}_j$, $U'_j \in \mathbf{B}'_j$, $U''_j \in \mathbf{B}''_j$ for $i \le j \le T$.

And similar to the definition of $Num({}_{r'_0}B_1^{2m})$, we define

$${}_{r'_{i-1}}Num(\mathbf{B}) := \sum_{\mathbb{B}\in Gen(\mathbf{B})} \left|{}_{r'_T}wTr(\mathbf{B}''_T)\right| \cdot \prod_{j=i}^{T} Imp(\mathbf{B}''_j) \cdot Coef(\mathbf{B}''_j \mid \mathbf{B}'_j) \cdot Coef_{Extr}(\mathbf{B}_j) \cdot Mult(\mathbf{B}_j) \cdot Coef(\mathbf{B}_j \mid \mathbf{B}''_{j-1}),$$

where $\mathbb{B} = (\mathbf{B}''_{i-1},\, \mathbf{B}_i,\, \mathbf{B}'_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) \in Gen(\mathbf{B})$.

For a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, similarly, we define

$$Gen(\mathbf{B}) := \{(\mathbf{B}_i,\, \mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) :\ \exists U \in \mathbf{B}\ s.t.\ F_i(U) \in (\mathbf{B}_i,\, \mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T)\}$$

where $F_i(U) = (U_i,\, U'_i,\, U''_i,\, \cdots,\, U_T,\, U'_T,\, U''_T)$ and $U_i = U$, $U'_j =_{r_j} Extr(U_j)$, $U''_j = U'_j$ and $U_{j+1} = U''_j$ for $i \le j < T$. And $F_i(U) \in (\mathbf{B}_i,\, \mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T)$ means $U_j \in \mathbf{B}_j$, $U'_j \in \mathbf{B}'_j$ and $U''_j \in \mathbf{B}''_j$ for $i \le j \le T$.

And for a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, we define

$${}_{r_i}Num(\mathbf{B}) :=$$

$$\sum_{\mathbb{B}\in Gen(\mathbf{B})} Coef(\mathbf{B}'_i \mid \mathbf{B}_i) \cdot \left|{}_{r'_T}wTr(\mathbf{B}''_T)\right| \cdot \prod_{j=i+1}^{T} Imp(\mathbf{B}''_j) \cdot Coef(\mathbf{B}''_j \mid \mathbf{B}'_j) \cdot Coef_{Extr}(\mathbf{B}_j) \cdot Mult(\mathbf{B}_j) \cdot Coef(\mathbf{B}_j \mid \mathbf{B}''_{j-1}),$$

where $\mathbb{B} = (\mathbf{B}_i,\, \mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) \in Gen(\mathbf{B})$.

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

Proof. According to Theorem 5 and Lemma 9, for a given class $\mathbf{B}$ in ${}_{r'_{i-1}}\mathcal{B}$, if $Max_2 < 2^{i-1}$, then for any $\mathbb{B} = (\mathbf{B}''_{i-1},\, \mathbf{B}_i,\, \mathbf{B}'_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T)$ in $Gen(\mathbf{B})$, we have that $Mult(\mathbf{B}_j) = 1$ for $i \le j \le T$.

For a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, if $Max_4 < 2^i$, then $Max_2 < 2^i$ for any $\mathbf{B}'$ in ${}_{r'_i}Gen(\mathbf{B})$. Therefore for a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, if $Max_4 < 2^i$, then for any $\mathbb{B} = (\mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) \in Gen(\mathbf{B})$, we have that $Mult(\mathbf{B}_j) = 1$ for $i < j \le T$.

If $Max_{2^{T-i}} < Impvalue$ for a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, then for any $\mathbb{B} = (\mathbf{B}'_i,\, \mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) \in Gen(\mathbf{B})$, we have that $Imp(\mathbf{B}''_j) = 1$ for $i \le j \le T$.

If $Max_{2^{T-i-1}} < Impvalue$ for a given class $\mathbf{B}$ in ${}_{r'_i}\mathcal{B}$, then for any $\mathbb{B} = (\mathbf{B}''_i,\, \cdots,\, \mathbf{B}_T,\, \mathbf{B}'_T,\, \mathbf{B}''_T) \in Gen(\mathbf{B})$, we have that $Imp(\mathbf{B}''_j) = 1$ for $i < j \le T$.

Thus, for a given class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, if ${}_{r_i}$ISEND $= 1$, then we have ${}_{r_i}Num(\mathbf{B}) = \binom{2^{n-r_i+1}}{Index(\mathbf{B})}$.

Similarly, for a given class $\mathbf{B}$ in ${}_{r'_i}\mathcal{B}$ if ${}_{r'_i}$ISEND $= 1$, then we have ${}_{r'_i}Num(\mathbf{B}) = \binom{2^{n-r_i}}{Index(\mathbf{B})}$.

Therefore, according to the definition of ${}_{r'_{i-1}}Num(\mathbf{B})$ for class $\mathbf{B}$ in ${}_{r'_{i-1}}\mathcal{B}$ and ${}_{r_i}Num(\mathbf{B})$ for class $\mathbf{B}$ in ${}_{r_i}\mathcal{B}'$, Algorithm 1 can compute the value of ${}_{r'_{i-1}}Num(\mathbf{B})$ and the value of ${}_{r_i}Num(\mathbf{B})$. $\square$

According to Theorem 9, once input ${}_{r'_0}B_1^{2m}$ to procedure ${}_{r'_0}$NUM$(\mathbf{B})$ in Algorithm 1, i.e. call procedure ${}_{r'_0}$NUM$({}_{r'_0}B_1^{2m})$, we will get the value of $Num(\mathbf{E}_{2m}^R)$. Since in many cases, values of $Coef(\mathbf{B}' \mid \mathbf{B})$ are zero and ${}_{r_i}$ISEND$(\mathbf{B}')$ are 1 for given $\mathbf{B}$ in ${}_{r'_{i-1}}\mathcal{B}$ and $\mathbf{B}'$ in $Extr({}_{r_i}Gen(\mathbf{B}))$, the execution of procedure ${}_{r'_0}$NUM$({}_{r'_0}B_1^{2m})$ is very fast, and thus it is very efficient to get the value of $Num(\mathbf{E}_{2m}^R)$. In Appendix D, we present the experiment results on $\mathcal{N}'_k(L)$ when k is even and the periodic 2^n is 64 using algorithms in this paper. The entire experiment costs only a few minutes.

Algorithm 1 Compute ${}_{r'_{i-1}}Num(\mathbf{B})$ for $\mathbf{B}$ in ${}_{r'_{i-1}}\mathcal{B}$ and ${}_{r_i}Num(\mathbf{B})$ for $\mathbf{B}$ in ${}_{r_i}\mathcal{B}$

procedure ${}_{r'_{i-1}}\textsc{Num}(\mathbf{B})$
  Input: $\mathbf{B} \in {}_{r'_{i-1}}\mathcal{B}$
  Output: ${}_{r'_{i-1}}Num(\mathbf{B})$
  $num \leftarrow 0$
  while $\exists \mathbf{B}' \in Extr({}_{r_i}Gen(\mathbf{B}))$ and $Coef(\mathbf{B}' \mid \mathbf{B}) \neq 0$ **do**
    if ${}_{r_i}\textsc{IsEnd}(\mathbf{B}')$=1 **then**
      $num \leftarrow num + Coef(\mathbf{B}' \mid \mathbf{B}) \cdot \binom{2^{n-r_i+1}}{Index(\mathbf{B}')}$
    else
      $num \leftarrow num + Coef(\mathbf{B}' \mid \mathbf{B}) \cdot {}_{r_i}\textsc{Num}(\mathbf{B}')$
    end if
  end while
  return num
end procedure

function ${}_{r_i}\textsc{IsEnd}(\mathbf{B})$
  Input: $\mathbf{B} \in {}_{r_i}\mathcal{B}'$
  Output: 0 or 1
  if $Max_{2^{T-i}} < Impvalue$ and $Max_4 < 2^i$ **then**
    return 1
  else
    return 0
  end if
end function

procedure ${}_{r_i}\textsc{Num}(\mathbf{B})$
  Input: $\mathbf{B} \in {}_{r_i}\mathcal{B}$
  Output: ${}_{r_i}Num(\mathbf{B})$
  $num \leftarrow 0$
  while $\exists \mathbf{B}' \in {}_{r_i}Gen(\mathbf{B})$ and $Coef(\mathbf{B}' \mid \mathbf{B}) \neq 0$ **do**
    if ${}_{r'_i}\textsc{IsEnd}(\mathbf{B}')$=1 **then**
      $num \leftarrow num + Coef(\mathbf{B}' \mid \mathbf{B}) \cdot \binom{2^{n-r_i}}{Index(\mathbf{B})}$
    else
      $num \leftarrow num + Coef(\mathbf{B}' \mid \mathbf{B}) \cdot {}_{r'_i}\textsc{Num}(\mathbf{B}')$
    end if
  end while
  return num
end procedure

function ${}_{r'_i}\textsc{IsEnd}(\mathbf{B})$
  Input: $\mathbf{B} \in {}_{r'_i}\mathcal{B}$
  Output: 0 or 1
  if $Max_{2^{T-i-1}} < Impvalue$ and $Max_2 < 2^i$ **then**
    return 1
  else
    return 0
  end if
end function

$\triangleright$ Here, Max_j is the sum of the maximal j elements in the multiset $p_l^{[d_l]} p_{l-1}^{[d_{l-1}]} \cdots p_1^{[d_1]}$ where $p_l > p_{l-1} > \cdots > p_1 \geq 1$ in $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l} B_{p_{l-1}}^{d_{l-1}} \cdots B_{p_1}^{d_1}$. Note that, there may be duplicate among the maximal j elements, for example Max_4 is $4 \cdot p_l$ when $d_l > 4$.

$\triangleright$ $Index(\mathbf{B})$ denote the set $\{d_l, d_{l-1}, \cdots, d_1\}$ for $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l} B_{p_{l-1}}^{d_{l-1}} \cdots B_{p_1}^{d_1} \in_{r_i} \mathcal{B}'$ or $\mathbf{B} = {}_{r'_i}B_{p_l}^{d_l} B_{p_{l-1}}^{d_{l-1}} \cdots B_{p_1}^{d_1} \in_{r'_i} \mathcal{B}$.

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

1. Ding, C., Xiao, G., Shan, W.: The stability theory of stream ciphers, vol. 561. Springer Science & Business Media (1991)
2. Fu, F.W., Niederreiter, H., Su, M.: The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity. In: Sequences and Their Applications–SETA 2006, pp. 88–103. Springer (2006)

3. Kavuluru, R.: 2^n-periodic binary sequences with fixed k-error linear complexity for $k = 2$ or 3. In: Sequences and Their Applications-SETA 2008, pp. 252–265. Springer (2008)
4. Kavuluru, R.: Characterization of 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity. Designs, Codes and Cryptography 53(2), 75–97 (2009)
5. Kurosawa, K., Sato, F., Sakata, T., Kishimoto, W.: A relationship between linear complexity and k-error linear complexity. Information Theory, IEEE Transactions on 46(2), 694–698 (2000)
6. Meidl, W.: On the stability of 2^n-periodic binary sequences. Information Theory, IEEE Transactions on 51(3), 1151–1155 (2005)
7. Ming, S.: Decomposing approach for error vectors of k-error linear complexity of certain periodic sequences. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 97(7), 1542–1555 (2014)
8. Rueppel, R.A.: Analysis and design of stream ciphers. Springer Science & Business Media (2012)
9. Stamp, M., Martin, C.F.: An algorithm for the k-error linear complexity of binary sequences with period 2^n. Information Theory, IEEE Transactions on 39(4), 1398–1401 (1993)
10. Zhou, J.: A counterexample concerning the 3-error linear complexity of 2^n-periodic binary sequences. Designs, Codes and Cryptography 64(3), 285–286 (2012)
11. Zhou, J., Liu, J., Liu, W.: The 4-error linear complexity distribution for 2^n-periodic binary sequences. CoRR abs/1310.0132 (2013), `http://arxiv.org/abs/1310.0132`
12. Zhou, J., Liu, W.: The k-error linear complexity distribution for 2^n-periodic binary sequences. Designs, Codes and Cryptography 73(1), 55–75 (2014)
13. Zhou, J., Liu, W., Zhou, G.: Cube theory and stable k-error linear complexity for periodic sequences. In: Information Security and Cryptology. pp. 70–85. Springer (2014)

A Proof of Corollaries and Lemmas

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 $supp(E+E') = (\bigcup_{j=1}^{d} U_j)\bigcup(\bigcup_{j=1}^{d'} V_j)$, where $U_j \in \mathbb{C}$, $V_j \in \mathbf{C}$, $d' \geq 0$ and d' is even.*

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

1. Sequentially take pair $U_1 = \{e_i, e_j\}$ out from V and put them into a set $\mathbb{U}_1$, where $d(e_i, e_j) > 2^{n-r_1}$. Denote the set of the remaining elements by V_1'. Note that pairs are chosen step by step without replacement.
   (a) We know that all those pairs $U_1 = \{e_i, e_j\}$ in $\mathbb{U}_1$ are cubes in $\mathbb{C}_2$ and $LC(\mathbb{U}_1) < L$, thus $LC(V_1') < L$.
   (b) We can prove that V_1' can be expressed in a form that $V_1' = \bigcup_{j=1}^{d_1} W_{1,j}$ where $d_1 = |V_1'|/2$ and $W_{1,j} \in \mathbf{C}_2$.

      Proof. i. For any $v, v' \in V_1'$, we have $d(v, v') \leq 2^{n-r_1}$.
      ii. Sequentially take pair $U_1' = \{e_i, e_j\}$ out from V_1' and put them into a set $\mathbb{U}_1'$, where $d(e_i, e_j) = 2^{n-r_1}$. Denote the set of the remaining elements by V_1''.
      iii. We know that for all U_1' in $\mathbb{U}_1'$, $LC(U_1') = 2^n - 2^{n-r_1}$, thus $U_1' \in \mathbf{C}_2$ and $LC(\mathbb{U}_1') \leq 2^n - 2^{n-r_1}$.
      iv. We can prove that $V_1'' = \emptyset$. If $V_1'' \neq \emptyset$, as $d(v, v') < 2^{n-r_1}$ for any $v, v' \in V_1''$ then $LC(V_1'') > 2^n - 2^{n-r_1}$ which leads to $LC(V_1') = LC(\mathbb{U}_1' + V_1'') = \max\{LC(\mathbb{U}_1' + V_1'')\} > 2^n - 2^{n-r_1} > L$ which contradict with $LC(V_1') < L$.
      v. Thus we have derived 1b.

2. Sequentially take pair $U_2 = \{W_{1,i}, W_{1,j}\}$ out from V_1 and put them into a set $\mathbb{U}_2$, where $d(W_{1,i}, W_{1,j}) > 2^{n-r_2}$. Denote the set of the remaining elements by V_2'.
   (a) We know that all $U_2 = \{W_{1,i}, W_{1,j}\}$ in $\mathbb{U}_2$ are union set of some disjoint cubes in $\mathbb{C}_4$ and $LC(\mathbb{U}_2) < L$, thus $LC(V_2') < L$.
   (b) We can prove that V_2' can be expressed in a form that $V_2' = \bigcup_{j=1}^{d_2} W_{2,j}$ where $d_2 = |V_2'|/2$ and $W_{2,j} \in \mathbf{C}_4$.

      Proof. i. For any $1 \leq i < j \leq d_2$, $d(W_{2,i}, W_{2,j}) \leq 2^{n-r_2}$
      ii. Sequentially take pair $U_2' = \{W_{2,i}, W_{2,j}\}$ out from V_2' and put them into a set $\mathbb{U}_2'$, where $d(W_{2,i}, W_{2,j}) = 2^{n-r_2}$. Denote the set of remaining elements by V_2''.
      iii. Similar to the reason why $V_1'' = \emptyset$, we can know V_2'' is also an empty set.
      iv. Thus we have derived 2b.

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

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

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

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

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

Lemma 14. *Let $\mathbb{B} = (\mathbf{B}''_0,\ \mathbf{B}_1,\ \mathbf{B}'_1,\ \mathbf{B}''_1,\ \cdots,\ \mathbf{B}_T,\ \mathbf{B}'_T,\ \mathbf{B}''_T) \in Gen({}_{r'_0}B_1^{2m})$. For any set $U \in {}_{r'_0}B_1^{2m}$, which satisfy that $F(U) \in \mathbb{B}$, there exists set $V \in \mathbf{C}(Impvalue)$ such that $V \subseteq U$, if and only if there exists j such that $Imp(\mathbf{B}''_j) = 0$, where $1 \le j \le T$.*

Proof. For the backward direction, suppose $\mathbf{B}''_j = {}_{r'_j}B_{q_s}^{e_s} B_{q_{s-1}}^{e_{s-1}} \cdots B_{q_1}^{e_1}$ where $q_s > q_{s-1} > \cdots > q_1$. According to the definition of the function Imp, if $Imp(\mathbf{B}''_j) = 0$ then $q_s \ge Impvalue$. Recall that $U \in \mathbf{B}''_j = {}_{r'_j}B_{q_s}^{e_s} B_{q_{s-1}}^{e_{s-1}} \cdots B_{q_1}^{e_1}$, thus there exists $U' \subseteq U$ such that $U' \in {}_{r'_j}B_{q_s}$, therefore $U' \in \mathbf{C}_{2^j}(q_s)$. By the remark after the the definition of the function Imp, there exists $V \in \mathbf{C}(Impvalue)$ such that $V \subseteq U' \subseteq U$.

For the forward direction, the proof is as follows:

Assume: There exist a set $V \in \mathbf{C}(Impvalue)$, such that $V \subseteq U$,
Prove: There exists j such that $Imp(\mathbf{B}''_j) = 0$, where $1 \le j \le T$.
Proof: Let $d(V) = 2^{n-r_l}$, $F(U) = (U''_0, U_1, U'_1, U''_1, \ldots, U_T, U'_T, U''_T)$. We prove $Imp(\mathbf{B}''_l) = 0$ by constructing a set V' from the set V, which satisfy that $V' \subseteq U''_l$ and $V' \in \mathbf{C}_{2^l}(Impvalue)$.

1. Because $V \in \mathbf{C}_{2^l}(Impvalue)$, we have $d(v, v') = 2^{r_j}$ for any $v, v' \in V$, where $1 \le j \le l$
   (a) For any r_i or r'_i, we have
      i. $V \bigcap {}_{r_i}U_j \in \mathbf{C}_{2^{i-1}}(|V \bigcap {}_{r_i}U_j|)$
      ii. $V \bigcap {}_{r'_i}U_j \in \mathbf{C}_{2^i}(|V \bigcap {}_{r'_i}U_j|)$ where $1 \le i \le l$.
   (b) Thus we can suppose
      i. ${}_{r_i}Tr(V) = \{v_{i,j} : 1 \le j \le d_i\}$ and ${}_{r'_i}Tr(V) = \{v'_{i,j} : 1 \le j \le d'_i\}$ for $1 \le i \le l$
      ii. $d(v_{i,j_1}, v_{i,j'_1}) = 2^{n-r_{t_1}}$, $d(v'_{i,j_2}, v'_{i,j'_2}) = 2^{n-r_{t_2}}$ for $1 \le j_1 < j'_1 \le d_i$ and $1 \le j_2 < j'_2 \le d'_i$, where $1 \le i \le l$, $i \le t_1 \le l$, and $t_2 > i$.
2. Suppose:
   (a) $\mathbf{B}_1 = {}_{r_1}B_{Q_t}^{h_t} B_{Q_{t-1}}^{h_{t-1}} \cdots B_{Q_1}^{h_1}$
   (b) ${}_{r_1}Tr(U_1) = \{u_{j,k} :\ 1 \le j \le t$ and $1 \le k \le h_j\}$,
   (c) $U_{j,k} \subseteq U_1$, where $U_{j,k} \in {}_{r_1}B_{Q_j}$ and ${}_{r_1}Tr(U_{j,k}) = \{u_{j,k}\}$ for $1 \le j \le t$ and $1 \le k \le h_j$.
   for a p, where $1 < p \le T$
   (a) $\mathbf{B}_p = {}_{r_p}B_{Q'_{t'}}^{h'_{t'}} B_{Q'_{t'-1}}^{h'_{t'-1}} \cdots B_{Q'_1}^{h'_1}$,
   (b) ${}_{r_p}Tr(U_p) = \{u'_{j,k} :\ 1 \le j \le t'$ and $1 \le k \le h'_j\}$,
   (c) $U'_{j,k} \subseteq U_p$, where $U'_{j,k} \in {}_{r_p}B_{Q'_j}$ and ${}_{r_p}Tr(U'_{j,k}) = \{u'_{j,k}\}$ for $1 \le j \le t'$ and $1 \le k \le h'_j$.
3. Construction:
   (a) Initially, let $V''_0 = V$.
   (b) Firstly, let $V_1 = V''_0$. Since $V_1 = V \subseteq U = U_1$, we have ${}_{r_1}Tr(V_1) \subseteq {}_{r_1}Tr(U_1)$. For all $U_{j,k}$, if ${}_{r_1}Tr(U_{j,k}) \in {}_{r_1}Tr(V_1)$, then we replace the points in $V_1 \bigcap U_{j,k}$ by $(U'_1 \bigcap U_{j,k})$ in V_1. We denote the resulted set by V'_1 after the replacing process on V_1. Considering that $U'_1 \bigcap U_{j,k} \in C_{2^0}(1)$ and $V_1 \bigcap U_{j,k} \in C_{2^0}(1)$, in addition, ${}_{r_1}Tr(U'_1 \bigcap U_{j,k}) = {}_{r_1}Tr(V_1 \bigcap U_{j,k})$, we get that ${}_{r_1}Tr(V'_1) = {}_{r_1}Tr(V_1)$ and $|V'_1| \ge |V_1|$, $V'_1 \subseteq U'_1$ and $V'_1 \in C_{2^l}(|V'_1|)$. Let $V''_1 = V'_1$.
   (c) Now, for $1 < p \le l$, suppose we have got V''_{p-1} which satisfy that $V''_{p-1} \subseteq U''_{p-1}$ and $V''_{p-1} \in C(|V''_{p-1}|)$ and $|V''_{p-1}| \ge |V|$. Similar to the construction of (V_1, V'_1, V''_1), we construct (V_p, V'_p, V''_p) inductively.
   Let $V_p = V''_{p-1}$. Since $V_p = V''_{p-1} \subseteq U''_{p-1} = U_p$, we have ${}_{r_p}Tr(V_p) \subseteq {}_{r_p}Tr(U_p)$. For all $U'_{j,k}$, if ${}_{r_p}Tr(U'_{j,k}) \in {}_{r_p}Tr(V_p)$, then we replace the points in $V_p \bigcap U'_{j,k}$ by $(U'_p \bigcap U'_{j,k})$ in V_p. We denote the resulted set by V'_p

after the replacing process on V_p. Considering that $U'_p \bigcap U'_{j,k} \in C_{2^{p-1}}(I_1)$ and $V_p \bigcap U'_{j,k} \in C_{2^{p-1}}(I_2)$, in addition, ${}_{r_p}Tr(U'_p \bigcap U'_{j,k}) = {}_{r_p}Tr(V_p \bigcap U'_{j,k})$, where $I_1 = |U'_p \bigcap U'_{j,k}|$ and $I_2 = |V_p \bigcap U'_{j,k}|$, and obviously $I_1 \geq I_2$, we get that ${}_{r_p}Tr(V'_p) = {}_{r_p}Tr(V_p)$ and $|V'_p| \geq |V_p|$, $V'_p \subseteq U'_p$ and $V'_p \in C_{2^l}(|V'_p|)$. 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 the definition of the function Imp, we have $Imp(\mathbf{B}''_l) = 0$. □

B Algorithms

Algorithm 2 Preliminary and Algorithm to Compute $Coef(\mathbf{B}' \mid \mathbf{B})$ for $\mathbf{B} \in_{r'_{i-1}} \mathcal{B}$ and $\mathbf{B}' \in Extr({}_{r_i}Gen(\mathbf{B}))$

▷ **Denote** class $\mathbf{B} = {}_{r'_i}B^{d_m}_{p_m} \cdots B^{d_1}_{p_1} \in {}_{r'_i}\mathcal{B}$ or $\mathbf{B} = {}_{r_i}B^{d_m}_{p_m} \cdots B^{d_1}_{p_1} \in {}_{r_i}\mathcal{B}'$ by a mixed-radix matrix: $\mathbf{B} = \begin{bmatrix} d_m & \cdots & d_1 \\ p_m & \cdots & p_1 \end{bmatrix}$, where $p_m > p_{m-1} > \cdots > p_1$. Denote a single term in $\mathbf{B}$ by $\mathbf{B}\begin{bmatrix} d_j \\ p_j \end{bmatrix}$, where $1 \leq j \leq m$. We say that the maximal term in $\mathbf{B}$ is $B\begin{bmatrix} d_m \\ p_m \end{bmatrix}$, and denote it by $\mathbf{B}\begin{bmatrix} d_{max} \\ p_{max} \end{bmatrix}$. The minimal term in $\mathbf{B}$ is $\mathbf{B}\begin{bmatrix} d_1 \\ p_1 \end{bmatrix}$, and we denote it by $\mathbf{B}\begin{bmatrix} d_{min} \\ p_{min} \end{bmatrix}$. We denote the number of terms in $\mathbf{B}$ by $|\mathbf{B}|$.

▷ For $\mathbf{B}_1 = {}_{r_i}B^{d_m}_{p_m} \cdots B^{d_1}_{p_1}$ and $\mathbf{B}_2 = {}_{r_i}B^{e_m}_{p_m} \cdots B^{e_1}_{p_1}$, we say that $\mathbf{B}_2 \subseteq \mathbf{B}_1$ if $0 \leq e_j \leq d_j$ for all j, where $1 \leq j \leq l$. In other words, $\mathbf{B}_2 \subseteq \mathbf{B}_1$ if for any $U_2 \in B_2$ there exists $U_1 \in B_1$ such that $U_2 \subseteq U_1$.

▷ **Define** a cube fragments set for $\mathbf{B}_1 = {}_{r_i}B^{d_m}_{p_m} \cdots B^{d_1}_{p_1}$ and $\mathbf{B}_2 = {}_{r_i}B^{e}_{q}$, which represents the set of all possibilities to assign cube fragments in $\mathbf{B}_1$ to $\mathbf{B}_2$, as follows:
$Assign(\mathbf{B}_1 \to \mathbf{B}_2) := \{{}_{r_i}B^{e_s}_{Q_s} \cdots B^{e_1}_{Q_1} : \sum_{i=1}^{s} e_i = e,\ \biguplus_{j=1}^{s}(\biguplus_{k=1}^{e_j} Q_j) = (\biguplus_{j=1}^{e} p_j^{[d_j]}) \biguplus q^{[e]}$ and $q \in Q_j$ for $1 \leq j \leq s\}$.

▷ **Define** a "+" operator between $\mathbf{B}_1 = \begin{bmatrix} d_m & \cdots & d_1 \\ p_m & \cdots & p_1 \end{bmatrix}$ and $\mathbf{B}_2 = \begin{bmatrix} e_s & \cdots & e_1 \\ q_s & \cdots & q_1 \end{bmatrix}$ as: $\mathbf{B}_1 + \mathbf{B}_2 = \begin{bmatrix} v_t & \cdots & v_1 \\ u_t & \cdots & u_1 \end{bmatrix}$, where $\{u_t, \cdots, u_1\} = \{p_m, \cdots, p_1\} \bigcup \{q_s, \cdots, q_1\}$ and

$$v_j = \begin{cases} d_{j'} & \text{if } u_j = p_{j'} \text{ and } \nexists q_{j''} \text{ s.t. } q_{j''} = u_j \\ e_{j'} & \text{if } u_j = q_{j'} \text{ and } \nexists p_{j''} \text{ s.t. } p_{j''} = u_j \\ d_{j'} + e_{j''} & \text{if } u_j = p_{j'} = q_{j''} \end{cases}.$$

▷ **Define** a "−" operator between $\mathbf{B}_1$ and $\mathbf{B}_2$ where $\mathbf{B}_2 \subseteq \mathbf{B}_1$ as: $\mathbf{B}_1 - \mathbf{B}_2 = \begin{bmatrix} d_m - e_m & \cdots & d_1 - e_1 \\ p_m & \cdots & p_1 \end{bmatrix}$, where $\mathbf{B}_1 = \begin{bmatrix} d_m & \cdots & d_1 \\ p_m & \cdots & p_1 \end{bmatrix}$ and $\mathbf{B}_2 = \begin{bmatrix} e_m & \cdots & e_1 \\ p_m & \cdots & p_1 \end{bmatrix}$. Note that since $\mathbf{B}_2 \subseteq \mathbf{B}_1$, it follows that $0 \leq e_j \leq d_j$, and terms $\begin{bmatrix} e \\ p \end{bmatrix}$ will be moved out if $e = 0$.

procedure PUSH(x)
  Store a copy of x to the top of the stack memory
end procedure

procedure POP(x)
  Restore a copy of x from top of the stack memory
end procedure

procedure COEF($\mathbf{B}'$, $\mathbf{B}$)
  Input: $\mathbf{B} = {}_{r'_{i-1}}B^{d_l}_{p_l} \cdots B^{d_1}_{p_1} \in {}_{r'_{i-1}}\mathcal{B}$, and $\mathbf{B}' = {}_{r_i}B^{e_l}_{p_l} \cdots B^{e_1}_{p_1} \in Extr({}_{r_i}Gen(\mathbf{B}))$
  Output: $Coef(\mathbf{B}' \mid \mathbf{B})$
  $\varsigma \leftarrow 0,\ \Delta \leftarrow \mathbf{B} - \mathbf{B}',\ \mathbf{B}'' \leftarrow \mathbf{B}',\ AssFree \leftarrow \emptyset$
  COMPUTECOEF
  Output ς
  ▷ We assign cube fragments in Δ to $\mathbf{B}'$. We use $AssFree$ to store cube fragments in Δ which can be freely assigned. After initiate those variables, we call the main procedure COMPUTECOEF, which recursively call itself. When it terminate, variable ς turns to be the value of $Coef(\mathbf{B}' \mid \mathbf{B})$.
end procedure

procedure COMPUTECOEF
  if $\mathbf{B}' = \emptyset$ **then**
    $\varsigma \leftarrow \varsigma + Coef(\mathbf{B}'' \mid \mathbf{B}) \cdot Coef_{Extr}(\mathbf{B}'') \cdot Mult(\mathbf{B}'')$
  else
    $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \leftarrow \mathbf{B}'\begin{bmatrix} d_{max} \\ p_{max} \end{bmatrix},\ \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \leftarrow \Delta\begin{bmatrix} d_{min} \\ p_{min} \end{bmatrix}$
    PUSH(Δ), PUSH($AssFree$)
    while $\beta + \delta \leq 2^{i-1}$ **do**
      $AssFree \leftarrow AssFree + \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$,
      $\Delta \leftarrow \Delta - \begin{bmatrix} \gamma \\ \delta \end{bmatrix},\ \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \leftarrow \Delta\begin{bmatrix} d_{min} \\ p_{min} \end{bmatrix}$
    end while
    if $|\mathbf{B}'| = 1$ **then**
      for all $Ass \in Assign(AssFree \to \mathbf{B}')$ **do**
        PUSH($\mathbf{B}''$), PUSH($\mathbf{B}'$)
        $\mathbf{B}'' \leftarrow \mathbf{B}'' - \mathbf{B}' + Ass,\ \mathbf{B}' \leftarrow \emptyset$
        COMPUTECOEF
        POP($\mathbf{B}'$), POP($\mathbf{B}''$)
      end for
    else
      for all $Tmp \subseteq AssFree$ **do**
        for all $Ass \in Assign(Tmp \to {}_{r_i}B^{\alpha}_{\beta})$ **do**
          PUSH($\mathbf{B}''$), PUSH($\mathbf{B}'$), PUSH($AssFree$)
          $\mathbf{B}'' \leftarrow \mathbf{B}'' - \begin{bmatrix} \alpha \\ \beta \end{bmatrix} + Ass,\ \mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
          $AssFree \leftarrow AssFree - Tmp$
          COMPUTECOEF
          POP($AssFree$), POP($\mathbf{B}'$), POP($\mathbf{B}''$)
        end for
      end for
    end if
    POP($AssFree$), POP(Δ)
  end if
end procedure

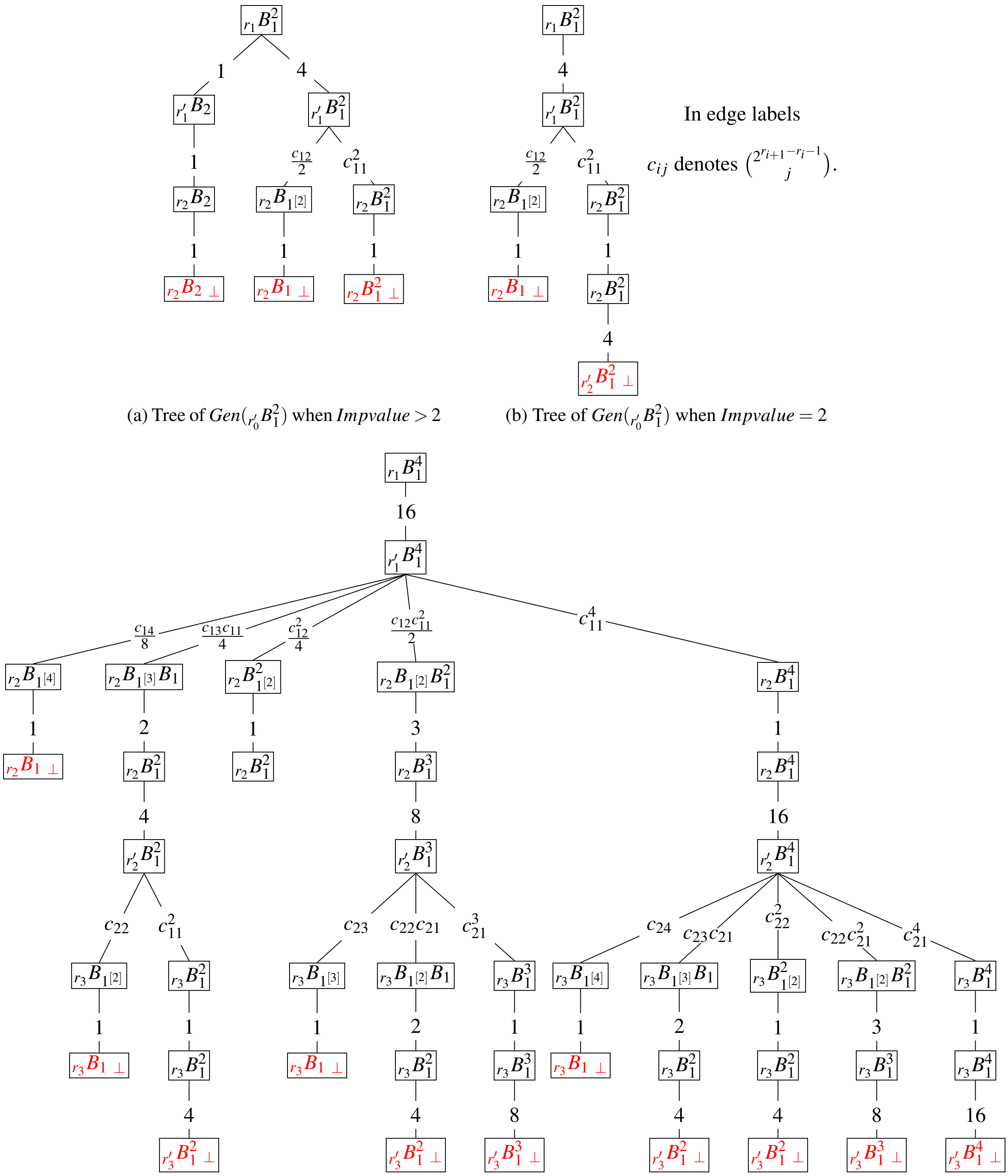
Algorithm 3 Algorithm to Generate set ${}_{r_i'}Gen(\mathbf{B})$ for class $\mathbf{B} \in_{r_i} \mathcal{B}'$

procedure GEN($\mathbf{B}$)
Input: $\mathbf{B} = {}_{r_i}B_{p_l}^{d_l} \cdots B_{p_1}^{d_1} \in {}_{r_i}\mathcal{B}'$
Output: ${}_{r_i'}Gen(\mathbf{B})$
$\mathbf{B}' \leftarrow \emptyset$, $GenSet \leftarrow \emptyset$
MAINGEN
Output $GenSet$
$\triangleright$ MAINGEN is the main generation procedure which handle the maximal terms $\begin{bmatrix} d_{max} \\ p_{max} \end{bmatrix}$ in $\mathbf{B}$ and determine whether class $\mathbf{B}' \in_{r_i} Gen(\mathbf{B})$ has been generated. It recursively call itself and the subroutine SUBGEN. When it terminate, $GenSet$ turns to be ${}_{r_i'}Gen(\mathbf{B})$.
end procedure

procedure MAINGEN
if $|\mathbf{B}| = \emptyset$ **then** $\triangleright$ a class $\mathbf{B}'$ has been generated
$GenSet \leftarrow_{add} \mathbf{B}'$
else
$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \leftarrow \mathbf{B} \begin{bmatrix} d_{max} \\ p_{max} \end{bmatrix}$
if $\alpha \geq 2$ **then**
if $2 \times \beta < Impvalue$ **then**
for $t \leftarrow \lfloor \alpha/2 \rfloor$ **to** 1 **do**
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} t \\ 2 \times \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} 2 \times t \\ \beta \end{bmatrix}$
if $\alpha - 2 \times t = 0$ **then**
MAINGEN
else
if $|\mathbf{B}| = 1$ **then**
$\begin{bmatrix} \gamma \\ \delta \end{bmatrix} \leftarrow \begin{bmatrix} \alpha - 2 \times t \\ \beta \end{bmatrix}$
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
MAINGEN
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
else
SUBGEN($|\mathbf{B}| - 1$)
end if
end if
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} t \\ 2 \times \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} 2 \times t \\ \beta \end{bmatrix}$
end for
end if
SUBGEN($|\mathbf{B}| - 1$)
else if $\alpha = 1$ **then**
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
MAINGEN
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
SUBGEN($|\mathbf{B}| - 1$)
end if
end if
end procedure

procedure SUBGEN(m')
$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \leftarrow \mathbf{B} \begin{bmatrix} d_{max} \\ p_{max} \end{bmatrix}$
if $m' = 0$ **then**
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
MAINGEN
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, $\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
else
for $j \leftarrow m'$ **to** 1 **do**
$\begin{bmatrix} \nu \\ \mu \end{bmatrix} \leftarrow \mathbf{B} \begin{bmatrix} d_j \\ p_j \end{bmatrix}$
if $\beta + \mu < Impvalue$ **then**
for $s \leftarrow \min(\alpha, \nu)$ **to** 1 **do**
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} s \\ \beta + \mu \end{bmatrix}$
$\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} s \\ \beta \end{bmatrix} - \begin{bmatrix} s \\ \mu \end{bmatrix}$
if $\alpha - s = 0$ **then**
MAINGEN
else
if $|\mathbf{B}| = 1$ **then**
$\begin{bmatrix} \gamma \\ \delta \end{bmatrix} \leftarrow \begin{bmatrix} \alpha - s \\ \beta \end{bmatrix}$
$\mathbf{B}' \leftarrow \mathbf{B}' + \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
$\mathbf{B} \leftarrow \mathbf{B} - \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
MAINGEN
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
$\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$
else
SUBGEN($j - 1$)
end if
end if
$\mathbf{B} \leftarrow \mathbf{B} + \begin{bmatrix} s \\ \beta \end{bmatrix} + \begin{bmatrix} s \\ \mu \end{bmatrix}$
$\mathbf{B}' \leftarrow \mathbf{B}' - \begin{bmatrix} s \\ \beta + \mu \end{bmatrix}$
end for
end if
end for
end if
end procedure

C Trees to Organize Symbolic Representations of Class of Error Sequences



In edge labels c_{ij} denotes $\binom{2^{r_{i+1}-r_i-1}}{j}$.

(a) Tree of $Gen({}_{r'_0}B_1^2)$ when $Impvalue > 2$ (b) Tree of $Gen({}_{r'_0}B_1^2)$ when $Impvalue = 2$

(c) Tree of $Gen({}_{r'_0}B_1^4)$ when $Impvalue = 2$

Note, A path from root node to leaf node represents an element $\mathbb{B}$ in $Gen({}_{r'_0}B_1^2)$ or in $Gen({}_{r_0}B_1^4)$. Red leaf node with a stop character $\perp$ indicates that $Mult(\mathbf{B}_k) = 1$ and $Impvalue(\mathbf{B}''_k) = 1$, for all $\mathbf{B}_k$ and $\mathbf{B}''_k$ after this element in $\mathbb{B}$. 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 $Coef(\mathbf{B}_2 \mid \mathbf{B}_1)$, $Coef(\mathbf{B}_3 \mid \mathbf{B}_2) \cdot Mult(\mathbf{B}_3)$ or $Coef_{Extr}(\mathbf{B}_3)$ where $\mathbf{B}_1 \in {}_{r_i}\mathcal{B}'$, $\mathbf{B}_2 \in {}_{r'_i}\mathcal{B}$ and $\mathbf{B}_3 \in {}_{r_{i+1}}\mathcal{B}$.

Fig. 1: Trees of $Gen({}_{r'_0}B_1^2)$ and $Gen({}_{r'_0}B_1^4)$ under various $Impvalue$

D Experiment Results

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

L	$\mathrm{w_H}$	$k=6$	$k=8$	$\cdots$	$k=26$	$k=28$	$k=30$
$\cdots$	≤ 1	0	0		0	0	0
16	2	32800768	843448320		0	0	0
24	2	12361216	105334272		0	0	0
28	2	1364608	2915424		0	0	0
30	2	127456	205896		0	0	0
31	2	32032	51480		0	0	0
40	2	114688	65536		0	0	0
44	2	6400	256		0	0	0
46	2	448	16		0	0	0
47	2	112	4		0	0	0
52	2	0	0		0	0	0
54	2	0	0		0	0	0
55	2	0	0		0	0	0
58	2	0	0		0	0	0
59	2	0	0		0	0	0
61	2	0	0		0	0	0
8	3	74698177	4269895680		0	0	0
12	3	73495057	4000596704		0	0	0
14	3	71447441	3611187752		0	0	0
15	3	68356625	3111545144		0	0	0
20	3	49468513	1797161728		0	0	0
22	3	46577129	1420375632		0	0	0
23	3	41906633	993236724		0	0	0
26	3	22363121	292078272		0	0	0
27	3	15385637	133105152		0	0	0
29	3	3774849	22800792		0	0	0
36	3	854113	7480320		0	0	0
38	3	753929	4554704		0	0	0
39	3	618185	2459764	$\cdots$	0	0	0
42	3	274577	361600		0	0	0
43	3	154997	122304		0	0	0
45	3	29265	16448		0	0	0
50	3	3985	0		0	0	0
51	3	901	0		0	0	0
53	3	65	0		0	0	0
57	3	1	0		0	0	0
4	4	75611761	4501725649		80627405461098496	17127899176960000	0
6	4	75611761	4501648441		7325469431074816	236126248960000	0
7	4	75611761	4501494025		2073916240700416	59031562240000	0
10	4	75154969	4385391113		19048518337536	139314069504	0
11	4	75154969	4384858301		4936272171264	34828517376	0
13	4	74325013	4190250125		609858701856	4353564672	0
18	4	51711097	2174133193		399572992	1048576	0
19	4	51711097	2172898813		101072896	262144	0
21	4	50589805	1979144701		12535808	32768	0
25	4	28803133	693096413		388864	1024	0
34	4	942649	11435209		0	0	0
35	4	942649	11396605		0	0	0
37	4	898381	9273725		0	0	0
41	4	418429	1975901		0	0	0
49	4	9949	9949		0	0	0
2	5	75611761	4501777129		765884877961138529	1149125482916201841	735663252850019217
3	5	75611761	4501777129		549379354729134933	488415562254909925	83465513150235525
5	5	75611761	4501751389		127414035703583729	39208852967342625	1678693908850625
9	5	75154969	4385746325		1928380228863833	175169988640833	2240855430049
17	5	51711097	2174956117		296601473321	9419426161	42981185
33	5	942649	11460949		36457	497	1
1	6	75611761	4501777129		956315644440505325	2075085937425745213	3695373947956092637

In the 2nd column, $\mathrm{w_H}$ indicates the value of $T=\mathrm{w_H}(2^n-L)$.
Note that $\mathcal{N}'_k(L)=Num_k(L)\cdot 2^{L-1}$, and for each column, it can be verified that $\mathcal{N}'_k(0)+\sum_{L=1}^{63} Num_k(L)\cdot 2^{L-1}=2^{63}$.