International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.169-184
http://dx.doi.org/10.14257/ijsia.2016.10.7.15

Cube Theory and *k*-error Linear Complexity Profile

Jianqin Zhou[1,2], Wanquan Liu[1],Xifeng Wang[2]

[1]*Department of Computing, Curtin University, Perth, WA 6102 Australia*
[2]*Computer Science School, Anhui Univ. of Technology, Ma'anshan, 243002 China*
[1]*zhou9@yahoo.com*
[2]*w.liu@curtin.edu.a*
[3]*wxf80106@163.com*

Abstract

The linear complexity and k-error linear complexity of a sequence have been used as important measures for keystream strength. In order to study k-error linear complexity of binary sequences with period 2^n, a new tool called cube theory is developed. In this paper, we first give a general decomposition approach to decompose a binary sequence with period 2^n into some disjoint cubes. Second, a counting formula for m-cubes with the same linear complexity is derived, which is equivalent to the counting formula for k-error vectors. The counting formula of 2^n-periodic binary sequences which can be decomposed into more than one cube is also investigated, which extends an important result by Etzion et al.. Finally, we study 2^n-periodic binary sequences with the given k-error linear complexity profile. Consequently, the complete counting formula of 2^n-periodic binary sequences with given k-error linear complexity profile of descent points 2, 4 and 6 is derived. The periodic sequences having the prescribed k-error linear complexity profile with descent points 1, 3, 5 and 7 are also briefly discussed.

Keywords: *Periodic sequence; linear complexity; k-error linear complexity; cube theory*

1. Introduction

It is well known that stream ciphers have broad applications in information security [13]. The linear complexity of a sequence s, denoted as $L(s)$, is defined as the length of the shortest linear feedback shift register (LFSR) that can generate s. The concept of linear complexity is very useful in the study of the security for stream ciphers. A necessary condition for the security of a key stream generator is that it produces a sequence with high linear complexity. However, high linear complexity can not necessarily guarantee the sequence is secure as the linear complexity of some sequences is unstable. If a small number of changes to a sequence greatly reduce its linear complexity, then the resulting key stream would be cryptographically weak. Ding, Xiao and Shan in their book [1] noticed this problem first, and presented the concepts of weight complexity and sphere complexity. Stamp and Martin [15] introduced k-error linear complexity, which is similar to the sphere complexity, and proposed the concept of k-error linear complexity profile. Suppose that s is a sequence over $GF(q)$ with period N. For $k(0 \le k \le N)$, the k-error linear complexity of s, denoted as $L_k(s)$, is defined as the smallest linear complexity that can be obtained when any k or fewer of the terms of the sequence are changed within one period.

One important result, proved by Kurosawa et al. in [9] is that the minimum number k for which the k-error linear complexity of a 2^n-periodic binary sequence s is strictly less than the linear complexity $L(s)$ of s is determined by $k_{\min} = 2^{W_H(2^n - L(s))}$, where $W_H(a)$ denotes the Hamming weight of the binary representation of an integer a. For binary

ISSN: 1738-9976 IJSIA

sequences with period p^n, where p is an odd prime and 2 is a primitive root modulo p^2, the relationship is shown in [11] between the linear complexity and the minimum value k for which the k-error linear complexity is strictly less than the linear complexity; moreover, an algorithm is obtained in [16] to compute the error linear complexity spectrum. In [18], for sequences over $GF(q)$ with period $2p^n$, where p and q are odd primes, and q is a primitive root modulo p^2, the minimum value k is presented for which the k-error linear complexity is strictly less than the linear complexity. For $k = 1; 2$, Meidl [12] characterized the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with the maximal possible linear complexity 2^n. Fu et al. [4] studied the linear complexity and the 1-error linear complexity of 2^n-periodic binary sequences, and then characterized such sequences with fixed 1-error linear complexity. For $k = 2; 3$, Zhu and Qi [21] further derived the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - 1$. The complete counting functions for the number of 2^n-periodic binary sequences with 3-error linear complexity are given by Zhou and Liu recently in [19].

Algebra [11], [12], [4], [21] and discrete Fourier transform [6] are two important tools to study the k-error linear complexity for periodic sequences. Etzion *et. al.*, [2] studied the sequences using algebra with two k-error linear complexity values exactly, namely its k-error linear complexity is only $L(s)$ or 0. To further study the sequences in general case, we develop a new tool called cube theory in this paper to study the k-error linear complexity of binary sequences with period 2^n. Furthermore, we give a general approach to decompose a binary sequence with period 2^n into some disjoint cubes, which is called standard cube decomposition.

By using the proposed cube theory, we are capable of studying the k-error linear complexity for periodic sequences from a new perspective. We can easily perceive the core problem and difficulty points of the k-error linear complexity for a 2^n-periodic binary sequence with more than one cube.

One significant benefit of the cube theory is for us to construct sequences with the maximum k-error linear complexity. Some examples are also given to illustrate the approach. Kurosawa *et. al.*, in [9] studied the minimum number k for which the first decrease occurs for the k-error linear complexity. With the cube theory, we further characterize the minimum number k for which the tth decrease occurs in the k-error linear complexity, $t > 1$.

Technically, for 2^n-periodic binary sequences s and e, if $W_H(e) = k_{\min}$ and $L(s+e) < L(s)$, then we define the sequence e as a k-error vector associated with s. A k-error vector is in fact an m-cube with the same linear complexity $L(s)$ as shown in this paper. Based on this observation, the counting formula of m-cubes with the same linear complexity will be derived with an approach much different from that used in [2] by Etzion *et. al.*, Based on the independence among cubes of a sequence, we can construct each cube independently. As a consequence, the counting formula of 2^n-periodic binary sequences which can be decomposed into more than one cube is also investigated.

The k-error linear complexity profile of a periodic sequence was first defined in [15], and it indicates how linear complexity decreases as the number of bits allowed to be modified per period increases. The same notion was defined as the error linear complexity spectrum for a periodic sequence in [10]. Based on the proposed cube theory, we can study the periodic sequences with the given k-error linear complexity profile. Consequently, the counting formula of 2^n-periodic binary sequences with some given k-error linear complexity profile is derived.

The rest of this paper is organized as follows. In Section 2, some preliminary results are presented. In Section 3, the definition of cube theory and a general decomposition approach to decompose a binary sequence with period 2^n into some disjoint cubes is given. In Section 4, The counting formula of 2^n-periodic binary sequences which can be decomposed into more than one cube is investigated, and the periodic sequences with the

given k-error linear complexity profile is also studied. Our conclusion is given in Section 5.

2. Preliminaries

We will consider sequences over $GF(q)$, which is the finite field of order q. Let $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ be vectors over $GF(q)$. Then we define

$$x + y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n).$$

If $q = 2$, we denote $x + y$ as $x \oplus y$ as well.

When n = 2m, we define Left(x) = $(x_1, x_2, \cdots, x_m)$ and Right(x) = $(x_{m+1}, x_{m+2}, \cdots, x_{2m})$.

The Hamming weight of an N-periodic sequence s is defined as the number of nonzero elements per period of s, denoted by $W_H(s)$. Let s^N be one period of s. If $N = 2^n$, s^N is also denoted as $s(n)$. The distance of two elements is defined as the difference of their indexes. Specifically, for an N-periodic sequence $s = \{s_0, s_1, s_2, s_3, \cdots, \}$, the distance of $s_{i,}, s_j$ is $j - i$, where $0 \le i \le j \le N$.

The linear complexity of a 2^n-periodic binary sequence s can be recursively computed by the Games-Chan algorithm [3] as follows.

Algorithm 2.1

Input: A 2^n-periodic binary sequence $s = [Left(s); Right(s)]$, $c = 0$.

Output: $L(s) = c$.

Step 1. If $Left(s) = Right(s)$, then deal with $Left(s)$ recursively. Namely, $L(s) = L(Left(s))$.

Step 2. If $Left(s) \neq Right(s)$, then $c = c + 2^{n-1}$ and deal with $Left(s) \oplus Right(s)$ recursively. Namely, $L(s) = 2^{n-1} + L(Left(s) \oplus Right(s))$.

Step 3. If $s = (a)$, then if $a = 1$ then $c = c + 1$.

The following lemmas are well known results on 2^n-periodic binary sequences and are required in this paper. Please refer to [12], [4], [21], [19] for details.

Lemma 2.1 Suppose that s is a binary sequence with period $N = 2^n$, then $L(s) = N$ if and only if the Hamming weight of a period of the sequence is odd.

If an element 1 is changed to 0 in a sequence whose Hamming weight is odd, the Hamming weight of the sequence will be changed to even, so the main concern hereinafter is about sequences whose Hamming weights are even.

Lemma 2.2 Let s_1 and s_2 be binary sequences with period $N = 2^n$. If $L(s1) \neq L(s2)$, then $L(s_1+s_2) = \max\{L(s_1); L(s_2)\}$; otherwise if $L(s_1) = L(s_2)$, then $L(s_1 + s_2) < L(s_1)$.

Suppose that the linear complexity of s can decrease when at most k elements of s are changed. By Lemma 2.2, the linear complexity of the binary sequence, in which only elements at exactly those k positions are nonzero, must be $L(s)$. Therefore, for the computation of k-error linear complexity, we only need to find the binary sequence whose Hamming weight is minimum and its linear complexity is $L(s)$.

3. Cube Theory and Main Results

We presented the cube theory in [20]. First we review some definitions.

Definition 3.1 Suppose that the difference of positions of two non-zero elements of sequence s is $(2x + 1)2^y$, both x and y are non-negative integers. Then the distance between the two elements is defined as 2^y.

Definition 3.2 Suppose that s is a binary sequence with period 2^n, and there are 2^m non-zero elements in s, and $0 \le i_1 < i_2 < \cdots < i_m < n$. If $m = 1$, then there are 2 non-zero elements in s and the distance between the two elements is 2^{i_1}, so it is called as a 1-cube. If $m = 2$, then s has 4 non-zero elements which form a rectangle, the lengths of 4 sides are 2^{i_1} and 2^{i_2} respectively, so it is called as a 2-cube. In general, s has 2^{m-1} pairs of non-zero elements, in which there are 2^{m-1} non-zero elements which form a $(m-1)$-cube, the other 2^{m-1} non-zero elements also form a $(m-1)$-cube, and the distance between each pair of elements are all 2^{i_m}, then the sequence s is called as an m-cube, and the linear complexity of s is called as the linear complexity of the cube as well.

Definition 3.3 A non-zero element of sequence s is called a vertex. Two vertexes can form an edge. If the distance between the two elements (vertices) is 2^y, then the length of the edge is defined as 2^y.

In [20], we have considered the linear complexity of a sequence with only one cube.

Theorem 3.1 Suppose that s is a binary sequence with period 2^n, and non-zero elements of s form an m-cube, if lengths of edges are $2^{i_1}, 2^{i_2}, \cdots, 2^{i_m}$ $(0 \le i_1 < i_2 < \cdots < i_m < n)$ respectively, then $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$.

Based on Algorithm 2.1, we may have a standard cube decomposition for any binary sequence with period 2^n.

Algorithm 3.1

Input: $s^{(n)}$ is a binary sequence with period 2^n.

Output: A cube decomposition of sequence $s^{(n)}$.

Step 1. Let $s^{(n)} = [Left(s^{(n)}); Right(s^{(n)})]$.

Step 2. If $Left(s^{(n)}) = Right(s^{(n)})$, then we only consider $Left(s^{(n)})$.

Step 3. If $Left(s^{(n)}) \neq Right(s^{(n)})$, then we consider $Left(s^{(n)}) \oplus Right(s^{(n)})$. In this case, some nonzero elements of s may be removed.

Step 4. After above operation, we can have one nonzero element. Now by only restoring the nonzero elements in $Right(s^{(n)})$ removed in Step 2, so that $Left(s^{(n)}) = Right(s^{(n)})$. In this case, we obtain a cube $c1$ with linear complexity $L(s^{(n)})$.

Step 5. With $s^{(n)} \oplus c_1$, run Step 1 to Step 4. We obtain a cube c_2 with linear complexity less than $L(s^{(n)})$.

Step 6. With these nonzero elements left in $s^{(n)}$, run Step 1 to Step 5 recursively we will obtain a series of cubes in the descending order of linear complexity.

Obviously, this is a cube decomposition of sequence $s^{(n)}$. We define it as the **standard cube decomposition** of sequence $s^{(n)}$.

Next we use a sequence {1101 1001 1000 0000} to illustrate the decomposition process. Note that the sequence can be considered as $1 + x + x^3 + x^4 + x^7 + x^8$.

As $Left \neq Right$, then we consider $Left \oplus Right$. Then the cube $1 + x^8$ is removed.

Recursively, as $Left \neq Right$, then we consider $Left \oplus Right$. This time the cube $x^3 + x^7$ is removed. Only cube $x + x^4$ is left. So the standard cube decomposition of $1 + x + x^3 + x^4 + x^7 + x^8$ is $\{x + x^4, x^3 + x^7; 1 + x^8\}$.

In order to achieve the maximal decrease of the linear complexity of a new sequence generated by superposing another sequence over the original one, according to Lemma 2.2, a direct method is, if possible, to use the linear complexity of the first cube and let it

be the same as the linear complexity of the second cube. For the polynomial $1 + x + x^3 + x^4 + x^7 + x^8$ with the standard decomposition $\{x + x^4, x^3 + x^7; 1 + x^8\}$, in order to make the linear complexity of $x + x^4$ to be the same as $x^3 + x^7$, we add $x^4 + x^5$ and obtain $x + x^5$, which has the same linear complexity of $x^3 + x^7$. Therefore, we have a conclusion that the critical points of $1 + x + x^3 + x^4 + x^7 + x^8$ are $(0; 2^n - 1)$,$(2; 2^n - (2 + 4))$,$(4; 2^n - (8 + 4 + 1))$,$(6; 0)$. $(4; 3)$ corresponds polynomial $1 + x^3 + x^4 + x^7 + x^8 + x^{11} + x^{12} + x^{15}$.

Suppose that the linear complexity of s can reduce when at least k elements of s are changed. By Lemma 2.2, the linear complexity of the binary sequence, in which elements at exactly those k positions are all nonzero, must be $L(s)$. According to Theorem 3.1 and Algorithm 3.1, it is easy to get the following conclusion.

Corollary 3.1 Suppose that s is a binary sequence with period 2^n, and $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$. If $k_{\min}$ is the minimum, such that $k_{\min}$-error linear complexity is less than $L(s)$, then $k_{\min} = 2^m$.

Corollary 3.1 was first proved by Kurosawa *et. al.*, [9], and later it was proved by Etzion *et. al.*, [2] with a different approach. Here we obtain this result from the cube theory and different from the previous approaches.

Consider a k-cube, if lengths of edges are $1,2,2^2, \cdots$, and 2^{k-1} respectively, and the linear complexity is $2^n - (2^k - 1)$. By Theorem 3.1 and Algorithm 3.1, we can obtain the following results on stability.

Corollary 3.2 Suppose that s is a binary sequence with period 2^n and its Hamming weight is even, then the maximum $2^k-1; \cdots ; (2^k - 2)$ or $(2^k - 1)$-error linear complexity of s is still $2^n - (2^k - 1)(k > 0)$.

The following is an example to illustrate Corollary 3.2.

Let s be the binary sequence $\{\overbrace{11\cdots11}^{2^k}0\cdots0\}$. Its period is 2^n, and there are only 2^k continuous nonzero elements at the beginning of the sequence. Then it is a k-cube, and the $2^{k-1}, \cdots, (2^k - 2)$ or $(2^k - 1)$-error linear complexity of s is still $2^n - (2^k - 1)$.

After at most $e(0 \le e \le 2^k - 1)$ elements of a period in the above sequence are changed, the linear complexity of all new sequences will not be decreased, so the original sequence possesses e-error linear complexity.

According to Lemma 2.2, if a sequence whose linear complexity is less than $2^n - (2^k - 1)$ is added to the sequence with linear complexity $2^n - (2^k - 1)$, then the linear complexity of the new sequence is still $2^n - (2^k - 1)$, and the $2^{k-1}; \cdots ; (2^k-2)$ or $(2^k - 1)$-error linear complexity of the new sequence is still $2^n - (2^k - 1)$.

By combining Corollary 3.1 and Corollary 3.2, we can achieve the following theorem.

Theorem 3.2 For $2^{l-1} \le k < 2^l$, there exists a 2^n-periodic binary sequence s with maximum k-linear complexity $2^n-(2^l-1)$, such that $L_k(s) = \max_t L_k(t)$, where t is any 2^n-periodic binary sequence.

It is reminded that CELCS (critical error linear complexity spectrum) has been studied by Etzion *et. al.*, [2]. The CELCS of the sequence s consists of the ordered set of points $(k, c_k(s))$ satisfying $c_k(s) > c_{k'}(s)$, for $k' > k$; these are the points where a decrease occurs in the k-error linear complexity, and thus are called critical points.

Let s be a binary sequence whose period is 2^n and it has only one m-cube. Then s has only two critical points: $(0, l(s))$, $(2^m, 0)$.

In the following we study binary sequences which consist of several cubes and the tth decrease in the k-error linear complexity, where $t > 1$. First we consider dependence relationship among different cubes.

In order to achieve the maximal decrease of the linear complexity of a new sequence by superposing another sequence over the original one, according to Lemma 2.2, a direct method is, if possible, to let the linear complexity of the first cube be the same as the linear complexity of the second cube. For Example 3.2, for the polynomial $1+x+x^3+x^4+x^7+x^8$ with standard decomposition $\{x + x^4, x^3 + x^7, 1 + x^8\}$, in order to make the linear complexity of $x + x^4$ to be the same as $x^3 + x^7$, we add $x^4 + x^5$ and obtain $x + x^5$, which has the same linear complexity of $x^3 + x^7$. Therefore, we can obtain that the critical points of $1 + x + x^3 + x^4 + x^7 + x^8$ is $(0; 2^n - 1),(2; 2^n - (2 + 4)),(4; 2^n - 8),(6; 0)$.

To further investigate the critical point issue, we consider another example.

Example 3.1 Consider $1+x^3+x^4+x^6+x^9+x^{11}+x^{12}+x^{14}$. Its standard cube decomposition is $\{1+x^9; x^3+x^{11}; x^4+x^6+x^{12}+x^{14}\}$. If we change $1+x^9$ to $x+x^9$, then $x+x^3+x^4+x^6+x^9+x^{11}+x^{12}+x^{14}$ is a 3-cube with the linear complexity $2^n - (1+2+8)$. So, both 2-error linear complexity and 4-error linear complexity of $1+x^3+x^4+x^6+x^9+x^{11}+x^{12}+x^{14}$ are all $2^n - (1 + 2 + 8)$. 6-error linear complexity is $2^n - (2 + 4 + 8)$.

From above examples, we can find that one cube change may affect other cubes in the cube decomposition. This phenomena make the critical points detection more difficult in general. In order to discuss the critical points easily, we give the following concept. If the change of one cube has an impact on other cubes, then the cube decomposition is defined as **power relation**. In Example 3.2, the change of $x+x^4$ to $x+x^5$ only has impact on one cube x^3+x^7, so the cube decomposition is defined as **first order power relation**. In Example 3.3, the change of $1 + x^9$ to $x + x^9$ has impact on two cubes, so the cube decomposition is defined as **second order power relation**.

It is easy to prove the following, which provides a general solution to find critical points of a 2^n-periodic binary sequence.

Theorem 3.3 Suppose that s is a binary sequence with period 2^n, and s has a standard cube decomposition without the tth order power relation with $t > 1$. If the cubes are in descending order of linear complexity, and their dimensions are $m_1, m_2, \cdots, m_j$, respectively, then k-error linear complexity will decrease when k is $2^{m_1}, 2^{m_1} + 2^{m_2}, \cdots, 2^{m_1} + 2^{m_2} + \cdots + 2^{m_j}$.

However, for some sequences the k-error linear complexity may decrease while k is not in $\{2^{m_1}, 2^{m_1} + 2^{m_2}, \cdots, 2^{m_1} + 2^{m_2} + \cdots + 2^{m_j}\}$. We will illustrate it by the following example.

Example 3.2 Consider sequence {1001 0101 0101 0000}. Its standard cube decomposition is a 1-cube {1001 0000 0000 0000} and a 2-cube {0000 0101 0101 0000}. Its first descent point is k = 2, but its second descent point is $k = 4$ and we obtain a 3-cube {0101 0101 0101 0101}.

4. The Counting Formula of 2^n-Periodic Binary Sequences

4.1. The Counting Formula of 2^n-Periodic Binary Sequences with One or More Cubes

We first consider the construction of sequences with one or more cubes. Suppose that s is a binary sequence with period 2^n, and $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$. We now derive the counting formula of m-cubes with the same linear complexity.

Theorem 4.1 Suppose that s is a binary sequence with period 2^n, and $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$. If sequence e is an m-cube with $L(e) = L(s)$, then the number of sequence e is $2^{2^m n - 2^{m-1} i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2}$

Proof: Suppose that $s^{(i_1)}$ is a 2^{i_1} -periodic binary sequence with linear complexity 2^{i_1} and $W_H(s^{(i_1)}) = 1$, then the number of these $s^{(i_1)}$ is 2^{i_1}

So the number of 2^{i_1+1} -periodic binary sequences $s^{(i_1+1)}$ with linear complexity $2^{i_1+1} - 2^{i_1} = 2^{i_1}$ and $W_H(s^{(i_1+1)}) = 2$ is also 2^{i_1} .

For $i_2 > i_1$, if 2^{i_2} -periodic binary sequences s^{i_2} with linear complexity $2^{i_2} - 2^{i_1}$ and $W_H(s^{(i_2)}) = 2$, then $2^{i_2} - 2^{i_1} - (2^{i_1+1} - 2^{i_1}) = 2^{i_2-1} + 2^{i_2-2} + \cdots + 2^{i_1+1}$.

Based on Algorithm 2.1, the number of these s^{i_2} can be given by $(2^2)^{i_2-i_1-1} \times 2^{i_1} = 2^{2i_2-i_1-2}$.

For example, suppose that $i_1 = 1$, $i_2 = 3$, then there are $(2^2)^{i_2-i_1-1} = 4$ sequences of $s^{(i_2)}$ correspond to one sequence {1010} of $s^{(i_1+1)}$, given by

{1010 0000}, {1000 0010}, {0010 1000}, {0000 1010}

So the number of 2^{i_2+1} -periodic binary sequences $s^{(i_2+1)}$ with linear complexity $2^{i_2+1} - (2^{i_2} + 2^{i_1}) = 2^{i_2} - 2^{i_1}$ and $W_H(s^{(i_2+1)}) = 4$ is also $2^{2i_2-i_1-2}$.

For $i_3 > i_2$, based on Algorithm 2.1, if 2^{i_3} -periodic binary sequences *si*3 with linear complexity $2^{i_3} - (2^{i_2} + 2^{i_1})$ and $W_H(s^{(i_3)}) = 4$, then the number of these s^{i_3} can be given by $(2^4)^{i_3-i_2-1} \times 2^{2i_2-i_1-2} = 2^{4i_3-2i_2-i_1-2-4}$.

. . . . . .

So the number of 2^{i_m+1} -periodic binary sequences $s^{(i_m+1)}$ with linear complexity $2^{i_m+1} - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) = 2^{i_m} - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_{m-1}})$ and $W_H(s^{(i_3)}) = 2^m$ is also $2^{2^{m-1}i_m - \cdots 2i_2 - i_1 - 2 - 4 - \cdots - 2^{m-1}}$.

For $n > i_m$, if 2^n-periodic binary sequences $s^{(n)}$ with linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$ and $W_H(s^{(n)}) = 2^m$, then the number of these $s^{(n)}$ can be given by

$$\begin{aligned} & (2^{2^m})^{n-i_m-1} \times 2^{2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2 - 4 - \cdots - 2^{m-1}} \\ = \; & 2^{2^m n - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2 - 4 - \cdots - 2^{m-1} - 2^m} \\ = \; & 2^{2^m n - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2} \end{aligned}$$

For 2^n-periodic binary sequences s and e, if $W_H(e) = k_{\min}$ and $L(s+e) < L(s)$, then the sequence e is called as a k-error vector. By cube theory, a k-error vector is in fact an m-cube with the same linear complexity $L(s)$.

Etzion *et. al.*, proved Theorem 3 in [2], which is equivalent to Theorem 4.1, with a much different approach. The approach here is much simpler.

Suppose that s is a 2^n-periodic binary sequence with more than one cube, and each cube has a given linear complexity. Now we consider the counting formula of these sequences.

Theorem 4.2 Suppose that s is a 2^n-periodic binary sequence with two independent cubes: C_1,C_2. C_1 has linear complexity $2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$, and C_2 has linear complexity $2^n - (2^{j_1} + 2^{j_2} + \cdots + 2^{j_l})$, where $0 \le j_1 < j_2 < \cdots < j_l < n$ and $2^{j_1} > 2^t$, where $t = \max\{x \mid i_x \le j_1, x \ge 1\}$. Then the number of sequence s is

$$(2^{2^m n - 2^{m-1}i_m - \cdots - 2i_2 - i_1 - 2^{m+1} + 2})[2^{2^l n - 2^{l-1}j_l - \cdots - 2j_2 - j_1 - 2^{l+1} + 2}(2^{j_1} - 2^t)]$$

Proof: The proof is very similar to that of Theorem 4.1.

Noted that $s^{(j_1)}$ is a 2^{j_1} -periodic binary sequence with linear complexity $2^{j_1}-(2^{i_1}+2^{i_2}+\cdots+2^{i_t})$ and $W_H(s^{(j_1)})=2^t$, the number of zero elements in $s(j1)$ is $2^{j_1}-2^t$.

Similar to the proof of Theorem 4.1, for each cube C_1, the number of cube C_2 is $2^{2^l n-2^{l-1}j_l-\cdots-2j_2-2j_1-2^{l+1}+2}(2^{j_1}-2^t)$

This completes proof.

Next we give an example to illustrate Theorem 4.2.

Example 4.1 Suppose that s is a 2^3-periodic binary sequence with 2 independent cubes: C_1,C_2. C_1 has linear complexity $2^n - 2^0$, and C_2 has linear complexity $2^n - 2^2$, where $2^2 > 2^1$ and $t = 1$. From sequence 11, we get 1100,0110,1001,0011, and from sequence 1100, we get 11000000,01001000,10000100,00001100. For each cube C_1, the number of cube C_2 is 2. For 11000000, we get 11100010 and 11010001. The total number is 32. The result is consistent with Theorem 4.2.

It should be noted that the main idea in the proof of Theorem 4.2 is that two cubes are relatively independent. So after determining the connecting part of two cubes, one can construct each cube independently. Given the linear complexities of $t(t > 2)$ cubes, with the approach of Theorem 4.2, we can discuss the number of sequence s with t cubes, of which each cube has a given linear complexity. Here we only give the results for $t = 3$.

Corollary 4.1 Suppose that s is a 2^n-periodic binary sequence with 3 independent cubes: C_1,C_2 and C_3. C_1 has linear complexity $2^n-(2^{i_1}+2^{i_2}+\cdots+2^{i_m})$, where $0 \le i_1 < i_2 < \cdots < i_m < n$, C_2 has linear complexity $2^n-(2^{j_1}+2^{j_2}+\cdots+2^{j_l})$, where $0 \le j_1 < j_2 < \cdots < j_l < n$ and $2^{j_1} > 2^t$, where $t = \max\{x \mid i_x \le j_1,\ x \ge 1\}$. and C_3 has linear complexity $2^n-(2^{k_1}+2^{k_2}+\cdots+2^{k_w})$, where $0 \le k_1 < k_2 < \cdots < k_w < n$ and $2^{k_1} > 2^u + 2^v$, where $u = \max\{x \mid i_x \le k_1, x \ge 1\}$ and $v = \max\{y \mid j_y \le k_1, y \ge 1\}$. Then the number of sequence s is

$$(2^{2^m n-2^{m-1}i_m-\cdots-2i_2-i_1-2^{m+1}+2})[2^{2^l n-2^{l-1}j_l-\cdots-2j_2-2j_1-2^{l+1}+2}(2^{j_1}-2^t)]$$

$$\cdot[2^{2^w n-2^{w-1}k_w-\cdots-2k_2-2k_1-2^{w+1}+2}(2^{k_1}-2^u-2^v)]$$

Proof: The proof is very similar to that of Theorem 4.2.

Noted that $s^{(j_1)}$ is a 2^{j_1} -periodic binary sequence with linear complexity $2^{j_1}-(2^{i_1}+2^{i_2}+\cdots+2^{i_t})$ and $W_H(s^{(j_1)})=2^t$, the number of zero elements in $s^{(j_1)}$ is $2^{j_1} > 2^t$, and $s^{(k_1)}$ is a 2^{k_1} -periodic binary sequence with $W_H(s^{(k_1)})=2^u+2^v$, the number of zero elements in $s^{(k_1)}$ is $2^{k_1}-2^u-2^v$.

Similar to the proof of Theorem 4.1, for each cube C_1 and C_2, the number of cube C_3 is $2^{2^w n-2^{w-1}k_w-\cdots-2k_2-2k_1-2^{w+1}+2}(2^{k_1}-2^u-2^v)$

This completes proof.

It should be noted that the mild requirement $2^{j_1} > 2^t$ in Theorem 4.2 is not critical and the idea of constructing cubes independently can also be used for cases not satisfying the condition, one can use the similar approach to find the number of 2^n-periodic binary sequences with more than one cube. We illustrate these cases by one following example.

Example 4.2 We now construct 2^n-periodic binary sequence with 2 independent cubes: C_1,C_2. C_1 has linear complexity $2^n - (1 + 2)$ and C_2 has linear complexity $2^n - (1 + 8)$. The number of 2^2-periodic binary sequence with linear complexity $2^n - (1+ 2)$ is 1. Namely sequence 1111. The number of 2^3-periodic binary sequence with linear complexity $2^n - (1+ 2)$ is 24. For instance sequence 11110000. Each 2^3-periodic binary

sequence has 4 options to put 2 non-zero elements with distance 1. The number of 2^4-periodic binary sequence with 2 independent cubes is $2^4 \times 2^4 \times 4$.

Finally the number of 2^n-periodic binary sequence with 2 independent cubes is $2^4 \times 2^4 \times 4 \times (2^8)^{n-4} = 2^{10} \times (2^8)^{n-4}$.

For $n = 4$, one example is 1111 1100 1100 0000.

4.2. The Counting Formula of 2^n-Periodic Binary Sequences with the Given k-Error Linear Complexity Profile: $0 = L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$

The k-error linear complexity profile of a periodic sequence was first defined in [15]. Based on the above cube theory, we investigate the periodic sequences $s^{(n)}$ with the given k-error linear complexity profile. Suppose that $0 = L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$.

To construct the desired sequence, the crucial step here is first to construct a sequence made up of a few cubes but with a small period, then to increase the period and add more cubes at the same time.

Theorem 4.3 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity less than 2^n. Suppose that $L_6(s^{(n)}) = 0$, $0 < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)})$ and $L(s^{(n)}) = 2^n - 2^{i_0}$, $L_2(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, $i_0 \ne i; j$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 \le p < q < n$, $j < q$, $p \ne i, j$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by □

□□□□□□□□□□

$$\begin{cases} 2^{6n-p-2j-i_0-i-9} & p < i < i_0 < j \\ 2^{6n-p-2j-i_0-i-8} & i < p < i_0 < j \text{ or } p < i_0 < i < j \\ 3\times 2^{6n-p-2j-i_0-i-9} & i < i_0 < p < j \\ 2^{6n-2q+p-2j-i_0-i-6} & i < i_0 < j < p \\ 2^{6n-p-2j-i_0-i-7} & i_0 < p < i < j \\ 3\times 2^{6n-p-2j-i_0-i-8} & i_0 < i < p < j \\ 2^{6n-2q+p-2j-i_0-i-5} & i_0 < i < j < p \end{cases}$$

Suppose that $L_4(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$, $0 \le p < q < r < n$, $j < r$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by □

□□□□□□□□□□□□□□

$$\begin{cases} 2^{6n-2j-i-p-i_0-8} & i_0 < p < i = q,\ j = r \\ 2^{6n-2j-i-p-i_0-9} & p < i_0 < i = q,\ j = r \\ 2^{6n-2j-i-q-p-7} & i_0 = p, i < q,\ j = r \\ 2^{6n-2j-q-p-i_0-7} & i_0 \ne p, i_0 < q, i = p,\ j = r \\ 2^{6n-2j-q-p-i_0-8} & i_0 \ne p, i_0 > q, i = p,\ j = r \\ 2^{6n-r-2q-j-p-7} & i_0 = p,\ j = q,\ j < r \\ 2^{6n-r-2q-i-p-7} & i_0 = p,\ j = q \\ 2^{6n-r-2q-i_0-p-7} & i = p,\ j = q \\ 2^{6n-r-3q-p-9} & i_0 = q, i = p, q < j < r \end{cases}$$

Proof: As $0 = L_6(s^{(n)}) < L_4(s^{(n)}) < L_2(s^{(n)}) < L(s^{(n)}) < 2^n$, $s^{(n)}$ can be decomposed into three 1-cubes or one 1-cube and one 2-cube by Algorithm 3.1.

i) First consider the case that $s^{(n)}$ can be decomposed into three 1-cubes c_1, c_2, c_3, $L(c_1) > L(c_2) > L(c_3)$. $L(s^{(n)}) = L(c_1) = 2^n - 2^{i_0}$. It is easy to show that $L_2(s^{(n)}) = 2^n - (2^i + 2^j)L$, $0 \le i < j < n$ and $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 \le p < q < n$.

As $i_0 < i$ or $i < i_0 < j$ and $j < q$, there are 8 possible cases: $p < i < i_0 < j$, $i < p < i_0 < j$, $i < i_0 < p < j$, $i < i_0 < j < p$, $p < i_0 < i < j$, $i_0 < p < i < j$, $i_0 < i < p < j$, $i_0 < i < j < p$. Now we will compute the number of sequences e with $W_H(e) = 6$, $L(e) = 2^n - 2^{i_0}$, $L_2(e) = 2^n - (2^i + 2^j)$ and $L_4(e) = 2^n - (2^p + 2^q)$.

Suppose that $s^{(i)}$ is a 2^i-periodic binary sequence with linear complexity 2^i and $W_H(s^{(i)}) = 1$. Then the number of these $s^{(i)}$ is 2^i.

So the number of 2^{i+1}-periodic binary sequences $s^{(i+1)}$ with linear complexity $2^{i+1} - 2^i = 2^i$ and $W_H(s^{(i+1)}) = 2$ is also 2^i.

For $j > i$, if 2^j-periodic binary sequences $s^{(j)}$ with linear complexity $2^j - 2^i$ and $W_H(s^{(j)}) = 2$, then $2^j - 2^i - (2^i + 1 - 2^i) = 2^j - 1 + 2^j - 2 + \cdots + 2^i + 1$.

Based on Algorithm 2.1, the number of these $s^{(j)}$ can be given by $(2^2)^{j-i-1} \times 2^i = 2^{2j-i-2}$.

So the number of 2^{j+1}-periodic binary sequences $s^{(j+1)}$ with linear complexity $2^{j+1} - (2^j + 2^i)$ and $W_H(s^{(j+1)}) = 4$ is also 2^{2j-i-2}.

In the case of $p < i < i_0 < j$. Note that the number of 2^q-periodic binary sequences $s^{(q)}$ with linear complexity $2^q - (2^j + 2^i)$ and $W_H(s^{(q)}) = 4$ is $2^{2j-i-2} \times (2^4)^{q-j-1} = 2^{4q-2j-i-6}$, and sequence {00000000 00000001 00000010 10001011} can be from both {00000000 00000001 00001010 00001011} and {00000000 00000001 10000010 10000011}. The number of these e can be given by

$$2^{4q-2j-i-6} \times (2^2 \times 2^{q-i_0-1}/2) \times 2^{q-p-1} \times 2^4 \times (2^6)^{n-q-1} = 2^{6n-p-2j-i_0-i-9}$$

For sequence {00000000 00000001 00000010 10001011}, $n = 5$, $i_0 = 2$, $i = 1$, $j = 3$, $p = 0$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00001010 00001011}. When change 4 bits, it becomes another 2-cube: {00000000 00000011 00000000 00000011}.

In the case of $i < p < i_0 < j$. The number of these e can be given by

$$2^{4q-2j-i-6} \times (2^2 \times 2^{q-i_0-1}/2) \times 2^{q-p} \times 2^4 \times (2^6)^{n-q-1} = 2^{6n-p-2j-i_0-i-8}$$

For sequence {00000000 00000001 00000010 01000111}, $n = 5$, $i_0 = 2$, $i = 0$, $j = 3$, $p = 1$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000110 00000111}. When change 4 bits, it becomes another 2-cube: {00000000 00000101 00000000 00000101}.

In the case of $i < i_0 < p < j$. The number of these e can be given by

$$2^{4q-2j-i-6} \times (2^2 \times 2^{q-i_0-1}/2) \times 2^{q-p-1} \times 3 \times 2^4 \times (2^6)^{n-q-1} = 3 \times 2^{6n-p-2j-i_0-i-9}$$

For sequence {00000000 00000001 00000010 00010111}, $n = 5$, $i_0 = 1$, $i = 0$, $j = 3$, $p = 2$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000110 00000111}. When change 4 bits, it becomes another 2-cube: {00000000 00010001 00000000 00010001}.

In the case of $i < i_0 < j < p$. Note that the number of 2^p-periodic binary sequences $s^{(p)}$ with linear complexity $2^p - (2^j + 2^i)$ and $W_H(s^{(p)}) = 4$ is $2^{2j-i-2} \times (2^4)^{p-j-1} = 2^{4p-2j-i-6}$. So the number of 2^p-periodic binary sequences e with $W_H(e) = 4$, $L(e) = 2^p - 2^{i_0}$ and $L_2(e) = 2^p - (2^i + 2^j)$ is $2^{4p-2j-i-6} \times (2^2 \times 2^{p-i_0-1}/2)$.

We further compute the number of sequences e with $W_H(e) = 6$, $L(e) = 2^n - 2^{i_0}$, $L_2(e) = 2^n - (2^i + 2^j)$ and $L_4(e) = 2^n - (2^p + 2^q)$. The number of these e can be given by

$$2^{4p-2j-i-6} \times (2^2 \times 2^{p-i_0-1}/2) \times 4 \times (2^4)^{q+1-p} \times (2^6)^{n-q-1} = 2^{6n-2q+p-2j-i_0-i-6}$$

For sequence {00000000 00000001 00000001 00011011}, $n = 5$, $i_0 = 1$, $i = 0$, $j = 2$, $p = 3$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000001 10011001}. When change 4 bits, it becomes another 2-cube: {00000001 00000001 00000001 00000001}.

In the case of $p < i_0 < i < j$. The number of these e can be given by

$$2^{4p-2j-i-6} \times (2^2 \times 2^{q-i_0-1}) \times 2^{q-p-1} \times 2^4 \times (2^6)^{n-q-1} = 2^{6n-p-2j-i_0-i-8}$$

For sequence {00000000 00000001 00000010 00101011}, $n = 5$, $i_0 = 1$, $i = 2$, $j = 3$, $p = 0$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00001010 00001011}. When change 4 bits, it becomes another 2-cube: {00000000 00000011 00000000 00000011}.

In the case of $i_0 < p < i < j$. The number of these e can be given by

$$2^{4p-2j-i-6} \times (2^2 \times 2^{q-i_0-1}) \times 2^{q-p} \times 2^4 \times (2^6)^{n-q-1} = 2^{6n-p-2j-i_0-i-7}$$

For sequence {00000000 00000001 00000010 00100111}, $n = 5$, $i_0 = 0$, $i = 2$, $j = 3$, $p = 1$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00100010 00100011}. When change 4 bits, it becomes another 2-cube: {00000000 00000101 00000000 00000101}.

In the case of $i_0 < i < p < j$. The number of these e can be given by

$$2^{4p-2j-i-6} \times (2^2 \times 2^{q-i_0-1}) \times 2^{q-p-1} \times 3 \times 2^4 \times (2^6)^{n-q-1} = 3 \times 2^{6n-p-2j-i_0-i-8}$$

For sequence {00000000 00000001 00000010 00011011}, $n = 5$, $i_0 = 0$, $i = 1$, $j = 3$, $p = 2$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00001010 00001011}. When change 4 bits, it becomes another 2-cube: {00000000 00010001 00000000 00010001}.

In the case of $i_0 < i < j < p$. The number of these e can be given by

$$2^{4p-2j-i-6} \times (2^2 \times 2^{p-i_0-1}) \times 4 \times (2^4)^{q+1-p} \times (2^6)^{n-q-1} = 2^{6n-2q+p-2j-i_0-i-5}$$

For sequence {00000000 00000001 00000001 00010111}, $n = 5$, $i_0 = 0$, $i = 1$, $j = 2$, $p = 3$, $q = 4$. When change 2 bits, it becomes a 2-cube and a 1-cube: {00000000 00000001 00000001 01010101}. When change 4 bits, it becomes another 2-cube: {00000001 000000001 00000001 00000001}.

ii) Second consider the case that $s^{(n)}$ can be decomposed into one 1-cube c_1 and one 2-cube c_2. Now we will compute the number of sequences e with $W_H(e) = 6$, $L(e) = 2^n - 2^{i_0}$, $L_2(e) = 2^n - (2^i + 2^j)$ and $L_4(e) = 2^n - (2^p + 2^q + 2^r)$.

Let $L(c_1) = 2^n - 2^{i_0}$ and $L(c_2) = 2^n - (2^i + 2^j)$. Let *max* be the maximum distance (please see Definition 3.1) between one nonzero element of c_1 and one nonzero element of c_2. If $i_0 < i$ and $max < i$, then there are two cases.

In the case of $i_0 < p < i = q$, $j = r$. The number of these e can be given by

$$2^{2j-i-2} \times (2^{i-p-1} \times 2^{i-i_0-1}) \times (2^2)^{j+1-i} \times (2^6)^{n-j-1} = 2^{6n-2j-i-p-i_0-8}$$

For sequence {1101 0001 0001 0001}, $n = 4$, $i0 = 0$, $i = 2$, $j = 3$, $p = 1$, $q = 2$, $r = 3$. When change 2 bits, it becomes a 2-cube: {0001 0001 0001 0001}. When change 4 bits, it becomes a 3-cube: {0101 0101 0101 0101}.

In the case of $p < i_0 < i = q$, $j = r$. The number of these e can be given by

$$2^{2j-i-2} \times (2^{i-p-1} \times 2^{i-i_0-1} / 2) \times (2^2)^{j+1-i} \times (2^6)^{n-j-1} = 2^{6n-2j-i-p-i_0-9}$$

For sequence {1011 0001 0001 0001}, $n = 4$, $i_0 = 1$, $i = 2$, $j = 3$, $p = 0$, $q = 2$, $r = 3$. When change 2 bits, it becomes a 2-cube: {0001 0001 0001 0001}. When change 4 bits, it becomes a 3-cube: {0011 0011 0011 0011}.

Let $L(c_1) = 2^n - 2^{i_0}$ and $L(c_2) = 2^n - (2^p + 2^r)$. If $i_0 = p$ and $p < max < r$, then there is only one case: $i < q$, $j = r$. The number of these e can be given by

$$2^{2j-p-2} \times (2^{j-q-1} \times 2^{j-i-1} \times 2) \times 2^2 \times (2^6)^{n-j-1} = 2^{6n-2j-i-q-p-7}$$

For sequence {0000 0011 0001 1011}, $n = 4$, $i_0 = 0$, $i = 1$, $j = 3$, $p = 0$, $q = 2$, $r = 3$. When change 2 bits, it becomes two 2-cubes: {0001 1011 0001 1011}. When change 4 bits, it becomes a 3-cube: {0011 0011 0011 0011}.

Let $L(c_1) = 2^n - 2^{i_0}$ and $L(c_2) = 2^n - (2^p + 2^r)$. If $i_0 \neq p$ and $p < max < r$, then there are two cases.

In the case of $i_0 \neq p$, $i_0 < q$, $i = p$, $j = r$. The number of these e can be given by

$$2^{2j-p-2} \times (2^{j-q-1} \times 2^{j-i_0-1} \times 2) \times 2^2 \times (2^6)^{n-j-1} = 2^{6n-2j-q-p-i_0-7}$$

For sequence {0000 0101 0001 0111}, $n = 4$, $i_0 = 0$, $i = 1$, $j = 3$, $p = 1$, $q = 2$, $r = 3$. When change 2 bits, it becomes a 2-cube: {0000 0101 0000 0101}. When change 4 bits, it becomes a 3-cube: {0101 0101 0101 0101}.

In the case of $i_0 \neq p$; $i_0 > q$, $i = p$, $j = r$. The number of these e can be given by

$$2^{2j-p-2} \times (2^{j-q-1} \times 2^{j-i_0-1}) \times 2^2 \times (2^6)^{n-j-1} = 2^{6n-2j-q-p-i_0-8}$$

For sequence {0000 0011 0100 0111}, $n = 4$, $i_0 = 2$, $i = 0$, $j = 3$, $p = 0$, $q = 1$, $r = 3$. When change 2 bits, it becomes a 2-cube: {0000 0011 0000 0011}. When change 4 bits, it becomes a 3-cube: {0000 1111 0000 1111}.

Let $L(c_1) = 2^n - 2^{i_0}$ and $L(c_2) = 2^n - (2^p + 2^q)$. If $i_0 = p$ and $q < max$, then $max = r$. There are two cases.

In the case of $i_0 = p$, $i = q$, $j < r$. Note that both {0010 1101} and {0000 1111} are 2-cubes with the same linear complexity. The number of these e can be given by

$$2^{2j-p-2} \times (2^4)^{r-q-1} \times (2^3 \times 2^{r-j-1} / 2) \times 2^4 \times (2^6)^{n-j-1} = 2^{6n-r-2q-j-p-7}$$

For sequence {0000 0001 0010 1111}, $n = 4$, $i_0 = 0$, $i = 1$, $j = 2$, $p = 0$, $q = 1$, $r = 3$. When change 2 bits, it becomes a 2-cube and a 1-cube: {0000 0001 1010 1011}. When change 4 bits, it becomes a 3-cube: {0000 1111 0000 1111}.

In the case of $i_0 = p$, $j = q$. The number of these e can be given by

$$2^{2j-p-2} \times (2^4)^{r-q-1} \times (2^3 \times 2^{r-j-1} / 2) \times 2^4 \times (2^6)^{n-r-1} = 2^{6n-r-2q-i-p-7}$$

For sequence {0000 0001 0011 1011}, $n = 4$, $i_0 = 0$, $i = 1$, $j = 2$, $p = 0$, $q = 2$, $r = 3$. When change 2 bits, it becomes a 2-cube and a 1-cube: {0000 0001 1010 1011}. When change 4 bits, it becomes a 3-cube: {0011 0011 0011 0011}.

Let $L(c_1) = 2^n - 2^{i_0}$ and $L(c_2) = 2^n - (2^p + 2^q)$. If $i_0 \neq p$ and $q < max$, then $max = r$. There are two cases.

In the case of $i = p$; $j = q$. The number of these e can be given by

$$2^{2q-p-2} \times (2^4)^{r-q-1} \times (2^2 \times 2^{r-i_0-1}) \times 2^4 \times (2^6)^{n-r-1} = 2^{6n-r-2q-i_0-p-7}$$

For sequence {0000 0001 0101 0111}, $n = 4$, $i_0 = 0$, $i = 1$, $j = 2$, $p = 1$, $q = 2$, $r = 3$. When change 2 bits, it becomes a 2-cube: {0000 0000 0101 0101}. When change 4 bits, it becomes a 3-cube: {0101 0101 0101 0101}.

In the case of $i_0 = q$, $i = p$, $q < j < r$. Note that both {0100 1011} and {0000 1111} are 2-cubes with the same linear complexity. The number of these e can be given by

$$2^{2q-p-2} \times (2^4)^{r-q-1} \times (2^2 \times 2^{r-(q+1)-1} / 2) \times 2^4 \times (2^6)^{n-r-1} = 2^{6n-r-3q-p-9}$$

For sequence {0000 0001 0100 1111}, $n = 4$, $i_0 = 1$, $i = 0$, $j = 2$, $p = 0$, $q = 1$, $r = 3$. When change 2 bits, it becomes a 2-cube and a 1-cube: {0000 0001 1100 1101}. When change 4 bits, it becomes a 3-cube: {0000 1111 0000 1111}.

This completes the proof.

4.3. The Counting Formula of 2^n-Periodic Binary Sequences with the Given k-error Linear Complexity Profile: $0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < 2^n$

Similarly, we could illustrate how to construct the 2^n-periodic binary sequences with the given k-error linear complexity profile:

$$0 = L_7(s^{(n)}) < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)}) < 2^n.$$

We first give an example to illustrate our basic approach. Let $n = 5$,$L_1(s^{(n)}) = 32 - (1 + 4)$, $L_3(s^{(n)}) = 32 - (2 + 8)$, $L_5(s^{(n)}) = 32 - (2 + 8 + 16)$, $L_7(s^{(n)}) = 0$. First construct $e_1 =$ 11001000;$L_1(e_1) = 8 - (1 + 4)$. Then $e_2 =$ 11101000 10100000;$L_3(e_2) = 16-(2+8)$. Finally $e_3 =$ 11101000 10100000 10000000 00000000;$L_5(e_3) = 32-(2+8+16)$. At the same time, $L_1(e_3) = 32 - (1 + 4)$;$L_3(e_3) = 32 - (2 + 8)$.

As an m-cube has 2^m nonzero elements and $L_7(s^{(n)}) = 0$, by Algorithm 3.1, the decomposition of $s^{(n)}$ does not include an m-cube for $m > 2$.

By Algorithm 3.1, $s^{(n)}$ can be decomposed into one 0-cube c_1 (one nonzero element) and three 1-cubes c_2, c_3, c_4, where $L(c_2) > L(c_3) > L(c_4)$, or one 0-cube c_1, one 2-cube c_2 and one 1-cube c_3 or one 0-cube c_1, one 1-cube c_2 and one 2-cube c_3, where $L(c_2) > L(c_3)$. This covers all possible cases.

We here only consider the case that $s^{(n)}$ can be decomposed into one 0-cube c_1 and three 1-cubes c_2, c_3, c_4, where $L(c_2) > L(c_3) > L(c_4)$. The detailed proof is omitted.

Theorem 4.4 Let $s^{(n)}$ be a 2^n-periodic binary sequence with linear complexity 2^n and $L_7(s^{(n)}) = 0 < L_5(s^{(n)}) < L_3(s^{(n)}) < L_1(s^{(n)})$. Suppose that $s^{(n)}$ can be decomposed into one 0-cube c_1 (one nonzero element), and three 1-cubes c_2, c_3, c_4 by Algorithm 2.2, we have the following four cases.

i) Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 \le p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y)$, $0 \le x < y < n$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ are given by□□□□□□□□□□□□□□□

$$\begin{cases} 3\times5\times2^{7n-y-x-q-p-j-i-9} & i<j<p<q<x<y \\ 2\times5\times2^{7n-y-x-q-p-j-i-9} & i<p<j<q<x<y \\ 5\times2^{7n-y-x-q-p-j-i-9} & p<i<j<q<x<y \\ 3\times4\times2^{7n-y-x-q-p-j-i-9} & i<j<p<x<q<y \\ 3^2\times2^{7n-y-x-q-p-j-i-9} & i<j<x<p<q<y \\ 3\times2\times2^{7n-y-x-q-p-j-i-9} & i<x<j<p<q<y \\ 3\times2^{7n-y-x-q-p-j-i-9} & x<i<j<p<q<y \\ 2\times4\times2^{7n-y-x-q-p-j-i-9} & i<p<j<x<q<y \\ 2\times3\times2^{7n-y-x-q-p-j-i-9} & i<p<x<j<q<y \\ 2\times2\times2^{7n-y-x-q-p-j-i-9} & i<x<p<j<q<y \\ 2\times2^{7n-y-x-q-p-j-i-9} & x<i<p<j<q<y \\ 4\times2^{7n-y-x-q-p-j-i-9} & p<i<j<x<q<y \\ 3\times2^{7n-y-x-q-p-j-i-9} & p<i<x<j<q<y \\ 2\times2^{7n-y-x-q-p-j-i-9} & p<x<i<j<q<y \\ 2^{7n-y-x-q-p-j-i-9} & x<p<i<j<q<y \end{cases}$$

ii) Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q)$,$0 \le p < q < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, $0 \le x < y < z < n$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\begin{cases} 3\times2^{7n-2z-y-x-j-i-8} & i<j<p=x<q=y<z \\ 3\times2^{7n-2z-y-x-j-i-8} & i<p=x<j<q=y<z \\ 3\times2^{7n-2z-y-x-j-i-8} & p=x>i>j>q=y>z \\ 2^{7n-z-2q-p-j-i-8} & i<j=x<p<q=y<z \\ 2^{7n-z-2q-p-j-i-7} & i=x<j<p<q=y<z \\ 3\times2^{7n-z-2q-p-j-i-9} & i=x<p<j<q=y<z \\ 3\times2^{7n-z-2q-p-2j-i-9} & i=x<j=y<p<q<z \\ 3\times2^{7n-z-2q-p-2j-i-9} & i=x<p<j=y<q<z \\ 2^{7n-z-q-p-2j-i-9} & p<i=x<j=y<q<z \\ 2^{7n-z-q-2p-j-i-7} & i=x<j<p=y<q<z \\ 2^{7n-z-q-2p-j-i-8} & i<j=x<p=y<q<z \\ 2^{7n-z-q-p-2j-i-9} & i<p=x<j=y<q<z \end{cases}$$

iii) Suppose that $L1(s(n)) = 2^n - (2i + 2j)$; $0 \le i < j < n$, $L3(s(n)) = 2^n - (2p + 2q + 2r)$; $0 \le p < q < r < n$ and $L5(s(n)) = 2^n - (2x + 2y)$; $0 \le x < y < n$. Then the number of 2^n-periodic binary sequences $s(n)$ can be given by

□□□□
$$\begin{cases} 5\times2^{7n-y-x-r-2j-i-9} & i=p<j=q<r<x \\ 2^{7n-y-x-r-2j-i-7} & i=p<j=q<x<r \\ 2^{7n-y-x-r-2j-i-8} & i=p<x<j=q \\ 2^{7n-y-x-r-2j-i-9} & x<i=p<j=q \end{cases}$$

iv) Suppose that $L_1(s^{(n)}) = 2^n - (2^i + 2^j)$, $0 \le i < j < n$, $L_3(s^{(n)}) = 2^n - (2^p + 2^q + 2^r)$, $0 \le p < q < r < n$ and $L_5(s^{(n)}) = 2^n - (2^x + 2^y + 2^z)$, $0 \le x < y < z < n$. Then the number of 2^n-periodic binary sequences $s^{(n)}$ can be given by

$$\begin{cases} 2^{7n-z-2r-2j-i-9} & i = p < j = q = x < r = y < z \\ 2^{7n-z-2r-2j-i-8} & i = p = x < j = q < r = y < z \end{cases}$$

5. Conclusion

By studying the linear complexity of binary sequences with period 2^n, especially the linear complexity may decline when the superposition of two sequences with the same linear complexity, a new approach to study *k*-error linear complexity has been proposed in this paper. We first give a general decomposition approach to decompose a binary sequence with period 2^n into some disjoint cubes. Second, a counting formula for m-cubes with the same linear complexity is derived, which is equivalent to the counting formula for *k*-error vectors. The counting formula of 2^n-periodic binary sequences which can be decomposed into more than one cube is also investigated, which extends an important result by Etzion *et. al.*, Finally, we study 2^n-periodic binary sequences with the given k-error linear complexity profile of descent points 2, 4 and 6, and the given *k*-error linear complexity profile of descent points 1, 3, 5 and 7.

From the perspective of cube theory, one can easily perceive the core problem and difficult points of the *k*-error linear complexity for a binary sequence with more than one cube.

In future, we may further study the essential relationship between the standard cube decomposition and the *k*-error linear complexity of a 2^n-periodic binary sequences and the *k*-error linear complexity profile of 3 or more descent points.

Acknowledgments

The research was partially supported by Anhui Natural Science Foundation (No.1208085MF106).

References

[1] C. S. Ding and G. Z. Xiao and W. J. Shan, "The Stability Theory of Stream Ciphers[M]", Lecture Notes in Computer Science, Berlin/ Heidelberg, Germany: Springer-Verlag, vol. 561, **(1991)**, pp. 85-88.
[2] Etzion T., Kalouptsidis N., Kolokotronis N., Limniotis K. and Paterson K. G., "Properties of the Error Linear Complexity Spectrum", IEEE Transactions on Information Theory, vol. 55, no. 10, **(2009)**, pp. 4681-4686.
[3] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n", IEEE Trans on Information Theory, vol. 29, no. 1, **(1983)**, pp. 144-146.
[4] Fu F., Niederreiter H. and Su M., "The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity", In: Gong G., Helleseth T., Song H.-Y. and Yang K. (eds.) SETA 2006. LNCS, Springer, vol. 4086, **(2006)**, pp. 88-103.
[5] Han Y. K., Chung J. H. and Yang K., "On the *k*-error linear complexity of *pm*-periodic binary sequences", IEEE Transactions on Information Theory, vol. 53, no. 6, **(2007)**, pp. 2297-2304.
[6] Hu H. and Feng D., "Periodic sequences with very large 1-error linear complexity over *Fq*", Journal of Software, vol. 16, no. 5, **(2005)**, pp. 940-945.
[7] Kaida T., Uehara S. and Imamura K., "An algorithm for the *k*-error linear complexity of sequences over GF(p^m) with period p^n", *p* a prime. Information and Computation, vol. 151, no. 1, **(1999)**, pp. 134-147.
[8] Kolokotronis N., Rizomiliotis P. and Kalouptsidis N., "Minimum linear span approximation of binary sequences", IEEE Transactions on Information Theory, vol. 48, **(2002)**, pp. 2758-2764.
[9] Kurosawa K., Sato F., Sakata T. and Kishimoto W., "A relationship between linear complexity and *k*-error linear complexity", IEEE Transactions on Information Theory, vol. 46, no. 2, **(2000)**, pp. 694-698.
[10] Lauder A. and Paterson K., "Computing the error linear complexity spectrum of a binary sequence of period 2^n", IEEE Transactions on Information Theory, vol. 49, no. 1, **(2003)**, pp. 273-280.

[11] Meidl W., "How many bits have to be changed to decrease the linear complexity?", Des. Codes Cryptogr., vol. 33, **(2004)**, pp. 109-122.
[12] Meidl W., "On the stablity of 2^n-periodic binary sequences", IEEE Transactions on Information Theory, vol. 51, no. 3, **(2005)**, pp. 1151-1155.
[13] Meziani M., Cayrel P. and Alaoui S., "An Efficient Code-based Stream Cipher", International Journal of Security and Its Applications, vol. 5, no. 4, **(2011)**, pp. 107-116
[14] Niederreiter H., "Periodic sequences with large *k*-error linear complexity", IEEE Transactions on Information Theory, vol. 49, **(2003)**, pp. 501-505.
[15] M. Stamp and C. F. Martin, "An algorithm for the *k*-error linear complexity of binary sequences with period 2^n", IEEE Trans. Inform. Theory, vol. 39, **(1993)**, pp. 1398-1401.
[16] M. Tang and Zhu S. X., "On the error linear complexity spectrum of p^n-periodic binary sequences", Applicable Algebra in Engineering, Communication and Computing, vol. 24, **(2013)**, pp. 497-505.
[17] S. M. Wei, G. Z. Xiao and Z. Chen, "A fast algorithm for determining the minimal polynomial of a sequence with period $2p^n$ over $GF(q)$", IEEE Trans on Information Theory, vol. 48, no. 10, **(2002)**, pp. 2754-2758.
[18] J. Q. Zhou, "On the *k*-error linear complexity of sequences with period $2p^n$ over $GF(q)$", Des. Codes Cryptogr., vol. 58, no. 3, **(2011)**, pp. 279-296.
[19] J. Q. Zhou and W. Q. Liu, "The *k*-error linear complexity distribution for 2^n-periodic binary sequences", Des. Codes Cryptogr., vol. 73, no. 1, **(2014)**, pp. 55-75.
[20] J. Q. Zhou, W. Q. Liu and G. L. Zhou, "Cube theory and stable *k*-error linear complexity for periodic Sequences", In: D. D. Lin, S. H. Xu and M. Yung, (eds.) INSCRYPT 2013, LNCS 8567, pp. 70-85.
[21] F. X. Zhu and W. F. Qi, "The 2-error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n-1", Journal of Electronics (China), **(2007)**, vol. 24, no. 3, pp. 390-395, http://www.springerlink.com/content /3200vt810p232769/

Authors

Jianqin Zhou received his B.Sc. degree in mathematics from East China Normal University, China, in 1983, and M.Sc. degree in probability and statistics from Fudan University, China, in 1989. From 1989 to 1999 he was with the Department of Mathematics and Computer Science, Qufu Normal University, China. From 2000 to 2002, he worked for a number of IT companies in Japan. He was a visiting scholar with Keio University in Japan, University of Florida in USA and Curtin University in Australia respectively. Since 2003 he has been with the Department of Computer Science, Anhui University of Technology, China. Since 2013, he has been a PhD candidate with the Department of Computing, Curtin University.

He published more than 110 papers, and proved a conjecture posed by famous mathematician Paul Erdos *et. al.*, His research interests include cryptography, coding theory and combinatorics.

